# DEEL II CYPHERPUNKS

## Hoofdstuk 8: De Cypherpunk Beweging

Tim May kon een glimp van de toekomst zien. Hij had een gave om het potentieel van nieuwe technologieën te herkennen en kon voorspellen hoe ze de samenleving zouden beïnvloeden voordat bijna iemand anders dat kon.

Het meest opvallend was dat May al vroeg inzag hoe belangrijk persoonlijke computers en het internet zouden worden. Zo vroeg als 1973 bemachtigde hij een primitieve DARPA-account op de campus van de UC Santa Barbara, waar hij natuurkunde studeerde. Een jaar later, op 22-jarige leeftijd, kreeg hij een baan bij Intel, waar hij zou werken in de Memory Products Division.

De jonge natuurkundige leverde een belangrijke bijdrage in de vroege geschiedenis van het bedrijf door het alfadeeltjesprobleem op te lossen: May ontdekte dat de geïntegreerde schakelingen van Intel onbetrouwbaar waren vanwege licht radioactief verpakkingsmateriaal. Dit zette hem op weg naar een geweldige carrière bij de snelgroeiende fabrikant van halfgeleiderchips.

Omdat hij een deel van zijn salaris in de vorm van aandelenopties ontving, had de natuurkundige van Intel ongeveer een decennium later, tegen midden jaren 80, een klein fortuin vergaard: op slechts vierendertigjarige leeftijd concludeerde May dat hij genoeg rijkdom had verzameld om de rest van zijn leven te onderhouden. Hij besloot vroegtijdig met pensioen te gaan en verhuisde naar Santa Cruz, een kustplaats zo’n dertig mijl ten zuiden van San Jose, Californië. Het grootste deel van het daaropvolgende jaar bracht hij door in een comfortabele strandstoel waarin hij boeken over economie, technische papers en cyberpunkromans las.

Een relatief nieuw genre in die tijd, speelden cyberpunkverhalen zich meestal af in hightech dystopieën. De boeken schilderden over het algemeen een grimmige versie van de toekomst, maar eentje waarin het internet (of een geëvolueerde versie ervan) een toevluchtsoord bood voor hun vrijheidsgezinde hoofdpersonen. In True Names van Vernor Vinge, verbergen een groep hackers zich voor de regeringssterke mannen door hun pseudonieme avatars vrijelijk te laten rondzwerven door een kleurrijke en driedimensionale representatie van het internet zelf. In Snow Crash van Neil Stephenson verloren naties grotendeels hun macht aan grote bedrijven en de maffia, terwijl mensen aan hun miezerig bestaan ontsnapten door alternatieve levens te leiden in een virtuele realiteitswereld. En Neuromancer van William Gibson presenteert evenzo een wereldwijd verbonden, virtuele realiteitsomgeving als een kleurrijk alternatief voor een vijandige onderwereldmaatschappij.

May was van plan om uiteindelijk zelf een cyberpunkroman te schrijven, gemodelleerd naar Ayn Rand’s Atlas Shrugged. In Rand’s verhaal, dat oorspronkelijk in 1957 werd gepubliceerd, omarmt een Amerika in verval socialistische doctrines, terwijl het Amerikaanse volk zich afkeert van de meest succesvolle ondernemers van het land. Sommige van deze ondernemers besluiten uiteindelijk om “in staking” te gaan: een kleine gemeenschap van doorgewinterde vernieuwers vestigt zich in een afgelegen bergketen genaamd “Galt’s Gulch,” en gebruiken een scherm van hittegolven en reflectoren om zich te verbergen voor de buitenwereld. De subtiele boodschap van het boek is dat Amerika’s meest ijverige ondernemers niet gedemoniseerd, maar gekoesterd en gevierd zouden moeten worden.

Na het lezen van Rand’s meesterwerk ‘Atlas Shrugged’ als tiener, had dit boek May op het spoor gezet om meer te leren over vrije markten en libertarisme. Uiteindelijk zou hij zich toeleggen op de studie van de Oostenrijkse economie, en in het bijzonder, op de theorieën van Friedrich Hayek.

Dit alles maakte dat de aspirant-schrijver zich als vanzelfsprekend thuis voelde in een niche subcultuur in Californië die in de jaren ’80 opkwam. Via enkele van zijn lokale vrienden leerde May de Extropians kennen en vond hij een ideologisch thuis. Hoewel hij niet volledig mee was met enkele van de meer buitensporige toekomstvisies van de transhumanisten - ideeën zoals eeuwig leven, het uploaden van de hersenen of een AI singulariteit - was hij wel toegewijd aan vrijheid en technologische vooruitgang.

In deze context raakte Tim May bevriend met Phil Salin, de “high-tech Hayekiaan” die tevergeefs had geprobeerd om een privé ruimtetransportindustrie op te zetten met zijn startup Starstruck. May en Salin deelden een passie voor zowel de Oostenrijkse economie als technologie. Beiden geloofden dat de voormalige verder kon worden ontwikkeld door de laatste te benutten.

### BlackNet

May had ongeveer een jaar op het strand doorgebracht met lezen toen Salin hem vertelde over AMIX, het ambitieuze internetproject waar hij aan werkte.

AMIX, legde Salin aan zijn vriend uit, zou een online marktplaats zijn voor het kopen en verkopen van informatie. Hij vertelde May hoe dit de transactiekosten sterk zou kunnen verlagen, wat een enorme voordelen zou opleveren voor de vrije markt. Hij vroeg May wat hij van het idee vond; Salin wilde graag de feedback van zijn vriend horen.

Het concept leek May inderdaad interessant. Maar na er even over na te denken, kwam hij tot de conclusie dat zijn interesse voor heel andere redenen werd gewekt dan die van Salin. May vertelde zijn vriend dat hij dacht dat deskundig advies of winkeltips - de soorten informatie waar Salin aan had gedacht - waarschijnlijk niet echt waardevol zouden zijn. Maar hij geloofde wel dat er een hoge vraag zou zijn naar een heel andere categorie van informatie.

Geheime informatie.

Mensen zouden bereid zijn om goed geld te betalen voor bedrijfsgeheimen, geclassificeerde overheidsdocumenten, militaire inlichtingen, kredietgegevens, medische dossiers, verboden religieus materiaal of illegale pornografie, stelde May voor.[^142] En belangrijk genoeg, sommige mensen die toegang hebben tot dit soort informatie zouden bijna zeker bereid zijn om het te verkopen voor de juiste prijs, als ze dat anoniem zouden kunnen doen.

Natuurlijk wist May dat het kopen en verkopen van dit soort informatie in veel gevallen illegaal zou zijn. Als het op AMIX zou worden gehost, zou Salin naar alle waarschijnlijkheid gedwongen worden om de handel ervan te verbieden. Maar May voorzag dat dit uiteindelijk geen echt verschil zou maken. De ontwikkelingen op het gebied van cryptografie die hij in academische tijdschriften had gelezen, zouden uiteindelijk in handen van mensen komen, legde hij aan Salin uit, dus het was slechts een kwestie van tijd totdat er een volledig anonieme variant van AMIX zou ontstaan waar gebruikers alleen bekend zijn bij hun pseudoniemen, en aankopen werden gedaan met anoniem digitaal geld.

May gaf deze vorm van informatiemarkt de naam BlackNet.

In de maanden na zijn eerste gesprek met Salin, bleef May nadenken over de bredere implicaties die een dienst als BlackNet met zich mee zou brengen. Door zijn eigen ideeën verder uit te werken, kwam hij tot de conclusie dat anonieme informatiemarkten uiteindelijk het fundamenteel onveilig konden maken voor grote bedrijven om hun medewerkers überhaupt met gevoelige informatie te laten omgaan. Deze medewerkers zouden immers altijd in de verleiding kunnen komen om een extra zakcentje te verdienen door de data online te verkopen.

Volgens May zou dit een soort catch-22 situatie kunnen introduceren. Bedrijfsgeheimen zouden bedrijven vermoedelijk een voorsprong op hun concurrenten geven als ze op grote schaal binnen het bedrijf worden gebruikt - maar in dat geval zou het waarschijnlijk slechts een tijdelijke voorsprong zijn voordat de informatie naar de concurrenten lekte. Of, de bedrijfsgeheimen zouden op een zeer beperkte schaal gebruikt kunnen worden om lekken te voorkomen - maar in dat geval zou de voorsprong op de concurrenten ook niet zo groot zijn.

Mogelijk, zo stelde May voor, zou het simpele bestaan van een BlackNet de economische prikkels die grote bedrijven in de eerste plaats levensvatbaar maken, fundamenteel kunnen schudden. In plaats van miljardenbedrijven zouden we door radicale transparantie een meer verspreide en levendige economie kunnen zien, gekenmerkt door een veel diverser aanbod aan kleinere bedrijven.

En May realiseerde zich uiteindelijk dat deze dynamiek niet alleen grote bedrijven zou beïnvloeden. Het zou ook net zo goed regeringen en hun strijdkrachten kunnen beïnvloeden, evenals andere openbare instellingen die vertrouwelijke informatie verwerken. Een enkele corrupte overheidsmedewerker met financieel gewin als motief zou voldoende zijn om allerlei geclassificeerde dossiers te verspreiden naar de meest betalende kopers op het internet. Niet in staat om gevoelige gegevens te beveiligen, zou de macht van de overheid aanzienlijk kunnen afzwakken. May was dol op dit idee.

Dus zou ook een andere lokale vriend van hem…

### Eric Hughes

Toen Eric Hughes in de late jaren 80 - toen hij halfweg de twintig was - wiskunde studeerde aan Berkeley, had de cryptografische revolutie zijn weg al in het curriculum gevonden. Tegen de tijd dat hij afstudeerde, was hij goed op de hoogte van de recente innovaties van mensen zoals Whitfield Diffie, Martin Hellman, Ralph Merkle en David Chaum. En net zoals zij, begreep Hughes intuïtief het veelbelovende potentieel van hun doorbraken in de context van een steeds meer gedigitaliseerde samenleving.

Hughes ontdekte dat fundamentele mensenrechten, zoals het recht op privacy, constant onder druk stonden van overheden. Zelfs al waren sommige van deze rechten juridisch gewaarborgd, leek het erop dat overheden altijd een manier vonden om inbreuk te maken als ze daartoe de mogelijkheid kregen.

Voor Hughes bood moderne cryptografie een methode om individuele privacy te beschermen, zonder te moeten vertrouwen op wetten, de interpretatie ervan door politici of rechters. Het recht op privécommunicatie kon in plaats daarvan gewaarborgd worden door technologieën zoals openbare sleutelcryptografie en mixnetwerken.

Hughes besefte dat het niveau van privacy dat bereikt kon worden met sterke cryptografie, uiteindelijk volledige immuniteit tegen fysieke bedreigingen en dwang kon bieden. Zolang anonieme internetgebruikers hun werkelijke identiteit geheim konden houden, kon niets dat ze online zouden doen of zeggen hen mogelijk in fysiek gevaar brengen.

Toen de jonge wiskundige hoorde dat Chaum een bedrijf had opgericht in Nederland om een elektronisch geldsysteem te implementeren, besloot de afgestudeerde van Berkeley om er te solliciteren. Net als Chaum geloofde hij dat geld hoe dan ook digitaal zou worden, en een privacybehoudende vorm van valuta kon het verschil betekenen tussen een vrije samenleving en een totalitaire dystopie. Bovendien geloofde Hughes dat de cryptografische protocollen van Chaum het potentieel hadden om dat verschil te maken. Chaum, op zijn beurt, geloofde dat Hughes een goede aanvulling zou zijn voor zijn bedrijf; hij werd aangenomen.

Toen Hughes in 1991 in Amsterdam aankwam om zijn nieuwe avontuur te beginnen, raakte hij vrij snel gedesillusioneerd door wat hij aantrof op de kantoren van DigiCash. Hij ontdekte tot zijn ontsteltenis dat Chaum smartcards, de fraudebestendige creditcard-sized computers speciaal ontworpen voor betalingen, tot hoeksteen van zijn ontwerp had gemaakt. In plaats van zich puur te verlaten op de kracht van wiskunde en het perfectioneren van de cryptografische protocollen die nodig waren om elektronisch geld voor het internet te implementeren, vond hij dat DigiCash zich concentreerde op dure en niet-controleerbare hardwareproducten om offline betalingen mogelijk te maken.

Hughes was van mening dat Chaum een ernstige strategische fout maakte door pragmatiek en kostenefficiëntie te onderschatten ten gunste van experimentele features. Uiteindelijk kwam de jonge wiskundige tot de conclusie dat DigiCash toch niet de plek voor hem was. Na slechts zes weken in Amsterdam vertrok hij bij de startup.

Eenmaal terug in Californië, overwoog Hughes op zoek te gaan naar een woning die iets dichter bij de zee lag. Hij besloot een paar dagen door te brengen met het zoeken naar een huis in Santa Cruz, waar hij kon verblijven bij een oude vriend die daar een paar jaar eerder naartoe was verhuisd: Tim May.

Toen Eric Hughes in 1991 in Santa Cruz aankwam, deelde May zijn visie voor anonieme informatie markten met hem. Hij legde uit hoe BlackNets gebruik zouden maken van het soort privacy tools die Hughes had bestudeerd en wilde bouwen, en hoe deze de macht van grote bedrijven en overheidsinstellingen konden verminderen, of zelfs volledig uit elkaar konden halen.

Hoewel Hughes zichzelf niet zozeer als een libertariër van de vrije markt beschouwde zoals Tim May dat deed, intrigeerde het concept van anonieme informatiemarkten hem net zo goed. De komende paar dagen konden ze het alleen maar hebben over het enorme potentieel van moderne cryptografie. Terwijl ze filosofeerden over de implicaties van anonieme netwerken, de levensvatbaarheid van pseudonieme reputatiesystemen, en de vooruitzichten van grenzeloze betalingen, moest huizenjacht even wachten.

Maar na enkele dagen te hebben gediscussieerd over mogelijk baanbrekende toepassingen voor public key encryptie, remailers en digitaal geld, leidden hun gesprekken steeds weer terug naar dezelfde knagende vraag.

Waarom waren er nog steeds geen softwarehulpmiddelen die deze protocollen implementeerden?

Geen van de baanbrekende crypto-innovaties die sinds de jaren 70 werden voorgesteld, werden in de praktijk gebracht door echte mensen, omdat er geen computerprogramma’s beschikbaar waren die deze protocollen implementeerden. Terwijl academische papers in detail uitlegden hoe Alice en Bob privé konden communiceren dankzij de Diffie-Hellman sleuteluitwisseling of RSA-encryptie, was dit aan het eind van de dag volledig nutteloos zolang er geen software bestond die deze taken voor Alice en Bob uitvoerde.

Toegegeven, er waren wel een paar van zulke projecten in ontwikkeling. In feite werkte Chaum aan een elektronisch betaalsysteem, hoewel hij dat niet helemaal ontwikkelde op de manier die Hughes graag zou zien. Daarnaast werkte een van May’s collega Extropians, de lokale Bay Area computerwetenschapper en cryptograaf Phil Zimmermann, aan een op RSA-gebaseerde openbare sleutelencryptiesoftware genaamd Pretty Good Privacy (PGP).

Toch leken dit erg magere resultaten, als je bedenkt hoe groot de doorbraken waren die May en Hughes zo enthousiast maakten voor de toekomst. Hoewel de nieuwe golf van crypto zich ongeveer vijftien jaar door het academia had verspreid, en een serie succesvolle Crypto-conferenties een reeks baanbrekende concepten hadden getoond, bleef de daadwerkelijke softwareontwikkeling ver achter.

### De Vergadering

Eric Hughes verhuisde uiteindelijk niet naar Santa Cruz. Maar de reis was zeker niet verspild. Gedurende zijn bezoek aan het stadje aan het strand kwamen Hughes en May overeen dat het tijd was om het gat tussen de academische wereld en de echte wereld te dichten, en zij concludeerden dat zij zelf het initiatief moesten nemen om dit te laten gebeuren. May en Hughes zette zich in voor het bijeenbrengen van een groep van enkele van de slimste en meest bekwame cryptografen en hackers uit de Bay Area, en gingen aan het werk.

De eerste persoon die ze bij hun plan betrokken was John Gilmore, een vroege medewerker van Sun Microsystems en medeoprichter van de digitale rechtenorganisatie Electronic Frontier Foundation (EFF). Hij had al geruime tijd gesproken over het brengen van cryptografie naar het grote publiek binnen lokale hackerskringen. De drie van hen - May, Hughes en Gilmore - begonnen vervolgens meer gelijkgestemde individuen uit te nodigen die volgens hen niet zouden terugdeinzen voor enige hands-on technologie activisme.

Een paar maanden verstreken, tot op een zaterdag in september een groep van ongeveer twee dozijn gelijkgestemde individuen zich verzamelde in Hughes’ nieuwe en op dat moment nog ongemeubileerde appartement in Oakland. De meeste aanwezigen waren afkomstig uit de hacker-gemeenschap in de Bay Area, terwijl May ook een kleine Extropian-delegatie had geregeld. Dit zorgde voor een bijzonder technologiebewuste groep mensen.

May opende de bijeenkomst met een inleiding over cryptografie. Hij bracht de aanwezigen op de hoogte van het veelbelovende potentieel van openbare-sleutel-cryptografie evenals enige van de innovatieve schema’s die waren voorgesteld sinds de doorbraak van Diffie en Hellman. Hierna deelde hij een door hemzelf samengesteld boekje uit waarin de basisprincipes werden uitgelegd en belangrijke termen werden gedefinieerd. De groep begon vervolgens te discussiëren over de mogelijke gevolgen voor de samenleving als cryptografische hulpmiddelen op grote schaal beschikbaar zouden worden en daarentegen de onrustbarende implicaties van een toekomst zonder dergelijke hulpmiddelen.

…mmarie… Middags experimenteerde de hele groep, zittend op de vloer bij gebrek aan meubilair, speels met analoge voorstellingen van crypto-protocollen. Ze bedachten het op papier gebaseerde “crypto-anarchie spel”, waarbij enveloppen fungeerden als een protocol voor het anonimiseren van berichten, een prikbord diende als een informatiemarkt, en Monopoly-geld werd rondgegeven als digitale valuta. Op een leuke manier kreeg iedereen een idee van hoe deze systemen zouden werken. In de namiddag begon de hele bende, vanwege een gebrek aan meubels zittend op de vloer, op speelse wijze te experimenteren met analoge representaties van cryptoprotocollen. Ze creëerden het op papier gebaseerde “crypto-anarchie-spel”, waarbij enveloppen fungeerden als een protocol voor het anonimiseren van berichten, een prikbord fungeerde als een informatiebeurs en Monopolie-geld werd rondgegeven alsof het digitale contanten waren. Op een leuke manier kreeg iedereen een gevoel van hoe deze systemen zouden functioneren.

De bijeenkomst was een succes. Aan het einde van een dag vol mini-seminars, brainstormsessies en spelletjes, was iedereen die het appartement van Hughes had bereikt voor deze speciale gelegenheid, aangestoken met hetzelfde gevoel van enthousiasme dat May, Hughes en Gilmore had aangezet om deze unieke groep mensen bij elkaar te brengen. Belangrijker nog, ze deelden nu de beoordeling van de organisatoren dat de crypto-protocollen waarover ze hadden geleerd, geïmplementeerd moesten worden als werkende software en zo ver mogelijk verspreid moesten worden. Om de zaak verder te bevorderen, gingen ze ermee akkoord om de bijeenkomst een maandelijks evenement te maken.

Op dit moment concludeerde de groep ook dat ze een pakkende naam nodig hadden om zichzelf mee te omschrijven. Hughes had het tot dan toe de Cryptologie Amateurs voor Sociale Onverantwoordelijkheid (of kortweg CASI) genoemd, maar nu overwogen ze suggesties zoals “De Crypto Vrijheid Liga”, “Privacy Hackers”, en “De Crypto Cabal”. Middenin al dit gepraat riep Hughes’ vriendin van dat moment, hacker Jude Milhon, gekscherend uit: “Jullie zijn gewoon een stel cypherpunks!”[^143]

Met de slimme woordspeling van “cipher” en “cyberpunk,” had de groep hun naam gevonden. Met de slimme samentrekking van “cipher” en “cyberpunk,” had de groep hun naam te pakken.

### De Cypherpunks

De bijeenkomsten die volgden, werden op wisselende locaties gehouden - vaak bij iemand thuis of in iemands werkruimte - en vormden een centraal punt voor het delen van informatie, discussie en projectcoördinatie. Natuurlijk bood het iedereen ook de kans om elkaar wat beter te leren kennen, terwijl nieuwe mensen welkom waren om zich aan te sluiten en meer te leren over het initiatief en hoe ze konden deelnemen.

De Cypherpunks hebben tijdens deze vroege bijeenkomsten toekomstige doelen geschetst en hun strategieën uitgewerkt om deze doelen te bereiken.

Allereerst hadden de Cypherpunks zich tot dusverre tot doel gesteld om een dystopische toekomst te voorkomen, een toekomst waarin digitale communicatie kan worden gemonitord, geanalyseerd en uiteindelijk misbruikt. Net zoals de cryptografen die hen inspireerden, waren ze bezorgd dat zo’n verlies aan privacy despoten en tirannen zou kunnen machtigen, ten koste van de individuele vrijheden; May kondigde op een gegeven moment half-grappend aan dat George Orwell’s ‘1984’ verplichte lectuur was voor iedereen binnen de groep.

Maar de Cypherpunks waren niet alleen van plan om privacy te promoten of zelfs te eisen. Ze zouden zich niet beperken tot het lobbyen bij verkozen ambtenaren, of werken via het politieke en juridische proces, zoals sommige bestaande belangenorganisaties (zoals de EFF) al deden.

Een belangrijk onderdeel van hun strategie was dat de Cypherpunks zelf de behoeder van hun privacy gingen worden.[^144]

“We moeten onze eigen privacy verdedigen als we verwachten er nog enige te hebben,” schreef Hughes in “Het Manifest van de Cypherpunk,” dat de mede-oprichter van de groep hardop voorlas tijdens een Cypherpunk-bijeenkomst begin 1993. “We moeten samenkomen en systemen creëren die anonieme transacties mogelijk maken. Mensen hebben eeuwenlang hun eigen privacy verdedigd met gefluister, duisternis, enveloppen, gesloten deuren, geheime handdrukken en koeriers. De technologieën van het verleden boden geen sterke privacy, maar elektronische technologieën doen dat wel.”

Ze hadden plannen om deze elektronische technologieën te ontwikkelen en deze als gratis software te verspreiden. In overeenstemming met de hacker ethiek, hadden ze niet de intentie om iemand om toestemming te vragen om dit te doen.

“Cypherpunks schrijven code”, verklaarde Hughes. “We weten dat iemand software moet schrijven om privacy te verdedigen, en wij gaan dat doen.”[^145]

“Cypherpunks schrijven code”. Dit werd de informele strijdkreet van de groep.

### De Mailinglijst

De maandelijkse bijeenkomsten van de Cypherpunks waren vrij en open van aard. Naast de vaste kern van reguliere deelnemers, kwamen er ook nieuwsgierige nieuwkomers om een indruk te krijgen van wat er gaande was. Om de coördinatie hiervan te vergemakkelijken, richtte Hughes een e-maillijst op, gehost op de computer van Gilmore, waar hij aankomende evenementen aankondigde. Elke abonnee ontving handig een bericht in hun inbox met daarin de datum en locatie.

Maar de mailinglijst van de Cypherpunks zou al snel een groter doel gaan dienen. Het duurde niet lang voordat de lijst werd gebruikt om discussies van de fysieke vergaderingen voort te zetten. Niet veel later werden er volledig nieuwe onderwerpen op de mailinglijst geïntroduceerd, die niets te maken hadden met wat er besproken was tijdens de persoonlijke bijeenkomsten. Toen het aantal berichten toenam, begon de mailinglijst van de Cypherpunks een eigen leven te leiden.

E-mail had natuurlijk als extra voordeel dat iedereen kon deelnemen, ongeacht de geografische afstand, en vanuit het comfort van hun eigen huis. Vrij voorspelbaar, groeide de Cypherpunks mailinglijst snel en overtrof die van de feitelijke Cypherpunk evenementen. Slechts weken na de lancering had de lijst al 100 abonnees - beduidend meer dan de paar dozijn hackers en cryptografen die de maandelijkse bijeenkomsten bijwoonden.

En de populariteit van de mailinglijst begon echt te exploderen toen het technologietijdschrift Wired in mei 1993 zijn coververhaal wijdde aan de Cypherpunks. “Rebellen met een reden (Jouw privacy)” stond er op de cover, net boven een foto van drie gemaskerde mannen die de Amerikaanse vlag vasthielden. (De uitdrukkingsloze witte maskers met codes erop gekrabbeld verborgen de gezichten van May, Hughes en Gilmore.) Dankzij dit coververhaal had nu vrijwel iedereen met interesse in computers gehoord van de groep privacyactivisten en door hun wereldwijde bereik, stroomden honderden mensen van over heel de Verenigde Staten en de rest van de wereld toe om zich aan te melden voor hun e-maillijst.

In de daaropvolgende jaren werd de Cypherpunks mailinglijst een klein fenomeen op het vroege internet. Met tot wel 2.000 abonnees en soms bijna evenveel e-mails per maand, bespraken de Cypherpunks een breed scala aan onderwerpen: van cryptoprotocollen, tot overheidsbeleid, tot implementaties van software, en tips voor boeken of films, evenals periodieke klaagzangen en verhitte discussies. De lijst bood een platform voor publieke discussie tussen enkele van de meest getalenteerde hackers op de planeet, terwijl Silicon Valley’s CEO’s en mainstream journalisten ook graag meelazen.

Tim May onderscheidde zich op de mailinglijst dankzij zijn vele mails: niemand was actiever dan hij, en niemand leverde een groter scala aan bijdragen. Hij schetste toekomstscenario’s, deelde ideeën, nam deel aan discussies, gaf technische uiteenzettingen, stelde strategieën voor, gaf commentaar op actuele gebeurtenissen, linkte naar relevante artikelen en deelde regelmatig “snel geschreven” essays - soms zelfs verscheidene op een dag.

Maar hij onderscheidde zich ook door zijn unieke gevoel voor humor. Soms voerde hij sarcastisch het woord tegen de Cypherpunk-agenda vanuit het perspectief van een Ingsociaanse overheid en berispte hij andere deelnemers aan de lijst als “burgereenheden”. Andere keren maakte hij opzettelijk politiek incorrecte grappen om de grenzen uit te dagen van wat als sociaal acceptabel werd beschouwd; zo veranderde hij op een gegeven moment bijvoorbeeld zijn e-mailhandtekening in “een bijbeltekst in afwachting van beoordeling onder de Communicatie Decency Act”, waarbij de begeleidende tekst een incestueuze orgie beschrijft.[^146] (Of misschien overschreed hij de sociaal aanvaardbare grenzen ronduit, afhankelijk van wie je het zou vragen; May leek er hoe dan ook niet veel om te geven.)

En zijn aanwezigheid op de mailinglijst diende ook nog een andere waardevolle doel. Hoewel de lijst volledig ongemodereerd was, speelde May vaak de rol van een onofficiële moderator, en begeleidde gesprekken waar nodig. Als een discussie dreigde te ontsporen, had hij de gewoonte om zijn kenmerkende analytische perspectief in te brengen, waarbij hij uitlegde waarom hij geloofde dat bepaalde opmerkingen of onderwerpen al dan niet geschikt waren voor de lijst, maar zonder daadwerkelijk iets te verbieden; hij wilde niet dat iemand die macht had, zelfs hijzelf niet. In plaats van anderen op te leggen hoe ze zich moeten gedragen, had May een manier om het voortouw te nemen door voorbeeld, en wanneer andere abonnees klaagden over de inhoud op de mailinglijst, moedigde hij hen ook aan om het voortouw te nemen door voorbeeld.

Voor veel van zijn abonnees was May in de maanden en jaren dat de lijst actief was waarschijnlijk het belichaming van wat de Cypherpunk-filosofie voorstelde. Door zijn sterke aanwezigheid, zowel qua inhoud als in zijn sturende rol, was hij een leidende en kenmerkende stem van de beweging geworden.

Hoewel May zelf vaak benadrukte dat hij niet de hele Cypherpunk-gemeenschap vertegenwoordigde. Net zoals hij geen enkele moderator in de controle wilde hebben over de mailinglijst, verwierp hij ten stelligste het idee dat hij, of wie dan ook, als een formele leider of woordvoerder van de beweging beschouwd zou moeten worden. Hij stond erop dat hij slechts één stem was onder velen.

“Hoewel ieder van ons wellicht zijn of haar persoonlijke [hiërarchische] rangorde van anderen heeft, is het belangrijk dat we nooit hebben geprobeerd deze rangordes te formaliseren of erover te ‘stemmen’. Of te stemmen om een Grote Leider te kiezen,” betoogde May op een gegeven moment. “Onze kracht zit in onze aantallen en in onze ideeën, niet in de man die we op een kantoor in Washington hebben geïnstalleerd zodat hij persconferenties kan geven en sound bites kan leveren voor journalisten. Onze kracht zit in ons meerkoppige (durf ik ‘Medusa’ te zeggen?), multinationale, informele gebrek aan structuur.”[^147]

Inderdaad, de Cypherpunks waren niet een organisatie in de traditionele zin. Het was een bewust informele, ongestructureerde en open groep. De Cypherpunks hadden geen stemprocedure, geen vertegenwoordigers, en ze gaven zelfs geen gezamenlijke verklaringen. Iedereen kon een Cypherpunk worden, maar alle Cypherpunks zetten zich uiteindelijk in als individuen. Ze hadden geen specifieke taken of regels - noch kon iemand anderen verantwoordelijk houden voor hun eigen acties.

Toch werd actie aangemoedigd. Als iemand vond dat de Cypherpunks een specifieke technologie zouden moeten ontwikkelen, aan een bepaald evenement zouden deelnemen of op een andere manier tot de zaak zouden bijdragen, was het aan die persoon om het initiatief te nemen en te kijken of anderen ook wilden helpen.

In feite werkte de Cypherpunk-beweging niet alleen aan een ander type toekomst. Voor May vertegenwoordigde het al die toekomst. Hij zag de open, toestemmingloze en niet-hiërarchische manier waarop de Cypherpunks en hun e-maillijst opereerden als een model voor een opkomende crypto-anarchistische samenleving.

### Crypto-Anarchie

De Extropians speculeerden soms over het creëren van vrije gebieden om te ondermijnen, zich te verbergen, of te ontsnappen aan staatscontrole over hun levens. Sommigen van hen stelden voor om steden te bouwen op grote drijvende eilanden in de zee - het zogenaamde seasteading - als de weg voorwaarts. Anderen geloofden dat het misschien mogelijk zou zijn om een klein eiland op te kopen om er een libertaire samenleving te stichten. Weer anderen suggereerden dat ze allemaal naar een specifieke jurisdictie zouden moeten verhuizen en proberen de lokale politieke structuren te beïnvloeden om zoveel mogelijk wetten en regulaties aan de kant te zetten.

Maar Tim May had eigenlijk niet echt zin om te verhuizen. Hij had een beter idee.

Sinds May de stukjes bij elkaar had gevoegd om het ontwrichtende potentieel van anonieme informatie markten te zien, was hij een toekomst gaan visualiseren dat leek op de werelden uit zijn cyberpunk boeken, terwijl hij tegelijkertijd analogieën maakte met Atlas Shrugged. Hij besefte dat het soort samenleving dat hij wilde beschrijven in zijn aankomende roman, werkelijkheid kon worden.

In de roman van Rand maken de productieve ondernemers hun ontsnapping mogelijk met behulp van futuristische technologie. Hoewel May erkende dat warmtestralingsschermen nog steeds tot het domein van de sciencefiction behoorden, was hij als medeoprichter van de Cypherpunk-beweging gaan inzien dat het internet en sterke cryptografie uiteindelijk een vergelijkbare ontsnapping uit de macht van de staat zouden kunnen faciliteren, net als in de verhalen van de cyberpunk-genre.

May schetste deze visie in “Het Crypto Anarchistisch Manifest.”[^148] Hij schreef het oorspronkelijk voor de editie van de Crypto-conferentie in 1988, las het korte manifest voor tijdens de allereerste bijeenkomst van de Cypherpunks in Hughes’s appartement en deelde het later ook via de Cypherpunks mailinglijst.

“Een spook waart rond in de moderne wereld, het spook van de crypto-anarchie,” begon het manifest met een knipoog naar het Communistisch Manifest van Karl Marx en Friedrich Engels, voordat het voorspelde dat computertechnologie en cryptografische protocollen “de aard van de overheidsregulering volledig zullen veranderen, het vermogen om de economische interacties te belasten en te controlen, het vermogen om informatie geheim te houden, en zelfs de aard van vertrouwen en reputatie zullen veranderen.”

Het lijkt erop dat je geen tekst hebt opgegeven om te vertalen. Kun je alsjeblieft de gewenste passage delen zodat ik deze kan vertalen en editoreren?

“Net zoals de technologie van drukken de macht van de middeleeuwse gilden en de sociale machtsstructuur heeft veranderd en verminderd, zo zullen cryptologische methoden de aard van bedrijven en de inmenging van de overheid in economische transacties fundamenteel veranderen.”[^149]

Het internet was nog niet getransformeerd naar de kleurrijke 3D-wereld zoals die in de romans van Vinge, Stephenson en Gibson werd voorgesteld. Maar als je deze verhalen meer als metaforische representaties van online domeinen beschouwde, had May ze toch als visionair leren waarderen. Terwijl het internet verder zijn onvermijdelijke pad naar massa-adoptie vervolgde, en mensen stapje voor stapje zouden leren om online zelf te organiseren, geloofde May dat de instellingen van de reële wereld uiteindelijk zouden worden vervangen door hun cyber-equivalenten. Het internet zou in toenemende mate dienen als facilitator voor een parallelle, digitale samenleving, met eigen gemeenschappen, ondernemingen en uiteindelijk ook eigen economieën.

“Dit maakt snelle experimentatie, zelfselectie en evolutie mogelijk,” stelde May voor op de Cypherpunks mailinglijst. “Als mensen moe worden van een bepaalde virtuele gemeenschap, kunnen ze deze verlaten. De cryptografische aspecten zorgen ervoor dat hun lidmaatschap van een bepaalde gemeenschap onbekend blijft voor anderen (vis-a-vis de fysieke of buitenwereld, oftewel, hun ‘echte namen’) en fysieke dwang vermindert.”

De opdracht is onduidelijk. Het lijkt erop dat je de mij een Engelse passage wilt geven om te vertalen naar het Nederlands, maar je hebt geen passage gegeven. Kan je alsjeblieft het deel dat je wilt dat ik vertaal opnieuw versturen?

“De elektronische wereld is geenszins volledig, aangezien we nog steeds een groot deel van ons leven in de fysieke wereld zullen doorbrengen. Maar de economische activiteit in het domein van het Net neemt sterk toe en deze ‘crypto-anarchie’ ideeën zullen de macht van fysieke staten om bewoners te belasten en te dwingen verder ondermijnen.”[^150]

Dit alles werd mogelijk gemaakt door de kracht van cryptografie. Niet alleen zouden crypto-hulpprogramma’s gebruikers helpen hun echte identiteit te beschermen, waardoor ze beschermd werden tegen fysiek geweld, maar dezelfde tools zouden ook toestaan dat elk tweetal personen zaken zou doen zonder dat een van hen ooit wist met wie ze te maken hadden.

“[…] sterke cryptografie is het ‘bouwmateriaal’ van cyberspace,” schreef May aan zijn mede-Cypherpunks, “de mortel, de bakstenen, de steunbalken, de muren. Niets anders kan de ‘permanentie’ bieden… zonder crypto zijn de muren onderhevig aan instorting bij de eerste aanraking door een kwaadwillend persoon of organisatie. Met crypto kan zelfs een 100 megaton H-bom de muren niet doorbreken.”[^151]

May voorzag dat Cypherpunk-tools mensen zouden helpen om hun economische activiteit voor de staat te verbergen en zo een “Galt’s Gulch in cyberspace” zouden creëren. Hij keek uit naar een toekomst waarin dit uiteindelijk zou leiden tot de volledige ineenstorting van regeringen. Zonder gedwongen herverdeling van welvaart, zou deze toekomstige economie zichzelf organiseren rondom vrijwillige interactie en vrije markten. Er zou een spontane orde ontstaan via het internet.

“In feite heeft Hayek héél véél met de Cypherpunks te maken!” schreef May op de Cypherpunk mailinglijst. “Van ‘The Road to Serfdom’ tot ‘Law, Legislation, and Liberty’, zijn werken hebben diepgaande invloed op mij gehad en op vele anderen. […] Ik zou zelfs zeggen dat Hayek een kandidaat zou zijn geweest om op de cover van ‘Wired’ te staan… natuurlijk ervan uitgaande dat hij 60 jaar jonger was, sommige van zijn lichaamsdelen had gepiercet, en beter nog, een Netchick was.”[152]

### Code

Tim May was er zich goed van bewust dat de crypto-anarchistische ideeën die hij verspreidde niet precies aantrekkelijk waren voor een breed publiek; niet iedereen verwacht een ineenstorting van regeringen. Waarschijnlijk zou het nog erger worden als men erachter zou komen dat onkraakbare encryptie en anonieme mixnetwerken grootschalige verspreiding van kinderpornografie mogelijk maakten en veilige communicatie voor terroristische cellen faciliteerden. Veel mensen zouden deze nieuwe instrumenten waarschijnlijk met angst en woede bekijken.

Echter, May weigerde de risico’s die deze nieuwe technologieën introduceerden te bagatelliseren.

“Privacy heeft zijn prijs”, betoogde hij simpelweg. “Het vermogen van mensen om misdaden te beramen en te plegen achter gesloten deuren is evident, en toch eisen we geen verborgen camera’s in woningen, appartementen en hotelkamers!”[^153]

Voor May was crypto-anarchie bovendien geen verre utopie die brede steun voor zijn ideeën vereiste: integendeel, hij beschouwde het bijna als een voldongen feit. Hij begreep dat de weg ernaartoe bezaaid kon zijn met tegenslagen en onderdrukkende wetten, gerechtvaardigd door beleidsmakers die angst inboezemden over de “Vier Ruiters van de Infocalyps”: terroristen, pedofielen, witwassers en pornografen. Maar cypherpunk tools waren goedkoop te verspreiden, makkelijk te gebruiken en konden niet on-uitgevonden worden. Op de lange termijn, geloofde May, was succes vrijwel gegarandeerd.

Dit betekende niet dat elke Cypherpunk Mays nogal radicale visie deelden - noch hoefden ze dat te doen. Vaker wel dan niet waren Cypherpunks libertariërs, maar velen onderschreven ook een gematigder wereldbeeld dan May. Sommige Cypherpunks waren zelfs helemaal geen libertariërs, met meerdere van hen die zichzelf identificeerden als socialist.

“Ik ben geen libertariër, en het is onwaarschijnlijk dat ik dat ooit zal zijn,” schreef Hughes aan de mailinglijst. “Het streven naar privacy staat los van de meeste partijpolitieke standpunten. Zo sterk als de libertarische aanwezigheid op deze lijst is, is het geenszins de enige visie. Juist omdat cypherpunk kwesties dwars door het politieke spectrum snijden, zijn ze zo krachtig.”[^154]

Wat van belang was, stemden May en Hughes mee in, was dat de Cypherpunks ongeacht hun politieke overtuiging konden werken aan een gezamenlijk doel: het ontwikkelen en verspreiden van tools voor privacy. Cypherpunks schrijven code.

Inderdaad, de groep was nauwelijks gestart toen Hughes een vroege versie ontwikkelde van de eerste ooit remailer, gebaseerd op het mixnetwerkvoorstel van David Chaum. De eerste uitvoering van deze remailer zou emails accepteren, details die naar de afzender verwezen verwijderen en vervolgens doorsturen naar, of de volgende remailer, of naar de bedoelde ontvanger van de email. Deze uitvoering van Hughes omvatte echter nog geen encryptietools; het was nog altijd in ontwikkeling.

Gelukkig kreeg Hughes al snel hulp van een andere Cypherpunk. Hal Finney, een van de Extropians die zich bij Tim May hadden aangesloten voor de Cypherpunk-bijeenkomsten, was net begonnen met het bijdragen aan de implementatie van Phil Zimmermann’s PGP. Met zijn nieuw verworven kennis van publieke-sleutelcryptografie was het niet lang voordat Finney PGP integreerde in de remailer-code van Hughes.

Slechts enkele weken na de eerste samenkomst hadden de Cypherpunks al een volledig werkende remailer ontwikkeld. En die gingen ze ook zelf beheren. Finney en een aantal andere Cypherpunks namen het initiatief om de remailer-programma’s uit te voeren, en ze verspreidden software en beginnershandleidingen zodat anderen zich bij hen konden aansluiten. Op deze manier werden remailers operationeel. Tegen het einde van 1992 kon iedereen met een computer en internetverbinding e-mails versturen zonder hun metadata te onthullen.

Zo rond diezelfde tijd was Zimmermann van plan om PGP 2.0 te lanceren. De bijdragen van Finney aan deze nieuwe versie hadden geleid tot aanzienlijke verbeteringen ten opzichte van de eerste versie, en de software beschikte nu over een web-of-trust systeem. Dit stelt gebruikers in staat om cryptografisch te garanderen dat een publieke sleutel werkelijk aan een bepaald persoon toebehoort.

Met de gloednieuwe remailer-software van Hughes en de verbeterde encryptietool van Zimmermann, gingen de Cypherpunks goed van start.

Maar het zou niet lang duren voordat ze gedwongen werden om defensief te handelen…

### De Crypto Oorlogen

Toen Bill Clinton in januari 1993 het ambt van de 42e President van de Verenigde Staten op zich nam, waren er door zijn nieuwe administratie snel zorgen geuit omtrent het mogelijk onheilspellende gebruik van persoonlijke computers en het internet. Ze kondigden aan dat wetshandhavingsinstanties nieuwe tools nodig zouden hebben om mee te kunnen gaan met het recente tempo van technologische vernieuwing.

Dit bleek een voorbode te zijn van de Crypto Oorlogen van de jaren negentig; de Amerikaanse overheid zou proberen het gebruik van cryptografie te beperken.

De eerste klap viel toen Zimmermann het onderwerp werd van een strafrechtelijk onderzoek. In deze periode in de Verenigde Staten werden cryptografische protocollen die sleutels gebruikten die groter waren dan 40 bits, geclassificeerd als munitie onder de definitie van de Arms Export Control Act. Het verzenden of meenemen van een sterk cryptosysteem naar het buitenland vereiste een vergunning, vergelijkbaar met de vergunning die nodig is voor internationaal vervoer van vuurwapens, munitie of explosieven.

Zimmermann bezat geen dergelijke licentie, maar hij verspreidde wel zijn gratis software via het internet. Omdat het internet geen landsgrenzen kent, insinueerde de overheid dat Zimmermann zijn software en de daarin opgenomen cryptoprotocollen illegaal geëxporteerd had.

En toen was er de Clipper-chip, een chipset ontwikkeld door de NSA en ondersteund door de regering Clinton. De Clipper-chip gebruikte cryptografie met openbare sleutels om data te versleutelen, maar de NSA had een speciale ontcijfersleutel toegevoegd aan het protocol. Het plan was dat telecombedrijven zoals AT&T de chipset zouden adopteren, zodat gebruikers hun telefoongesprekken konden versleutelen. De telecombedrijven zouden echter een ontcijfersleutel bewaren, die op verzoek aan de regering kon worden overhandigd. Dergelijke sleutelbewaring was noodzakelijk voor nationale veiligheidsredenen, stond de regering Clinton erop: de autoriteiten moesten in staat zijn om de telefoongesprekken van potentiële en verdachte terroristen te beluisteren.

De Clipper-chip werd tegengewerkt door voorstanders van privacy en belangenorganisaties voor burgerlijke vrijheden in het hele land, waaronder de Electronic Frontier Foundation (EFF), het Electronic Privacy Information Center (EPIC) en de American Civil Liberties Union (ACLU). Ook technologietijdschriften zoals Wired, cryptografie-startups zoals RSA van Ron Rivest, Adi Shamir en Leonard Adleman, en enkele politici (zowel Democraten als Republikeinen) voerden oppositie. Critici waren van mening dat de zogenaamde sleutel vrijgave de kans vergrootte dat burgers onderworpen zouden worden aan verhoogde en mogelijk onwettige overheidssurveillance.

Uiteraard wezen de Cypherpunks de Clipper-chip ook af; de weerstand tegen de NSA-chip werd een van de eerste regelmatig terugkerende onderwerpen op de mailinglijst. Het was duidelijk dat het overhandigen van decryptiesleutels aan telecombedrijven (en, in verlengde daarvan, aan overheidslichamen die de telecoms regelen) deze cryptografische protocollen bijna nutteloos zou maken.

Voor de Cypherpunks betekende privacy in grote mate vrijheid van overheidsinmenging; zo konden ze een Orwelliaanse toekomst voorkomen. Uiteraard zou de crypto-anarchistische visie waarschijnlijk niet ver komen met hun eigen ‘Galt’s Gulch’ in cyberspace als de cryptografische bouwstenen die hen beschermde tegen de staat poreus bleken te zijn.

Tegelijkertijd stelden de Cypherpunks dat het verplichten van het gebruik van gecompromitteerde of zwakke encryptieprotocollen de wereld in geen enkele zin betekenisvol veiliger zou maken. Kwaadwillende actoren zouden nog steeds degelijke encryptie kunnen gebruiken onder de zwakke Clipper-chip encryptie laag om de inhoud van hun communicatie te verbergen. Dus zelfs als overheidsagenten hun toegewezen decryptiesleutel zouden gebruiken, zouden ze enkel meer versleutelde tekst tegenkomen.

Tim May was van mening dat de Cypherpunks een cruciale rol konden spelen in de naderende cryptografische conflicten. In tegenstelling tot gevestigde belangengroepen die beter georganiseerd, beter gefinancierd en beter in contact stonden met beleidsmakers en toezichthouders, zag May in het anarchistische organisatiemodel van de Cypherpunks juist een sterkte. Verspreid over de Verenigde Staten en daarbuiten, en zonder formeel leider of organisatiestructuur, waren de Cypherpunks niet te coöpteren. Terwijl organisaties zoals EFF, EPIC en ACLU bereid waren tot zachtaardige onderhandelingen, weigerden de Cypherpunks elke vorm van gematigdheid te adopteren.

“Op een bepaalde manier vervullen de Cypherpunks een belangrijke ecologische niche door het voeren van de radicale, buitensporige kant… misschien een beetje zoals de rol die de Zwarte Panters, Yippies en Weather Underground een generatie geleden speelden,” schreef May. [^155]

Inderdaad, in allerlei vormen nam het verzet van de Cypherpunks vorm aan; juist omdat ze geen formele organisatie hadden, handelden de Cypherpunks uiteindelijk uit eigen beweging. Sommigen van hen verspreidden flyers met informatie over de Clipper-chip in lokale winkelcentra. Anderen analyseerden hoe de chip werkte om te proberen fouten in het ontwerp te vinden. En natuurlijk was het schrijven van code de voornaamste strategie van de Cypherpunks.

“Potentiële inbreuk in de echte wereld zou het volledig verbieden van sterke crypto kunnen zijn, waarbij cijfers goedgekeurd door de overheid verplicht worden,” opperde May in zijn denken over verdere escalatie van de Crypto Oorlogen. “Zo’n verbod zal een zwaar, verwoestend effect hebben op onze privacy, op ons vermogen om de cyberspace-werelden op te bouwen die ik heb beschreven, en over het algemeen op computer-gemedieerde markten.”

Ik geloof dat je bij het beschrijven van het verzoek om een tekst te vertalen, vergeten bent om de daadwerkelijke tekst die vertaald moet worden in te voeren. Kun je alsjeblieft de tekst voorleggen die vertaald moet worden? Dan zal ik deze op de juiste manier verwerken.

“Ons onmiddellijke doel moet zijn om ervoor te zorgen dat de ‘geest uit de fles is’, dat er voldoende crypto gereedschappen en kennis wijdverspreid zijn zodat zo’n overheidsverbod zinloos wordt.”[^156]

### Sucessen

De Cypherpunks waren gemotiveerd en gedreven, maar stonden tegenover de volle kracht van de Amerikaanse overheid. Weinigen zouden hebben verwacht dat ze als overwinnaars uit de Crypto Oorlogen zouden komen.

Toch boekten ze het ene succes na het andere.

Een van de meest opmerkelijke overwinningen kan worden toegeschreven aan Matt Blaze, een beveiligingsonderzoeker bij Bell Labs en een frequente deelnemer aan de Cypherpunks mailgroep. In 1994, heeft Blaze een pijnlijke klap uitgedeeld aan de Clipper-chip door een paper te publiceren dat een fout aantoonde in het ontwerp van de chip, die gebruikers toestond om de speciale ontsleutelingssleutel uit te schakelen. Terwijl de reputatieschade van de Clipper-chip al groeide door de hevige tegenstand die het te verduren had, blijkt nu dat de Clipper-chip zelfs niet deed waarvoor hij verondersteld werd ontworpen te zijn.

Dit was voldoende om telecombedrijven ervan te overtuigen de NSA technologie niet te adopteren. Het project zou geheel ter ziele gaan tegen 1996.

In een vergelijkbare lijn wisten Cypherpunks Ian Goldberg en David Wagner in 1995 de gesloten bron- en export-grade encryptiestandaard van Netscape te kraken. Dit deden ze in het kader van een wedstrijd, ontworpen door Hal Finney, en ze hadden hier slechts enkele uren voor nodig. Het schaadde het imago van een van de vooraanstaande bedrijven van Silicon Valley.

Als reactie op de inbreuk, beweerde Netscape dat ze wettelijk verhinderd waren om sterkere encryptiestandaarden aan te bieden in het buitenland. Hoewel dit maar een deel van het probleem was, bood het weinig geruststelling aan potentiële klanten buiten de VS. Het incident benadrukte ook een ander probleem als gevolg van de classificatie van encryptie als munitie: Amerikaanse technologiebedrijven liepen het risico marktaandeel te verliezen aan buitenlandse concurrenten.[^157]

Weer een andere Cypherpunk, Brad Huntting, kwam in 1994 met een slim idee om de exportrestricties op dergelijke crypto-protocollen uit te dagen: hij publiceerde code in een fysieke vorm om aan te tonen dat verboden op software distributies in strijd zijn met fundamentele rechten.

“Het recht op vrije meningsuiting wordt beschermd door de Amerikaanse grondwet. We hoeven alleen maar aan te tonen dat encryptiesoftware gelijk staat aan spraak,” schreef hij aan de mailinglijst. “Dit zou niet te moeilijk moeten zijn (misschien een beetje pijnlijk, maar niet moeilijk). De daad zou een gepubliceerd werk moeten betreffen (bij voorkeur in de gedrukte zin).”[^158]

Ongeveer een jaar later publiceerde Zimmermann ‘PGP: Broncode en Interne Werking’: hij had de volledige PGP-broncode in een boek afgedrukt. Zoals Huntting inderdaad had aangegeven, vallen boeken (inclusief de export ervan) in de VS onder de bescherming van het Eerste Amendement. Door dezelfde informatie die hem onderwerp van een strafrechtelijk onderzoek had gemaakt, vrij en legaal in harde kaft te verspreiden, legde Zimmermann de absurditeit van de regelgeving rondom crypto-export bloot.

Hoewel het nooit werd bevestigd dat het iets te maken had met de publicatie van zijn boek, liet de Amerikaanse overheid Zimmermann’s zaak vroeg in 1996 vallen.

Bovendien zouden de exportverboden tegen het einde van dat jaar volledig worden opgeheven. Een combinatie van juridische uitdagingen, economisch schadelijke beperkingen op de Amerikaanse technologie-industrie, en de onomkeerbaar wijdverbreide verspreiding van crypto-protocollen buiten de Verenigde Staten bewoog de Clinton administratie om commerciële encryptie volledig van de Munitielijst te schrappen.

De Cypherpunks hadden dit niet alleen gedaan: de beweging om cryptografie te verdedigen tijdens de Crypto-oorlogen was breder dan enkel zij. Maar, zij hadden onmiskenbaar een belangrijke rol gespeeld. Het losse collectief van hackers en cryptografen, verenigd door weinig meer dan een mailinglijst op het internet, was de strijd aangegaan met de Amerikaanse overheid, en had gewonnen.

## Hoofdstuk 9: Cypherpunk Valuta

De Cypherpunks hadden zich tot doel gesteld de privacy in het digitale tijdperk te verdedigen. Ze begrepen dat de privacy die fysiek geld biedt, in gevaar was. Als elektronische betalingen papiergeld en metalen munten zouden vervangen, konden banken en andere transactieverwerkers (en bij uitbreiding de regeringen die hen reguleren) alle economische activiteit monitoren.

De cryptographer David Chaum en zijn eCash-systeem dienden als grote inspiratiebron en echoënden zijn waarschuwingen. De Cypherpunks waren van mening dat dit uiteindelijk het einde van de menselijke vrijheid zou kunnen betekenen.

“[…] als de overheid deze cashloze samenleving creëert, dan zal de overheid ongekende controle hebben over vrijwel elk aspect van ons leven,” zo zou Tim May stellen op de Cypherpunk mailinglijst.

“Elke transactie, hoe onbeduidend ook, zal worden vastgelegd, bewaard en geanalyseerd. Er zal een volledige audittrail bestaan van alle aankopen, voedselvoorkeuren, entertainmentkeuzes, contacten met anderen, enzovoort,” schreef hij. “Bovendien kunnen transacties die als politiek incorrect worden beschouwd, en er zijn tientallen duidelijke voorbeelden om uit te kiezen, simpelweg worden …rboden…oor het typen van een paar regels instructies in de relevante databanken.”[^159]

May gaf in zijn bericht vrij alledaagse voorbeelden om dit punt duidelijk te maken. Iemand die ooit was gearresteerd voor rijden onder invloed zou zo bijvoorbeeld kunnen worden geweigerd bier te kopen bij een slijterij, of zwangere vrouwen (“en onder Clintons geautomatiseerde zorgsysteem zal dit allemaal bekend zijn”) zouden kunnen worden verhinderd sigaretten te kopen. Overheidscontrole over transacties zou niet alleen invloed hebben op gevaarlijke criminelen of extreme politieke dissidenten, de Cypherpunk wilde benadrukken, het zou uiteindelijk leiden tot totale controle over alle burgers: “Vergis je niet, een door de overheid gerunde maatschappij zonder contant geld zal erger zijn [dan] het allerergste van Orwell.”[^160]

Dit is waarom May tijdens de allereerste bijeenkomst van de Cypherpunks het concept van elektronisch geld presenteerde, en waarom de losse verzameling van hackers en cryptografen die samenkwamen in het ongemeubileerde appartement van Eric Hughes het idee direct omarmden. De creatie van een digitaal betalingssysteem met sterke privacygaranties, zo geloofden de Cypherpunks, kon helpen zo’n dystopische toekomst te voorkomen.

Maar dit was niet de enige reden waarom de Cypherpunks digitaal geld wilden creëren; zij waren van mening dat internetgeld hun beweging op meer dan één manier zou kunnen bevorderen.

Behalve privacy, waren sommige Cypherpunks ook zeer geïnteresseerd in andere functies die elektronisch geld mogelijk kon bieden, zoals snelle transactieafhandeling, onomkeerbaarheid, of kostenefficiëntie. Ze waren enthousiast over de nieuwe mogelijkheden die dergelijke functies mogelijk zouden kunnen ontsluiten: internetgeld kon online diensten en spellen ten goede komen, speculeerden ze, of machine-to-machine betalingen mogelijk maken. Dit zou op zijn beurt misschien innovatieve nieuwe soorten markten kunnen faciliteren, zoals de markten voor het toewijzen van computerbronnen voorgesteld door de hightech Hayekianen.

Dichter bij huis zouden digitale contanten voordelen kunnen bieden voor projecten van Cypherpunks, zoals remailers. De door Eric Hughes en Hal Finney ontwikkelde remailers werden aanvankelijk gratis aangeboden door Cypherpunks, maar het was niet duidelijk of deze regeling stand kon houden. Naarmate deze diensten in de loop van de tijd populairder zouden worden, zou het beheren van een remailer uiteindelijk te veel van een belasting kunnen worden voor vrijwillige hobbyisten; Hughes verwachtte dat beheerders op een dag kosten zouden moeten gaan rekenen. Voor de hand liggende redenen zouden dergelijke betalingen anoniem moeten zijn: gebruikers zouden hun identiteit niet moeten onthullen om remailers te gebruiken.

Evenzo was de ontwikkeling van anonieme informatiemarkten - BlackNets - afhankelijk van het bestaan van een privacybeschermende vorm van digitaal geld. Voor mensen om bereid te zijn geclassificeerde documenten of geheime rapporten via internet te verkopen, moesten ze er zeker van zijn dat superieuren bij hun overheidsinstantie of bedrijf niet konden ontdekken dat zij het waren die deze gegevens voor een beetje extra geld verkochten: dit betekende, dat dit beetje extra geld vrij van elke identificerende eigenschap moest zijn.

En elektronisch geld was uiteindelijk een crucieel bouwsteen in Tim May’s crypto-anarchistische visie voor de toekomst. Het opzetten van een parallelle samenleving in de digitale ruimte—een “Galt’s Gulch in cyberspace”—vereiste dat mensen hun inkomen en rijkdom verborgen konden houden voor hun overheid. Een anonieme digitale valuta zou mensen in staat stellen belastingheffing te ontlopen.

May begreep goed dat elektronisch geld op zichzelf niet meteen de belastingambtenaar overbodig zou maken. Mensen die zichtbaar deelnemen aan de economie - “de man die werkt bij Lockheed of achter de toonbank bij Safeway” - zouden nog steeds de rekening betalen voor diensten van de overheid. Maar volgens May zou, als een significant deel van de economie succesvol en consequent belastingen kon ontduiken, dit uiteindelijk een verandering in het publieke sentiment veroorzaken dat dan weer een veel grotere sociale verandering zou teweegbrengen.

“[D]e impact zal zijn […] een ondermijning van …eun…oor belastingen, wanneer het nieuws zich verspreidt dat veel consultants, schrijvers, informatieverkopers en dergelijke een groot deel van hun inkomen afschermen door gebruik te maken van netwerken en sterke crypto,” schreef May. “Het belastingstelsel is al wankel - een nationale schuld van € 5 biljoen, die elk jaar groeit - en het zou niet veel van een duw nodig kunnen hebben om een ‘faseverandering’ te veroorzaken; een belastingopstand.”[^161]

En tot slot was er nog de mogelijkheid van monetaire hervorming.

In het bijzonder zagen sommige van de Cypherpunks, zoals Tim May - die ook deel uitmaakte van de Extropian gemeenschap, in elektronisch geld een instrument voor de verwezenlijking van Friedrich Hayek’s vrije bankeneconomie. Ze beseften dat aangezien elektronisch geld in alles wat de markt wil kan worden uitgedrukt, dit concurrentie tussen valuta’s sterk praktischer kon maken en veel moeilijker te stoppen. Vrije banken konden overal ter wereld gevestigd zijn, terwijl iedereen met een internetverbinding hun valuta, anoniem, zou kunnen gebruiken.

“De sterke encryptie die wordt gebruikt, biedt meer flexibiliteit in het omzeilen van normale valutaregels en kan gebruikers in staat stellen om onderling overeen te komen welke valuta ze willen gebruiken,” schreef May op de Cypherpunk mailinglijst. En: “een van de potentiële voordelen van sterke encryptie is de vaak besproken ‘denationalisatie van geld.’”

In totaal, het stelde elektronisch geld voor als iets dat vergelijkbaar is met de heilige graal van de Cypherpunks.

### Het compromis van Chaum

Toen de Cypherpunks in de vroege jaren ’90 net op het toneel verschenen, was David Chaum’s eCash het enige elektronische geldproject dat een sterke privacy garandeerde. In hun discussies over digitaal geld tijdens bijeenkomsten of op de Cypherpunks mailinglijst, maakten Tim May en de andere Cypherpunks vaak expliciet of impliciet verwijzingen naar Chaum’s ontwerp. Hij had met zijn methode van blinde handtekeningen een cruciaal onderdeel van de privacy puzzel opgelost.

Verschillende van de Cypherpunks brachten zelfs zelf een bezoek aan Amsterdam, om een tijdje te werken bij Chaum’s start-up voor digitale valuta. Naast mede-oprichter van de Cypherpunks Eric Hughes en computerwetenschapper (en Extropian) Nick Szabo, waren dit bijvoorbeeld ook beveiligingsspecialist Bryce “Zooko” Wilcox-O’Hearn en de vroege Cypherpunk Lucky Green.

Chaum daarentegen, was niet bijzonder gecharmeerd van de meer radicale crypto-anarchistische aspiraties die May en sommige van de andere Cypherpunks voorstonden. Deze cryptograaf was niet bezig met een digitaal cashsysteem om digitale zwarte markten te faciliteren en hij had geen verlangen om mensen te helpen regeringen omver te werpen door middel van massale belastingontduiking. Chaum vond privacy noodzakelijk om de democratie te redden - niet om ervan af te komen. Hoewel niet alle Cypherpunks May’s meer radicale visie deelden, gaf Chaum de voorkeur aan geen enkele associatie met hun beweging en hij heeft zich nooit aangesloten bij hun mailinglijst.

Intussen waren ook niet alle Cypherpunks zonder meer tevreden met Chaum en zijn werk.

Hughes had natuurlijk besloten om DigiCash te verlaten na slechts enkele weken bij het bedrijf; zijn teleurstelling in Chaum’s zakelijke strategie diende uiteindelijk als motivatie om de Cypherpunk-beweging op te richten. In de daaropvolgende jaren bewees Hughes zich op de mailinglijst van de Cypherpunks als een consequente en soms harde criticus van zijn voormalige werkgever: hij bekritiseerde regelmatig de voortdurende focus van de startup op hardwareproducten.

De hoop van de Cypherpunks dat Chaum zijn belofte van digitaal geld zou waarmaken, brokkelde verder af toen men ontdekte dat eCash werd ontworpen zonder sterke privacygaranties voor verkopers (ontvangers van eCash transacties). Hoewel het elektronische geldsysteem van DigiCash robuuste privacy bood voor kopers (zenders van transacties), kon de echte identiteit van een eCash-ontvanger worden onthuld als de zender en de bank samenwerkten om dit te doen. Kortom, de zender zou de onbeschermde digitale contanten met de bank moeten delen, zodat wanneer de ontvanger de eCash-notities stortte, de bank dit kon koppelen aan de echte naam gekoppeld aan de rekening van de ontvanger.

Tot de verbazing van veel Cypherpunks, beschouwde Chaum dit als een aantrekkelijke functie. Chaum, de CEO van DigiCash, redeneerde dat door de optie om ontvangers te deanoniemiseren, eCash minder snel gebruikt zou kunnen worden voor afpersing, ontvoering of andere verontrustende criminele activiteiten. Dit zou daarnaast waarschijnlijk het digitale geldsysteem aantrekkelijker maken voor banken en andere financiële instellingen, en met name voor de toezichthouders die toezicht houden op deze instellingen.

### Privacy zonder compromissen

Voor de meeste Cypherpunks was het compromis over de anonimiteit van de verkoper in eCash een grote teleurstelling.

Hun voornaamste doel was om de bestaande privacy die contant geld al bood te behouden. Dit omvatte anonimiteit aan beide zijden van een transactie: bij het wisselen van een dollarbiljet onthullen noch kopers, noch verkopers hun persoonlijke gegevens. Bovendien vereiste May’s crypto-anarchistische visie volledige anonimiteit van zowel kopers als verkopers: niemand zou gestolen legerdocumenten te koop aanbieden op een BlackNet als het voor de koper heel eenvoudig was om hun echte naam te achterhalen.

De meeste Cypherpunks hadden daarom geen enkele wens of intentie om compromissen te sluiten op het gebied van privacy om elektronische geldtechnologie minder aantrekkelijk te maken voor criminelen. Ook waren ze niet geïnteresseerd in het ontwerpen van softwaretools om digitaal geld acceptabeler te maken voor regelgevers: overheden werden zelf beschouwd als de grootste mogelijke bedreiging voor hun privacy, zeker in de dystopische toekomst die ze probeerden te voorkomen. Ze waren ervan overtuigd dat elke zwakheid in privacy-systemen misbruikt zou worden.

“Ieder systeem dat de overheid in staat stelt om een transactie te traceren, of om een bericht te traceren, of om toegang te krijgen tot sleutels, gooit in feite de vrijheid bevorderende voordelen van cryptografie volledig weg,” betoogde May op de mailinglijst. “Vraag jezelf eens af of de regering van Myanmar, bekend als SLORC, haar ‘Overheidstoegang tot Sleutels’ niet zou gebruiken om de dissidenten in de jungle op te pakken. Zouden Hitler en Himmler ‘sleutelherstel’ hebben gebruikt om te achterhalen met wie de Joden communiceerden zodat ze allemaal konden worden opgepakt en vermoord? Zou de Oost-Duitse Stasi e-cash transacties hebben getraceerd? Voor elke regering op de planeet […] kan men makkelijk tientallen voorbeelden bedenken waar toegang tot sleutels, toegang tot dagboeken, toegang tot uitgavenrecords, etc., zou worden misbruikt.”[^164]

En hoewel het waar is dat afpersers, ontvoerders en andere criminelen ook zouden profiteren van een volledig anoniem betalingssysteem, geloofde May niet dat de soorten privacycompromissen die Chaum nastreefde ook maar iets realistisch konden oplossen. Hij merkte op dat de situatie waarin een ontvoerder wordt gepakt omdat zijn identiteit wordt onthuld door samenwerking tussen de betaler en de bank waarschijnlijk nooit echt zou voorkomen; omdat de ontvoerder in eerste instantie dit systeem met aangetaste privacyfuncties niet zou gebruiken.

Eerder zou, zolang er ergens in de wereld een privé-betaaloplossing bestond, de kans groot zijn dat ontvoerders zouden eisen dat het geld gewoon via dat systeem naar hen wordt verzonden… en er zou waarschijnlijk altijd wel ergens een privé-betaaloplossing bestaan.

“Het kan een fysieke bank zijn, à la de Bank van Albanië, of het kan een ondergronds betalingssysteem zijn, à la de maffia, de Tongs, de Triades, of wat dan ook,” suggereerde May. “Helaas voor [financiële toezichthouders], en jammer genoeg voor de slachtoffers van dergelijke misdaden, lijkt een wereldwijde stopzetting van al dergelijke systemen niet mogelijk, zelfs met draconische politiestaatsmaatregelen. Er zijn gewoon te veel tussenruimtes waarin de bits zich kunnen verstoppen. En er is te veel economische prikkel voor sommige personen of banken om dergelijke fondsoverdrachtmethoden aan te bieden.”[^165]

Chaum had, door middel van eCash, mede vorm gegeven aan hoe May en zijn collega privacy-activisten dachten over online privacy en elektronische betalingen. Maar een paar jaar na het starten van zijn digitale geldproject, maakte deze baanbrekende cryptograaf fundamenteel andere afwegingen dan de meeste van de Cypherpunks.

Teleurgesteld schreef May naar de Cypherpunks mailinglijst:

“Als het gaat om volledig ontraceerbaar digitaal geld - het echte e-geld - dan zijn wij misschien wel de vaandeldragers hiervan.”[^166]

### Octrooien

Sommige van de Cypherpunks kwamen met oplossingen om een eCash-achtig systeem te creëren met volledige privacy voor zowel kopers als verkopers.

Zooko stelde bijvoorbeeld dat het probleem makkelijk opgelost kon worden als gebruikers pseudonieme bankrekeningen mochten hebben: banken kunnen een eCash-betaling niet aan een echte identiteit koppelen als ze de echte identiteit van hun rekeninghouders überhaupt niet kennen. (De Cypherpunks spraken soms over offshore bankieren in deze context.)

Nick Szabo stelde een andere aanpak voor. Verkopers zouden misschien de eCash die ze hebben ontvangen kunnen ruilen met de eCash van een ander persoon, en dan deze ‘nieuwe’ eCash naar de bank sturen. Op deze manier zou de oorspronkelijke betaling niet gelinkt kunnen worden aan de echte identiteit van de ontvanger. Natuurlijk, dit zou wel vertrouwen vergen in de persoon die de eCash uitwisselt. De uitwisselaar zou immers nog steeds kunnen samenwerken met de bank om de identiteit van de eCash-ontvanger te onthullen, of zelfs de eCash kunnen stelen door halverwege de transactie af te haak.

Een derde optie werd voorgesteld door een anonieme deelnemer aan de mailinglijst die een plan bedacht waarbij de verkoper betrokken was bij de aanvankelijke creatie van de eCash. In het originele eCash-protocol zijn alleen de koper en de bank betrokken bij de generatie van blinde sleutels en blinde handtekeningen. Echter, in dit protocol zou ook de uiteindelijke ontvanger van de elektronische valuta een laag van versleuteling toevoegen.

Maar voor al deze oplossingen was er één groot probleem: David Chaum bezat het patent op het algoritme voor de blindhandtekening. En de Cypherpunks waren van mening dat hij zijn product alleen zou licenseren aan “respectabele” organisaties die zijn technologie, naar zijn mening, niet in diskrediet zouden brengen. Het spreekt voor zich dat de Cypherpunks concludeerden dat hij het niet aan hun gevarieerde groep van crypto-anarchisten en privacyfundamentalisten zou licenseren. [^167]

Deze realiteit was een bron van frustratie voor de Cypherpunks, wellicht het best verwoord in een uitgebreide post op een mailinglijst door Tim May. Door zowel de hacker-ethiek als de Extropian-filosofie te belichamen, betoogde de medeoprichter van de groep dat technologische vooruitgang het best werd bereikt door experimenteren en concurrentie. Hij bepleitte dat softwarepatenten beide belemmerden.

Fysieke producten, zelfs als ze gepatenteerd zijn, kunnen tenminste naar wens van de koper gebruikt worden na aankoop, merkte May op. Bijvoorbeeld, gepatenteerde microchips werden in de jaren ’80 vrijelijk gebruikt door onafhankelijke technologen om hun eigen computers te bouwen, wat de revolutie van de persoonlijke computer in gang zette. In vergelijking daarmee leggen softwarelicentieregelingen allerlei beperkingen op hoe de software gebruikt kan worden, zelfs nadat deze is aangeschaft, wat effectief verdere innovatie doodt.

“[…] het punt van zorg is dat de patenten op de software-ideeën en -concepten betekenen dat experimenteerders, ontwikkelaars, en hackers geen licentie kunnen kopen voor digicash op dezelfde manier als ze zouden doen voor sommige IC’s; en vervolgens experimenteren, ontwikkelen en hacken,” legde May uit. “De man in de garage die probeert een ‘digitale postzegel’ te ontwikkelen, kan bijvoorbeeld de Chaumiaanse verblindingsprotocollen niet gebruiken zonder advocaten in te huren, Chaum zijn voorafgaande vergoeding te betalen, en zijn ontwerpen en bedrijfsplannen (die hij waarschijnlijk zelfs niet heeft!) te openbaren.”[^168]

Hierdoor verwachtte May dat de ontwikkeling van digitaal geld tot stilstand zou komen.

Hoewel David Chaum ongetwijfeld een pionier was op dit gebied, begonnen de Cypherpunks de cryptograaf steeds meer te zien als iemand die de toekomst van het elektronisch geld eerder hinderde dan bevorderde.

### Alternatieven

Als de Cypherpunks het eCash protocol wilden verbeteren, moesten ze daarvoor nog een decennium wachten tot de patenten van Chaum verlopen waren - en dat leek een eeuwigheid. Tim May, Eric Hughes en John Gilmore hadden de Cypherpunk beweging juist opgezet omdat ze al gefrustreerd waren door de gebrek aan voortgang in de cryptografie, en dat al ruim tien jaar na de publicatie van Chaum’s eerste digitale geld papers.

Het was tijd voor een elektronische vorm van geld, en de Cypherpunks schrijven code; ze zouden een manier moeten vinden om de patenten heen te werken.

Een manier om dit te doen was door naar alternatieven te zoeken. Chaum’s voorstellen uit de jaren 80 hadden het begin gemarkeerd van een reeks publicaties in de jaren 90: binnen enkele jaren werden ongeveer 200 papers gepubliceerd over het onderwerp elektronisch geld en werden enkele tientallen nieuwe patenten ingediend. [^169] Als een van de meer opvallende voorbeelden ontwierpen Ron Rivest en Adi Shamir (bekend van RSA) in 1996 twee micropayment-schema’s genaamd PayWord en MicroMint, terwijl in datzelfde jaar de NSA ook een elektronisch geldschema zou presenteren. [^170]

Van tijd tot tijd stelden diverse Cypherpunks ook alternatieve ontwerpen voor elektronisch geld voor op de mailinglijst. Als een vroeg - en nogal origineel - voorbeeld heeft de informatica student Hadon Nash een digitaal valutaschema gepresenteerd dat hij “Digital Gold” noemde. In zijn bericht beschreef Nash een systeem waarbij gebruikers “eigenaar” zouden zijn van getallen; om het even welk getal, maar lagere getallen zouden een lagere waarde hebben. Een getal claimen was net zo simpel als het produceren van een cryptografische handtekening met dat getal, en de eerste persoon die het claimde zou het “bezitten”. Het overdragen van het eigendom van een getal werd gedaan met een bericht dat de nieuwe eigenaar bevatte, alleen geïdentificeerd met een openbare sleutel, en een cryptografische handtekening die aantoonde dat de oorspronkelijke eigenaar de overdracht goedkeurde. De eigendomsgeschiedenis van elk getal kon dan worden gevolgd door een reeks cryptografische handtekeningen.[^171]

De meeste ontwerpen voor elektronisch geld introduceerden echter niets baanbrekends. Als het over privacyfuncties gaat, waren er veel, waaronder het door de NSA voorgestelde schema, die slechts variaties waren op of iteraties van het ontwerp van Chaum. En degenen die wel een vernieuwende aanpak introduceerden, hadden vaak andere fundamentele beperkingen. Zo konden de elektronische geldschema’s van Rivest en Shamir bijvoorbeeld alleen echt nuttig zijn voor tamelijk specifieke soorten betalingen van een lage waarde, omdat de geldigheid van de valuta-eenheden snel zou verlopen.

Andere ideeën waren op een fundamenteler niveau gebrekkig - zoals Nash’s ‘Digital Gold’-oplossing, die geen rekening hield met het probleem van dubbel uitgeven. Zoals Hal Finney op de Cypherpunks mailinglijst aangaf, als hetzelfde nummer werd overgedragen aan meerdere publieke sleutels, zouden verschillende gebruikers kunnen eindigen met uiteenlopende eigendomsregistraties. (Nash stelde wel een systeem voor waarin gebruikers bij ‘agentschappen’ zouden moeten controleren of een munt door hen zou worden geaccepteerd voordat ze deze zelf accepteerden - wat zou bewijzen dat het nummer niet dubbel werd uitgegeven - maar dit deel van het voorstel was niet erg goed uitgewerkt.)

“Ik moet echter wel zeggen,” schreef Finney, “dat ondanks het feit dat ik niet echt denk dat het voorstel voor digitaal goud technisch haalbaar is, het idee om eigenaar te zijn van getallen enorm brutaal is en behoorlijk creatief.”[^172]

### De Experimenten

Omdat er niet veel veelbelovende alternatieven leken te zijn, was een populaire methode om Chaum’s patenten te omzeilen dus om onder de radar te blijven.

Verschillende Cypherpunks zouden uiteindelijk hun eigen versies van eCash implementeren, maar om rechtszaken te voorkomen, waren deze digitale geldsystemen alleen bedoeld voor testdoeleinden. Ze gingen ervan uit dat hun experimentele projecten getolereerd zouden worden, zolang ze geen commerciële intenties hadden en niet gebruikt zouden worden om echte waarde over te dragen.

Midden 1994 vertegenwoordigden de speelgeldschema’s een kleine trend onder de Cypherpunks. Bijvoorbeeld, Matt Thomlinson, een bijdrager aan de mailinglijst, lanceerde een implementatie van eCash die hij Ghostmarks noemde. Tegelijkertijd lanceerde Pr0duct Cypher, een pseudonieme individu die ook bijdroeg aan PGP, Magic Money. En Mike Duvos, een andere reguliere op de mailinglijst, beheerde een Magic Money implementatie die hij Tacky Tokens noemde.

Bovendien presenteerde iemand die zichzelf Black Unicorn noemt, zelfs het “volledig gesteunde” DigiFrancs systeem:

“DigiFrancs worden ondersteund door 10 kratten Diet Coke, die zich bevinden in de ‘kluis’ reserves van UniBank in Washington, DC. DigiFrancs kunnen worden ingeruild voor hun equivalent in ongekoelde, 16 oz Diet Coke blikjes op aanvraag, en vrij aan boord in Washington, DC. Deze regeling impliceert geen overeenkomst tussen enige van de partijen en de Coca-Cola maatschappij.”[^173]

Hoewel dit uiteraard bedoeld was als een grap - zelfs de door Diet Coke ondersteunde DigiFrancs waren niet daadwerkelijk bedoeld om als geld te worden gebruikt - kregen de verschillende soorten elektronisch geld toch enige bekendheid als ruilmiddel. Sommige Cypherpunks accepteerden deze speelvaluta’s in ruil voor digitale snuisterijen zoals GIFs.

Inderdaad, het waren niet bepaald grote waardeoverdrachten, maar het riep wel een interessante vraag op.

“Nu, als je nog wakker bent, komt het leuke deel,” kondigde Pr0duct Cypher aan, nadat hij de technische details van Magic Money op de mailinglijst had uitgelegd, “Hoe introduceer je echte waarde in je digicash systeem? Hoe krijg je mensen eigenlijk zover dat ze het willen proberen?”

Chaum wilde zijn eCash-systeem implementeren via bestaande financiële instellingen, waar digitale geld-eenheden inwisselbaar zouden zijn voor echte dollars (of andere fiatvaluta). eCash zou in feite gedekt worden door geld op de bank, wat — hopelijk — mensen gerust genoeg zou stellen om te beginnen met het accepteren van dit nieuwe type geld als betaling.

Maar Pr0duct Cypher stelde nu voor dat deze inlosbaarheid voor een dollar misschien niet echt nodig was. Misschien, speculeerde hij, zou digitaal geld helemaal geen back-up nodig hebben.

“Wat maakt goud waardevol?” vroeg hij retorisch. “Het heeft enkele nuttige eigenschappen: het is een goede geleider, is bestand tegen corrosie en chemicaliën, enzovoorts. Maar die zijn pas recent van belang geworden. Waarom is goud al duizenden jaren waardevol? Het is mooi, het glanst, en het allerbelangrijkste, het is schaars.”

Pr0duct Cypher concludeerde:

“Jouw digigeld zou schaars moeten zijn.”[^174]

### Gedekt Digitaal Geld

Gedurende de volgende paar jaar, - de midden jaren negentig - kwamen onderwerpen als de aard van geld, waarde en valuta backing regelmatig ter sprake op de mailinglijst van de Cypherpunks. Het was logisch dat de Cypherpunks deze kwesties bespraken; om elektronisch geld te creëren, moesten ze begrijpen wat het eigenlijk waarde zou geven. Waarom zou iemand echte producten of diensten opgeven in ruil voor een nummer op een scherm?

Het bleek dat diverse leden van de lijst zeer uiteenlopende ideeën hierover hadden.

Sommigen beschouwden digitale contant geld echt niet als iets waardevols en dachten zelfs dat het een beetje ongepast was om er in monetaire termen over te praten. Software ontwikkelaar Perry Metzger, een van de actievere leden in discussies over digitale contant geld, beweerde bijvoorbeeld dat een term zoals “anonieme digitale bankcheques” in feite een nauwkeurigere beschrijving zou zijn.

“Hetzelfde geldt voor een cheque die kan worden GEBRUIKT voor geld, maar in feite een manier is om geld OVER TE DRAGEN, digicash is van zichzelf geen bron van waarde - het is een boekhoudsysteem voor iets dat waarde heeft,” schreef hij. “Dat iets kan dollars zijn, goud, cocainefutures gecontracteerd op de Bogota Commodity Exchange, padvinders koekjes, of alles wat mensen besluiten een goed ruilmiddel te zijn.”[^175]

Anderen, zoals Eric Hughes, hadden er geen probleem mee om digitale cash als een vorm van geld te beschouwen, maar waren het ermee eens dat de bits en bytes ondersteund moesten worden door iets van waarde; in de meeste gevallen zou een conventionele fiat-valuta zoals de dollar of het pond de voor de hand liggende keuze zijn. Hij geloofde dat voor de popularisatie van elektronisch geld, gebruikers de garantie moesten krijgen dat ze hun digitale geld kunnen inruilen voor een vastgesteld bedrag aan ‘echt’ geld.

Een andere visie kwam van Robert Hettinga, een Cypherpunk die (in zijn eigen woorden) ooit in “de kooi van Morgan Stanley in Chicago” werkte.[^176] Als een andere zeer actieve deelnemer in discussies over geld en elektronisch geld op de Cypherpunk mailinglijst, betoogde Hettinga dat de behoefte aan inwisselbaarheid voor “echt” geld na verloop van tijd zou verdwijnen, aangezien mensen langzaam het vertrouwen in de nieuwe digitale munteenheid zouden leren.

De vertaling in het Nederlands moet zijn: “Hij maakte een analogie met de evolutionaire biologie, hij schreef:”

“Vergeet niet dat de eerste vleugels geëvolueerd zijn door op vijvers scherende insecten zodat ze sneller over vijvers konden glijden. Na verloop van tijd, toen die beginnende vleugels uiteindelijk volledige vleugels werden, hadden de vliegende insecten geen vijvers meer nodig. Met dat idee in gedachten, zullen digitale waardepapieren voorlopig nog moeten interfacen met de wereld van fysieke boekhouding, om te kunnen worden omgezet in andere activa.”

Maar, zo voorspelde Hettinga: “Uiteindelijk zullen die activa op een gegeven moment niet langer boekvermeldingen zijn.”[^177]

Ondertussen geloofde Tim May niet dat geld in de eerste plaats gedekt hoefde te zijn. In lijn met het vooruitziende principe van vrijbankieren van Hayek, stelde hij dat het uiteindelijk allemaal neerkwam op toekomstige verwachtingen: mensen hadden slechts vertrouwen nodig dat geld zijn koopkracht zou behouden.

“Ik geloof dat …le…ormen van geld, of het nu harde valuta of fiat is, voortkomen uit de verwachting dat het geld in de toekomst ongeveer dezelfde waarde zal hebben,” schreef hij. “Noem het de ‘grotere dwaas theorie van geld.’ Alles wat je belangrijk vindt, is dat een grotere dwaas het geld zal aanvaarden.”[^178]

Echter, May zag elektronische valuta niet echt als geld op zich. Hij beschouwde het eerder als iets nieuws, een manier om geld over te maken van de ene bankrekening of opslagplaats naar de andere - eerder vergelijkbaar met checks of bankoverschrijvingen. Hoewel hij dus niet geloofde dat digitale valuta op de traditionele manier ‘gedekt’ hoefde te worden, ging May er wel van uit dat banken of bankachtige instanties die valuta uitgeven, uiteindelijk controle zouden hebben over de daadwerkelijke munteenheid die onder het elektronisch geld ligt: “Wat digitale valuta echt ondersteunt, is de reputatie van de instanties.”[^179]

En toen was er een Britse Cypherpunk die dacht dat elektronisch geld helemaal niet gedekt hoefde te zijn…

### Adam Back

Adam Back, een postdoc in de informatica aan de Universiteit van Exeter en midden in de twintig, had nog nooit een face-to-face cypherpunk bijeenkomst bijgewoond. Echter, hij had de mailinglijst online gevonden. Hij raakte bijzonder geïnteresseerd in elektronisch geld en werd snel een van de meest actieve deelnemers in de discussies over dit onderwerp.

Back had zelf een beetje geëxperimenteerd met CyberBucks en had uit eerste hand ervaren dat mensen waarde konden toekennen aan puur digitale, ongedekte munten. CyberBucks, gebaseerd op niet veel meer dan een belofte over het totale aanbod, werden verhandeld voor echt geld en gebruikt in echte handel, zelfs als het slechts in een kleine niche in een obscure hoek van het internet was.

Hoewel CyberBucks op het moment dat de server van DigiCash offline ging direct waardeloos werd, zag Back geen enkele reden waarom een nieuw en beter elektronisch geldsysteem geen waarde zou kunnen krijgen op dezelfde manier - en het zelfs beter zou kunnen doen.

“Waarom koppel je je ecash systeem niet los van US dollars door credit cards/ debit cards/ cheques / cash, en zet je een volledig op zichzelf staand systeem op?” stelde hij voor op de Cypherpunks mailinglijst in april 1997.[^180]

“Wat we willen, is volledig anonieme eenheden van uitwisseling, met ultra lage transactiekosten en overdraagbaarheid. Als we dat voor elkaar krijgen […] dan zullen de banken verworden tot de verouderde [dinosaurussen] die ze verdienen te zijn,” voegde Back een paar dagen later toe in een vervolg-email. “Ik denk dat dit een goede uitkomst zou zijn, en ik zie dit liever gebeuren dan dat iemand veel moeite doet om de banken erbij te betrekken.”[^181]

Back geloofde dat, net als elk ander product dat op de vrije markt wordt verhandeld, de krachten van vraag en aanbod de waarde van digitale valuta zouden reguleren. Gebruikers zouden het kopen en verkopen voor traditionele valuta en het accepteren in ruil voor goederen en diensten. Zodra er een marktwaarde werd vastgesteld, kon deze elektronische valuta worden gebruikt om met een simpele muisklik waarde over het internet te verzenden. En wat vooral belangrijk was, je hoefde niet te maken te hebben met financiële instellingen.

Back voorspelde dat de waarde die mensen zouden hechten aan een niet-ondersteunde digitale valuta uiteindelijk afhing van de eigenschappen ervan. Een digitale valuta die anoniem gebruikt kan worden - net als contant geld - zou naar verwachting meer gewaardeerd worden dan een vergelijkbare digitale valuta die sporen nalaat van de uitgavenpatronen van gebruikers, bijvoorbeeld. Een digitale valuta die kan blijven bestaan, ongeacht het faillissement van een specifiek bedrijf, zou waarschijnlijk meer waard zijn dan een valuta die het risico loopt ’s nachts nutteloos te worden door het offline gaan van een enkele server. En zo verder.

Back presenteerde uiteindelijk een shortlist van zes wenselijke eigenschappen voor elektronisch geld[^182]:

1…noniem (privacy behoudend, zowel ontvanger als betaler blijven onbekend)

Vertaal deze tekst naar het Nederlands. Voeg niets toe, en laat niets weg uit de vertaling. Wees accuraat en zorg ervoor dat de vertaling de juiste betekenis behoudt. Herformuleer de vertaling vervolgens in jouw eigen woorden, zodat het natuurlijker klinkt in het Nederlands. Je mag enige vrijheid nemen in het aanpassen van de grammatica en zinsbouw. Vermijd passieve zinsconstructies. Splits te lange zinnen op in aparte zinnen. Let op spelling en leestekens. Lokaliseer culturele uitdrukkingen of verwijzingen zodat ze nauwer aansluiten bij het Nederlands. Geef alleen de definitieve versie en behoud voetnoten. De tekst om te vertalen is: 2)   gedistribueerd (om het moeilijk te maken om het af te sluiten)

Vertaling: 3) hebben enige ingebouwde schaarste

Sorry, maar er is geen tekst gegeven om te vertalen naar het Nederlands. Kunt u de tekst geven die vertaald moet worden?

5)   bij voorkeur offline (moeilijk te realiseren met alleen software)

Het lijkt erop dat de tekst om te vertalen niet volledig is. Het enige woord dat gegeven is, is “reusable”. In het Nederlands kan dit worden vertaald als “herbruikbaar”.

Elk systeem dat deze zes eigenschappen kon bieden, zou echte waarde aantrekken, voorzag Back, en zou zo een echte, niet-ondersteunde, digitale munteenheid worden.

Het klonk misschien simpel genoeg, hoewel de postdoctorale onderzoeker in de informatica wist dat het dat zeker niet was. Sommige eigenschappen waren lastig te realiseren, zelfs in de meest algemene informatica context, terwijl het integreren daarvan in een digitaal valutasysteem hoogstwaarschijnlijk aanzienlijk moeilijker zou zijn. Het succesvol combineren van alle zes in één systeem zou nog veel moeilijker zijn.

Desalniettemin, in echte Cypherpunk-stijl, praatte Adam Back niet alleen over elektronisch geld.

Het lijkt erop dat de tekst die je wilt laten vertalen ontbreekt. Zou je de Engelse tekst die je wilt laten vertalen kunnen toevoegen? Ik help je graag verder.

## Hoofdstuk 10: Hashcash

Opgegroeid in de East Midlands van Engeland had Adam Back op dertienjarige leeftijd genoeg gespaard om de populaire Sinclair ZX81 thuiscomputer te kopen. Dit apparaat, dat voor het eerst uitkwam in januari 1981, was ongeveer de omvang van een faxmachine, had een ingebouwd toetsenbord en kon worden aangesloten op de televisie van het gezin. Hierdoor kon de jongen de 8-bit wonderen van dit apparaat ontdekken, gewoon in het comfort van zijn eigen woonkamer.

Toen hij na schooltijd met de computer speelde - naast daadwerkelijke videogames soms gewoon door berekeningen te maken om een bepaald effect te bereiken dat hij interessant vond - raakte de jonge Adam Back gefascineerd door de mogelijkheden van de computerwereld.

En hij had er een talent voor, ook. Omdat er geen native assembler beschikbaar was om mens-leesbare broncode om te zetten naar machine-leesbare binaire code (enen en nullen), bedacht de jongen hoe hij zelf een assembler kon coderen voor de ZX81. Dit vereiste van hem dat hij de meest basale interne werking van de computer reverse-engineerde, waarbij hij zelfs binaire codering moest terugvertalen naar broncode om te begrijpen hoe andere programma’s werkten.

Toen Back naar de universiteit ging op ongeveer zestienjarige leeftijd, had hij al een geavanceerd begrip van de werking van computers en hij wist dat hij deze discipline wilde blijven verkennen. Hoewel informatica op dat moment geen officieel vak was op zijn school, was er wel een computerlab op de campus. Back maakte dankbaar gebruik van deze faciliteit en besteedde vaak lange dagen in het lab om zelfstandig meer geavanceerde programmeertalen te leren.

Na het college ging Back computerwetenschappen studeren aan de Universiteit van Exeter, gelegen in het zuidwesten van Engeland. Tijdens zijn studie raakte hij bijzonder geïnteresseerd in gedistribueerd computergebruik, waarbij meerdere computers via een netwerk samenwerken aan hetzelfde probleem, meestal door het probleem op te delen in kleinere delen (“parallelle computing”).

Gedreven door zijn verlangen om het curriculum te beheersen, scoorde Back gedurende zijn drie jaar als bachelorstudent regelmatig het hoogst in zijn klas. Dit zette hem begin jaren ’90 in een positie waardoor hij zijn interesse diepgaand kon nastreven. Op eenentwintigjarige leeftijd stond de Universiteit van Exeter het Back toe om zijn Master over te slaan, en accepteerde ze hem direct in een PhD-programma gefocust op gedistribueerd computergebruik. Gedurende de volgende vier jaar zou hij verschillende coördinatiemethoden voor netwerkcomputers bestuderen - en de mogelijke foutmodi ervan.

Hier werd Back geconfronteerd met langlopende uitdagingen in gedistribueerd computergebruik, zoals het Byzantijnse Generaalsprobleem, waarmee computerwetenschappers al worstelden sinds de late jaren ’70. De kern van dit probleem was dat coördinatie over meerdere computers lastig kon zijn op open netwerken, waar kwaadwillende (of zelfs per ongeluk onbetrouwbare) knooppunten zich konden aansluiten en de pogingen van eerlijke deelnemers om een consensus te bereiken konden frustreren.

Het klassieke metaforische verhaal, voor het eerst beschreven door computergoeroe Leslie Lamport, ging over een groep (inderdaad) Byzantijnse generaals die een stad omsingelden.[^183] Terwijl elk van hen de situatie inschatte, zouden ze via boodschappers communiceren om te coördineren of ze zouden aanvallen of zich terugtrekken. Hoewel beide opties acceptabel zouden zijn, zouden ze allemaal moeten overeenkomen met de gekozen optie; het zou een ramp zijn als sommige generaals zouden aanvallen, terwijl anderen besluiten zich terug te trekken.

Het probleem is echter dat er ook verraderlijke generaals (en/of boodschappers, afhankelijk van de versie van de allegorie) zijn, die tegenstrijdige boodschappen - “aanval” of “terugtrekken” - aan verschillende generaals zouden kunnen zenden, wat tot onenigheid kan leiden. Omdat directe communicatie tussen verschillende partijen onmogelijk is, zouden sommigen eerst de ene instructie (“aanval”) te zien krijgen, terwijl anderen aanvankelijk de andere instructie (“terugtrekken”) zouden zien.

De uitdaging was dus om een protocol te ontwerpen dat elke eerlijke deelnemer onafhankelijk zou kunnen volgen, zodat ze allemaal tot dezelfde conclusie zouden komen. Of dit nu de beslissing was om een stad wel of niet aan te vallen, of om consensus te bereiken over hoe een gedeelde computertaak te coördineren.

Dit waren precies het soort uitdagingen waar Adam Back graag zijn hersens over kraakte.

### “De Cypherpunk”

Als PhD-kandidaat kwam Back in contact met een masterstudent aan dezelfde universiteit die probeerde het RSA-encryptieprotocol te optimaliseren voor parallelle rekenen. Dit leek Back een interessant project, en het lag dicht bij zijn eigen onderzoeksgebied, dus hij besloot om te helpen. Dit betekende dat hij zich moest verdiepen in het RSA-algoritme, wat hem op zijn beurt ook leidde naar het bestuderen van Phil Zimmermann’s nieuwe PGP-project.

Inmiddels had Back ook een interesse in vrije markten ontwikkeld, en hij stond sympathiek tegenover anarcho-kapitalisme. De hyperlibertaire ideologie waarin alle functies van de staat volledig worden vervangen door op de markt gebaseerde oplossingen leek op de toekomstige samenleving beschreven in een van zijn favoriete boeken: de cyberpunk-klassieker Snow Crash.

Zo vond Back de cryptografische hulpmiddelen waar hij over leerde op een sociologisch niveau zeer interessant.

“Minder privacy is negatief voor de vrije markteconomie, omdat een afname van privacy leidt tot een toename van overheidsinterventies, grotere overheidsapparaten, fascisme, etc. waardoor de vrije markteconomie naar de knoppen gaat”, zou hij later verklaren. “Hierdoor zullen armoede en voedseltekorten ontstaan, vergelijkbaar met wat er gebeurde in de voormalige USSR, die nog steeds langzaam herstelt van de ondergang die veroorzaakt werd door fascistische overheidsbeleid.”

Daarnaast realiseerde de afgestudeerde student zich snel dat dit soort technologieën individuen de middelen kunnen bieden om fundamentele rechten uit te oefenen zoals vrijheid van meningsuiting en vrijheid van vergadering. In wezen ontdekte Back dat cryptografie aanzienlijke implicaties kon hebben voor het evenwicht van macht tussen individuen en de staat.

Toen hij op het internet naar plaatsen zocht om deze soorten onderwerpen te bespreken, ontdekte de jonge PhD-kandidaat uit Exeter dat hij niet de enige was die tot dit inzicht was gekomen.

Halverwege de wereld hadden de Cypherpunks net hun reguliere bijeenkomsten georganiseerd en - nog belangrijker - de Cypherpunks mailinglijst gelanceerd. Al op jonge leeftijd programmeur, was Back erg geïnspireerd door hun doel om software te schrijven die een positieve sociale impact heeft en hij meldde zich snel aan voor de mailinglijst.

“Dat was een interessante uitlaatklep”, herinnerde Back zich later aan zijn eerste interacties met de Cypherpunks mailinglijst, “want mensen waren bezig met andere dingen dan PGP, andere dingen die je kon bouwen met encryptie en cryptografie. Ik heb een groot deel van mijn doctoraat eigenlijk niet besteed aan werken aan gedistribueerde systemen, maar aan leren over cryptografie protocollen, voornamelijk met als toegepaste interesse om te denken over wat een bepaald cryptografie artikel je zou toestaan om te bouwen.”[^185]

Gedurende de jaren werd Back een van de meest actieve deelnemers aan deze lijst, soms droeg hij zelfs tientallen e-mails bij in een enkele maand. Hij had een sterke interesse in filosofische onderwerpen zoals privacy, vrije meningsuiting en libertarisme, en hij nam deel aan diepgaande technische discussies over onderwerpen zoals anonieme remailers of versleutelde bestandssystemen - technologieën waaraan hij ook heeft bijgedragen.

Back raakte ook betrokken bij de ‘crypto-oorlogen’ die niet al te lang na zijn toetreding tot de mailinglijst uitbraken, en werd op veel manieren zeer direct beïnvloed door deze strijd. Toen de Amerikaanse overheid cryptografie reguleerde onder de US Munitions List, was het Amerikanen wettelijk niet langer toegestaan om, bijvoorbeeld, het RSA-algoritme te delen met Back, of met een van zijn landgenoten. (In het geval van RSA kende Back natuurlijk al het algoritme.)

Het verbod raakte een gevoelige snaar bij de pas ontdekte Cypherpunk. Hij was van mening dat de betwiste cryptografische protocollen in werkelijkheid individuen alleen maar toestonden om de rechten uit te oefenen die zij juridisch gezien al moesten hebben: als privégesprekken zijn toegestaan, waarom zou public key cryptografie dan niet toegestaan zijn? En wellicht nog belangrijker, cryptografie was in feite gewoon wiskunde. Back vond het zowel absurd als zorgwekkend dat de VS in feite het delen van bepaalde getallen en vergelijkingen illegaal maakten.

Dit inspiratie leidde de Britse Cypherpunk ertoe om op een unieke manier zijn punt te bewijzen. Volgens de activistische ethos van de groep, maakte Back “munitie” shirts: zwarte t-shirts met het RSA-protocol erop gedrukt in witte letters. Volgens de wet was iedereen die Back’s kleding droeg tijdens het overschrijden van de grens om de Verenigde Staten te verlaten, technisch gezien een wapenexporteur. Hij zou de shirts verkopen aan zijn mede-Cypherpunks en, passend, DigiCash’s proefvaluta CyberBucks als betaling accepteren.

Passend genoeg, want mogelijk meer dan wat dan ook, was Adam Back bijzonder geïnteresseerd in elektronisch geld.

### In Actie Komen

Toen Adam Back zich aansloot bij de mailinglijst van de Cypherpunks, was DigiCash werkelijk het enige spel in de stad als het gaat om anonieme digitale valuta. Maar de voortgang op eCash verliep minder snel dan hij en vele anderen hadden gewenst.

Terug deelde de beoordeling van de Cypherpunks dat dit grotendeels kwam omdat David Chaum zijn patenten gebruikte om zijn technologie exclusief te houden. Hij vond dat het beleid van DigiCash, met zijn ingewikkelde licentieschema’s en beperkingen op wat gebruikers wel en niet met de eCash-technologie konden doen, ervoor zorgde dat hackers en knutselaars geen kans kregen om met de technologie te experimenteren en deze te verbeteren. Door dit beleid was de technische vooruitgang vrijwel tot stilstand gekomen.

Samenvattend verpersoonlijkte Back de Cypherpunk-filosofie. Echter, hij was niet het type dat rustig zou afwachten tot de zaken veranderden.

In de hoop dat het de zaken zou versnellen, schreef Back initieel softwarebibliotheken (broncode die door andere ontwikkelaars kon worden gebruikt) voor zowel eCash als Brands Cash. Laatstgenoemde is een op eCash geïnspireerd elektronisch geldsysteem ontworpen door voormalig DigiCash-medewerker Stefan Brands. Terwijl hij hiermee bezig was, ontdekte Back ook hoe hij Brands’s systeem kon uitbreiden om offline transacties te vergemakkelijken, zonder de noodzaak om bij elke betaling te controleren op dubbele uitgaven bij de bank. (Hoewel toen Back zijn oplossing met Brands besprak, bleek dat iemand anders dat probleem al eerder had opgelost.)

Toen eCash in het midden van de jaren 90 nog steeds niet echt van de grond kwam, begon Adam Back echter nogal ongeduldig te worden.

“Technologie voor blinde handtekeningen bestaat al geruime tijd, maar er is niet één online geval van een praktisch, echt wereldwijd gebruik van deze technologie,” schreef Back gefrustreerd naar de Cypherpunks mailinglijst in oktober 1995.[^186]

Hij merkte op dat niet-anonieme internetbetaalsystemen snel marktaandeel veroverden, wat betekende dat de toekomst van digitale transacties een gevaarlijke richting insloeg. Als eenmaal deze privacy-schendende alternatieven zich zouden verankeren in de gewoonten van mensen als hun standaard online betalingsoplossingen, geloofde hij dat het aanzienlijk moeilijker zou zijn om internetgebruikers over te laten stappen naar anoniem digitaal geld.

Het was tijd om actie te ondernemen. Aangezien Back niet veel vertrouwen had in de voortgang van DigiCash, en het leek alsof niemand anders werkte aan haalbare alternatieven voor eCash, concludeerde hij dat de snelste weg naar succes misschien wel was om samen te werken met Chaum. Hij stelde voor dat een groep Cypherpunks een start-up bank zou oprichten en eigenlijk de technologie van DigiCash zou licentiëren om zelf door fiatgeld gedekte eCash uit te geven.

“Ik meen het serieus en zou erin willen investeren,” maakte Back duidelijk op de Cypherpunks mailinglijst. “Wat denken jullie ervan? De eerste DigiCash-bank, ‘gerund’ en eigendom van een groep cypherpunks?”[^187]

De enige persoon die reageerde op zijn voorstel wees erop dat dit plan waarschijnlijk ook niet zou werken: tenslotte wilde Chaum zijn technologie niet in licentie geven aan een bende Cypherpunks.[^188] Het idee stierf een stille dood.

Twee jaar later, in de zomer van 1997, kwam Back terug naar de lijst om het idee van een gedistribueerde bank voor te stellen. Nu hij met succes zijn doctoraatsprogramma had afgerond en als postdoc-onderzoeker aan de universiteit werkte, maakte hij deze keer echt gebruik van zijn expertisegebied. Hij legde uit dat de operaties van een bank over een netwerk van verschillende mensen of entiteiten verspreid konden worden. Ze zouden in staat zijn om een virtuele computer te simuleren door berichten uit te wisselen en gecodeerde functies te berekenen, opperde Back, waarbij de virtuele computer in feite zou functioneren als een reguliere bank.

Door de bank op te splitsen in meerdere onderling afhankelijke partijen, zou er geen enkele entiteit volledig vertrouwd hoeven te worden met de bankoperaties. En hoewel het Byzantijnse Generaalsprobleem nog steeds niet volledig was opgelost, kon het systeem alleen worden misleid als een bepaald aantal deelnemers samenspanden.

“De bank zou bestaan in het netwerk, in deze virtuele CPU,” schreef Back. “Individuele knooppunten kunnen komen en gaan, maar de beveiligde software-entiteit, die de bank en de accountinformatie is, zou blijven voortbestaan.”[^189]

Hij kreeg geen antwoord op zijn e-mail.

### Spam

In de tweede helft van de jaren ’90 moest elke e-mailservice op het internet omgaan met ogenschijnlijk steeds toenemende hoeveelheden junkmail, of spam: ongevraagde berichten die in bulk werden verzonden, doorgaans door adverteerders. De Cypherpunks werden hierbij niet gespaard; promoties voor afslankpillen, producten voor penisvergroting en snelle geldverdienende schema’s veroorzaakten alsmaar meer vervuiling in de mailinglijst.

Het probleem was vooral ernstig voor de remailers. De anoniem makende diensten die door verschillende Cypherpunks werden beheerd, werden gemakkelijk en vaak misbruikt om spam te versturen. Sommige van de beheerders vermoedden zelfs dat hun remailers specifiek het doelwit waren van zogenoemde denial-of-service (DOS) aanvallen; het doel zou zijn geweest om de remailers te overladen met nutteloze e-mails om deze services onbruikbaar te maken voor legitiem gebruik.

Adam Back, die zelf ook een remailer beheerde, was lid van een groep Cypherpunks die zich toelegde op het oplossen van dit probleem. En nog belangrijker, ze probeerden dit probleem op te lossen zonder terug te vallen op oplossingen die internetgebruikers verplichtten zich te identificeren. Want voor remailers was privacy het belangrijkste punt.

Ze wilden ook niet afhankelijk zijn van wetten en regelgeving. Hoewel er stemmen opgingen om eenvoudigweg spam e-mails illegaal te maken, was het niet de manier van de cypherpunks om de overheid in te schakelen om hun problemen op te lossen.

Dit was ook belangrijk omdat het niet altijd duidelijk was wat precies als spam beschouwd kon worden. Als de staat de autoriteit krijgt om dat onderscheid te maken, zou dat effectief regeringen toestaan om te bepalen welke vormen van communicatie tussen internetgebruikers acceptabel zijn en welke niet. Dit zou de deur kunnen openen voor politiek gemotiveerde censuur, waarschuwden Cypherpunks zoals Tim May.[190]

Adam Back benadrukte dat om spammers wettelijk verantwoordelijk te kunnen houden, ze ook geïdentificeerd dienen te worden. Als een overheidsdienst tegen spam de taak krijgt om de daders te vangen, waarschuwde Back zijn mede-Cypherpunks, dan zouden remailers waarschijnlijk een groot doelwit worden, met mogelijk ernstige gevolgen voor de online privacy in het algemeen.[^191]

“De gevaren van de overheid inzetten om spammers aan te vallen, is dat dit het internet is, en we willen geen regulering van de inhoud door overheden, noch pogingen om ‘escrow van identiteit’, ‘internetrijbewijzen’ of iets anders af te dwingen,” schreef Back aan de Cypherpunk mailinglijst. “We kunnen ze zelf redden zonder de behoefte aan overheidsinterventie, hartelijk dank.”[^192]

De cypherpunks waren het er in het algemeen over eens dat een betere oplossing zou zijn om een digitaal equivalent van postzegels te creëren. Als het verzenden van een email kosten met zich mee zou brengen, zou dit spammers ontmoedigen, vooral omdat spammers meestal tienduizenden, zo niet miljoenen, ongewenste e-mails moeten versturen om winst te maken uit hun activiteiten. Op dezelfde manier vereiste het bombarderen van remailers massa’s ongewenste e-mails.

Digitale postzegels zouden op verschillende manieren kunnen functioneren. E-mail doorstuurders kunnen bijvoorbeeld postzegels in rekening brengen voor het doorsturen van e-mails. Dit zou niet alleen spamtelefoongesprekken ontmoedigen die via deze diensten worden verzonden, maar het zou ook, als leuk extraatje, een financiële prikkel introduceren om e-mail doorstuurders te runnen. Als alternatief, of daarnaast, zou postzegelvergoeding kunnen worden toegekend aan de ontvanger wiens e-mailsoftware geprogrammeerd kan worden om berichten met onvoldoende vergoeding af te wijzen.

De eigenlijke postzegel kon op verschillende manieren worden ontworpen, maar de meeste ideeën hielden een uitgever van elektronische zegels in. Deze uitgever zou bijvoorbeeld unieke grote getallen kunnen genereren en deze kunnen verkopen (wellicht voor digitaal geld). Het unieke nummer zou dan in een e-mail moeten worden opgenomen, en zodra een remailer of het e-mailprogramma van de ontvanger het bericht ontvangt, zou het bij de uitgever controleren of het nummer inderdaad een geldige postzegel is. Als dat zo is, kan de remailer of ontvanger misschien wat geld (digitaal geld?) terugkrijgen van de uitgever, afhankelijk van de specifieke ontwerpkenmerken van het systeem. Als de postzegel niet geldig was, zou de e-mail simpelweg terugstuiteren.

Een andere optie zou zijn om gewoon digitale contanten direct als postzegel te gebruiken. Een e-mail kan in dit geval een heel klein beetje digitale valuta bevatten in een speciaal veld, dat de beoogde ontvanger er dan kan uithalen. Er was een tijd waarin het leek alsof dit een goede toepassing voor eCash zou kunnen zijn.

Helaas bleek het in de praktijk ingewikkelder te zijn. Ten eerste waren de vroege uitgaven van eCash nog niet in staat om de zeer specifieke soorten overboekingen die nodig waren voor postzegels te verwerken. Bovendien zou het gebrek aan anonimiteit van de ontvanger in het elektronische contantsysteem van Chaum betekenen dat de verzender van een bericht kon worden (gedwongen om) samen te werken met de bank om de echte identiteit van een remailer-operator en/of de e-mailontvanger te onthullen.

Het maakte DigiCash’s eCash grotendeels ongeschikt voor postzegels, na alles.

### De Eerste Elektronische Postzegel

Wat Adam Back niet wist was dat het postprobleem al een paar jaar eerder was opgelost, en op een heel andere manier dan de Cypherpunks hadden overwogen.

In de vroege jaren ’90 realiseerden Cynthia Dwork en Moni Naor, twee computerwetenschappers bij IBM, zich dat een elektronisch mailsysteem veel voordelen had ten opzichte van de traditionele post: e-mail was veel sneller, veel goedkoper, en bood veel meer mogelijkheden dan de postdienst ooit zou kunnen bieden. Maar ze realiseerden zich ook dat e-mail zijn eigen uitdagingen met zich meebracht. Ze voorzagen dat met de toenemende populariteit van e-mail, ook spam zou toenemen.

“Met name de eenvoud en lage kosten om elektronische post te versturen, en dan vooral het gemak om eenzelfde bericht naar veel verschillende partijen te sturen, nodigen in principe uit tot misbruik”, legden ze uit in hun paper uit 1992, getiteld “Pricing via Processing of Combatting Junk Mail.”[^193].

Er was een oplossing nodig, stelden ze vast, en dat was precies wat het artikel leverde. Dwork en Naor stelden een systeem voor waarbij afzenders een beetje extra data aan hun e-mail moeten toevoegen. Deze data zouden de oplossing zijn voor een wiskundig probleem, afgeleid van de eigenschappen van de e-mail zelf, en dus uniek voor die e-mail. Zonder de correcte oplossing toegevoegd, zouden e-mailclients de e-mail volledig moeten afwijzen.

In hun artikel stelden Dwork en Naor drie mogelijke puzzels voor, allen gebaseerd op cryptografische algoritmen zoals handtekeningsschema’s. In alle gevallen zou het toevoegen van de juiste oplossing aan een e-mail niet al te moeilijk zijn (voor een computer); het zou wellicht een paar seconden aan verwerkingskracht vereisen. Toch zou dit een kleine kostenpost betekenen. Controleren of de oplossing correct is, zou daarentegen zeer makkelijk zijn en nauwelijks enige verwerkingskracht kosten.

De kerngedachte achter dit systeem was dat het oplossen van een juiste oplossing voor een puzzel niet veel moeite zou kosten voor individuele gebruikers die af en toe een e-mail zouden sturen naar collega’s, familie of vrienden. Maar voor spammers zou het snel oplopen. Om duizenden of zelfs miljoenen berichten op een enkele dag te sturen, zouden zij evenveel puzzels moeten oplossen, wat in totaal aanzienlijke hoeveelheden verwerkingskracht zou vereisen.

“Het hoofdidee is om een gebruiker een matig moeilijke, maar niet onoplosbare, functie te laten berekenen om toegang te krijgen tot de bron, en zo lichtzinnig gebruik te voorkomen”, legden Dwork en Naor uit. Ze stelden voor om spammen te veranderen in een kostbare bezigheid.

Hoewel Dwork en Naor de term zelf niet hebben voorgesteld, zou de soort oplossing die zij introduceerden later bekend komen te staan als een “proof-of-work”-systeem. Het oplossen van het wiskundige probleem zou bewijzen dat er daadwerkelijk werk is verricht.

Het was een handige oplossing. Maar of het nu kwam omdat het idee iets te vooruitstrevend was voor die tijd, of omdat het simpelweg niet breed genoeg werd geadverteerd, kreeg dit voorstel uit de vroege jaren 90 buiten een vrij kleine groep academici niet veel aandacht. Het postzegelsysteem van Dwork en Naor is nooit uitgevoerd, laat staan gebruikt, en veel van de Cypherpunks waren waarschijnlijk onbekend met dit idee.

Gelukkig genoeg zou het concept spoedig opnieuw worden uitgevonden.

### Hashcash

[ANNOUNCE] implementatie van hash cash porto

Op 28 maart 1997 kregen de inmiddels ongeveer 2000 abonnees van de Cypherpunks mailinglijst een bericht in hun inbox.[^194] Het bericht werd verstuurd door Adam Back en bevatte een beschrijving en vroege implementatie van wat hij “hashcash” noemde: een “postzegelsysteem gebaseerd op gedeeltelijke hash-botsingen”. Hij had succesvol een postzegel-oplossing voor e-mail ontworpen.

Net als het schema van Dwork en Naor, zou de Hashcash port niet betaald worden aan de operators van remailers, of aan de ontvangers van een e-mail, of aan wie dan ook. In plaats daarvan zou het alleen extra kosten met zich meebrengen voor de verzenders.

Een week eerder had Back al nagedacht over het tegengaan van spam door de kosten van massamail te verhogen, hoewel nog vrij oppervlakkig: “Een nevenvoordeel van het gebruik van PGP is dat PGP-versleuteling enige overhead zou moeten toevoegen voor de spammer - hij kan waarschijnlijk minder berichten per seconde versleutelen dan hij kan spammen via een T3-link,” merkte hij op in een discussie over het toevoegen van meer privacy aan remailers.[^195]

Back’s nieuwe voorstel maakte dit algemene idee nog explicieter: het zou vereisen dat afzenders een bewijs van werk aan hun e-mails toevoegen. Inderdaad, hashcash was op verschillende manieren vergelijkbaar met het postzegelschema van Dwork en Naor: het bewijs van werk zou uniek zijn voor de e-mail, en het zou een beetje verwerkingskracht vereisen om te produceren.

Zoals de naam al doet vermoeden, was het voorstel van Back echter gebaseerd op hashing.

Hashing – de cryptografische truc die alle data omzet in een unieke en schijnbaar willekeurige reeks getallen van een specifieke lengte – is een volkomen onvoorspelbaar proces. Hoewel dezelfde data altijd hetzelfde hashresultaat oplevert, is de enige manier om te ontdekken hoe de hash van een stuk data er in de eerste plaats uit zal zien, om het daadwerkelijk te hashen. Het is deze onvoorspelbaarheid waar hashcash op slimme wijze gebruik van maakte.

Om ‘hashcash’ te genereren, moest een gebruiker een hash creëren uit de metadata van een e-mail (zoals het adres van de verzender, het adres van de ontvanger, de tijd enz.) en een willekeurig nummer, een zogenaamde ‘nonce’. Maar hier zat een addertje onder het gras: niet elke resulterende hash werd als “geldig” beschouwd. In plaats daarvan moest de binaire versie van een geldige hash beginnen met een vastgesteld aantal nullen. En er was maar één manier om een hash te genereren die met voldoende nullen begon: de gebruiker moest verschillende nonces proberen en nieuwe hashes maken totdat hij er één vond die toevallig aan de norm voldeed. Simpel trial and error.

Het aantal voorafgaande nullen dat vereist is, bepaalt hoe moeilijk het zou zijn om een geldige hash te vinden. Meer nullen zouden het moeilijker maken, omdat computers gemiddeld meer pogingen zouden moeten doen.

“Het idee van het gebruik van partiële hashes is dat ze naar willekeur duur in berekening kunnen worden gemaakt,” legde Back het voordeel van het gebruik van hashes uit, “en toch kunnen ze onmiddellijk geverifieerd worden.”

Net als bij de oplossing van Dwork en Naor was het idee dat gewone gebruikers vrij snel - binnen enkele seconden - een geldige hash moeten kunnen vinden om met een e-mail te versturen. Tegelijkertijd zouden spammers niet in staat moeten zijn om dit duizenden of miljoenen keren te doen en nog steeds winstgevend te blijven.

“[…] als het geen 20 bit hash heeft […] heb je een programma dat het terugstuurt met een bericht waarin de vereiste porto wordt uitgelegd, en waar de software te vinden is,” legde Back uit op de Cypherpunks mailinglijst. “Dit zou spammers van de ene op de andere dag uit de handel halen, aangezien 1.000.000 x 20 = 100 MIP jaren, wat meer rekenkracht is dan ze hebben.”

Een subtiele verandering ten opzichte van Dwork en Naor’s oplossing was dat hun ‘proof-of-work’ systeem niet onderhevig was aan toeval. Hun ‘portzegel’ schema vereist in principe het oplossen van een vrij eenvoudige puzzel, wat betekent dat een krachtigere computer de puzzel elke keer sneller zou oplossen dan een zwakkere computer.

Het genereren van een geldige hash is daarentegen een kwestie van gokken. Hoewel een krachtigere computer meer gokjes per seconde zou kunnen doen, zou een zwakkere computer nog steeds af en toe geluk kunnen hebben en sneller een geldige hash vinden. (Hoewel spammers hoe dan ook duizenden of miljoenen geldige hashwaarden zouden moeten genereren per spamsessie, zou het kleine beetje variatie bij het genereren van een enkele hashcash proof-of-work niet echt een verschil maken - althans niet binnen de context van het stoppen van ongewenste mail.)

“Hashcash kan een tussenoplossing bieden totdat digicash breder wordt toegepast,” concludeerde Back in zijn aankondiging. “Hashcash is gratis, het enige dat je hoeft te doen is wat processorkracht van je PC gebruiken. Het sluit aan bij de online cultuur van vrije communicatie, waarin de financieel minder bedeelden op gelijke voet kunnen concurreren met miljonairs, gepensioneerde overheidsfunctionarissen en dergelijke.”

Het lijkt erop dat er geen tekst is gegeven om te vertalen. Kun je alsjeblieft de tekst opgeven die je vertaald wilt hebben?

“Hashcash kan ons een alternatieve methode bieden voor het beheersen van spam als digicash misgaat (verboden wordt of vereist dat gebruikersidentiteiten in escrow worden gehouden).”

### Digitale Schaarste

Hashcash werd in de jaren na de aankondiging van Adam Back enigszins geadopteerd. De oplossing werd geïmplementeerd in Apache’s open source SpamAssassin platform, terwijl Microsoft het idee in zijn incompatibele Postmark systeem uitprobeerde. Adam Back, samen met enkele andere academici, kwamen ondertussen op alternatieve toepassingen voor het proof-of-work systeem, waaronder oplossingen tegen DDoS-aanvallen.

Maar de postzegel van hashcash is nooit echt mainstream gegaan. De innovatieve aard van de oplossing was waarschijnlijk niet voldoende om de opstarthindernis te overwinnen: iemand kon niet echt beginnen met het eisen van hashcash voor binnenkomende e-mails als niemand anders het gebruikte, omdat dit zou leiden tot afwijzing van alle binnenkomende berichten door hun e-mailclient. Tegelijkertijd was er geen aanmoediging om hashcash te gebruiken voor uitgaande e-mails als niemand het eiste. Net als David Chaum’s eCash, leed ook het elektronische porto-systeem van Back aan een kip-en-ei-probleem, waarvoor geen gemakkelijke oplossing leek te zijn.

Adam Back maakte zich hier echter niet zoveel zorgen om. Back, die inmiddels onderzoeker was bij de Universiteit van Exeter en werkte aan een gecodeerd berichtensysteem voor medische data, dacht vrijwel onmiddellijk na de publicatie van zijn voorstel aan de Cypherpunks mailinglijst al verder dan enkel hashcash. Het oplossen van het postprobleem was een goede uitdaging, maar deze computeringenieur was vooral gefascineerd door de gedachte om digitaal geld voor algemene doeleinden te creëren.

En hoewel veel Cypherpunks nog steeds aannamen dat een elektronisch geldsysteem zou moeten worden geïntegreerd in de bestaande financiële infrastructuur, zoals eCash dat was, had Back een andere visie. Hij geloofde dat hashcash een geheel nieuwe richting van onderzoek kon bieden om die visie te verwezenlijken.

De sleutelinnovatie van hashcash was dat het puur digitale data (in wezen getallen) aan echte bronnen in de fysieke realiteit koppelde. Het creëren van een bewijs van werk vereiste rekenkracht, en deze rekenkracht zelf verbruikt elektriciteit, die op zijn beurt energie kost om te produceren. Terwijl de meeste digitale dingen kosteloos en bijna eindeloos gekopieerd kunnen worden, kon het bewijs van werk op een bepaalde manier de fundamentele schaarste aan energie in de fysieke realiteit naar de digitale wereld overbruggen.

Inderdaad, hashcash was digitaal, maar toch schaars. Het totale aantal hashcash “valuta-eenheden” (bij gebrek aan een beter woord) was in zekere mate beperkt: er zou nooit meer hashcash zijn dan er zou kunnen worden geproduceerd met de hoeveelheid energie die mensen bereid en in staat zouden zijn om eraan te spenderen.

Dit was een cruciaal inzicht, omdat ingebouwde schaarste een van de zes eigenschappen was die Adam Back op zijn lijstje voor een ideaal elektronisch geldsysteem had gezet. Tot voor kort kon digitale schaarste slechts gecreëerd worden als een belofte, zoals DigiCash’s belofte om een harde limiet te stellen aan het totale aantal CyberBucks dat ze zouden creëren. Maar beloftes kunnen natuurlijk gebroken worden. Back geloofde dat proof-of-work de mogelijkheid bood om schaarste te garanderen op een veel fundamenteler niveau.

Tegelijkertijd wist hij dat hashcash niet kon functioneren als volwaardig digitaal geld. Hoewel het anoniem kon worden gebruikt, moeilijk te stoppen was, geen vertrouwen in een individu vereiste en ook enige mate van schaarste had, voldeed dit eigenlijk slechts aan drie van de zes criteria op de shortlist van Back.

Het grootste probleem was dat hashcash niet herbruikbaar was. Elke munteenheid was op maat gemaakt om bij een specifieke email te passen, dus het kon niet elders opnieuw worden uitgegeven en leverde geen extra voordeel op voor de ontvangers.

Back overwoog daarom dat hashcash - of meer algemeen het proof-of-work principe - de basis zou kunnen vormen voor een ander soort elektronisch geldsysteem.

Eén van zijn eerste suggesties was een Chaumiaans systeem. Hierin zou de bank elektronisch geld uitgeven bij ontvangst van hashcash: gebruikers zouden bewijs van werk (proof of work) creëren en daarvoor ongedekt digitaal geld terugkrijgen. Dit geld zou anoniem, herbruikbaar en enigszins schaars zijn—hoewel de schaarste in de praktijk eerlijk gezegd vrij zwak zou zijn, omdat mensen altijd meer bewijs van werk zouden kunnen creëren als ze dat zouden willen. En met computerprocessors die elk jaar krachtiger worden, zou het produceren van geldig bewijs van werk in de loop van de tijd steeds goedkoper worden.[196](Back,)

Inderdaad, de fundamentele schaarste van hashcash was meer technisch van aard. Als het echt de basis zou vormen voor een elektronische valuta, zouden nieuwere en krachtigere computers uiteindelijk de markt overspoelen met verse valuta-eenheden en zou de valuta hyperinflateren.

Bovendien zouden gebruikers de bank moeten vertrouwen dat deze geen geld uit het niets creëert. Net als elk elektronisch geldsysteem dat Chaum’s ontwerp volgt, zou de entiteit die de digitale valuta uitgeeft en dubbele uitgaven voorkomt, zelf ook vertrouwd moeten worden om niet onterecht zelf rijker te worden.

Echter, Back geloofde dat vrije marktcompetitie mogelijk kon helpen dit probleem op te lossen.

“Dus, wellicht zou je meerdere banken kunnen hebben en laat reputaties ze sorteren, als je de protocollen zo kunt regelen dat het duidelijk zou zijn of een bank meer geld aan het drukken was dan het aan hash-botsingen had ontvangen. [. . .] Maar als je meerdere banken hebt dan moet je een uitwisselingsmechanisme hebben. De markt zou hier waarschijnlijk zorg voor kunnen dragen, door wisselkoersen te bepalen op basis van de reputaties van banken,” suggereerde hij, in wat nu heel erg leek op een vrijbankiersysteem zoals beschreven door Friedrich Hayek.

Desalniettemin geloofde de jonge Cypherpunk uit Exeter dat ze het misschien zelfs nog beter konden doen dan dat:

“Het zou beter zijn om iets te hebben dat geen vertrouwen vereist en dat geen mogelijkheid heeft voor bedrog, in plaats van te vertrouwen op reputatie om ze te sorteren.”[^197]

## Hoofdstuk 11: Bit Gold

De vader van Nick Szabo was een van de 200.000 Hongaren die hun land verlieten nadat Sovjettroepen de anti-communistische opstand van 1956 hadden neergeslagen. Terwijl tienduizenden van zijn mede-vrijheidsstrijders werden opgesloten of geïnterneerd, en in sommige gevallen zelfs geëxecuteerd, besloot hij alles achter te laten. Uiteindelijk vond hij een nieuw thuis aan de andere kant van de Atlantische Oceaan, in het land van de vrijheid.

Hoewel dit bijna een decennium voor zijn geboorte gebeurde, zou de ervaring van zijn vader Nick vormen. Als de zoon van een vluchteling, opgroeiend ver weg van het onderdrukkende Sovjetgezag over Oost-Europa, werd bij de Amerikaanse jongen van de tweede generatie al vroeg een diep wantrouwen tegen alles wat ook maar enigszins leek op communisme of overheidsinmenging ingeplant.[^198]

Uiteindelijk vond Szabo een grote bron van inspiratie in de werken van Friedrich Hayek. Het boek The Road to Serfdom leek de transformatie van de Sovjet-Unie naar een totalitaire staat nauwkeurig te hebben beschreven, met de onderdrukking van de Hongaarse revolutie als een van de eerste grote voorbeelden hiervan buiten het Russische thuisland. Szabo zou later Hayek’s boek uit 1988, The Fatal Conceit—een andere, meer politieke, weerlegging van het socialisme, dat de historische belangrijkheid van privé-eigendom benadrukte—noemen als een van de belangrijkste boeken die hij ooit heeft gelezen.[^199]

Ondertussen raakte de jonge Szabo geïnteresseerd in computers, een nieuwe technologie die in die tijd snel evolueerde in de VS en de rest van de Westerse wereld, terwijl het communistische Oosten ver achterbleef. Toen in de late jaren ’70 en vroege jaren ’80 de eerste persoonlijke computers hun weg vonden naar Amerikaanse huizen en kantoren - zijn moeder nam regelmatig haar Apple II mee naar huis van haar werk - zag hij al snel de potentie van deze machines. Tegen het midden van de jaren ’80 had dit hem ertoe gebracht om informatica te gaan studeren aan de Universiteit van Washington in Seattle.

Tijdens zijn studie, deed Szabo een jaar stage bij het Jet Propulsion Laboratory (JPL), een onderzoekscentrum van NASA, voordat hij in 1989 zijn diploma in de informatica behaalde. Nu midden in zijn twintiger jaren, besloot hij zo’n 1300 kilometer naar het zuiden te verhuizen, naar de San Francisco Bay Area, waar zijn vaardigheden bijzonder gewild waren. Hij vond een programmeerbaan bij IBM, dat gedurende de jaren ’80 de standaard had gezet voor thuiscomputers met zijn relatief goedkope microcomputers.

Szabo’s persoonlijke interesses waren echter altijd breder dan alleen informatica. Als een echte veelweter, genoot hij ervan om een scala aan onderwerpen in zijn vrije tijd te bestuderen: van politiek tot biologie en van geschiedenis tot economie, met een speciale focus op vrije markteconomie. Het was niet anders dan Hayek, die vooral in deze latere fase van zijn carrière economische concepten gebruikte om hardnekkige politieke realiteiten uit te leggen, Szabo waardeerde hoe het combineren van multi-disciplinaire kennis hem kon helpen nieuwe inzichten op te doen. Hij hield ervan deze inzichten te benutten om te speculeren over de toekomst van technologie, samenleving en mensheid.

Dit maakte hem perfect passend bij de Extropians.

De techno-utopische futuristische beweging kreeg tijdens zijn eerste jaren in de Bay Area steeds meer vaart, met name in en rond Silicon Valley, en Szabo zou zichzelf profileren als een vooraanstaand lid van de Extropian gemeenschap. De informaticus publiceerde essays en brieven in het Extropy magazine over onderwerpen als ruimtekolonisatie (geïnspireerd door zijn ervaring bij JPL), kunstmatige intelligentie, nanotechnologie en meer.

Het was ook via de Extropian gemeenschap dat Szabo kennis maakte met Tim May.

### De Crypto-Anarchist

Op een dag nodigde May Szabo uit om deel te nemen aan een bijeenkomst van de Cypherpunks. Szabo ging graag op de uitnodiging in; hij was zelf ook ongerust over de schijnbare terugloop van privacy in het opkomende digitale tijdperk.

Toen Szabo een paar weken later de groep daadwerkelijke privacy-activisten ontmoette, wist hij dat hij op de juiste plek was gekomen.

Gedurende de volgende paar jaar hielp Szabo, waar hij kon, aan de zaak van de Cypherpunks. Opvallend genoeg nam hij al vroeg een voortrekkersrol op zich in het verzet tegen de Clipper Chip van de NSA, zowel op de mailinglijst van de Cypherpunks als in het echte leven: hij gaf lezingen over het onderwerp tijdens verschillende evenementen en deelde soms flyers uit om mensen te informeren over de risico’s verbonden aan dit soort surveillancetechnologie. Hij had een manier om de verontrustende implicaties van de opdoemende inbreuken op de privacy over te brengen naar een niet-technisch publiek, en was blij om zijn aanpak te delen met de andere Cypherpunks, zodat zij hetzelfde konden leren doen.

Echter, Szabo’s interesse in digitale privacy was uiteindelijk slechts een deel van een veel groter geheel. Hij omarmde het idee van een “Galt’s Gulch in cyberspace.” Zoals uitvoerig beschreven in de vele posts op de mailinglijst door zijn vriend Tim May, had Szabo zich gerealiseerd dat de benodigde instrumenten om individuen te beschermen tegen staatsmacht niet langer alleen voorbehouden waren aan fictieve literatuur. De computerwetenschapper met Hongaarse roots was het eens met het feit dat cryptografie het ideaal van echt vrije markten, ongevoelig voor het gebruik van fysieke macht of staatsdwang, dichter bij de realiteit kon brengen.

“Als we een stap terug nemen en kijken naar wat veel cypherpunks proberen te bereiken, dan is er een hoofdthema van een Ghandiaanse cyberspace waar geweld slechts een illusie kan zijn, of het nou in Mortal [Kombat] of ‘flame wars’ is,” schreef hij in de Cypherpunks mailinglijst. “Cypherpunks willen dat onze telefoonnetwerken, internetbedrijven, etc., zowel beschermd zijn tegen geweld en niet afhankelijk van geweld voor hun bestaan. Onze informatiesystemen uit de 20e eeuw, van uitgeverijen tot creditcards, zijn vaak sterk afhankelijk geweest van de dreiging van geweld, meestal via de wetshandhaving, om intellectuele eigendomsrechten te beschermen, fraude te voorkomen, schulden in te vorderen, enzovoort.”

Het voorstel van hem was:

“Er is geen utopie in zicht waar dergelijke bedreigingen volledig kunnen worden geëlimineerd, maar we kunnen erkennen dat ze bestaan en zorgvuldig werken aan het verminderen van onze afhankelijkheid ervan.”[200]

### Slimme Contracten

Misschien wel meer dan wie dan ook, was Szabo zich er zeer van bewust dat het realiseren van May’s visie op crypto-anarchie, private communicatie slechts een eerste stap was.

Als leerling van Hayek’s werk - inclusief diens latere, meer politieke geschriften - was de Cypherpunk tot het inzicht gekomen dat welvarende samenlevingen zo goed presteerden omdat ze bepaalde regels hadden aangenomen, in de vorm van wetten, die menselijk gedrag reguleerden. Het vergelijkend met het gelaagde ontwerp van computerprotocollen, erkende Szabo dat de wetten die de basis vormden van de samenleving (zoals grondwetten) de meest basale, maar ook de belangrijkste regels van allemaal waren. Alle andere regels zijn gebaseerd op deze fundamenten.

Szabo ontdekte dat twee van de fundamentele bouwstenen in de “basislaag” van elke welvarende samenleving inderdaad eigendomsrechten en contractrecht waren. Eigendomsrechten vergemakkelijken en stimuleren investeringen, productie en uitbreiding, terwijl contractrecht handel en specialisatie mogelijk maakt. Hij geloofde dat een samenleving die eigendomsrechten en contractrecht handhaaft, uiteindelijk kan evolueren tot een moderne kapitalistische samenleving.

Maar Szabo was zich ervan bewust dat eigendomsrechten en contractrecht in moderne kapitalistische samenlevingen worden gehandhaafd door de staat. Eigendom en de overdracht van eigendom worden uiteindelijk afgedwongen door rechtbanken en de politie, die gebruikmaken van het staatsmonopolie op geweld. Dit kan impliciet gebeuren door (de dreiging van) boetes of gevangenisstraf, of expliciet door iemands eigendom met geweld te beschermen of terug te geven.

Om een staatloze en geweldloze cyberspace-economie te creëren, concludeerde Szabo dat crypto-anarchisten eerst een nieuwe basis moesten leggen.

Het eerste deel van deze basis - de eigendomsrechten - kon met behulp van openbare-sleutelcryptografie worden gerealiseerd, zoals uitvoerig door Tim May is uitgelegd; persoonlijke gegevens zouden worden beveiligd met wiskunde in plaats van met fysieke kracht.

Maar het was niet meteen duidelijk hoe twee mensen deze gegevens konden uitwisselen zonder risico op wanprestatie van de tegenpartij. Bij dergelijke transacties moest een partij altijd eerst hun gegevens verzenden of hun deel van de afspraak afronden. Op dat moment kon de tegenpartij verdwijnen en zijn verplichting niet nakomen. In de cyberspace waren er geen rechtbanken of politie om contractrecht te handhaven.

Een mogelijke oplossing was het gebruik van arbitrage om geschillen te beslechten, waarbij een scheidsrechter de middelen zou krijgen om de betreffende data te verplaatsen van de ene handelspartner naar de andere (op eigen discretionaire bevoegdheid, of wellicht in samenwerking met een van de handelspartners). Dit zou echter vereisen dat beide partijen de arbiter vertrouwen om niet te stelen of samen te zweren met hun tegenpartij. Dit vertrouwen zou misschien kunnen worden opgebouwd door de reputatie van de arbiter na verloop van tijd: een onberispelijke staat van dienst van de arbiter zou op een bepaalde manier kunnen dienen als een haalbaar alternatief voor de handhaving door de staat, hoewel het nooit volledig risicovrij zou zijn.

Maar halverwege de jaren 90 meende Szabo dat hij een beter idee had. Hij bedacht een oplossing die niet door een van de handelspartijen kon worden bedrogen en geen betrouwbare scheidsrechter nodig had. Szabo stelde slimme contracten voor - digitale contracten die uit zichzelf hun eigen voorwaarden zouden afdwingen, zoals vastgelegd in computercodes.[^201]

Als een eenvoudig voorbeeld, stel dat Alice een geheime code van Bob wil kopen voor € 10. Een slim contract kan dan zo worden geprogrammeerd dat zodra Bob de geheime code invoert op een vooraf afgesproken plek waar Alice hem kan vinden (misschien door het toe te voegen aan het contract zelf, niet ongelijk aan een digitale handtekening), de code van het contract dit herkent en verifieert, om vervolgens automatisch € 10 van Alice’s account af te trekken en over te maken naar Bob. (Szabo gebruikte een frisdrankautomaat als een primitieve analogie: het “contract” tussen een consument en een frisdrankautomaat stelt dat als de consument een muntje in de automaat stopt, de machine—door een geautomatiseerde respons—een blikje frisdrank of een reep chocolade uitgeeft, zonder verdere menselijke tussenkomst.)

In theorie zouden smart contracts buitengewoon complex kunnen worden opgesteld, en kunnen ze in principe alle soorten contractuele clausules bevatten, waaronder pandrechten, obligaties, of omschrijving van eigendomsrechten. Dit zou zelfs volledig nieuwe zakelijke regelingen mogelijk maken, opperde Szabo, waarbij hij het voorbeeld gaf van een smart contract voor een autolening dat, bij het niet terugbetalen van de lening, automatisch de controle over de digitale autosleutels terug zou geven aan de bank.

Nick Szabo geloofde dat de meeste eigenschappen en kenmerken die een slim contract zou moeten bevatten, konden worden geïmplementeerd door gebruik te maken van de steeds groter wordende toolkit van de Cypherpunks: “Protocollen gebaseerd op wiskunde, genaamd cryptografische protocollen, zijn de fundamentele bouwstenen die de verbeterde afwegingen tussen waarneembaarheid, verifieerbaarheid, privaatrechtelijkheid, en afdwingbaarheid in slimme contracten implementeren,” schreef hij. [^202]

De grootste uitdaging was echter om ervoor te zorgen dat het contract automatisch, betrouwbaar en onvoorwaardelijk uitgevoerd zou worden. Dit hield vooral in dat geen van de partijen bij het contract verantwoordelijk zou moeten zijn voor de uitvoering ervan.

Als algemeen vertrekpunt vermoedde Szabo dat de beste oplossing te vinden was in het domein van gedistribueerd computergebruik, waar deelnemende computers strikte protocollen moesten volgen om met elkaar overeen te stemmen. Hoewel het Byzantijnse generaalsprobleem (het coördinatieprobleem dat Adam Back op de universiteit leerde kennen) inderdaad nog niet volledig was opgelost - er bleven enkele risico’s als er te veel onbetrouwbare deelnemers waren - geloofde hij dat er robuuste protocollen waren ontworpen voor de meeste scenario’s.

“De termen van contractuele relaties kunnen vaak worden geformaliseerd en gestandaardiseerd, en vervolgens worden uitgevoerd via netwerkgebaseerde protocollen,” legde Szabo uit op de Cypherpunks mailinglijst. “Deze protocollen, samen met economische prikkels, beschermen de uitvoering van het contract tegen zowel fraude door de hoofdpartijen als aanvallen van derden.” [^203]

Dat gezegd hebbende, zouden de meeste slimme contracten vermoedelijk ook een vorm van geld nodig hebben: meestal moet minstens een van de partijen een betaling doen als onderdeel van de deal. Bovendien moest dit een soort valuta zijn die over het internet kon worden overgedragen, en die autonoom door een computerprogramma kon worden verstuurd… bij voorkeur anoniem.

Voor slimme contracten is elektronisch geld noodzakelijk.

### Vertrouwde Derde Partijen

Als digitale equivalenten van eigendomsrechten en contractwetgeving twee van de fundamentele bouwstenen waren die nodig zijn om een “Galt’s Gulch in cyberspace” te realiseren, was een digitaal equivalent voor geld de derde.

Nick Szabo is een prominent figuur onder de Extropians en Cypherpunks en was één van de eersten die deze inzichten herkende. Toen Hal Finney voor het eerst de voordelen van elektronisch geld begon te bepleiten in het Extropy-magazine, was Szabo de Extropian die naar Amsterdam was verhuisd om voor David Chaum te werken. Rond dezelfde tijd dat de eerste webshops hun virtuele deuren openden, trad Szabo toe tot DigiCash als internetprogrammeur.

Tijdens de vroege jaren ’90 werkte hij een tijdje op het kantoor van het bedrijf, en kreeg Szabo de kans om uit eerste hand te ervaren hoe het eraan toe ging bij de meest beloftevolle start-up voor elektronisch geld ter wereld. Hij kon zien hoe DigiCash het eerste Chaumiaanse digitale geldproduct op de markt bracht in de vorm van CyberBucks, het niet-ondersteunde prototype van eCash, waarvoor de start-up beloofde nooit meer dan een miljoen eenheden uit te geven. Hij was ook getuige hoe CyberBucks een beetje koopkracht verwierf, aangezien sommige Cypherpunks en andere geïnteresseerde technofielen bereid waren om kleine bedragen van het digitale geld te kopen met reguliere valuta, of het te accepteren in ruil voor goederen of diensten met een lage waarde.

Het systeem van CyberBucks was volledig afhankelijk van het bedrijf DigiCash: Szabo realiseerde zich dat het startup van Chaum simpelweg meer dan een miljoen van het elektronische geld kon uitgeven als ze van gedachten zouden veranderen, of als ze vanaf het begin gelogen hadden, of als een oneerlijke medewerker het systeem zou proberen te bedriegen, enzovoorts. Bovendien zou er geen enkele manier zijn om het te detecteren als ze het deden. (Om nog maar te zwijgen over het feit dat CyberBucks onmiddellijk waardeloos zou worden als de servers van DigiCash ooit uitvielen, wat uiteindelijk ook gebeurde.)

Szabo beschouwde dit als aanzienlijke problemen.

“Een van de dingen die ik daar leerde, was hoe gemakkelijk het was om met mensen hun saldo’s te knoeien in een centraal gereguleerde valuta,” herinnerde de pionier van de digitale valuta zich later. “Wie zou zijn rijkdom toevertrouwen aan een stel slordige Frank Zappa-fans in het verre Amsterdam?”[^204] (Ze hielden ervan om platen van Frank Zappa op het kantoor van DigiCash te draaien.)

Net als Scott Stornetta en Stuart Haber een aantal jaar eerder, wakkerde dit bij Szabo de neiging aan om dieper na te denken over de rol van betrouwbare entiteiten in het groeiende online ecosysteem. Hoewel cryptografie privacy en beveiliging kon bieden op een niveau dat gelijk of zelfs beter was dan wat mogelijk is in de fysieke wereld, merkte Szabo op dat protocolontwikkelaars doorgaans een bepaald type risico leken te negeren. Het was het risico dat inherently was verbonden aan de afhankelijkheid van een vertrouwde derde partij (TTP).

Het typische voorbeeld is een certificaatautoriteit die een register bijhoudt van de werkelijke identiteiten gekoppeld aan hun openbare sleutels. Hoewel dit een handige manier is om iemands openbare sleutel te vinden, zijn deze openbare sleutels eigenlijk net zo veilig te gebruiken als de certificaatautoriteit zelf. Als een openbare sleutel die door een certificaatautoriteit wordt vermeld, eigenlijk toebehoort aan een aanvaller, zou Szabo benadrukken, kan deze aanvaller elk bericht ontcijferen dat bedoeld is voor wie dan ook die geassocieerd is met de openbare sleutel in het register.

In zijn essay over dit onderwerp, toepasselijk genaamd “Trusted Third Parties are Security Holes” [^205], legde Szabo later uit dat vertrouwde derde partijen vaak niet werden opgenomen in de kosten van een ontwerp, en waarom hij geloofde dat dit een vergissing was. Vertrouwde derde partijen zijn veiligheidsgaten, beargumenteerde de Cypherpunk, zelfs als ze zelf daadwerkelijk eerlijk zijn: ze kunnen aantrekkelijke doelwitten worden voor kwaadwillige hackers, of misschien zelfs voor naties en hun regelgevende instanties tijdens periodes van politieke instabiliteit of onderdrukking.

Een gecompromitteerde vertrouwde derde partij kan dus enorm kostbaar blijken te zijn. Szabo beargumenteerde dat de kosten van een mogelijke inbreuk moeten worden meegenomen bij het ontwerpen van protocollen, wat volgens hem zou leiden tot het feit dat veel protocollen opnieuw ontworpen moeten worden om de vertrouwde derde partijen volledig te elimineren.

Szabo stelde nogmaals dat mogelijke oplossingen misschien wel te vinden zijn in de wereld van gedistribueerde informatica.

“De beste ‘TTP’ van allemaal is er een die niet bestaat, maar waarvan de noodzaak is geëlimineerd door het protocolontwerp, of die geautomatiseerd en verdeeld is over de deelnemers aan een protocol”, concludeert hij in zijn paper.

### Vrij Bankieren

Net als Chaum waren de meeste Cypherpunks vooral geïnteresseerd in elektronisch geld vanwege de mogelijkheden tot privacy die het kon bieden. Maar Szabo, May, en enkele andere Cypherpunks die zich bij de beweging hadden aangesloten vanuit de Extropian community, waren ook gedreven door monetaire hervorming. Ze waren voornamelijk geïnteresseerd in de ideeën van Hayek over vrij bankieren, zoals ook beschreven door Max More in de digitale geldeditie van Extropy.

Bovendien had Szabo het werk van George Selgin bestudeerd - wiens boek “The Theory of Free Banking” in datzelfde tijdschrift was besproken - en dat van Selgin’s collega Lawrence H. White, die zelf een artikel aan het tijdschrift had bijgedragen. Met Hayek die net voor de oprichting van de Cypherpunk beweging overleed, dacht Szabo dat de medeoprichters van de door Hayek geïnspireerde moderne school voor vrij bankieren wellicht konden helpen bij het informeren over het ontwerp van een elektronisch geldsysteem.

Ergens midden jaren ’90 besloot hij een nieuwe, meer themagerichte mailinglijst te maken: de Libtech-lijst. Hier zouden vrije bankiers als Selgin en White, evenals geïnteresseerde Extropianen en Cypherpunks, gerichte discussies voeren over bankieren, monetaire economie en het allerbelangrijkste - de ontwerpen voor digitale valuta.[^206]

Toen twee zeer verschillende werelden elkaar ontmoetten op de Libtech lijst, keek Szabo met een frisse blik naar de inzichten uit de Oostenrijkse economie, door zijn eigen ervaring als computerwetenschapper. Dit stelde hem in staat nog duidelijker dan voorheen de gebreken van fiat-geld te zien. Waar Hayek uitvoerig had gewaarschuwd voor de mankementen van centrale banken, zag Szabo in dat dit uiteindelijk te wijten was aan een fundamenteel ontwerpfout aan het huidige monetaire systeem.

Centrale banken waren TTP’s.

“Het probleem, kort gezegd, is dat ons geld momenteel afhankelijk is van het vertrouwen in een derde partij voor zijn waarde”, betoogde Szabo later. “Zoals vele inflatoire en hyperinflatoire episodes in de 20e eeuw hebben aangetoond, is dit geen ideale situatie.”

Door deze fundamentele zwakte centraal te stellen, bevestigde Szabo op een bepaalde manier Hayek’s analyse - althans voor zichzelf.

Maar tegelijkertijd betwistte hij enigszins het monetaire ecosysteem dat Selgin voorspelde dat zou ontstaan in een vrije bankomgeving. Als het probleem van het moderne monetaire systeem was dat iedereen een centrale bank moest vertrouwen, dan zou vrij bankieren gewoon particuliere banken tot de nieuwe vertrouwde derde partijen maken. Zelfs als concurrentie hen eerlijk kon houden, vertegenwoordigden deze TTP’s (Trusted Third Parties) een bredere reeks veiligheidsrisico’s - variërend van losgeslagen werknemers tot draconische overheden - die marktdynamieken niet noodzakelijkerwijs volledig zouden oplossen.

Als en wanneer deze nieuwe vertrouwde derde partijen – de banken – het vertrouwen van hun klanten zouden schenden, zouden mensen niet simpelweg overstappen naar hun concurrenten, zo voorspelde Szabo. In plaats daarvan zouden mensen opnieuw aandringen op waarborgen van de centrale bank - zo was het moderne monetaire systeem immers in de eerste plaats ontstaan.

Voordat vrij bankieren een haalbaar alternatief kon zijn, concludeerde Szabo, moest er vanaf de basis een vorm van elektronisch geld worden ontworpen dat het vertrouwen minimaliseerde. Net zoals eigendomsrechten en contractrecht voor cyberspace vanaf nul opnieuw moesten worden uitgevonden, zou ook een digitale munteenheid moeten worden gecreëerd door te starten vanuit de eerste principes.

### De Oorsprong van Geld

Om geld te kunnen creëren, moest Szabo het eerst begrijpen.

De Cypherpunk was natuurlijk niet de eerste die de natuur van geld bestudeerde - hij dacht ook niet dat hij dat was. Hij was goed op de hoogte van de theorieën van Carl Menger en Ludwig von Mises over de oorsprong van geld, en deelde grotendeels hun assessment dat geld is voortgekomen uit ruilhandel. Maar waar Menger en Mises hun stelling hadden ontwikkeld door logica en redeneren, ging Szabo op zoek naar daadwerkelijke historische documenten, en zelfs archeologische resten.

De zoektocht van Szabo bracht hem diep in de prehistorie van de mensheid en naar pre-industriële samenlevingen zoals die van de Native Americans. Hij ontdekte dat geld zelfs ouder was dan tekst: vroege vormen van valuta werden al gebruikt door jager-verzamelaarstammen. Dit leidde uiteindelijk tot zijn hypothese dat geld letterlijk zo oud zou kunnen zijn als de mensheid zelf. Zoals eerst gesuggereerd door evolutiebioloog Richard Dawkins in zijn baanbrekende werk The Selfish Gene,[^208] zou het vermogen om geld te gebruiken diep ingebed kunnen zijn in het menselijk DNA en zou het de overleving van de soort ten voordele gekomen kunnen zijn.

In zijn latere essay “Shelling Out: The Origins of Money,”[^209] legt Szabo uit hoe.

Een van de grote voordelen van de mensheid in de meedogenloze overlevingsstrijd van moeder natuur, ontdekte Szabo, is dat de meeste leden van de soort bereid en in staat zijn om samen te werken om hun krachten te bundelen of om arbeid te verdelen en zich te specialiseren om vervolgens de opbrengst te delen. Dit is waarschijnlijk altijd zo geweest: prehistorische jagers die succesvol een wild zwijn doodden, zouden het vlees delen met hun stamleden. Hun medestamleden zouden een andere keer de gunst retourneren, misschien door de blauwe bessen of eetbare paddenstoelen te delen die ze de volgende dag verzamelden.

Deze vorm van altruïstisch gedrag zou iedereen kunnen ten goede komen, zolang alle stamleden elkaar kenden en min of meer konden bijhouden wat ieders bijdragen waren. Alle stamleden hadden een publieke reputatie. Omdat profiteurs - degenen die nooit iets bijdroegen aan de stam - uiteindelijk konden worden uitgesloten van de deelrondes of zelfs uit de stam konden worden verbannen, was iedereen sterk gemotiveerd om bij te dragen en hun deel te doen.

Maar dit model zou onhoudbaar worden als een stam (of vaker: een groep stammen) te groot werd. Menselijke hersenen kunnen slechts een beperkt aantal sociale relaties onderhouden (populair bekend als “Dunbar’s nummer”, wat 150[^210] is), dus het wordt moeilijk om iedereens reputatie bij te houden als er meer mensen dan dit nummer zijn. Als niemand zich kan herinneren wie met de anderen heeft gedeeld en wie niet, breekt het “publieke reputatiesysteem” af, en krijgen profiteurs vrij spel op kosten van iedereen.

Om te voorkomen dat er misbruik van ze wordt gemaakt, zou het zelfs rationeel worden voor elk individu om zelf ook te stoppen met delen en een profiteur te worden - ook al zou iedereen beter af zijn als iedereen zou delen. Met andere woorden, er zou iets van een groot gevangenendilemma[^211] ontstaan.

Maar Szabo legde uit dat genen strategieën kunnen coderen om oplossingen te vinden voor uitdagingen in de gametheorie van de echte wereld. Gedurende lange perioden en via natuurlijke selectie zouden de beste eigenschappen - die de overleving van een soort bevorderen - dominant worden.

Het gebruik van geld werd door de Cypherpunk als zo’n eigenschap beschouwd.

Voor het grootste deel van de menselijke geschiedenis was dit echter een heel ander soort geld dan wat moderne samenlevingen gebruiken.

Doorheen de eeuwen en over verschillende culturen heen, droegen mensen juwelen, zoals kettingen, iets wat geen enkel ander dier doet. De oppervlakkige uitleg hiervoor is dat mensen simpelweg plezier beleven aan het dragen van dergelijke sieraden. Maar Szabo begreep dat er een fundamenteelere vraag schuilging onder deze simpele verklaring - het soort vraag dat een evolutionair bioloog zou stellen. Waarom hebben mensen zich zo ontwikkeld dat ze plezier beleven aan het dragen van sieraden?

Net als Dawkins vermoedde Szabo dat mensen in de loop van de eeuwen een voorliefde voor ornamenten hadden ontwikkeld omdat dit een evolutionair voordeel bood: het stelde hen in staat om te coöpereren en middelen te ‘delen’ op een grotere schaal dan alleen binnen hun eigen stam.

Szabo ontdekte bijvoorbeeld dat halskettingen en andere verzamelobjecten verhandeld werden tussen stammen in ruil voor voedsel, wapens of bruiden. De ornamenten konden later teruggeruild worden of met een andere stam geruild worden voor andere bronnen. In plaats van te onthouden wie wat gedeeld had, diende de sieraden als een soort proto-geld en bevorderden ze wat evolutionaire psychologen wederzijds altruïsme noemen.

Het stelde stammen in staat een mate van samenwerking en specialisatie tussen hen te bevorderen. Verschillende stammen jaagden bijvoorbeeld op verschillende soorten dieren in verschillende delen van het jaar, wat uiteindelijk aan hen allemaal ten goede kwam.

### Proto-Money

Niet zomaar elk sieraad voldeed echter.

Toen hij de resten van pre-civiele samenlevingen analyseerde, ontdekte Szabo dat mensen uit alle culturen de neiging hadden om zich te richten op verzamelobjecten met enkele zeer specifieke eigenschappen. Hoewel archeologen voorbeelden van proto-geld hadden gevonden die zo uiteenlopend waren als schelpen van een zeldzaam type slak, tot struisvogelei-scherven, tot mammoet-tanden, deelden ze allemaal drie algemene kenmerken.

Allereerst waren de verzamelobjecten relatief makkelijk te beschermen tegen onopzettelijk verlies en diefstal. Kettingen zijn waarschijnlijk het beste voorbeeld in dit opzicht: ze zijn bijna onmogelijk te verliezen als ze om de nek worden gedragen. Alternatief gezien, waren ornamenten die niet op iemands lichaam gedragen konden worden, doorgaans minstens makkelijk te verbergen.

Ten tweede, de verzamelobjecten vertegenwoordigden een niet-te-vervalsen schaarste. Dat wil zeggen, ze zouden kostenlijk zijn om te maken of moeilijk te vinden: een mammoettand was schaars omdat een mammoet doden niet gemakkelijk is, terwijl struisvogel eieren moeilijk te bemachtigen zijn.

“Op het eerste gezicht lijkt de productie van een product uitsluitend omdat het duur is, volledig verspillend,” werkte Szabo later uit in “Shelling Out”. “De onvervalsbaar dure grondstof voegt echter voortdurend waarde toe door welvarende overdrachten mogelijk te maken. Steeds meer van de kosten worden terugverdiend bij elke transactie die mogelijk wordt gemaakt of goedkoper wordt gemaakt. De kosten, aanvankelijk volledig verspild, worden omgeslagen over vele transacties.”

En ten derde, het was doorgaans vrij eenvoudig om vast te stellen dat het proto-geld inderdaad onvervalsbaar zeldzaam was, door simpelweg observaties of metingen te doen. De zeldzame slakkenhuisjes bijvoorbeeld, zou iedereen in deze stammen eenvoudig herkend hebben, terwijl het namaken ervan onmogelijk zou zijn geweest met de gereedschappen die ze ter beschikking hadden.

Szabo ontdekte dat de oudste vormen van geld meestal makkelijk te beveiligen waren en aantoonbaar moeilijk te verkrijgen.

Moderne fiatvaluta’s bezaten volgens velen in wezen geen van de drie kwaliteiten van proto-geld. Ze waren niet bijzonder gemakkelijk te beschermen tegen diefstal, en de meeste mensen deed zelfs geen poging om hun eigen geld te beveiligen, in plaats daarvan vertrouwden ze op derde partijen (banken) voor veilige bewaring. Maar wellicht nog belangrijker: fiatvaluta was niet fundamenteel schaars; regeringen en centrale banken konden naar believen meer drukken, of zelfs meer ervan digitaal maken.

Szabo benadrukte dat het drijvende fiatvalutasysteem dat al tientallen jaren de wereldstandaard was, een grote historische uitzondering was. Rekening houdend met de weinige soortgelijke voorbeelden waarvan hij wist - sommige in het dynastieke China, twee in het Frankrijk van de achttiende eeuw en de Confederatie dollar tijdens de Amerikaanse burgeroorlog - verwachtte hij niet dat het nieuwe monetaire experiment zou blijven duren. Hij was ervan overtuigd dat fiatvaluta uiteindelijk zouden ten onder gaan.

Veel Oostenrijkse economen waren uiteraard tot vergelijkbare conclusies gekomen als Szabo. Degenen die een terugkeer naar de goudstandaard voorstaan, geloven specifiek dat het edelmetaal de beste vorm van geld is, grotendeels vanwege de onvervalsbare schaarste ervan.

Szabo was echter niet overtuigd dat goud de beste vervanging was: hoewel het edelmetaal inderdaad moeilijk te verkrijgen was, was het ook moeilijk te beveiligen.

“Dure metalen en verzamelobjecten hebben een onvervalsbaar tekort vanwege de hoge creatiekosten. Dit gaf geld ooit een waarde die grotendeels onafhankelijk was van een vertrouwde derde partij. Edelmetalen hebben echter problemen. Het is te kostbaar om metalen steeds opnieuw te testen voor gewone transacties. Daarom werd een vertrouwde derde partij (meestal geassocieerd met een belastingontvanger die de munten accepteerde als betaling) gevraagd om een standaard hoeveelheid van het metaal in een munt te stempelen. Het vervoeren van grote hoeveelheden waardevol metaal kan zeer onzeker zijn, zoals de Britten ontdekten toen ze tijdens de Eerste Wereldoorlog goud vervoerden over een door U-boten geïnfecteerde Atlantische Oceaan naar Canada om hun goudstandaard te ondersteunen,” schreef Szabo.

Het spijt me, maar er lijkt een vergissing te zijn gemaakt bij het verstrekken van gegevens voor de vertaak. U heeft niet aangegeven welke specifieke tekst moet worden vertaald. Kunt u mij de te vertalen tekst geven? Dan kan ik u beter van dienst zijn.

“Erger nog, je kunt online niet betalen met metaal.”[^212]

De Cypherpunk wilde de wenselijke monetaire eigenschappen van goud reproduceren in een elektronisch geldsysteem - een digitale valuta met onvervalsbaar kostbaarheid.

Toen Adam Back in 1997 hashcash aankondigde, leek dit eindelijk mogelijk te zijn.

### Bit Goud

Minder dan een jaar later, in 1998, had Szabo zijn eigen voorstel voor een digitale munteenheid ontworpen: Bit Gold. Hoewel hij Bit Gold nog niet in code had geïmplementeerd - het was tot dan toe slechts een idee - deelde hij een beschrijving ervan op de Libtech lijst.

Net als Hashcash, was Bit Gold ontworpen rondom het concept ‘proof of work’. De vereiste rekenkracht om deze ‘proof of work’ te genereren koppelde de creatie van de valuta aan de kosten voor energie, met als gevolg iets wat lijkt op digitale schaarste. Vanuit Szabo’s visie vertegenwoordigde de ‘proof of work’ een onvervalsbaar waardevolle inzet.

Bit Gold’s proof-of-work systeem zou starten met een ‘kandidaat-string’ - in wezen een willekeurig getal. Het idee was dat iedereen deze string kon nemen en combineren met hun eigen nonce om iets te produceren dat lijkt op een hash.[^213] Volgens de aard van het hashen, zou de resulterende hash een nieuwe, schijnbaar willekeurige reeks getallen zijn. Herschreven: Het proof-of-work systeem van Bit Gold zou beginnen met een ‘kandidaat-string’, wat in feite een willekeurig getal is. De gedachte hierachter was dat iedereen deze string kon pakken en samenvoegen met hun eigen nonce om zo iets te creëren dat op een hash lijkt. Gezien de kenmerken van hashen, zou de daaruit voortkomende hash een nieuwe, op het eerste gezicht willekeurige, reeks cijfers zijn.[^213]

Het trucje, dat ook door hashcash wordt gebruikt, was dat niet alle hashes volgens het Bit Gold protocol als geldig werden beschouwd. In plaats daarvan moest een geldige hash beginnen met een vooraf bepaald aantal nullen. Door de onvoorspelbare aard van hashing, was de enige manier om zo’n hash te vinden door middel van trial and error, waarbij een nieuwe nonce werd gebruikt bij elke poging.

Wanneer iemand een geldige hash zou vinden, zou deze hash de nieuwe kandidaat-string worden. De volgende geldige hash zou dan gegenereerd moeten worden vanuit deze nieuwe kandidaat-string en een ander nonce. Zodra een tweede geldige hash gevonden zou worden, zou deze op zijn beurt de nieuwe kandidaat-string worden, en zo verder.

Het systeem van Bit Gold zou na verloop van tijd een lange reeks hashes genereren, waarbij de meest recente hash altijd fungeert als de nieuwe kandidaat-string.

Het geldgedeelte leek in grote lijnen op dat van de eerdere voorstel tot het bezit van cijfers van Hadon Nash aan de Cypherpunks-mailinglijst. Wie een geldige hash produceerde zou letterlijk dit hash “bezitten”. Eigendom van hashes zou worden vastgelegd in een digitaal eigendomsregister, waar alle hashes zouden worden toegewezen aan de publieke sleutels van hun eigenaren.[^214] Aangezien het register alleen publieke sleutels zou gebruiken - geen namen - kon Bit Gold vrij anoniem worden gebruikt.

Om een hasj “uit te geven”, zou de eigenaar een bericht moeten ondertekenen waarin wordt aangegeven wie de nieuwe eigenaar is (opnieuw, door naar deze persoon te verwijzen alleen door hun openbare sleutel). Als de digitale handtekening overeenkomt met de openbare sleutel die in het eigendomsregister staat vermeld, zou de overdracht geldig zijn en zou het register worden bijgewerkt om de nieuwe eigenaar van de hasj te reflecteren. Zonder een geldige handtekening, zou de overdracht afgewezen moeten worden en zou de hasj in het bezit blijven van de huidige eigenaar.

Het bewijs van werk zou ervoor zorgen dat Szabo’s elektronische geld aantoonbaar moeilijk te verkrijgen is, terwijl openbare-sleutelcryptografie het veilig zou maken.

Dat is natuurlijk onder de voorwaarde dat het register zelf veilig is.

### Het Register

Dus wie zou het register onderhouden?

Szabo begreep dat elke enkele entiteit die het register zou bijhouden, een vertrouwde derde partij zou zijn. Hoewel zelfs deze derde partij niet in staat zou zijn om bewijs van werk te vervalsen - iedereen kon onmiddellijk herkennen dat de hashes ongeldig zijn - kon het potentieel nog steeds hashes dubbel uitgeven, of transacties censureren, of misschien zelfs hashes stelen van andere gebruikers.

In Szabo’s voorstel zou het eigendomsregister dus onderhouden worden door een Bit Gold “eigendomsclub”. Deze club bestond uit “clubleden” (oftewel internetservers) die het eigendomsregister tussen hen zouden dupliceren en gezamenlijk bijhouden wie wat bezit. Als een van de clubleden zou proberen vals te spelen of te stelen, zouden de andere clubleden dit opmerken en de overdracht afwijzen, waardoor het vertrouwen tussen hen wordt verdeeld.

Szabo stelde voor om dit te implementeren met behulp van dezelfde soorten verdeelde rekenprotocollen die hij voorzag voor slimme contracten. Uitgelegd in zijn paper “Veilige Eigendomstitels met Eigenaarsautoriteit”, waren deze ontwerpen het best te begrijpen als geavanceerde stemsystemen; zolang de meeste servers eerlijk bleven, zouden ze consensus bereiken over de toestand van het register. Als slechts een minderheid van de servers zou falen of uit de pas zou lopen, zou het systeem als geheel prima moeten blijven functioneren.

Dit was echter niet perfect; het zogeheten Byzantijnse Generaalsprobleem was niet volledig opgelost. Er konden vooral vervelende problemen ontstaan als het register het doelwit zou worden van een Sybil-aanval. In dit soort computer aanval slaagt één kwaadwillig persoon erin zich voor te doen als meerdere verschillende deelnemers, waardoor de stemprocedures worden overrompeld. Szabo zou dit later omschrijven als het “Sokpop probleem”. [^215]

Toch geloofde Szabo dat dit zichzelf zou kunnen oplossen. Hij opperde dat zelfs in een scenario waarin een meerderheid van de clubleden zou proberen te valsspelen, het register openbaar zou zijn. Dus cryptografische bewijzen zoals (het ontbreken van) geldige handtekeningen konden worden gebruikt om Bit Gold-gebruikers op de hoogte te stellen van dit wangedrag. De eerlijke minderheid van registerbeheerders kon dan afsplitsen om een concurrerend eigendomsregister te creëren. Wanneer ze de keuze hadden tussen een aantoonbaar oneerlijk meerderheidsregister of een eerlijk minderheidsregister, achtte Szabo het waarschijnlijk dat gebruikers de laatste zouden prefereren.

“Als de regels worden overtreden door de winnende stemmers, kunnen de correcte verliezers de groep verlaten en een nieuwe groep vormen, waarbij ze de oude titels erven,” legde hij uit. “Gebruikers van de titels (vertrouwende partijen) die correcte titels willen behouden, kunnen zelf veilig verifiëren welke afsplitsing de regels correct heeft gevolgd en overschakelen naar de juiste groep.”[^216]

Szabo was zich ervan bewust dat het niet de meest elegante oplossing was en er bleven nog belangrijke vragen onbeantwoord: in het geval van een dubbele uitgave-aanval, hoe zouden offline gebruikers weten welke transactie eerst kwam? En in het verlengde daarvan, als deze dubbele uitgave zou resulteren in het creëren van een concurrerend register omdat verschillende leden van de eigendomsclub verschillende transacties eerst zagen, hoe zouden deze gebruikers dan weten welke ‘correct’ is?

Desondanks zag Szabo dit in zijn ogen als een betere oplossing dan vertrouwen op een derde partij.

### Het Beheersen van Inflatie

Het laatste probleem dat Szabo moest oplossen was inflatie.

Naast de onmogelijkheid om het eigendom van het bewijs van werk over te dragen, had het ‘hashcash’-systeem van Adam Back nog een groot probleem. Het genereren van geldige hashes zou na verloop van tijd eenvoudiger worden, aangezien computers elk jaar krachtiger werden. Daarom konden de hashes niet goed functioneren als geld: hyperinflatie (of zelfs alleen al de vooruitzichten van hyperinflatie) zou waarschijnlijk maken dat zo’n munteenheid niet van de grond zou komen.

Szabo bedacht ook hiervoor een oplossing.

Omdat alle geldige Bit Gold hashes dienst deden als kandidaat-reeksen voor de volgende hash, werden ze noodzakelijkerwijs tijdgestempeld, in die zin dat de volgorde ervan niet kon worden veranderd. Bovendien konden nieuwe hashes mogelijk afzonderlijk worden tijdgestempeld op daadwerkelijke tijd-stempelservers om een registratie bij te houden van wanneer ze werden gegenereerd.

Szabo legde uit dat deze tijdstempels een goed idee zouden geven van hoe moeilijk het moet zijn geweest om een Bit Gold-hash te produceren: een oudere hash zou moeilijker te produceren zijn geweest dan een recentere hash.

Deze verschil moet dan volgens Szabo meegenomen worden in de waarde van een hash:

“De kosten van de reeks zijn evenredig met de onwaarschijnlijkheid van de reeks. We hebben empirisch bewijs dat aantoonbaar onwaarschijnlijke documenten, bijvoorbeeld zeldzame drukfouten op postzegels, behoorlijk waardevol worden - hoe zeldzamer en hoe verifieerbaarder, hoe waardevoller.”[^217]

Met andere woorden, een geldige “1998 hash” zou meer waard moeten zijn dan een geldige “2008 hash.”

Om de waarde van de hashes vast te stellen, wilde Szabo gebruikmaken van een beproefde en oude oplossing: de markt. Hij wilde een speciale marktplaats creëren waar Bit Gold hashes tegen elkaar verhandeld konden worden. Kopers en verkopers kunnen op die manier een eerlijke relatieve prijs voor elk van hen vinden. Misschien zou één hash uit 1998 het kunnen opnemen tegen tien hashes uit 2008, waarbij de exacte wisselkoers vermoedelijk zou worden bepaald door de gedaalde kosten van rekenkracht gedurende dat decennium.

Maar dit zou nog een ander probleem creëren, wist Szabo: “de bits (de puzzeloplossingen) van de ene periode [. . .] naar de volgende zijn niet verhandelbaar.”[^218]

De Cypherpunk begreep dat fungibiliteit - waarbij elke eenheid van een valuta gelijk is in waarde aan elke andere eenheid van dezelfde denominatie - een cruciale eigenschap is van geld. Een winkelier moet een betaling kunnen accepteren zonder te hoeven nadenken over de exacte waarde van het ene bankbiljet ten opzichte van het andere; elk dollarbiljet zou moeten volstaan. Als hashes verschillend gewaardeerd zouden worden, zou het de fungibiliteit van Bit Gold verbreken.

Nick Szabo, de bedenker van ‘Bit Gold’, heeft ook hiervoor een oplossing bedacht: hij zag een ‘vrije bank’ geïnspireerde ‘tweede laag’ bovenop de ‘basisslaag’ van Bit Gold voor zich. Deze tweede laag zou bestaan uit een speciaal soort banken, die veilig controleerbaar zouden moeten zijn vanwege het openbare karakter van het Bit Gold-register. Deze banken zouden verschillende hashes uit verschillende tijdperioden verzamelen en, op basis van hun relatieve marktwaarde, deze bundelen tot pakketten met een standaardwaarde. Een pakket van bijvoorbeeld “1998” zou slechts één hash kunnen bevatten, terwijl een pakket van “2008” er tien zou bevatten.

Deze pakketten zouden uiteindelijk opgesplitst worden in een specifiek aantal eenheden, wellicht uniek per bank. Alice Bank kon bijvoorbeeld 10,000 Alicebucks per bundel uitgeven, of deze bundel nu een 1998 pakket of een 2008 pakket was. Het zijn deze eenheden die uiteindelijk als het onderling inwisselbare geld gebruikt zouden worden door reguliere gebruikers voor dagelijkse uitgaves, idealiter in de vorm van privé, Chaumiaanse eCash. Tegelijkertijd zouden gebruikers van Alice Bank altijd in staat moeten zijn om hun Alicebucks in te wisselen voor de daadwerkelijke hashes die deze onderbouwen.

“Samengevat,” concludeerde Szabo zijn voorstel, “is al het geld dat de mensheid ooit heeft gebruikt op de een of andere manier onzeker geweest. Deze onzekerheid heeft zich op vele manieren gemanifesteerd, van vervalsing tot diefstal, maar de meest schadelijke is waarschijnlijk inflatie geweest. Bit gold kan ons mogelijk een geldvorm geven met een ongekende veiligheid tegen deze gevaren.”[^220]

Nick Szabo had gelijk - tenminste in theorie. Waar hashcash het concept van digitale schaarste had geïntroduceerd, liet het voorstel van Bit Gold zien hoe dit kan worden omgezet in overdraagbaar elektronisch geld.

## Hoofdstuk 12: B-geld (en BitTorrent)

Niet lang nadat Bit Gold had laten zien hoe proof-of-work in overdraagbaar elektronisch geld kon worden omgezet, werd er een enigszins vergelijkbaar voorstel voor digitale valuta ingediend bij de Cypherpunks mailinglijst. De auteur, Wei Dai, was een bekende naam binnen de Cypherpunk gemeenschap, maar dan alleen bij naam.

Inderdaad, privacy was het oprichtingsbeginsel van de Cypherpunks, maar weinigen lukte het om deze principes zo effectief uit te voeren als Wei Dai. Hoewel zijn betrokkenheid bij de Extropians het vermoeden wekte dat hij in de Bay Area woonde, verscheen Dai nooit bij de persoonlijke bijeenkomsten van de Cypherpunks. Gedurende enige tijd waren de leden van de mailinglijst niet eens zeker of ze correspondentie voerden met een man of een vrouw. Hun onzekerheid ging zo ver dat de Cypherpunks zich zelfs afvroegen of Dai wel echt bestond, speculerend dat de naam wellicht een pseudoniem was; sommigen vermoedden dat het eigenlijk een alter-ego van Nick Szabo was.

In werkelijkheid was Wei Dai - een hij - een jonge informaticus die toevallig enkele jaren jonger was dan Szabo aan de Universiteit van Washington – hoewel de twee elkaar nooit op de campus hebben ontmoet. Als liefhebber van cyberpunk boeken, had Dai als student een interesse ontwikkeld in cryptografie omdat hij geloofde dat het de mensheid kon helpen beschermen tegen toekomstige entiteiten zoals de Blight, een kunstmatige superintelligence die diende als de voornaamste antagonist in Vernor Vinge’s roman ‘A Fire Upon the Deep’.[^221]

Zijn interesse in cryptografie leidde Dai uiteindelijk naar de Cypherpunks mailinglijst, waar hij kennis maakte met de talrijke bijdragen van Tim May. Terwijl hij zich verdiepte in Mays visie op de toekomst van de samenleving, raakte de jonge informaticus nog meer gefascineerd door het transformatieve potentieel van cryptografie, nu met een sterke nadruk op privacy en vrijheid van overheidsinmenging.

Dai, wiens naam aangeeft dat hij van Chinese afkomst is, begon zich uiteindelijk te mengen in de gesprekken op de Cypherpunks mailinglijst. In het midden van de jaren ’90 betrok Dai zichzelf bij discussies over allerlei onderwerpen, variërend van de economie van digitale reputatiesystemen tot de toepassing van speltheorie op het gebied van cryptografie, voorstellen om traceerbare betalingssystemen om te zetten in anonieme, en nog veel meer.

Gedurende deze jaren nam Dai de filosofie en missie van de Cypherpunks als zijn eigen aan.

“Er heeft nooit een regering bestaan die niet vroeg of laat probeerde de vrijheid van haar onderdanen te verminderen en meer controle over hen te verkrijgen, en waarschijnlijk zal er nooit een dergelijke regering zijn” vat Dai op een bepaald moment samen wat hij beschouwt als de bindende ethos van de beweging. “Daarom zullen we, in plaats van te proberen onze huidige regering te overtuigen om het niet te proberen, de technologie (bijvoorbeeld, remailers en elektronisch geld) ontwikkelen die het voor de regering onmogelijk zal maken om te slagen.” [^222]

Cypherpunks schrijven code.

Ook Wei Dai ontwikkelde een aantal tools om de Cypherpunk-zaak te bevorderen. Dit bevatte een versleuteld tunneling-protocol (dat de overdracht van data van het ene netwerk naar het andere mogelijk maakte), een veilig systeem om bestanden te delen en de Crypto++ softwarebibliotheek (die vrij beschikbare cryptografische algoritmen bevat geschreven in de programmeertaal C++). Door zijn werk in codering en zijn doorgaans intelligente en inzichtelijke e-mails, verdiende Dai’s bijdragen hem een reputatie als een van de meest productieve en waardevolle deelnemers aan de Cypherpunks mailinglijst - ondanks zijn meer ongrijpbare persoonlijkheid.

Hoewel het op het eerste gezicht vreemd kan lijken, is het niet zo ongelooflijk dat sommigen vermoeden dat Nick Szabo en Wei Dai eigenlijk dezelfde persoon zijn: de twee hadden veel gemeen. Naast het volgen van dezelfde universitaire studies en deel uitmaken van zowel de Cypherpunk als de Extropian gemeenschappen, hadden Szabo en Dai een bijzondere interesse in elektronisch geld, en om vele van dezelfde redenen. Ze wilden helpen om Tim May’s “Galt’s Gulch in cyberspace” te realiseren, en beiden begrepen het belang van digitale contracten in deze context.

In november 1998, net na zijn afstuderen aan de universiteit, kondigde Wei Dai informeel zijn eigen elektronisch geldvoorstel aan. Dit voorstel werd bijna terloops aangekondigd in een mail waarin hij ook een geüpdatete versie van zijn anoniem communicatieprotocol, bekend als PipeNet, bekendmaakte. Dit gebeurde slechts weken nadat Szabo voor de eerst zijn digitale munteenheid systeem besprak op de Libtech mailinglijst. Dai, die ook actief was op deze lijst, had b-geld gecreëerd.

“Ik ben gefascineerd door Tim May’s crypto-anarchie,” legde Dai zijn motivatie uit in het voorstel. “In tegenstelling tot de gemeenschappen die traditioneel geassocieerd worden met het woord ‘anarchie’, wordt in een crypto-anarchie de regering niet tijdelijk vernietigd, maar permanent verboden en overbodig. Het is een gemeenschap waar de dreiging van geweld machteloos is omdat geweld onmogelijk is, en geweld onmogelijk is omdat de deelnemers niet in verband kunnen worden gebracht met hun daadwerkelijke namen of fysieke locaties.”

Het spijt me, maar er is geen tekst die vertaald moet worden. De zin “To conclude:” op zich staat, biedt geen inhoud om te vertalen naar het Nederlands.

…mmarie…t is november 1998. Wei Dai, een recent afgestudeerde, brengt onopvallend zijn eigen voorstel voor elektronisch geld naar voren, haast als een voetnoot in de bijgewerkte versie van zijn anonieme communicatieprotocol, PipeNet. Hij kondigde dit aan in dezelfde e-mail waarin hij ‘b-geld’ had ontworpen, slechts enkele weken nadat Szabo zijn digitale muntsysteem had beschreven op de Libtech-mailinglijst, waar Dai ook actief was. Het protocol dat in dit artikel wordt voorgesteld, maakt het mogelijk voor ontraceerbare pseudonieme entiteiten om efficiënter samen te werken, door hen te voorzien van een ruilmiddel en een manier om contracten af te dwingen. [. . .] Ik hoop dat dit een stap is in de richting van het praktisch mogelijk maken van crypto-anarchie, naast de theoretische mogelijkheid.”[^224]

### B-geld

B-geld leek in belangrijke opzichten op Bit Gold - hoewel het op andere punten verschilde.

Net als Bit Gold, zou b-money in principe bestaan op een grootboek (wat Szabo een “register” noemde). Dit grootboek zou openbare sleutels vermelden, en het aantal toegeschreven munteenheden aan elke openbare sleutel aangeven. Om de elektronische contant geld te verplaatsen, zouden gebruikers cryptografisch een bericht ondertekenen dat aangeeft hoeveel munteenheden er worden uitgegeven van de bijbehorende openbare sleutel, en naar welke openbare sleutel ze werden uitgegeven. Als de transactie geldig was (de openbare sleutel had voldoende geld en de handtekening klopte), zou het grootboek dienovereenkomstig worden bijgewerkt.

Net zoals Szabo, legde Dai een sterke nadruk op het belang van contracten. B-geld was ontworpen om de nakoming van contracten te vergemakkelijken, en een significant deel van het voorstel was gewijd aan het uitleggen van de taken van bemiddelaars in geschillenoplossing. (Hoewel het niet helemaal de autonome slimme contracten waren die Szabo oorspronkelijk in gedachten had, waren er enige cryptografische veiligheidsmaatregelen opgesteld om bepaalde vormen van fraude te voorkomen.)

Szabo was er ook in geslaagd om Wei Dai ervan te overtuigen dat het minimaliseren van vertrouwen essentieel was. Vertrouwde derde partijen zijn beveiligingsrisico’s, gaf Dai toe, en hij kwam tot de conclusie dat een elektronisch geldsysteem niet zou mogen leunen op één enkele entiteit om de saldo’s van gebruikers bij te houden, transacties mogelijk te maken of dubbele uitgaven te voorkomen.

In plaats daarvan bedacht Dai twee alternatieve oplossingen.

De eerste variant van b-geld was met name zeer ambitieus. In deze variant was er geen centrale instantie, maar onderhield elke gebruiker van het systeem zijn eigen exemplaar van het grootboek. Bij elke nieuwe b-geldtransactie zou iedere gebruiker afzonderlijk de geldigheid ervan controleren en hun eigen versie van het grootboek bijwerken als de transactie in orde bleek. Zolang iedereen actueel bleef, zouden de grootboeken gesynchroniseerd blijven onder alle gebruikers.

In theorie is het grote voordeel van zo’n gedistribueerd systeem dat corruptie onmogelijk zou zijn. Als iemand bijvoorbeeld te veel geld toeschrijft aan zijn eigen publieke sleutels, zou dit geen enkel effect hebben op iemand anders; alle andere grootboeken zouden onveranderd blijven. Als de bedrieger zou proberen zijn vervalste geld uit te geven, zou niemand anders die transactie als geldig zien. Net zoals bij de tijdstempeloplossing van Scott Stornetta en Stuart Haber zou iedereen ervoor zorgen dat iedereen anders eerlijk zou blijven.

Het leek ideaal om het grootboek over alle gebruikers te verspreiden - in theorie.

Helaas wist Wei Dai dat het in de praktijk niet haalbaar zou zijn. Om dubbele uitgaven te voorkomen, vereiste het systeem een “synchroon en onverstoorbaar anoniem uitzendkanaal”[^225]. Alleen als alle gebruikers zeker konden zijn dat zij allemaal dezelfde transacties ontvingen in precies dezelfde volgorde, kon iedereen er vertrouwen in hebben dat hun grootboeken gesynchroniseerd waren en dat een betaling die zij zouden ontvangen door iedereen anders ook zou worden geregistreerd. Dit leek onwerkbaar; dubbele uitgavetransacties konden tegelijkertijd naar verschillende delen van het netwerk worden gestuurd, terwijl onbetrouwbare deelnemers eenvoudigweg konden liegen over de volgorde van de transacties die ze hadden ontvangen.

In technische termen: Wei Dai’s eerste oplossing negeerde het Byzantijnse generaalsprobleem.

Dit is waarom Dai met een tweede oplossing kwam in hetzelfde voorstel.

In deze tweede versie van het b-geld systeem, zou niet iedereen een versie van het hoofdregister bijhouden. In plaats daarvan zou het systeem bestaan uit twee soorten deelnemers: reguliere gebruikers en “servers”. Net zoals de “eigendomsclub” van Szabo’s Bit Gold voorstel, zouden alleen deze servers de b-geld hoofdregisters bijhouden. Om er zeker van te zijn dat een transactie werd voltooid, zouden reguliere gebruikers moeten checken met een willekeurige subset van de servers, en een betaling pas als final beschouwen als al deze servers deze erkenden.

Natuurlijk, bracht dit wel weer wat vertrouwen terug in het systeem. De servers hadden potentieel wel de mogelijkheid om samen te werken om overdrachten te blokkeren, transacties dubbel uit te geven, mogelijk fondsen te stelen of zelfs regelrecht geld voor zichzelf te creëren.

Wei Dai stelde daarom een manier voor om de servers eerlijk te houden.

“Hij stelde voor dat elke server verplicht is om een bepaald bedrag in een speciale rekening te storten, dat zou worden gebruikt als potentiële boetes of beloningen voor bewijzen van wangedrag”, stelde hij voor. “Ook moet elke server periodiek zijn huidige geldcreatie en geldbezit databases publiceren en zich daaraan committeren. Elke deelnemer moet controleren of zijn eigen rekeningsaldi kloppen en dat de som van de rekeningsaldi niet groter is dan het totale bedrag aan gecreëerd geld.”

Echter, het voorstel van b-geld ging niet in detail in op een van deze oplossingen. Wellicht het meest problematisch was dat Dai niet uitlegde wie zou bepalen of er wangedrag plaatsvond, als dit niet werd bepaald door de (samenzwerende) servers zelf, of hoe de boetes konden worden afgedwongen. Net zoals Bit Gold geen oplossing had geboden om conflicten tussen servers te beslechten, had b-geld dat ook niet gedaan.

### B-geld’s Monetaire Beleid

Net als Bit Gold zou b-geld een zuiver digitale munteenheid zijn. Er zou geen bank of bedrijf zijn die de digitale eenheden ondersteunt met dollars of goud, en uiteindelijk geen garantie dat iemand de munteenheid zou accepteren voor betaling.

Maar net zoals Szabo, dacht Dai niet dat dit een probleem zou zijn.

“Denk er op deze manier over na,” betoogde hij op de Cypherpunks mailinglijst. “In het geval van commodity geld, wordt de waarde deels bepaald door de industriële/esthetische waarde van de commodity en deels door het nut van het commodity geld als ruilmiddel. In het geval van fiat geld en b-geld, komt alle waarde voort uit het nut als ruilmiddel.”[^226]

In tegenstelling tot Szabo, wilde Dai zijn valuta echter voorzien van een gericht monetair beleid. Waar de koopkracht van Bit Gold overgelaten zou moeten worden aan de markt, met geldige proof-of-work hashes die vrij verhandeld worden voor wat kopers en verkopers bereid zijn te accepteren, was b-geld specifiek ontworpen om een voorspelbare koopkracht te bieden.

Net als Irving Fisher en de Stable Money Association ongeveer 80 jaar eerder, stelde Dai voor om de koopkracht van zijn munteenheid te koppelen aan een consumentenprijsindex. Hij wilde dat dezelfde hoeveelheid b-geld-eenheden op elk moment een gelijk aandeel van deze index zou kunnen kopen. Met andere woorden, de gemiddelde prijs van goederen en diensten, uitgedrukt in b-geld, moest stabiel blijven.

Als we het breder bekijken, zou het creëren van valuta in b-geld vergelijkbaar werken met Bit Gold: iedereen zou nieuwe valuta-eenheden kunnen genereren door middel van een bewijs van werk door een geldige hash te produceren, vermoedelijk ook gebaseerd op een bepaalde string. Wie de hash creëerde, mocht deze houden. (Of misschien zouden ze een equivalent in b-geld-eenheden krijgen; een geldig bewijs van werk zou heel goed op de grootboek kunnen worden weerspiegeld als 100 digitale “munten.”)

Het belangrijkste verschil met Bit Gold, was echter dat de moeilijkheidsgraad om een geldig bewijs van werk te genereren, kon veranderen.

Alle gebruikers van het systeem (b-geld versie 1) of de servers (b-geld versie 2) zouden voortdurend moeten bepalen hoeveel een mandje goederen zou kosten in verhouding tot de productie van een geldige hash. Dat wil zeggen, als het creëren van een hash goedkoper wordt (door verbeteringen in computerhardware) in verhouding tot de prijsindex, dan zou de moeilijkheidsgraad om een geldige hash te produceren naar boven moeten worden bijgesteld: de hash zou met meer nullen moeten beginnen. Een nieuwe hash zou dan alleen aan het grootboek worden toegevoegd als aan de meest recente drempelwaarde was voldaan.

Als alternatieve benadering om een vergelijkbaar resultaat te bereiken, wat Wei Dai vermeldde in de bijlage van zijn voorstel, kon het aanmaken van geld gebeuren via een veiling. In dit geval zouden alle gebruikers (b-geld versie 1) of de servers (b-geld versie 2) eerst de optimale uitbreiding van de geldvoorraad bepalen, waarna deze nieuwe eenheden b-geld geveild zouden worden aan degene die bereid en in staat was om het met het meeste bewijs van werk te betalen.

Een grote voordeel van deze benaderingen was dat alle b-geld hashes, ongeacht wanneer ze werden gecreëerd, dezelfde waarde zouden moeten hebben: ze zouden fungibel zijn. Dit elimineerde de noodzaak om een hele andere bank laag te ontwerpen bovenop de basislaag van de valuta, zoals Szabo had voorgesteld voor Bit Gold.

Het was een innovatieve aanpak, maar opnieuw bleef er veel ongespecificeerd. Zowel voor de aanpassingsmethode voor de moeilijkheidsgraad als het veilingmodel, bleef het onduidelijk in het voorstel van b-geld hoe gebruikers (of servers) zouden beslissen over de volgende moeilijkheidsgraad voor proof-of-work, of de optimale toename van de geldvoorraad… en hoe geschillen in dit deel van het proces zouden kunnen worden opgelost. (Het Byzantijnse Generaalsprobleem kwam inderdaad het hele voorstel door terug.)

“B-geld was nog niet een volledig praktisch ontwerp,” erkende Dai later. [^227] Het voorstel bood een ruwe schets van hoe een elektronisch geldsysteem eruit zou kunnen zien, maar er waren nog meerdere problemen die moesten worden opgelost voordat het als een daadwerkelijke digitale valuta zou kunnen functioneren.

Dai zelf besloot echter dat hij niet degene zou zijn die deze problemen zou oplossen.

### Ontgoocheling

In zijn voorstel voor b-geld leek Wei Dai nog altijd optimistisch over de mogelijkheden en potentie van Tim May’s crypto-anarchistische visie. Maar in werkelijkheid was de ongrijpbare informaticus al begonnen met het opgeven van de droom van de Cypherpunk.

“Ik ben niet verder gegaan met het ontwerpen omdat ik, tegen de tijd dat ik klaar was met het opschrijven van b-geld, eigenlijk al wat gedesillusioneerd was geraakt door cryptoanarchy”, herinnerde Dai zich later. “Ik had niet voorzien dat een systeem zoals dat, eenmaal geïmplementeerd, zoveel aandacht en gebruik zou aantrekken buiten een kleine groep van hardcore cypherpunks.”[^228]

Dai’s ontgoocheling weerspiegelde een groeiend sentiment binnen de Cypherpunk-gemeenschap tegen het einde van de jaren 90. Het internet was inmiddels echt mainstream geworden, maar de Cypherpunks ontdekten dat het grote publiek nogal onverschillig was over online privacy. Het leek erop dat de meeste mensen er volkomen tevreden mee waren om betalingsverwerkers volledig inzicht te geven in hun uitgavenpatroon, en ze leken er ook geen probleem mee te hebben om een ​​spoor van hun andere online activiteiten achter te laten. De gemiddelde internetgebruiker dacht zelfs niet eens aan het versleutelen van hun e-mails.

Sinds de Cypherpunks voor het eerst bijeen kwamen in het ongemeubileerde appartement van Eric Hughes, hadden ze bijna tien jaar besteed aan het transformeren van revolutionaire crypto-protocollen in werkende software. Tot hun grote teleurstelling bleek dat bijna niemand hierin geïnteresseerd was. Het doorzettingsvermogen in hun activisme voor privacy had hen weliswaar geholpen de cryptoorlogen te winnen, maar dit leek nu een tamelijk nutteloze inspanning te zijn geweest. De meeste internetgebruikers bleken namelijk perfect op hun gemak met het opgeven van zowat al hun persoonlijke informatie in ruil voor iets meer gemak.

Hughes had zich inmiddels vrijwel volledig teruggetrokken uit de gemeenschap en de mailinglijst. Maar niet voordat hij zijn nuchtere herbeoordeling van de filosofie “cypherpunks schrijven code” had aangeboden, kenmerkend voor de recente desillusie van Wei Dai, hemzelf en andere Cypherpunks.

“Misschien is het belangrijkste dat ik van de cypherpunks heb geleerd dat alleen code niet voldoende is. Niet alleen code, niet wijdverspreide code, zelfs niet veelgebruikte code,” schreef Hughes aan de Cypherpunks mailinglijst. “Er is een zekere mate van tolerantie in de samenleving nodig voor activiteiten die in privé worden ondernomen voor langdurig succes. Niet alleen gemakkelijk of makkelijker, maar noodzakelijk.”[^229]

Hughes was tot het inzicht gekomen dat het essentieel was dat het grote publiek zou begrijpen waarom privacy belangrijk was. Code was uiteraard ook nog steeds nodig — code maakte privacy in eerste instantie mogelijk. Maar hij geloofde nu dat code uiteindelijk alleen maar nuttig was als er een brede publieke consensus bestond dat mensen daadwerkelijk het recht zouden moeten hebben om hun privacy te beschermen. Zonder zo’n publieke consensus zou het gebruik van cryptografie kunnen worden gemarginaliseerd en wellicht zelfs verboden, met als risico dat de overblijvende gebruikers mogelijk zouden worden geviseerd en vervolgd.

“Hetzelfde geldt voor anonieme transacties”, schreef Hughes. “Tenzij er een soortgelijke consensus bestaat, zullen we weer te maken krijgen met een marginale activiteit. Ik beschouw dit als een verlies.”[^230]

Het optimisme en de assertiviteit die de beweging in de begindagen kenmerkten, werden steeds meer overschaduwd door een gevoel van somberheid en verlatenheid.

In plaats daarvan kwamen sommige van de meer hoopvolle impulsen voor de Cypherpunk-missie in de late jaren ’90 van relatieve buitenstaanders van de gemeenschap.

### Zero-Knowledge Systems

De Canadese broers Austin en Hamnett Hill waren nog maar halverwege de twintig toen ze TotalNet, de internetprovider die ze hadden opgericht en die de derde grootste van hun land werd, verkochten. Met wat geld in hun handen en tijd om te besteden, zochten de twee naar hun volgende project toen ze op de Cypherpunks mailinglijst stuitten, en raakten ze volledig in de ban van het techno-libertarische ethos van de beweging.

In 1997 besloten de twee broers, samen met hun vader Hammie Hill, om hun middelen, connecties, en zakelijke talenten in te zetten, en richtten ze Zero-Knowledge Systems op. Het nieuwe bedrijf nam zich voor om de visie van de Cypherpunks werkelijkheid te laten worden, en om er tegelijkertijd ook wat geld mee te verdienen.

In het middelpunt van de startup was een privacy netwerk dat ze “Vrijheid” noemden. Vrijheid was gebaseerd op Wei Dai’s PipeNet, het anonieme communicatieprotocol waarvan een bijgewerkte versie zou worden aangekondigd in dezelfde Cypherpunks-mailinglijstpost die b-geld introduceerde. Net als PipeNet, werden in Vrijheid’s verhullingstechnieken een geavanceerdere variant van David Chaum’s originele remailer-protocol ingebed, maar waar remailers alleen e-mails anonimiseerden, paste Vrijheid de mengtechnologie toe om alle soorten internetgegevens te verbergen: e-mails, web browsing, tekst-chat en meer.

Gebruikers van Freedom konden in wezen op het internet “inloggen” onder verschillende identiteiten: misschien een reguliere identiteit voor professioneel werk, een pseudonieme identiteit voor politieke betrokkenheid, en nog een pseudoniem voor seksueel getinte webactiviteiten. Niemand, zelfs Zero-Knowledge Systems niet, zou in staat zijn de pseudonieme online identiteiten te koppelen aan een echte identiteit, of aan andere pseudoniemen.

De start-up wekte behoorlijk wat interesse op binnen de Cypherpunk-gemeenschap en, belangrijker nog, de oprichters van Zero-Knowledge Systems wisten de durfkapitalisten uit te leggen waarom ze de kans niet mochten missen om te investeren in de toekomst van privacy. Binnen een paar jaar slaagde de start-up erin om tientallen miljoenen dollars op te halen.

Waarschijnlijk konden de Hills beter verkopen dan de meeste Cypherpunks. Ze wisten ook op een goede manier de ambitieuze doelen van Zero-Knowledge Systems aan het grote publiek te presenteren. Er verschenen aantrekkelijke printadvertenties in bekende tijdschriften zoals Wired, Forbes en Fortune, met teksten als “Ik ben geen stuk van je inventaris”, “Ik ben een individu en je zult mijn privacy respecteren” en “Op het net heb ik de controle”. Bijzonder scherpe lezers konden ook een verborgen boodschap ontrafelen uit een binaire code op de pagina’s, die zich vertaalde naar “Wie is John Galt?” - een beroemde zin uit Ayn Rand’s Atlas Shrugged.

En wellicht nog het belangrijkst van alles, Zero-Knowledge Systems wist de top van het talent in de privacy-sector aan te trekken. Enkele van de bekendste cryptografen en computerwetenschappers op de Cypherpunks-mailinglijst besloten zich bij de start-up te voegen, waaronder Ian Goldberg - die tijdens de Crypto Wars het crypto-protocol SSL van Netscape had doorbroken en het bedrijf als ‘Hoofdwetenschapper en Hoofd Cypherpunk’ zou dienen - en Adam Back. Stefan Brands, de uitvinder van Brands Cash, werd ook aangenomen en zijn patenten op elektronisch geld werden eveneens door de start-up gekocht.

De Hills waren zeker niet kort van ambitie. Freedom was het hoofdproject van het bedrijf, maar Zero-Knowledge Systems wilde uiteindelijk op een brede manier de idealen van Cypherpunk realiseren. Het onderzoeks- en ontwikkelingsteam van de startup, ook wel de “kwaadaardige genieën” genoemd, kreeg de taak om aanvullende producten te ontwerpen. Dit omvatte onder andere een elektronisch geldsysteem gebaseerd op het ontwerp van Brands, codenaam Zorkmid; een verwijzing naar de munteenheid van een vroeg online spel.

Echter, ondanks alles, leek één probleem aan te houden. De meeste internetgebruikers gaven gewoon niet veel om privacy.

Zero Knowledge Systems had het plan om tegen 2000 ruimte te bieden aan 2,5 miljoen gebruikers van Freedom. Maar hoewel de 250 medewerkers zich flink hebben ingezet om dit mogelijk te maken, waren er rond de eeuwwisseling slechts iets meer dan twaalfduizend actieve gebruikers op het netwerk. Dat is minder dan een procent van het oorspronkelijke doel.

Dit kwam deels doordat veel mensen moeite hadden met het installeren van de software, maar zelfs degenen die erin slaagden Freedom operationeel te krijgen, ontdekten dat hun internetsnelheid aanzienlijk afnam bij het gebruik van de service. Buiten een relatief technisch onderlegde kern van gebruikers (voornamelijk mannen tussen de 25 en 35 jaar) waren weinig mensen bereid dit voor lief te nemen, en daarnaast nog de jaarlijkse vergoeding van € 50 aan Zero-Knowledge Systems te betalen. Aan het einde van de rit zagen mensen gewoonweg geen reden om Freedom te gebruiken; de voordelen voor de privacy waren voor hen onzichtbaar.

Vertaald naar het Nederlands zou dit worden: “Of zoals Austin Hill het een paar jaar later uitlegde:”iedereen zegt dat ze om privacy geven, maar mensen zouden een DNA-monster geven voor een ‘gratis’ Big Mac.”[^231]” In mijn eigen woorden en aangepast naar natuurlijk klinkend Nederlands: “Of in de woorden van Austin Hill, een paar jaar later:”Iedereen beweert te geven om privacy, maar men zou zo een DNA-staal afstaan voor een ‘gratis’ Big Mac.”[^231]”

Om het bedrijf te redden, heeft Zero Knowledge Systems uiteindelijk haar strategie veranderd. In plaats van op de algemene internetgebruiker te focussen, zou de startup vanaf 2001 haar inspanningen richten op gevestigde bedrijven, zoals financiële instellingen en telecombedrijven. Ze boden hen beveiligde database- en communicatiesystemen aan. Tot grote ontsteltenis van zijn kleine, maar toegewijde gebruikersbasis werd Freedom stopgezet.

Hiermee liet de startup grotendeels het Cypherpunk ethos achter zich, en personen zoals Back en Brands vertrokken kort daarna. Toen het bedrijf uiteindelijk zijn naam veranderde in Radialpoint, was Zero Knowledge Systems in alle opzichten vervangen door een totaal ander IT-bedrijf.

Ondanks een hoopvol begin, was dit een nieuwe tegenslag voor het doel van de Cypherpunks.

### Mojo Nation

Nog een positieve impuls kwamen van twee tot dusver onbekende tieners die een compleet ander deel van de cyberspace ontregelden: in 1999 gooide Shawn Fanning en Sean Parker - achttien en negentien jaar oud respectievelijk - de digitale variant van een handgranaat recht in het hart van de muziekindustrie toen ze Napster lanceerden.

Napster was een krachtig idee om één specifieke, technische reden. In tegenstelling tot de meeste internetdiensten tot dat moment, die vertrouwden op een centrale server om gebruikers te voorzien van wat ze nodig hadden, was Napster ontworpen als een peer-to-peer (P2P) netwerk. De peers (Napster-gebruikers) op het Napster-netwerk fungeerden als gelijken, ze hielpen elkaar indien nodig; specifieker, ze deelden hun eigen muziekbestanden met elkaar. Omdat Napster zelf geen muziekbestanden verspreidde, dachten Fanning en Parker dat ze claims wegens inbreuk op auteursrechten konden omzeilen, terwijl gebruikers nog steeds gratis nummers konden downloaden.

Maar toen de populariteit van Napster ontplofte, lanceerde de muziekindustrie een succesvolle tegenaanval. Fanning en Parker deelden misschien zelf geen muziek, maar artiesten en platenmaatschappijen beweerden dat de service desondanks actief inbreuk maakte op het auteursrecht: Napster bood gebruikers een platform, het beheerde en bewaarde de indexen om alle muziekbestanden te vinden, en de service koppelde peers dienovereenkomstig. Al snel bezweken Fanning en Parker onder de enorme juridische druk, en in juli 2001 haalden ze Napster offline.

Uiteindelijk was Napster een kortstondig project. Het heeft echter in zijn paar jaar in de schijnwerpers de P2P-technologie gepopulariseerd, waardoor een hele nieuwe klasse van vernieuwers geïnspireerd werd. Alternatieve bestandsdelingsdiensten zoals Kazaa en eDonkey doken al snel op, elk van hen ontworpen om nog decentraler te zijn dan de creatie van Fanning en Parker. Gedurende de volgende paar jaar waren de makers van deze nieuwe protocollen betrokken bij een hoogtechnologisch kat-en-muis-spel met de platenlabels die probeerden hun projecten te sluiten.[^232]

De eenendertigjarige Cypherpunk, Jim McCoy, besloot dat hij ook wilde meespelen. Begin 2000 nam hij ontslag bij Yahoo - “Ik werd het zat om niets revolutionairs te doen”[^233] - en samen met verschillende andere Cypherpunks, waaronder DigiCash-alumnus Bryce “Zooko” Wilcox, richtte McCoy Autonomous Zone Industries op.

De naam van het bedrijf was geïnspireerd op “tijdelijke autonome zones”, een term die voor het eerst werd gebruikt in 1991 door de anarchist Hakim Bey om niet-permanente lokale samenlevingen te beschrijven die vrij zijn van de overheid. De startup zou een ambitieus open-source softwareproject genaamd Mojo Nation ontwikkelen. Net als Napster was Mojo Nation in essentie een P2P bestandsdeelsysteem. Maar McCoy, als ervaren Cypherpunk, had een paar extra tools in zijn crypto-gereedschapskist om het ontwerp van Fanning en Parker te verbeteren.

Een van Mojo Nation’s meest interessante innovaties was dat alle bestanden op het netwerk in kleine stukjes werden opgedeeld, gecodeerd en strategisch gekopieerd en verspreid over het netwerk. Als iemand een bestand ging downloaden, downloadden ze in feite al deze kleine gecodeerde stukjes van verschillende gebruikers over het netwerk, om uiteindelijk deze puzzelstukjes bij elkaar te brengen en in één keer het volledige bestand te decoderen. Omdat alle uploaders slechts een beetje bandbreedte nodig hadden om hun stukje te delen, kon de downloadsnelheid worden verhoogd. Dit stelde Mojo Nation-gebruikers in staat om grotere bestanden te delen dan de typische MP3’s. Bovendien bood het meer privacy: gebruikers die de gecodeerde stukjes deelden, wisten vaak niet wat voor soort inhoud ze deelden (of deze inhoud al dan niet auteursrechtelijk beschermd was.)

Daarnaast werden sommige taken die Napster nog steeds als een centrale coördinator uitvoerde, in Mojo Nation overgedragen aan de gebruikers. Gebruikers die als contenttrackers fungeerden zouden bijvoorbeeld de indexen van bestanden die op het netwerk werden gehost bijhouden, terwijl andere gebruikers, die als zoekagenten fungeerde, zoekopdrachten via deze indexen zouden aanbieden. Door dergelijke verantwoordelijkheden in de handen van de gebruikers te leggen, geloofde McCoy dat Mojo Nation niet vatbaar zou zijn voor het soort rechtszaken waarmee Napster te maken had gehad. In plaats daarvan zouden de gebruikers zelf verantwoordelijk zijn als ze de wetten van hun jurisdictie overtraden—maar al deze individuele mensen waren natuurlijk veel moeilijker te vinden dan Fanning en Parker dat waren geweest.

Wat dit alles liet draaien was wellicht de meest interessante functie van Mojo Nation: een digitale valuta genaamd Mojo.

### Mojo

Mojo is ontworpen als een niet-ondersteunde digitale valuta die eigenlijk alleen nuttig was binnen de context van het bestandsuitwisselingsnetwerk.

Specifiek had Mojo de taak om een markt voor bestandsdeling en andere taken mogelijk te maken. Waar Napster gebruikers hun eigen bestanden gratis deelden, konden Mojo Nation gebruikers elkaar betalen voor de service, en de prijzen zouden worden bepaald door vraag en aanbod. Iemand zou bijvoorbeeld kunnen aanbieden om 1.000 Mojo te betalen voor elk gecodeerd deel van een bestand dat weer in elkaar gezet kan worden als een DVD-rip van The Matrix; wie een of meerdere van deze gecodeerde delen had, kon het aanbod accepteren als ze dachten dat het hun tijd, moeite en bandbreedte waard zou zijn om ze te uploaden. De verdiende Mojo’s konden vervolgens worden gebruikt om andere diensten op het netwerk te kopen, of misschien in te ruilen voor dollars op een speciale Mojo-beurs.[^234]

“De mensen die betaald krijgen, zijn degenen die de diensten uitvoeren. Dus die agenten die je hebben geholpen om dat blok [bestand] te vinden, worden betaald,” legde McCoy uit. “De verspreide zoekagenten krijgen betaald. Alle verschillende blokservers waar je blokken van hebt gekocht krijgen betaald, en als de gebruiker via een relay-server werkte, hetzij omdat ze achter een firewall zaten of omdat ze hun privacy wilden beschermen, zou de persoon die die berichten doorgaf ook een deel van de betaling ontvangen.”[^235]

McCoy’s visie was dat heel Mojo Nation zou worden gestuurd door marktprocessen, waarbij de ene gebruiker’s probleem de volgende gebruiker’s gelegenheid was om wat geld te verdienen door het op te lossen. Dit zou het Mojo Nation-netwerk quasi-autonoom laten functioneren, hoopte de Cypherpunk, met zeer weinig dagelijkse betrokkenheid van Autonomous Zone Industries.

Een opvallende uitzondering op deze regel bestond echter wel. De munteenheid van Mojo, de Mojo zelf, werd beheerd door Autonomous Zone Industries, via een speciale tokenserver die de rekeningsaldi bijhield en dubbele uitgaven voorkwam. Bovendien functioneerde de server als een gecentraliseerde muntfabriek: het kon nieuwe Mojo uitgeven wanneer McCoy en zijn collega’s geloofden dat dit nodig was, zonder technische beperking op hoeveel ervan gecreëerd kon worden.

Dit resulteerde uiteindelijk in de vernietiging van de munteenheid. Toen sommige gebruikers slimmigheidjes ontdekten om anderen te bedriegen om hun munten naar hen te sturen, besloot het team van Mojo Nation de slachtoffers te compenseren met nieuw geld. Dit leidde uiteindelijk tot de uitgifte van zoveel Mojo dat het uiteindelijk resulteerde in hyperinflatie. Mojo was afhankelijk geweest van een vertrouwde derde partij - de muntfabriek - en dat vertrouwen was geschonden.

Voor iets als Mojo Nation om echt te werken, had het waarschijnlijk een onafhankelijke digitale munteenheid vereist.

” […] we bestudeerden MojoNation kritisch, omdat ons hoofddoel was - en tot op zekere hoogte nog steeds is - een werkzame gemeenschapsmunt voor p2p-diensten,” schreef informaticus Daniel A. Nagy kort na het einde van Mojo Nation aan Jim McCoy, “Als reden voor het falen, wezen we hyperinflatie aan. MN had geen inflatiebeperkende maatregelen en op den duur leidde dit ertoe dat de Mojo geheel werd geïnflateerd.”

Hij voegde eraan toe dat “Ik heb mij volledig ingekocht in de visie dat de wereld dringend behoefte heeft aan een p2p-cashsysteem. Zonder zo’n systeem zal e-commerce een grote PITA blijven.” [^236]

Dat gezegd hebbende, was het vertrouwen op een gecentraliseerd digitaal valutasysteem niet het enige probleem waarmee Mojo Nation te kampen had. Hoewel de software door meer dan 100.000 mensen werd gedownload en gebruikt,[^237] bleken meerdere onderdelen van het systeem erg moeilijk om draaiende te krijgen (en te houden). Met problemen variërend van netwerkinstabiliteit tot ontbrekende bestandsfracties en een gebrek aan vertrouwen tussen gebruikers,[^238] was de dienst waarschijnlijk te ambitieus voor het bescheiden budget van Autonomous Zone Industries: het bedrijf was binnen een paar jaar door zijn geld heen en de negatieve publiciteit rond Napster maakte het moeilijk om meer financiering te verkrijgen.

In 2002 zag McCoy zich gedwongen om de meeste werknemers te ontslaan.

### BitTorrent

Hoewel Mojo Nation ten onder ging, waren er enkele ontwikkelaars bij de startup die hun vooruitstrevende technologieën niet wilden laten vergaan. Zo besloot Wilcox bijvoorbeeld de code van Mojo Nation te kopiëren (forken) om een versie van het protocol genaamd Mnet uit te brengen. Daarnaast bracht ook een andere medewerker van Autonomous Zone Industries, de 28-jarige softwareontwikkelaar en Cypherpunk Bram Cohen, zijn eigen op Mojo Nation geïnspireerde bestandsdelingsoplossing uit.

Hij noemde het: BitTorrent.

Cohen had Mojo Nation in feite tot op de bot gestript. BitTorrent nam sommige van McCoy’s ideeën over, zoals het opdelen van bestanden in kleinere fracties. Maar verder was het protocol vrij eenvoudig: er waren geen ingebouwde content-trackers (indexen, torrent-bestanden genoemd, werden buiten het protocol onderhouden en verspreid), er waren geen zoekagenten (gewone websites, opnieuw buiten het protocol, konden gebruikers helpen specifieke torrent-bestanden te vinden), en er was geen eigen valuta.

BitTorrent had geen eigen munteenheid nodig, omdat niemand hoefde te betalen voor bestanden. In plaats daarvan uploaden gebruikers die de verschillende delen van een bestand downloaden deze delen gelijktijdig naar andere downloaders. Dit betekende dat bestanden technisch gezien altruïstisch gedeeld werden, maar op zo’n manier dat de last op hulpbronnen voornamelijk werd gedragen door degenen die ook profiteerden van de bestandsoverdrachten.

Met dat, had Cohen een echt peer-to-peer en volledig gedistribueerd bestandsoverdrachtprotocol ontworpen. Waar Napster’s P2P-netwerk effectief kon worden uitgeschakeld door juridische druk uit te oefenen op het bedrijf erachter en zelfs het veel ambitieuzere Mojo Nation niet kon functioneren zonder dat de Autonomous Zone Industries een valutasysteem voor het netwerk onderhield, was BitTorrent niet van enige betrouwbare derde partij afhankelijk.

Vanuit een juridisch oogpunt waren gebruikers nu voor het eerst volledig verantwoordelijk voor hun eigen file sharing activiteiten. Net als e-mail (SMTP) of zelfs het internet zelf (IP), was BitTorrent in wezen slechts een internetprotocol. Bram Cohen was op geen enkele wijze aansprakelijk voor hoe mensen het protocol gebruikten, zelfs al werd er op grootschalige wijze illegaal auteursrechtelijk beschermde bestanden uitgewisseld via BitTorrent.

Bovendien, als Cohen om welke reden dan ook legale druk zou ondervinden, zouden noch hijzelf, noch het door hem later opgerichte BitTorrent-bedrijf op technisch niveau controle over het BitTorrent-netwerk kunnen uitoefenen. Hoewel Cohen de bestandsdeling-software initieel creëerde, werd deze bediend door mensen over de hele wereld. Het netwerk werd al snel bijna onmogelijk om te censureren en zo goed als onstopbaar - en zelfs de schepper kon dit niet veranderen.

BitTorrent zou zich in de volgende jaren vestigen als een standaard voor bestandsoverdrachten. Ongeveer een decennium na Cohen’s eerste software release, in het begin van de jaren 2010, had het protocol op elk moment van de dag minstens vijftien miljoen gelijktijdige gebruikers,[^239] en in een typische maand waren er wereldwijd zo’n 150 miljoen mensen verbonden aan het netwerk.[^240] Alles bij elkaar opgeteld, werd geschat dat BitTorrent-gebruikers verantwoordelijk waren voor zo’n 25 tot 30 procent van al het internetverkeer in de wereld, wat meer was dan enig ander protocol in die tijd.[^241]

Zonder een centrale entiteit die ze nog konden aanklagen, hadden muziekartiesten en platenmaatschappijen weinig andere keuze dan zich ook aanpassen aan de nieuwe realiteit. In plaats van te proberen hun muziek van het internet te verwijderen, verschoven ze uiteindelijk hun inspanningen om te concurreren met bestandsdeelservices door hun nummers gemakkelijk beschikbaar te maken via handige softwaretoepassingen (zoals Apple’s iTunes) en later, streamingservices. Slechts een paar jaar na de introductie van BitTorrent zou het kopen van een fysieke cd (of zelfs het bezit van muziek in het algemeen) ouderwets lijken.

Misschien had deze kennis de doorgewinterde Cypherpunks einde jaren ’90 enige hoop kunnen bieden. Een van “hun” technologieën zou niet alleen de wereld veroveren, maar, nog relevanter: Cohen’s code revolutioneerde hoe mensen het internet gebruikten en ernaar keken. Dit dwong uiteindelijk een gehele transformatie van de entertainmentindustrie af.

Waar Wei Dai, Eric Hughes, en andere Cypherpunks dachten dat elektronisch geld en andere crypto-tools alleen succesvol zouden zijn als het publieke bewustzijn over het belang van online privacy toenam, zou BitTorrent jaren later aantonen dat het ook andersom kon werken: een krachtige genoeg technologie kon, op zichzelf, helpen de heersende cultuur te veranderen.

## Hoofdstuk 13: RPOW

In het begin van de jaren 2000 had de Cypherpunk-beweging het grootste deel van zijn momentum verloren.

Terwijl sommige van de oorspronkelijke Cypherpunks gedesillusioneerd raakten en stopten met deelnemen aan de Cypherpunks-mailinglijst, ging de algehele kwaliteit van dit discussieplatform achteruit, met veel nieuwe berichten die weinig meer waren dan gescheld en schreeuwpartijen - of zelfs regelrechte spam. John Gilmore, de oorspronkelijke host van de lijst, had eind jaren 90 geprobeerd om een moderatiebeleid te introduceren, maar dit werd streng afgewezen door mensen zoals Tim May, die zich in reactie daarop uitschreef. [^242] (May keerde terug toen het beleid werd aangepast om vlammen en ander inhoud van lage kwaliteit om te leiden in plaats van te censureren, hoewel hij nog steeds niet blij was met de veranderingen.)

Gilmore besloot uiteindelijk te stoppen met het hosten van de Cypherpunks mailinglijst, waarna enkele van de overgebleven abonnees nieuwe groepen creëerden en overstapten naar Usenet, die op een meer verspreide manier konden worden gehost door meerdere mensen tegelijk.[^243] Desalniettemin, zou het verval van de beweging alleen maar versnellen. Na de terroristische aanslagen van 11 september 2001, maakte een scherpe toename van digitale surveillance mensen huiverig om discussies over radicale privacytools te faciliteren, en toen de enige resterende Cypherpunks-server werd gehost vanaf het webadres al-qaeda.net, besloot zelfs Tim May dat het tijd was om te vertrekken. Dit keer, voorgoed.

Dat betekende niet dat de Cypherpunk-ethos verloren of volledig vergeten was. Velen van de cypherpunks behielden hun interesse in bestaande privacytools zoals PGP, evenals in nieuwe technologieën zoals Tor (The Onion Router): het privacy-netwerk dat in 2002 werd gelanceerd leek op Zero-Knowledge Systems’s Freedom, maar vereiste geen betaald abonnement. Tor stelde iedereen in staat om anoniem het internet te gebruiken.

Veel van de Cypherpunks bleven ook in contact via andere middelen. Online migreerden nogal wat van hen uiteindelijk naar de strikter gemodereerde Cryptografie mailinglijst, die soms werd beschouwd als de feitelijke opvolger van de Cypherpunks-lijst. Offline liepen enkele van de Cypherpunks elkaar regelmatig tegen het lijf op cryptografieconferenties of hacker-evenementen.

Ondertussen kwamen er vele andere initiatieven voor elektronisch geld. Rond de overgang van het millennium werkten honderden startups aan online betalingssystemen, en veel van deze bedrijven omschreven hun oplossingen als een vorm van digitaal geld. Hoewel dat vaak gewoon betekende dat de betaalsystemen snel, goedkoop en gemakkelijk te gebruiken waren, waren ze niet per se privé. CyberCash, bijvoorbeeld, trok veel media-aandacht voor zijn digitaal geldsysteem, genaamd CyberCoin, dat specialiseerde zich in kleine betalingen in plaats van anonimiteit. Hetzelfde gold voor het systeem van elektronisch geld van Compaq, dat veel aandacht trok, genaamd Millicent.

Andere initiatieven die enige potentie toonden, zoals n-Count (medeontworpen door een voormalige werknemer van DigiCash), Proton (een project van samenwerkende Europese banken), of Mondex (een initiatief van de Britse bank NatWest dat later werd verkocht aan Mastercard), waren vooral gebaseerd op het concept van fysieke slimme kaarten. Net zoals de slimme kaart die in ontwikkeling was bij de start-up van David Chaum, moesten deze creditcard-formaat stukken hardware vooraf geladen worden met een waarde die fiat valuta vertegenwoordigde, om vervolgens te worden gebruikt voor persoonlijke transacties. Hoewel de meeste van deze privacyfuncties aanboden, waren ze vooral ontworpen om fysiek geld te vervangen in plaats van te dienen als anonieme valuta voor cyberspace.

Misschien nog dichter bij de visie van de Cypherpunks, richtte Robert Hettinga - die sinds 1996 de jaarlijkse Financial Cryptography conferenties had georganiseerd - in 1999 de Internet Bearer Underwriting Corporation op. Na het falen van DigiCash, wilde deze Cypherpunk financiering veiligstellen om een nieuw soort eCash-systeem te ontwikkelen, maar deze keer geoptimaliseerd voor goedkope transacties. Hij was van mening dat sterke privacygaranties niet alleen individuen beschermen tegen Big Brother, maar dat ze ook de wrijving kunnen verminderen en dus economische voordelen kunnen opleveren.

Echter, geen van deze projecten heeft haar beloftes kunnen waarmaken. Hoewel sommige technologieën banenbrekend waren in specifieke sectoren - zoals het openbaar vervoer of voor betaalkaarten voor telefooncellen - slaagde digitaal geld er niet in om veel aantrekkingskracht te winnen bij het algemene publiek. Door het gebrek aan interesse begon de financiering ook te verminderen.

“Eerlijk gezegd is het dot-com geld verdwenen,” concludeerde Hettinga in 2001, nadat hij er niet in geslaagd was genoeg geld op te halen om het elektronische geldsysteem van zijn bedrijf te ontwikkelen. “We gaan ook over terrein waar CyberCash, DigiCash en veel andere mensen hun vingers aan gebrand hebben.”[^244]

In plaats van het investeren in nieuwe crypto-initiatieven, richtten traditionele banken en financiële dienstverleners zich op het verbeteren van bestaande cashloze betalingsystemen, zoals transacties via creditcards en betaalpassen. Intussen wonnen flamboyante nieuwe web-gebaseerde betalingsverwerkers zoals PayPal snel aan marktaandeel en het leek erop dat privacy (laat staan ​​monetaire hervorming) geen grote zorg was voor de meesten van hen. De dystopische toekomst waar Chaum en veel van de Cypherpunks voor gewaarschuwd hadden - een toekomst waarin alle financiële transacties konden worden gemonitord, geregistreerd en mogelijk gecensureerd - werd snel realiteit.

Toch was niet iedereen bereid de hoop op te geven…

### Hal Finney

Geboren in het voorjaar van 1956 in het kleine Californische dorpje Coalinga, toonde Hal Finney al vroeg een interesse in codes nog als een jong kind: op de basisschool, vond hij het leuk om codes met letters en cijfers te maken voor willekeurige teksten die hij tegenkwam.

Iets later, in zijn tienerjaren, ontwikkelde Hal een fascinatie voor computers. Gelukkig was de middelbare school die hij bezocht zijn tijd ver vooruit: de schooladministratie maakte al gebruik van een computer voor het beheer en de opslag van leerlinggegevens jaren voordat dit gebruikelijk werd. Jonge Hal, enthousiast om met de machine te werken, bood vrijwillig zijn hulp aan het schoolpersoneel aan, waardoor hij tussen de lessen door een soort bijbaantje kreeg.

Finney behaalde in 1974 zijn middelbareschooldiploma als beste student van zijn klas en werd toegelaten tot het California Institute of Technology (Caltech), één van de meest prestigieuze en selectieve universiteiten ter wereld. Omdat Caltech toen nog geen bacheloropleiding in informatica aanbood, besloot hij een opleiding in techniek te volgen, terwijl hij tegelijkertijd zoveel mogelijk programmeercursussen volgde.

Rond dezelfde tijd ontwikkelde Finney een sterke waardering voor logica en omarmde hij de libertaire filosofie. Hij ging graag filosofische discussies aan met zijn medestudenten aan de universiteit, waar een combinatie van prikkelende ideeën, stevige argumentaties en een bedachtzame benadering van gesprekken hem veel aandacht opleverde van zijn leeftijdsgenoten. Onder hen was Fran, het meisje met wie hij later zou trouwen en de rest van zijn leven zou doorbrengen.

Kort na zijn afstuderen aan Caltech in 1978, vond Finney zijn eerste serieuze baan als programmeur bij het kleine ingenieursfirma APh Technological Consulting. APh was zojuist een samenwerking gestart met speelgoedfabrikant Mattel om het besturingssysteem voor hun Intellivision-spelcomputer te ontwikkelen, naast een aantal vroege spellen. In de daaropvolgende jaren zette Finney werk voort in het ontwikkelen van baanbrekende videogames zoals Space Battle en Star Strike voor de Intellivision, alsook Adventures of Tron, Astroblast! en Space Attack voor het Atari Video Computersysteem.

Als algemeen optimistisch mens, was Finney ervan overtuigd dat de wereld van morgen beter zou zijn dan die van vandaag, en stond hij open voor verandering. Dus toen de Extropian gemeenschap eind jaren ’80 begon te vormen, paste hij er ook goed in. Het vooruitzicht van technologische vernieuwingen zoals nanotechnologie, kunstmatige intelligentie en geest uploaden maakte hem enthousiast. En als een overtuigd atheïst die niet in het hiernamaals geloofde, was Finney al erg geïnteresseerd in het potentieel van cryonics sinds hij over het concept las tijdens zijn eerste jaar op de universiteit.

Zoals Fran het later zei: “Hij geloofde niet in God. Hij geloofde in de toekomst.”[^245]

### Cypherpunk Realisme

Toen het internet begin jaren ’90 voor het eerst publiek toegankelijk werd, was Finney een van de allereerste gebruikers die zich een verbinding wist te bemachtigen.

Terwijl hij de verschillende - op dat moment enkel op tekst gebaseerde - hoeken van de gloednieuwe informatiesnelweg verkende, herkende Finney al snel het revolutionaire potentieel van de ontluikende digitale domein. Voor het eerst zou de mensheid over de hele wereld verbonden zijn, ongeacht geografische afstanden, willekeurige grenzen of culturele verschillen. Hij geloofde dat de gevolgen hiervan de wereld zouden veranderen.

Maar al snel besefte hij dat er ook een nadeel was aan de digitalisering van communicatie. Kenner van de technische architectuur van het internet, wist Finney dat zonder beschermende maatregelen, cyberspace rampzalige inbreuken op individuele privacy kon faciliteren; alles dat iemand online doet, kon potentieel bespioneerd worden. Hij voorzag dat het internet eigenlijk een bedreiging voor de menselijke vrijheid kon worden.

Dit was ook het geval voor gewone communicatie, en Finney beredeneerde dat dit net zo goed opging voor financiële transacties.

“Er kunnen dossiers worden gemaakt die de uitgavenpatronen van ons allemaal volgen,” waarschuwde Finney. “Als ik nu iets bestel via de telefoon of elektronisch met mijn Visa kaart, wordt er een record bijgehouden van precies hoeveel ik heb uitgegeven en waar ik het heb besteed. Naarmate de tijd vordert, kunnen er meer transacties op deze manier plaatsvinden, en het uiteindelijke resultaat kan een groot verlies aan privacy zijn.”[^246]

Het internet had behoefte aan een ontraceerbare vorm van geld, concludeerde Finney—digitale contanten. En hij was opgetogen te ontdekken dat zo’n systeem al in ontwikkeling was.

“Het leek me zo duidelijk,” herinnerde Finney zich later. “We worden geconfronteerd met problemen zoals het verlies van privacy, oprukkende computarisering, enorme databases en meer centralisatie - en Chaum biedt een volledig andere weg om in te slaan, eentje die macht in handen van individuen legt in plaats van regeringen en bedrijven. De computer kan eerder als instrument gebruikt worden om mensen te bevrijden en te beschermen, in plaats van hen te controleren.”[^247]

Finney had daarom een uitnodiging aanvaard van mede-Extropian Tim May, die een ontmoeting organiseerde met een groep lokale hackers en cryptografen uit de Bay Area, die zichzelf spoedig de Cypherpunks zouden noemen.

Kort daarna bevond Finney zich in de positie waar hij Chaum’s eCash-project aan het promoten was onder zijn mede-Extropianen, en op een bepaald moment een zeven pagina’s tellende uitleg voor het Extropy magazine schreef. Finney schreef aan de techno-libertarische menigte dat cryptografie individuen kon beschermen tegen overheidsmacht, inmenging, en controle, en legde uit hoe elektronisch geld de Extropiaanse zaak kon bevorderen.

En, als een echte Cypherpunk, schreef Finney code. De game-ontwikkelaar was verantwoordelijk voor een vroeg Cypherpunk-succes toen hij Eric Hughes hielp de allereerste Chaumian remailer te ontwikkelen. Het was ook Finney’s idee om de uitdaging te organiseren om de (verzwakte) export-grade encryptie standaard van Netscape te kraken, een uitdaging die voltooid werd door mede-Cypherpunk Ian Goldberg. Dit vormde een grote overwinning in de crypto-oorlogen.

Maar Finney’s meest opmerkelijke bijdragen werden waarschijnlijk gedaan aan PGP: nadat Phil Zimmermann voor het eerst de encryptietool had uitgebracht, werd Finney een belangrijke bijdrager aan het project. De tweede versie van de software, een grote verbetering ten opzichte van versie 1, werd grotendeels door hem ontwikkeld, hoewel dit een beetje stil werd gehouden om Finney te behoeden voor mogelijke juridische problemen zoals Zimmermann die ondervond. Een paar jaar later zou Finney de eerste werknemer worden van Zimmermann’s PGP-bedrijf.

Finney stond echter niet achter de visie van Tim May om met behulp van Cypherpunk-hulpmiddelen een crypto-anarchistische samenleving te stichten.

Dit was niet omdat hij het idee om de staat uit economische interacties te verwijderen niet leuk vond, of omdat de ideeën van May op dat vlak te radicaal voor zijn smaak waren. Als een Extropiaan en libertariër vond Finney in feite dat May’s visie in principe geweldig klonk. Hij geloofde echter niet dat May’s idee om een anarchistische samenleving te bereiken door middel van cryptografie erg realistisch was.

“[…] er is geen zoiets als cyberspace,” schreef Finney op een gegeven moment aan de mailinglijst van de Cypherpunks in reactie op een van de betogen van May. “Ik ben nu niet in cyberspace; ik ben in Californië. Ik val onder de wetten van Californië en de Verenigde Staten, ook al communiceer ik met een andere persoon, of het nu per post of elektronisch is, via telefoon of TCP/IP-verbinding. Wat betekent het om te spreken over een regering in cyberspace? Het is de regering in de fysieke ruimte die ik vrees. Haar agenten dragen fysieke wapens die echte kogels afvuren. Totdat ik in mijn computer kan leven en elektronen kan eten, zie ik de relevantie van cyberspace niet in.” [248]

Hoewel individuen Cypherpunk hulpmiddelen konden gebruiken om hun privacy te beschermen, geloofde Finney niet dat de meeste mensen hun hele leven in de cyberspace zouden kunnen “verbergen”. Zelfs als Cypherpunk-hulpmiddelen een kleine groep technisch onderlegde elite zouden kunnen helpen om bepaalde wetten te omzeilen, verwierp hij de gedachte dat dit de beschaving ingrijpend zou veranderen, omdat hij uiteindelijk niet geloofde dat een libertaire samenleving gerealiseerd kon worden zonder wijdverspreide steun van de bevolking.

In plaats van een anarchistisch utopia om naar te migreren, zag Finney het internet eerder als een plek voor intellectuele uitwisseling; in plaats van een Galt’s Gulch, zag hij cyberspace als een plek om ideeën vrijelijk uit te wisselen en te bediscussiëren. En dit, zo geloofde Finney, was de echte sleutel tot het bereiken van ware vrijheid; de beste en enige manier om een vrije samenleving te creëren was om de massa ervan te overtuigen dat een vrije samenleving een goed idee is.

“In de kern geloof ik dat we de soort samenleving zullen hebben die de meeste mensen wensen. Als we vrijheid en privacy willen, moeten we anderen overtuigen dat deze waardevol zijn. Er zijn geen snelkoppelingen. Terugtrekken in technologie is als het over je hoofd trekken van de dekens. Het voelt even goed, totdat de realiteit je inhaalt.”[^249]

### Elektronisch Geld

Ondanks zijn nuchtere en misschien wel meer realistische kijk op de mogelijkheden van cryptografie, was Finney altijd gedreven om elektronisch geld te realiseren. Hij voerde uitvoerige gesprekken over de mogelijkheden hiervan met zowel de Extropians als de Cypherpunks op hun respectievelijke mailinglijsten, en ook op de Libtech mailinglijst van Nick Szabo.

Op de Cypherpunks mailinglijst was hij bij gesprekken over digitale valuta regelmatig één van de meest actieve deelnemers en hij nam soms zelfs een soort sturende rol aan. Hoewel sommige Cypherpunks hevig konden twisten over de beste benadering van elektronisch geld, stond Finney meer open voor verschillende ideeën. In plaats van vast te houden aan één oplossing, gaf hij liever een overzicht van de verschillende compromissen die elk van hen met zich meebracht.

Finney leek bijvoorbeeld grotendeels onbeslist, of misschien beter gezegd, open-minded over het onderwerp van backing. Hij merkte op dat het ondersteunen van elektronisch geld met fiatvaluta werkte, maar speculeerde soms ook over digitale valuta’s ondersteund door een mandje van goederen, of door een synthetisch gemiddelde van meerdere nationale valuta’s, of helemaal niet ondersteund.

Elke keer dat er een nieuw voorstel voor elektronisch geld opdook op de Cypherpunks mailinglijst, was Finney altijd enthousiast om het te beoordelen, met een speciale nadruk op hun privacyfuncties. Na het bestuderen van het ontwerp, kwam hij vaak terug op de mailinglijst om in zijn eigen woorden uit te leggen hoe het werkte, hoe het zich verhield tot eerdere voorstellen, en wat hij van het idee vond. Naast (meestal constructieve) feedback voor de indiener, bood Finney in wezen een openbare dienst aan andere Cypherpunks door hen te helpen de mogelijkheden en beperkingen van verschillende benaderingen te begrijpen.

Finney had ook een speciale interesse in de wettelijkheid van elektronisch geld, een onderwerp dat hem in de begindagen van de Cypherpunks-gemeenschap naar de geschiedenis van het geld leidde. Hier kwam hij voor het eerst het werk van George Selgin over vrije banken tegen. Terwijl hij wetten over wettig betaalmiddel, belastingregels, bankregulering en meer bestudeerde, deelde Finney zijn bevindingen op de mailinglijst van de Cypherpunks en begon hij de mogelijkheden en risico’s in kaart te brengen. (Het was bijvoorbeeld Finney die ontdekte dat niet-commerciële experimenten voor systemen zoals eCash getolereerd zouden moeten worden, zelfs als ze gebruik maakten van Chaum’s gepatenteerde blind ondertekeningschema.)

Tegelijkertijd stelde Finney zich terughoudend op tegenover enkele uitspraken die geïnspireerd waren door crypto-anarchie over de beloften van elektronisch geld. Ook hier was hij sceptisch over enkele van de meer radicale voorspellingen met betrekking tot massale belastingontduiking en hoe elektronisch geld dit zou mogelijk maken.

“We zijn verblind door het beeld van monetaire stromen die over de hele wereld flitsen. Wat ik echter nooit precies kan plaatsen is, wat precies verhindert dat zoiets vandaag de dag wordt gedaan?” stelde Finney aan de mailinglijst. “Als je in goud wilt investeren, kun je toch naar de muntwinkel gaan en wat kopen? Of je kunt je geld in een beleggingsfonds in goud stoppen en het als een betaalrekening gebruiken. Als je yen of marken wilt, kun je daarin investeren. Als het punt is om dit in het geheim te doen, waarom zou het dan gemakkelijker zijn om je salaris per post naar de digicash-bank in de Bahamas te sturen dan naar een bestaande bank daar?”[250]

Ook hier was het niet zo dat Finney de meer radicale beloftes van Tim May onaantrekkelijk vond. Hij beschouwde ze gewoon niet als erg realistisch. Afgezien van het feit dat de meeste mensen hun belastingen toch al rechtstreeks van hun salaris betaalden, moest iedereen uiteindelijk in de fysieke wereld leven, waar belastingontduiking nog steeds illegaal zou zijn. Het was voor Finney verre van duidelijk dat het verbergen van rijkdom in cyberspace de meeste mensen in het echte leven ten goede zou komen.

“Het lijkt mij dat de zwakte in deze plannen om de overheid te omzeilen met digitaal geld zit in de omzetting van fysiek geld naar digitaal geld. Dat lijkt het knelpunt te zijn waar de overheid nog steeds controle kan houden,” concludeert Finney. [^251]

### Herbruikbare Bewijzen van Werkzaamheid

In de jaren 2000, ongeveer tien jaar nadat Finney in Extropian kringen begon te pleiten voor elektronisch geld, was er nog steeds geen succesvol elektronisch geldsysteem. Hoewel een reeks ideeën was besproken op de mailinglijst van de Cypherpunks, en Finney veel van de voorstellen persoonlijk had beoordeeld, was geen van hen van de grond gekomen. In sommige gevallen, zoals bij de startups van Chaum of Hettinga, was dit omdat het product uiteindelijk commercieel niet haalbaar bleek te zijn - of althans zo leek het. Maar in andere gevallen, zoals bij het Bit Gold van Nick Szabo of de b-money voorstellen van Wei Dai, waren de systemen in de eerste plaats nooit geïmplementeerd.

Wellicht was het omdat zijn verwachtingen voor het potentieel van elektronisch geld meer ingetogen waren dan die van Tim May en andere crypto-anarchisten in de eerste plaats, of misschien was het gewoon vanwege zijn over het algemeen optimistische karakter, maar waar vele andere Cypherpunks tegen deze tijd ontgoocheld waren geraakt, wilde Finney het idee nog een kans geven. Hij besloot uiteindelijk om een proof-of-work gebaseerd elektronisch geldsysteem te ontwikkelen - zelfs als het in een vereenvoudigde vorm moest.

In 2004 lanceerde hij Reusable Proofs of Work, of kortweg RPOW (uitgesproken als “arpow”). Hij nodigde mensen uit om het systeem te testen, adverteerde het elektronische geld-schema op een eenvoudige blauw-groene webpagina met een RPOW-logo in stripboekstijl. (Denk aan de “POW” letters die de plek markeren waar Batman’s uppercut de kaak van een ongelukkige handlanger raakt.)

“Beveiligingsonderzoeker Nick Szabo heeft de term bit gold bedacht om een soortgelijk concept van tokens, dat inherent een bepaald niveau van inspanning vertegenwoordigt, te omschrijven,” schreef Finney op de website van het project. “Het concept van Nick is complexer dan het eenvoudige RPOW-systeem, maar zijn inzicht is van toepassing: op sommige manieren kun je een RPOW-token zien als het hebben van de eigenschappen van een zeldzame stof zoals goud. Het kost moeite en uitgaven om goud te delven en munten te slaan, waardoor ze inherent zeldzaam zijn.”[^252]

Waar Bit Gold was ontworpen rondom een ‘eigendomsclub’, zou ook RPOW beheerd worden door specifieke servers. Voor het prototype had Finney zelf een RPOW-server opgezet. Deze voerde de basisbewerkingen uit die nodig zijn voor het elektronische geldsysteem: het gaf nieuwe RPOW-tokens uit (de munteenheden), en controleerde of tokens niet twee keer werden uitgegeven.

Het is belangrijk te vermelden dat de RPOW-server alleen nieuwe tokens zou uitgeven als aan één van de twee voorwaarden was voldaan: er moest een geldige hash worden ingediend, of een ouder token moest worden ingeleverd als wisselgeld.

De eerste optie was een eenvoudige proof-of-work functie. Als gebruiker Alice een RPOW-token wilde, moest ze verbinding maken met Finney’s server (mogelijk via Tor voor optimale privacy), een aantal gegevens die uniek zijn voor de server en voor haarzelf nemen, en beginnen met hashen tot ze een geldige hash (beginnend met genoeg nullen) vond. Vervolgens zou ze de hash naar de server sturen, die deze op geldigheid zou controleren, en (indien geldig) een unieke RPOW-token terugsturen - in feite gewoon een unieke gegevensreeks. De server zou ook een kopie van de token in een lokale database bewaren.

Wanneer Alice een RPOW-token wilde uitgeven, bijvoorbeeld om een MP3-bestand te kopen, zou ze het simpelweg naar de beoogde ontvanger, Bob, sturen. Technisch gezien maakte het voor het RPOW-systeem niet uit hoe ze het verzond, zolang ze er maar zeker van was dat het bij Bob terechtkwam zonder dat iemand het onderschepte. (Een bericht aan Bob gecodeerd met zijn publieke sleutel zou het klusje klaren.)

Wanneer Bob de RPOW-token zou ontvangen, zou hij deze moeten valideren en controleren dat deze niet dubbel was uitgegeven. Hij zou daarom de token direct doorsturen naar de RPOW-server, die zou nagaan of de token in de interne database stond en of deze niet dubbel was uitgegeven. Als de token geldig was, zou de server dit aan Bob bevestigen. Hierdoor kon Bob het MP3-bestand naar Alice sturen. De server zou ook de RPOW-token als uitgegeven bestempelen, waardoor deze in de toekomst niet meer gebruikt kon worden.

Ten slotte zou de server Bob een nieuw RPOW-token geven, en dit nieuwe token opnemen in zijn interne database. Op deze manier kon Bob dit nieuwe token later uitgeven.

Stel je voor dat Bob zijn nieuwe RPOW-token wil gebruiken om toegang te krijgen tot Carol’s website. Als Carol de RPOW-token van Bob krijgt, stuurt ze hem weer door naar de RPOW-server van Finney. De server bevestigt dan dat de token echt is, markeert deze als besteed in zijn interne database en geeft vervolgens een nieuwe RPOW-token uit aan Carol. Deze wordt ook toegevoegd aan de interne database van de server.

Op deze manier kon het bewijs van werk, vertegenwoordigd door een enkele geldige hash (gemaakt door Alice), effectief oneindig blijven circuleren. Het was inderdaad herbruikbaar bewijs van werk.

### Betrouwbaar Computergebruik

In het Nederlands: Het systeem zoals tot dusver beschreven zou vrij goed werken - behalve dat het vertrouwen vereist in de beheerder van de RPOW-server om geen dubbele uitgaven te doen of RPOW-tokens voor zichzelf te maken zonder een bewijs van werk te leveren. Finney wilde echter niet dat de gebruikers de beheerder van de RPOW-server moesten vertrouwen, zelfs als die beheerder hijzelf was. Daarom voegde Finney nog een speciale eigenschap toe aan het ontwerp.

Ten eerste zou de RPOW-server gebruik maken van gratis en open source software. Iedereen kon online de broncode van RPOW vinden en controleren hoe het functioneerde.

En, als de hoofdinnovatie van het systeem, was de RPOW-server gehost op een veilige hardwarecomponent, de IBM 4758. Dit maakte “vertrouwd rekenen” mogelijk.

Kortom, de sabotagebestendige hardware bevatte een privésleutel, ingebed door IBM, die niemand - zelfs niet de eigenaar van de veilige hardwarecomponent - kon manipuleren of eruit kon halen. Met behulp van een techniek die “remote attestation” wordt genoemd, kon de privésleutel vervolgens de gratis en open source software die op de veilige hardwarecomponent was geïnstalleerd, cryptografisch ondertekenen. Met deze handtekening en de bijbehorende openbare sleutel van IBM kon iedereen verifiëren dat de veilige hardwarecomponent daadwerkelijk de RPOW-broncode uitvoerde die Finney had gepubliceerd, zonder achterdeuren of aanpassingen.

Zolang men IBM vertrouwde om niet mee te werken met Finney om een valse handtekening te fabriceren (en aannemende dat de centrale server niet volledig offline ging), konden RPOW-gebruikers er zeker van zijn dat het elektronische geldsysteem naar behoren functioneerde.

“[…] Het RPOW-systeem is ontworpen met één overkoepelend doel: het onmogelijk maken dat iemand, zelfs de eigenaar van de RPOW-server of zelfs de ontwikkelaar van de RPOW-software, in staat zou zijn om de regels van het systeem te overtreden en RPOW-tokens te vervalsen,” legde Finney uit op de RPOW-website. “Zonder zo’n garantie tegen vervalsbaarheid, zouden RPOW-tokens het werk dat is gedaan om ze te creëren niet geloofwaardig kunnen vertegenwoordigen. Vervalsbare tokens zouden meer lijken op papiergeld dan op bit-goud.”[^253]

### Het lot van RPOW

De eerste RPOW-release was weliswaar nog erg basaal, maar Hal Finney had het voornemen het project in de loop van de tijd te verbeteren. Wellicht het belangrijkst, hij plande om het systeem te upgraden zodat het op meerdere, onafhankelijk van elkaar opererende, servers zou draaien. Zo zou het volledige RPOW-systeem niet onderuit gaan als zijn server om welke reden dan ook offline ging.

Ondertussen vond de Cypherpunk het ook leuk om te experimenteren en te sleutelen aan de RPOW-software. Zo heeft hij bijvoorbeeld een BitTorrent-client aangepast om samen te werken met zijn elektronische geldsysteem. Dit leek op het Mojo Nation concept en stelde gebruikers in staat om andere gebruikers te betalen als ze hun download wilden versnellen. In een even creatieve toepassing van de RPOW-technologie werkte hij aan een peer-to-peer pokerapplicatie. Hier konden gebruikers tegen elkaar spelen, waarbij de RPOW-tokens automatisch naar de digitale portemonnee van de winnaar werden overgemaakt.

Finney kreeg al snel hulp van een jongere ontwikkelaar genaamd Gregory Maxwell, die een actieve interesse toonde in het elektronische geldsysteem. Maxwell droeg bij aan het project met code, en overwoog om geavanceerde bestedingsvoorwaarden zoals escrow betalingen te implementeren. Hij besprak ook mogelijke oplossingen voor sommige van de meer subtiele technische uitdagingen met Finney, zoals het instellen van vervaltermijnen voor tokens, of de relatief zwakke versleuteling die het veilige hardwarecomponent beveiligde.

Helaas voor Finney bleek Maxwell echter de zeldzame uitzondering. Omdat bijna niemand anders interesse toonde in het elektronische geldsysteem, lukte het RPOW niet om door te breken.

Dit was waarschijnlijk ten minste gedeeltelijk te wijten aan het feit dat RPOW geen heel goede vorm van geld was. Geconfronteerd met hetzelfde probleem als Adam Back’s hashcash - een probleem dat Szabo en Dai geprobeerd hadden op een omslachtige manier op te lossen - zouden computationele verbeteringen op den duur het goedkoper maken om geldige hashes te genereren, wat suggereert dat de markt uiteindelijk zou worden overspoeld met RPOW-tokens. De verwachting van hoge inflatie werkte ontmoedigend om de RPOW-valuta-eenheden te bezitten.

“Het klopt dat als de Wet van Moore blijft gelden, de kosten voor het vervaardigen van een ‘proof of work’-token gestaag en exponentieel zullen dalen”, gaf Finney toe op de website van het project. “Maar onthou dat dit geen geld is en niet bedoeld is als een stabiel middel om waarde op te slaan. Het is eerder bedoeld als een gemakkelijk te ruilen weergave van computerverspilling.”[^254]

Inderdaad, het elektronische geldsysteem van Finney fungeerde niet zozeer als een breed geaccepteerde waardeopslag of rekeneenheid. Het werd vooral nuttig geacht als ruilmiddel op plaatsen waar hashcash zinvol kan zijn - bijvoorbeeld om te dienen als ‘postzegels’ voor het beperken van spam.

Maar waarschijnlijk slaagde het elektronische geldsysteem er ook niet in om van de grond te komen omdat het de opstartuitdaging niet kon overwinnen. Geld is enkel nuttig als anderen het accepteren als betaalmiddel, maar zonder een economische stimulans om RPOW-tokens te bewaren, hadden de meeste mensen daar geen reden toe. En zonder dat er iemand was die de tokens als betaling accepteerde, was er ook niemand aan wie ze konden worden uitgegeven, wat betekende dat er nog minder reden was voor iemand om ze in eerste instantie te accepteren als betaling…

“Het had het probleem dat er min of meer niets was om het mee te gebruiken,” concludeerde Maxwell ook, terugkijkend op het RPOW-project jaren later, “wat het moeilijk maakte om de aandacht erop gericht te houden.”[255](Gregory%20Maxwell,%20IRC%20message%20to%20author,%20August%2013,%202020.)

Net als eCash en hashcash voorheen, leed ook RPOW aan een kip-en-ei probleem.

### E-goud

Ondanks de beste bedoelingen van Hal Finney is RPOW halverwege de jaren 2000 geëindigd als nog een mislukte poging om elektronisch geld te creëren.

Het was op dit moment dat sommige techno-libertariërs begonnen om wat perspectief te vinden in een alternatieve vorm van internetgeld, die met een zeer verschillend ontwerp, succesvoller leek te zijn: e-goud.

Het project van Douglas Jackson, een digitale valuta gesteund door goud, groeide snel rond het midden van de jaren 2000. Het voldeed aan verschillende van de eisen die de Cypherpunks hadden gesteld aan elektronisch geld: transacties konden met enige mate van anonimiteit worden uitgevoerd, het systeem ondersteunde microtransacties tot op één tienduizendste van een gram goud en, natuurlijk, goud zelf vertegenwoordigde onvervalste kostbaarheid. Naarmate de technologie van e-goud verbeterde, konden ontwikkelaars zelfs computerprogramma’s in het systeem integreren via een Application Programming Interface (API), waardoor oplossingen die op slimme contracten leken werden gefaciliteerd.

Maar natuurlijk, er was één vakje dat e-goud niet kon aftikken. De ervaring met DigiCash’s Cyberbucks had de cypherpunks geleerd wat er kon gebeuren met een digitale munteenheid als het afhankelijk was van één enkel bedrijf, en de klanten van Douglas Jackson zouden deze les binnenkort ook leren. Met de CEO gearresteerd en het kantoor van het bedrijf in 2006 door federale agenten binnengevallen, was er weer een internetvalutaproject mislukt. Szabo’s stelling klonk nogmaals luid en duidelijk: vertrouwde derde partijen zijn veiligheidslekken.

Na meer dan twintig jaar van niet-gerealiseerde voorstellen, verlaten projecten en mislukte startups, bestond er nog steeds geen elektronisch geld.

Intussen werd de noodzaak van een alternatief voor fiduciair geld steeds groter…

# Endnotes

[141]: More, “Hayek’s Denationalisation of Money,” 20.

[142]: Tim May, “Untraceable Digital Cash, Information Markets, and BlackNet ,” The Computers Freedom & Privacy Conference , accessed via [https://web.archive.org/web/20130501134401/https://osaka.law.miami.edu/…oomkin/articles/tcmay.htm.]

[143]: Tim May, “The Cyphernomicon,” originally distributed through the Cypherpunks mailing list, September 10, 1994, available via [https://nakamotoinstitute.org/static/docs/cyphernomicon.txt.]

[144]: Hal Finney, “Chaum on the wrong foot?” originally sent to the Cypherpunks mailing list, August 22, 1993 available via [https://cypherpunks.venona.com/date/1993/08/msg00652.html.]

[145]: Eric Hughes, “A Cypherpunk’s Manifesto,” originally sent to the Cypherpunks mailing list, March 17, 1993, available via [https://cypherpunks.venona.com/date/1993/03/msg00392.html.]

[146]: Tim May, “Degrees of Freedom,” originally sent to the Cypherpunks mailing list, February 8, 1996, available via [https://cypherpunks.venona.com/date/1996/02/msg00637.html.]

[147]: Tim May, “‘Who shall speak for us?’,” originally sent to the Cypherpunks mailing list, Available via [https://cypherpunks.venona.com/date/1995/09/msg02189.html.]

[149]: Tim May, “The Crypto Anarchist Manifesto,” originally sent to the Cypherpunks mailing list, November 22, 1992, available via [https://cypherpunks.venona.com/date/1992/11/msg00204.html.]

[150]: Tim May, “Libertaria in Cyberspace,” originally sent to the Cypherpunks mailing list, August 9, 1993, accessed via [https://cypherpunks.venona.com/date/1993/08/msg00168.html.]

[151]: Tim May, “Cyberspace, Crypto Anarchy, and Pushing Limits,” originally sent to the Cypherpunks mailing list, April 3, 1994, accessed via [https://cypherpunks.venona.com/date/1994/04/msg00096.html.]

[152]: Tim May, “Hayek ,” originally sent to the Cypherpunks mailing list, August 27, 1996, Accessed via [http://cypherpunks.venona.com/date/1996/08/msg02102.html.] As a funny aside, Tim May concluded a different email with a compliment to one of his fellow Cypherpunks: “I just want to end on a positive note before leaving for the holidays .” See: Tim May, “Re: The War on Some Money long,” originally sent to the Cypherpunks mailing list, December 21, 1995, accessed via [https://cypherpunks.venona.com/date/1995/12/msg01044.html.]

[153]: Tim May, “‘Stopping Crime’ Necessarily Means Invasiveness,” originally sent to the Cypherpunks mailing list, October 17, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/10/msg01269.html.]

[154]: Eric Hughes, “No digital coins ,” originally sent to the Cypherpunks mailing list, August 24, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00690.html.]

[155]: Tim May, “Crypto Activism and Respectability,” originally sent to the Cypherpunks mailing list, April 21, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/04/msg00400.html.]

[156]: Tim May, “Opportunities in Cyberspace,” originally sent to the Cypherpunks mailing list, September 8, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/09/msg00140.html.]

[157]: Michelle Quinn, “The Cypherpunks Who Cracked Netscape,” San Francisco Chronicle, September 20, 1995, [https://people.eecs.berkeley.edu/…w/press/iang/ian1.html.]

[158]: Tim May, “Re: Stalling the crypto legislation for 2-3 more years,” originally sent to the Cypherpunks mailing list, July 23, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/07/msg01245.html.]

[159]: Tim May, “Scenario for a Ban on Cash Transactions,” originally sent to the Cypherpunks mailing list, November 24, 1992, accessed via: [https://cypherpunks.venona.com/date/1992/11/msg00211.html.]

[161]: Tim May, “Crypto Anarchy, the Government, and the National Information Infrastructure,” originally sent to the Cypherpunks mailing list, November 29, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/11/msg01106.html.]

[162]: Tim May, “DigiCash can use whatever currencies are valued,” originally sent to the Cypherpunks mailing list, May 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00243.html.]

[163]: Tim May, “Re: Hettinga’s e€ yllogism,” originally sent to the Cypherpunks mailing list, June 28, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/06/msg01637.html.]

[164]: Tim May, “‘Stopping Crime’ Necessarily Means Invasiveness,” originally sent to the Cypherpunks mailing list, October 17, 1996, accessed via: [http://cypherpunks.venona.com/date/1996/10/msg01269.html.]

[165]: Tim May, “Untraceable Payments, Extortion, and Other Bad Things,” originally sent to the Cypherpunks mailing list, December 21, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/12/msg01468.html.]

[167]: Douglas Barnes, “Re: cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 8, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/10/msg00731.html.]

[168]: Tim May, “Software Patents are Freezing Evolution of Products,” originally sent to the Cypherpunks mailing list, October 7, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/10/msg00685.html.]

[169]: Eduard de Jong, “Electronic Money: From Cryptography and Smart Cards to Bitcoin and Beyond,” Fraunhofer SmartCard Workshop 2017 .

[170]: Laurie Law, Susan Sabett, and Jerry Solinas, “How To Make a Mint: The Cryptography of Anonymous Electronic Cash,” National Security Agency Office of Information Security Research and Technology, Cryptology Division, June 18, 1996,              [https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm.]

[171]: Hadon Nash, “Digital Gold,” originally sent to the Cypherpunks mailing list, August 24, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00698.html.]

[172]: Hal Finney, “Digital Gold, a bearer instrument?,” originally sent to the Cypherpunks mailing list, August 26, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00788.html.]

[173]: Black Unicorn, “DigiCash Announcement,” originally sent to the Cypherpunks mailing list, May 10, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00616.html.]

[174]: Pr0duct Cypher, “Magic Money Digicash System,” originally sent to the Cypherpunks mailing list, February 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/02/msg00247.html.]

[175]: Perry E. Metzger, “Re: Virtual Cash,” originally sent to the Cypherpunks mailing list, May 3, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00131.html.]

[176]: Robert Hettinga, “Re: digital cc transactions, digital checks vs real digital cash,” originally sent to the Cypherpunks mailing list, May 3, 1997, accessed via: <https://cypherpunks.venona.com/date/1997/05/msg00147.html>

[177]: Robert Hettinga, “Re: Bypassing the Digicash Patents,” originally sent to the Cypherpunks mailing list, April 29, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/04/msg00811.html.]

[178]: Tim May, “Re: alternative b-money creation,” originally sent to the Cypherpunks mailing list, December 11, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/12/msg00455.html.]

[179]: Tim May, “What backs up digital money?,” originally sent to the Cypherpunks mailing list, March 27, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/03/msg01576.html.]

[180]: Adam Back, “Re: Bypassing the Digicash Patents,” originally sent to the Cypherpunks mailing list, April 30, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/04/msg00822.html.]

[181]: Adam Back, “digital cc transactions, digital checks vs real digital cash,” originally sent to the Cypherpunks mailing list, May 2, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/05/msg00104.html.]

[183]: Leslie Lamport, Robert Shostak, and Marshall Pease, “The Byzantine Generals Problem,” ACM Transactions on Programming Languages and Systems : 382–401.

[184]: Adam Back, “Re: ‘why privacy’ revisited,” originally sent to the Cypherpunks mailing list, March 22, 1997, available via: [https://cypherpunks.venona.com/date/1997/03/msg00586.html.]

[185]: Adam Back, “The Bitcoin Game #59: Dr. Adam Back,” interview by Rob Mitchell, The Bitcoin Game, YouTube, October 25, 2018, <https://youtu.be/xxYsRjanphA?si=XVdLXPWGUk6oVPXg&t=647> 10:47–11:19.

[186]: Adam Back, “Re: cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 8, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/10/msg00734.html.]

[187]: Adam Back, “cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 7, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/10/msg00690.html.]

[189]: Adam Back, “distributed virtual bank,” originally sent to the Cypherpunks mailing list, August 27, 1997, accessed via: <https://cypherpunks.venona.com/date/1997/08/msg01289.html>.

[190]: Tim May, “Re: More on digital postage,” originally sent to the Cypherpunks mailing list, February 15, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/02/msg02295.html.]

[191]: Adam Back, “Re: bulk postage fine ,” originally sent to the Cypherpunks mailing list, August 3, 1997 accessed via: [https://cypherpunks.venona.com/date/1997/08/msg00070.html.]

[192]: Adam Back, “no government regulation of the net ,” originally sent to the Cypherpunks mailing list, August 3, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/08/msg00087.html.]

[193]: Cynthia Dwork and Moni Naor, “Pricing via Processing or Combatting Junk Mail,” Advances in Cryptology—Crypto ’92 : 139–147.

[194]: Adam Back, “ANNOUNCE hash cash postage implementation,” originally sent to the Cypherpunks mailing list, March 28, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/03/msg00774.html.]

[195]: Adam Back, “Re: Remailer problem solution?” March 23, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/03/msg00631.html.]

[198]: Nick Szabo, “Why Cryptocurrency? Governments Abuse Their Power—Nick Szabo Interview Part 1,” interview by Zulu Republic, Zulu Republic, YouTube, October 25, 2018, [https://youtu.be/LZw4LNLYUgc?si=…lNeaFnWxpvv9U.]

[199]: Nick Szabo , “Some of the most important books I’ve read,” X, January 31, 2016, [https://twitter.com/NickSzabo4/status/693682157525401601.]

[200]: Nick Szabo, “Re: Crypto + Economics + AI = Digital Money Economies,” originally sent to the Cypherpunks mailing list, September 19, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/09/msg01303.html.]

[201]: Nick Szabo, “Smart Contracts: Building Blocks for Digital Free Markets,” Extropy 16 : 50–64.

[202]: Szabo, “Smart Contracts,” 51.

[203]: Nick Szabo, “Re: Crypto + Economics + AI = Digital Money Economies,” originally sent to the Cypherpunks mailing list, September 19, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/09/msg01303.html.]

[205]: Nick Szabo, “Trusted Third Parties are Security Holes,” Satoshi Nakamoto Institute , [https://nakamotoinstitute.org/trusted-third-parties/.]

[206]: Nick Szabo, “Nick Szabo on Cypherpunks, Money and Bitcoin,” interview by Peter McCormack, What Bitcoin Did, November 1, 2019, [https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin.]

[207]: Nick Szabo, “Bit Gold,” Unenumerated, December 27, 2008, [https://unenumerated.blogspot.com/2005/12/bit-gold.html.]

[209]: Nick Szabo, “Shelling Out: The Origins of Money,” Satoshi Nakamoto Institute , [https://nakamotoinstitute.org/shelling-out/.]

[210]: It is worth noting however that this number—named after primatologist Robin Dunbar—has been criticized, and isn’t, in the scientific community today, held with the specificity that it suggests. While there is a limit on the number of stable social relationships people can maintain, the actual number isn’t necessarily 150 for everyone. See for instance Patrick Lindenfors, Andreas Wartel, and Johan Lind, “‘Dunbar’s Number’ Deconstructed,” Biology Letters, May 5, 2021: <https://royalsocietypublishing.org/doi/10.1098/rsbl.2021.0158>

[211]: Strictly speaking a “public goods game” is the more precise game theory analogy.

[213]: In Szabo’s original proposal, Bit Gold would actually use a “secure benchmark function,” which is slightly different from a hash function, but similar enough that referring to the product as a “hash” and the act of producing it as “hashing” is accurate enough for the purpose of understanding Bit Gold’s mechanics .

[214]: Nick Szabo, “Secure Property Titles with Owner Authority,” Satoshi Nakamoto Institute , [https://nakamotoinstitute.org/secure-property-titles/.]

[215]: Nick Szabo, “Nick Szabo — The Quiet Master of Cryptocurrency … Hosted by Naval Ravikant” interview by Tim Ferriss, The Tim Ferriss Show, YouTube, August 12, 2017, <https://youtu.be/3FA3UjA0igY>

[217]: Nick Szabo, “Bit Gold: Towards Trust-Independent Digital Money” , accessed via [https://web.archive.org/web/20140406003811/http://szabo.best.vwh.net/bitgold.html.]

[218]: Nick Szabo, “Bit Gold Markets,” Unenumerated, December 27, 2008, [https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html.]

[221]: Wei Dai, “Work on Security Instead of Friendliness?” GreaterWrong, July 21, 2012, [https://www.greaterwrong.com/posts/m8FjhuELdg7iv6boW/work-on-security-instead-of-friendliness.]

[222]: Wei Dai, “Law vs Technology,” originally sent to the Cypherpunks mailing list, February 10, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/02/msg00508.html.]

[223]: Wei Dai, “PipeNet 1.1 and b-money,” originally sent to the Cypherpunks mailing list, November 26, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/11/msg00941.html.]

[224]: Wei Dai, untitled b-money description, 1998, accessed via [https://web.archive.org/web/20090415130807/https://www.weidai.com/bmoney.txt.]

[226]: Wei Dai, “Re: alternative b-money creation,” originally sent to the Cypherpunks mailing list, December 11, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/12/msg00448.html.]

[227]: Wei Dai, comment in the discussion thread “AALWA: Ask any LessWronger anything,” LessWrong, 2014, [https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything.]

[229]: Eric Hughes, “Kid Gloves or Megaphones,” originally sent to the Cypherpunks mailing list, March 14, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/03/msg00932.html.]

[233]: Damien Cave, “The Mojo solution,” Salon, October 9, 2000, [https://www.salon.com/2000/10/09/mojo\_nation/.]

[236]: Daniel A. Nagy, comments in response to “The Mojo Nation Story—Part 2,” Financial Cryptography, October 12, 2005, <https://www.financialcryptography.com/mt/archives/000572.html>

[237]: Bryce Wilcox-O’Hearn, “Experiences Deploying A Large-Scale Emergent Network,” Peer-to-Peer Systems : 104–110.

[239]: Liang Wang, “BitTorrent Mainline DHT Measurement,” MLDHT, 2013, accessed via: [https://www.cl.cam.ac.uk/…525/MLDHT/.]

[240]: BitTorrent, “BitTorrent and µTorrent Software Surpass 150 Million User Milestone; Announce New Consumer Electronics Partnerships,” BitTorrent.com, January 9, 2012, accessed via [https://web.archive.org/web/20140326102305/http://www.bittorrent.com/intl/es/company/about/ces\_2012\_150m\_users.]

[241]: Hendrik Schulze and Klaus Mochalski, “Internet Study 2008/2009,” ipoque .

[242]: Tim May, “My Departure, Moderation, and ‘Ownership of the List,’ originally sent to the Cypherpunks mailing list, February 2, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/02/msg02898.html]

[243]: ​Mark Frauenfelder, “Homeless Cypherpunks Turn to Usenet,” Wired, February 17, 1997, [https://www.wired.com/1997/02/homeless-cypherpunks-turn-to-usenet/.]

[244]: Declan McCullagh, “Digging Those Digicash Blues,” Wired, June 14, 2001, [https://www.wired.com/2001/06/digging-those-digicash-blues/.]

[245]: Nicole Weinstock, “Member Profile: Hal Finney,” Cryonics 40, issue 2 : 9.

[246]: Hal Finney, “Re: Physical to digital cash, and back again,” originally sent to the Cypherpunks mailing list, August 19, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00581.html]

[247]: Hal Finney, “Why remailers…,” originally sent to the Cypherpunks mailing list, November 15, 1992, accessed via: [https://cypherpunks.venona.com/date/1992/11/msg00108.html.]

[248]: Hal Finney, “Re: Voluntary Governments?” originally sent to the Cypherpunks mailing list, August 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/08/msg00239.html.]

[249]: Hal Finney, “POLI: Politics vs Technology,” originally sent to the Cypherpunks mailing list, January 2, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/01/msg00014.html.]

[250]: Hal Finney, “Re: Re: re: re: digital cash,” originally sent to the Cypherpunks mailing list, March 16, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/03/msg00694.html.]

[252]: Hal Finney, “Reusable Proofs of Work,” RPOW website index page, accessed via: [https://web.archive.org/web/20090217090451/http://rpow.net/index.html.]

[253]: Hal Finney, “RPOW Theory,” RPOW website theory page, accessed via [https://web.archive.org/web/20040815154951/http://rpow.net/theory.html.]

[254]: Hal Finney, “RPOW FAQs,” RPOW website FAQ page, accessed via [https://web.archive.org/web/20090217090439/http://rpow.net/faqs.html#inflation.]