NLCoin

Een digitale staatsmunt die geldschepping door de Staat op orde houdt.

Bachelorscriptie
Luuk de Waal Malefijt - 3349209
luuk@waalmalefijt.nl
Februari 2014
begeleiders: dr. G. Tel & dr. M.R. Spruit
dpt. Informatie- en Computerwetenschappen
Universiteit Utrecht

NLCoin

Een onderzoek naar de haalbaarheid om (1) een nationale munt te baseren op het Bitcoin-protocol, met de Staat als enige autoriteit voor geldcreatie, en (2) deze in de processen van het Nederlandse overheids- en bankwezen te integreren.

abstract

Sinds het uitbreken van de financiële crisis in 2007/2008 is het duidelijk dat er iets mis is met het geldsysteem, en is er steeds meer aandacht voor alternatieve geldsystemen. Een plan van twee onderzoekers van het IMF beoogt de crisis op te lossen door de Staat het klassieke monopolie op (digitale) geldcreatie terug te geven. Op deze manier kan schuld- en rentevrij geld in omloop worden gebracht. Dit plan wordt echter veelal kritisch bejegend vanwege de diepgewortelde, vaak onterechte, vooroordelen over een dergelijke constructie. Tegenstanders waarschuwen voor een imminente hyperinflatie door monetaire financiering.

Innovaties zoals Bitcoin scheppen echter nieuwe mogelijkheden voor transparantie en regelgeving omtrent het geldsysteem in het algemeen en geldcreatie in het bijzonder. De innoverende eigenschappen van het Bitcoin-protocol zouden het vertrouwen kunnen scheppen dat nodig is om digitaal staatsgeld te kunnen implementeren. In dit paper zal onderzocht worden of er (technische) garanties gegeven kunnen worden tegen de vernomen gevaren van geldcreatie door de overheid en zal getracht worden de vraag of het mogelijk is digitaal staatsgeld te implementeren op basis van het Bitcoin-protocol te beantwoorden. Tevens wordt onderzocht wat er voor nodig is in de IT-structuur van het Nederlands overheids- en bankwezen om een dergelijke munt te kunnen ondersteunen, en hoe enkele hedendaagse betaalproducten vervangen kunnen worden op basis van '*smart contracts*'.

keywords

bitcoin, nlcoin, soeverein geld, digitaal geld, staatsgeld, staatsmunt, cryptogeld, geldsysteem, smart contract, wederzijdse claimaanvaarding

Inhoudsopgave

0. Inleiding

Door de crisis in 2007/2008 ben ik gaan nadenken over geld. Wat het (tegenwoordig) voorstelt, waar het vandaan komt en hoe er opeens te weinig van kon zijn. Ik kwam in 2012 tijdens mijn zoektocht naar inzicht uiteindelijk in aanraking met Positive Money uit Engeland, een denktank die pleit voor een staatsmonopolisering op digitaal geld. In deze periode leerde ik tevens Bitcoin kennen. Toen heb ik me afgevraagd waarom Positive Money wél het concept van geld wilde 'moderniseren', maar dat niet beoogde ook op een technisch vlak te doen, op basis van Bitcoin bijvoorbeeld. In deze scriptie wilde ik ingaan op die mogelijkheid. Alles dat behandeld zal worden zal in dienst staan van het beantwoorden van de vraag: '*kan je een staatsmunt baseren op Bitcoin*?'. Vraagstukken over de uiteindelijke inrichting van het monetair systeem vallen buiten de scope van het onderzoek. Het is niet de bedoeling hier een standpunt in te nemen over of we (bijvoorbeeld) de Euro zouden moeten houden of niet, en of we staatsgeld nodig zouden hebben of niet. Het onderzoek is een uiting van academische interesse naar de manier waarop een staatsmunt op basis van Bitcoin ingericht zou kunnen worden. Of dat politiek de juiste keuze zou zijn is hier niet belangrijk.

Het paper bestaat grofweg uit twee delen. Het eerste deel is het theoretisch kader waarin de werking van Bitcoin wordt uitgelegd. Hier wordt ook de aard van geld besproken en de relatie tot het hedendaagse geldsysteem. Met deze achtergrondinformatie is het makkelijker de drie systemen, zijnde het hedendaagse geldsysteem, Bitcoin en NLCoin, uiteindelijk te vergelijken. Ondanks dat het theoretisch kader voor begrip ondersteunend is, is het niet essentieel. Wanneer er slechts interesse is voor de (technische) beantwoording van de onderzoeksvragen kan dit kader in het geheel worden overgeslagen.
Het tweede deel behelst het onderzoek en bestaat uit vijf deelvragen. Het eerste paar van vragen ('*Bitcoinimplementatie van staatsgeld*' en '*Protocollimiet op geldschepping & drempelvorming*') zijn van technische aard en bespreken het resultaat van de implementatie van een prototype. De derde vraag ('*Schaalvergroting van Bitcoin naar Nederlandse proporties*') is op basis van literatuur- en brononderzoek waarbij er wordt gekeken naar alternatieve algoritmen en ontwerpbeslissingen. De laatste twee vragen ('*Inbedding in banksysteem en regelgeving'* en *'Technische ondersteuning in het bankwezen*') zijn dan weer theoretisch van aard. In deze vragen wordt een implementatie beredeneerd met hulp van interviews die zijn afgenomen met enkele technici van banken. De opgenomen *educated guesses* en standpunten zijn van

persoonlijke aard en interesse geweest en vertegenwoordigen geenszins de mening van de respectievelijke bank.

Er is nog niet veel onderzoek gedaan naar de mogelijkheid om staatsmunten te baseren op Bitcoin. Enkele voorbeelden uit de praktijk die de vraag raken zijn opgenomen in de introductie, maar er is nog weinig over geschreven. Dit kan komen door de politieke aard van Bitcoin, die geworteld is in het wantrouwen in overheid en autoriteit, en daarmee onderzoek naar een synergie onwaarschijnlijk maakt. Het onderzoek dat hier gepresenteerd wordt zal ondanks de explorerende aard hopelijk leiden tot meer diepgaand onderzoek van hetzelfde soort.

1. Introductie

In 2007/2008 begon de financiële crisis, de meest recente episode van een serie van financiële crises die al gaande zijn sinds het begin van het 'moderne' financieel systeem[1] Directe oorzaak was het springen van de vastgoedbubbel in de V.S. Deze bubble was onstaan doordat de Amerikaanse overheid jarenlang huizenbezit stimuleerde en zelfs verordende dat het ook makkelijk moest zijn voor Amerikanen (met lage inkomens) om een hypotheek te verkrijgen[1]. Steeds riskantere hypotheken werden verstrekt. Bovendien werden de hypotheken gesecuritiseerd en overgewaardeerd verkocht in zogeheten CDO's ('*collateralized debt obligations'*) door een complex spel tussen banken en kredietbeoordelaars. De Financial Services Agreement (FSA) van het WTO uit 1997 had de deur geopend om deze producten internationaal te verkopen. Na het springen van de bubbel, ingeleid door de val van de Lehman Brothers bank, werden er internationaal grote verliezen geleden door partijen die waardeloze derivaten in handen hadden, zoals banken en pensioenfondsen. Hiermee sloeg de crisis over naar Europa en kwamen Europese banken in de problemen.

Het werd duidelijk dat er veel economische en systeem-structurele instabiliteit is door de wijze waarop het bank- en geldsysteem is opgebouwd. Er werd onder de programmanaam 'Quantitative Easing' internationaal veel nieuw geld gecreëerd om te dienen als liquiditeit voor banken, met angst voor inflatie als gevolg. Het wantrouwen in financiële instituten en overheden laaide op en langzaamaan is er een groter bewustzijn ontstaan over de vraag wat geld eigenlijk is, waar het vandaan komt en wie het zou moeten uitgeven.

Inmiddels is er een internationale beweging[2] die beweert dat (schulden)crises en recessies worden veroorzaakt door de manier waarop geld wordt gecreëerd; verrassenderwijs niet door overheden maar door private commerciële banken. Zo zijn er o.a. het American Monetary Institute (US), Positive Money (UK, NZ), Monetative (DE) en Ons Geld (NL) als onderdeel van de beweging. Zij beogen de schuldencrisis op te lossen door Full-reserve banking te implementeren. Full-reserve banking is een relatief onbekende term uit de boekhouding die in de uitvoering resulteert in het wegnemen van de status van 'geldscheppende instelling'[2] zijnde

[1] In Nederland dreigt nu hetzelfde te gebeuren: bloomberg.com/news/2013-10-27/dutch-copy-fannie-mae-seen-by-blackrock-as-taxpayer-risk.html
[2] International Movement for Monetary Reform (IMMR)

die banken momenteel nog genieten. De voorstellen van deze Full-reserve proponenten zijn op basis van het Chicago Plan van Irving Fisher[3] en het vernieuwde plan van twee onderzoekers van het IMF[1].

Er is echter een vast repertoire van tegenargumenten afkomstig van de tegenstanders van de voorgenoemde plannen. Deze tegenstanders zijn veelal bankiers en hun repliek laat zich makkelijk typeren. Zo beargumenteert Wim Boonstra, hoofdeconoom van de Rabobank het volgende:

> *"De verleiding om dan maar door te gaan met het aanmaken van geld is (...) altijd aanwezig, (...) De geschiedenis heeft laten zien dat die verleiding vaak te groot is. Bij het drukken van geld kan de geldhoeveelheid sneller toenemen dan de beschikbare hoeveelheid verhandelbare goederen en diensten en dat kan zich vertalen in een snelle stijging van het gemiddelde prijspeil. Eerder werd er al op gewezen dat bijna alle periodes van hyperinflatie (zeer snelle geldontwaarding) kunnen worden teruggevoerd op overheden die misbruik maakten van hun monopolie op de productie van geld."*[4].

Ondanks dat deze kritiek makkelijk te pareren is[1], [5], [6] impliceert het wel een aantal zaken waar publieke geldcreatie dus blijkbaar aan zou moeten voldoen om door grote partijen in deze tijden[3] geaccepteerd te worden. Zo zal er o.a. maatschappelijke controle mogelijk moeten zijn op geldschepping die een nog ongeziene mate van transparantie vereist. Met nieuwe innovaties uit de informatietechnologie is het wellicht mogelijk procedurele of algoritmische limieten af te dwingen die met grote zekerheid kunnen garanderen dat Zwarte Zwanen als bovengenoemde hyperinflaties hier niet zullen voorkomen.

In 2008 publiceerde Satoshi Nakamoto[4] zijn paper[7] met de uitleg voor het Bitcoin protocol, een decentrale munteenheid, onafhankelijk van centrale banken, op basis van cryptografie (om deze

[3] vóór ~1600 werd het als vanzelfsprekend gezien dat het privilege van geldcreatie inherent in handen moest zijn van de soevereine macht

[4] Ondanks dat de auteur nog lange tijd na de publicatie van het paper in de openbaarheid heeft meegewerkt aan de broncode en veel technische uitleg heeft gegeven op het Bitcoin-forum, is de identiteit in nevelen gehuld. Het laatste wat van de auteur is vernomen is een bericht op het Bitcoin-forum op 12 December 2010. Er wordt online veel gespeculeerd over de ware identiteit, met name vanwege de vermoedens dat hij of zij eigenaar is van een aantal Bitcoins waarvan de waarde ten tijde van schrijven vele miljoenen Euro's overstijgt.

reden behoort de munteenheid tot de noemer '*cryptovaluta*') die (tot nog toe) niet te vervalsen is en voor het eerst écht het 'double spending'-probleem oploste (Nakamoto (2008)). Dit betalingssysteem toonde in contrast met het gangbare banksysteem zeer stabiel te zijn[5] in veiligheid[6] en functie en heeft waarschijnlijk om die reden veel aan populariteit gewonnen. Er moet gezegd worden dat er andere digitale munteenheden zijn geweest in het verleden, maar die waren vaak toch op de een of andere manier van een centrale autoriteit afhankelijk.

Zoals het citaat van Boonstra illustreert is er (in voornamelijk financiële kringen) weerzin tegen geldcreatie door de staat. Aan de andere kant is er ook een publiek ongenoegen over de manier waarop commerciële banken opereren. Een innovatie als Bitcoin kan daar aan beide kanten veranderingen in aanbrengen door zowel de benodigde transparantie te bieden in het proces van geldcreatie door de staat, als in de boekhouding van financiële instituten. Dit vermeldt de officiële website van Bitcoin op de pagina *'Innovation'* onder het kopje '*Trust and integrity*' (2013):

> *Bitcoin offers solutions to many of the trust problems that plague banks. With selective accounting transparency, digital contracts, and irreversible transactions, Bitcoin can be used as a ground to restore trust and agreement. Crooked banks cannot cheat the system to make a profit at the expense of other banks or the public. A future in which major banks would support Bitcoin could help to reinstate integrity and trust in financial institutions.* [8]

Dat de ontwikkeling van schuld- en rentevrij geld uitgegeven door de Staat op basis van een cryptovaluta een mooie dialectische synthese zou zijn, van de wens voor een digitale staatsmunt enerzijds en de opkomst van Bitcoin anderzijds, getuigt zich uit de gemoederen van een auteur, 'Democraatus', die anoniem wenste te verblijven[7], op de blog Zaplog.nl waar hij of zij op 4 November 2013 o.a. het volgende schreef:

---

[5] vanuit systeemperspectief gezien. De valuta is nog zeer volatiel.

[6] hiermee doel ik op de veiligheid van de systematiek van het betalingsnetwerk zelf; er zijn immers al talloze voorbeelden van diefstallen van Bitcoins bekend, maar die zijn niet te wijten aan defecten van het protocol.

[7] Ik heb met de auteur contact gezocht in de hoop dat hij of zij wat meer zou willen vertellen over hoe het idee is ontstaan, maar deze wenste er niet dieper op in te gaan.

Het geld ligt op straat

Er ligt een gouden kans voor ons om een eigen munt in te voeren: de Dutchcoin. Stel je voor, een cryptocurrency van eigen bodem gebaseerd op Bitcoin software. De Staat der Nederlanden rolt eigen Bitcoin software uit (open source) en zorgt voor de beschikbaarheid van programma's voor Mac/PC en mobiele apparaten. Het netwerk ligt er allang; het Internet, de daarop aangesloten betaalsystemen en het zeer wijdverbreide smartphone netwerk dat inmiddels op 4G overgaat.

Bij lancering geeft de Staat iedereen via zijn Digi-ID een vast bedrag aan Dutchcoins (bijvoorbeeld DTC 10.000). Eventueel wordt in de software ingebakken dat de Staat per jaar 1% nieuwe Dutchcoins krijgt voor het jaarlijkse overheidsbudget. Ook is denkbaar dat over dit jaarlijkse percentage wordt gestemd ieder jaar, ook weer via de Digi-ID. Een belangrijk element: de Staat accepteert Dutchcoin voor het betalen van belasting. Verder wordt de Dutchcoin aan de vrije markt overgelaten.

Het geld zijn wij

Het resultaat is schuldvrij geld. De Staat voorziet in een klap in geld dat niemands schuld is. Er lekt geen rente meer weg naar private partijen die ooit het privilege hebben gekregen[8] *om ons geld 'uit de lucht' te printen. De Staat vermijdt immense bedragen aan rente. Het first mover voordeel*[9] *biedt een uitgelezen kans om de bestaande staatsschuld in de oude geldeenheid snel af te lossen met in waarde stijgende Dutchcoins. Logisch, want de waarde van geld zijn wij zelf.*

---

[8] er wordt hier de incorrecte notie gemaakt dat banken dit privilege ‘verkregen’ hebben, maar in realiteit is dit een toeëigening geweest door schijnende afwezigheid van regulatie door staatsmonopolisering zoals dat wel is gebeurd met cash-geld.

[9] Met het ‘first mover voordeel’ wordt hier gerefereerd naar het voordeel dat een partij behaalt door als eerste een bepaald marktsegment in te nemen. Hierna is het namelijk moeilijker voor latere partijen om nog een dergelijk groot segment te veroveren. Denk hierbij bijvoorbeeld aan Bitcoin, de allereerste cryptovaluta. Alternatieve cryptovaluta hebben veel moeite het marktsegment van Bitcoin te benaderen, puur omdat Bitcoin de eerste is in zijn soort. De notie is hier echter irrelevant omdat de Staat zich per definitie een monopoliepositie kan verwerven als zij dat wenst. Een schrijver aanhangig aan de Oostenrijkse school zei het volgende dat het punt illustreert: "*The overwhelming reason that Bitcoin is superior to its altcoin competitors is that it is overwhelmingly more popular. Some of its competitors might have worked as well or better had they been invented first, but given the history that led us here, none of them should be considered remotely competitive to Bitcoin.*" - http://themisescircle.org/blog/2013/08/22/the-problem-with-altcoins/

De stabiele geldhoeveelheid waaraan nooit tekort hoeft te zijn is een feit, en de onlangs door de overheid gepropageerde participatiemaatschappij kan een feit worden.”[9]

De Canadese regering leek op dezelfde conclusie te zijn gekomen. In 2012 kondigde[10] de 'Royal Canadian Mint', het instituut dat de verantwoording draagt voor de fysieke geldcreatie in Canada, aan dat het een digitale valuta zou introduceren: 'MintChip'. Ze verklaarden de ontwikkelingen van elektronisch geld “al jaren in het oog te hebben gehouden” en vonden het tijd een digitale valuta te introduceren[11].

"*With the explosion of mobile commerce, a significant increase in electronic transactions over the past ten years, and the growing popularity of micro transactions (under $10) and nano-transactions (under $1), the Mint saw an opportunity in the virtual space for a new currency option.*"[12]

"*there has been no electronic solution that cost-effectively addresses the very-low-value transaction markets, protects privacy, is available to everyone and emulates the characteristics of cash*"

Ondanks dat het klinkt alsof ze hiermee een revolutionaire digitale staatsmunt introduceren werkt het systeem op basis van een chip die een waarde vast moet houden. Het is de bedoeling dat de chip zó wordt ontworpen dat er niet mee gesjoemeld kan worden.

"*The MintChip chip is a Tamper Resistant Module (TRM), sometimes also called a Hardware Security Module (HSM). The Value Transfer Protocol cannot be modified without detection*."

.. leest het op de website[13]. De techniek is dus afhankelijk van een soort DRM en de geschiedenis leert dat DRM-systemen toch doorgaans gekraakt worden. Een blogpost op 5 April 2012 op de website 'Bitcoin Magazine' illustreert dit:

"*About two years ago, the supposedly “unhackable” Infineo chip was hacked by Christopher Tarnovsky using an electron microscope, needles and acid, and one can only imagine how quickly such a feat would be repeated when doing so gives you*

essentially gives you an unlimited license to print money. The paradox of simultaneously giving users' devices the ability to arbitrarily modify their balance and denying that ability to the users themselves, even while the devices are in the users' hands, seems far less compelling a basis for a sound digital currency system than cryptographic digital signature algorithms and a proof-of-work based distributed public blockchain."[14]

MintChip is een substituut voor cash geld (en wordt dus gedekt door het officiële overheidsgeld) en de credits voor op de chip dienen aangekocht te worden bij daarvoor aangewezen 'brokers'. De overheid behoudt de mogelijkheid updates en patches voor de techniek geforceerd uit te rollen. De nieuwe digitale munt in Canada is dus niet het soort revolutionair staatsgeld dat we hier voor ogen hebben, zoals ook wordt beaamd in het artikel '*Mintchip Misses the Point of Digital Currency*'.[15]

Op 27 December 2013 kondigde het '*Oyate Initiative*'[16] van de Oglála, een van de zeven stammen van de Lakota-Sioux[17] woonachtig in het indianenreservaat '*Pine Ridge Indian Reservation*'[18], aan een soevereine munt te gaan gebruiken op basis van Bitcoin:

"The MazaCoin Development Team is proud and honored to have been commissioned by the Oglala Lakota Nation to create for them the first ever Sovereign National Crypto-Currency. It is rare in history when we witness any nation creating a new sovereign coinage. This alone makes this an historic moment. The Oglala Lakota Nation have internationally recognized sovereignty, and their right to mint currency is guaranteed by treaty. And in fact the Oglala Lakota Nation has already exercised that right symbolically by minting collectible coinage and trading rounds. Choosing to deploy a genuine and functional national currency is nevertheless a bold initiative."[19]

50 Miljoen van deze munten zullen gedolven worden en naar de regering gaan, en 50 miljoen gaan naar een eigen liefdadigheidsfonds. Nadat deze munten zijn gedolven zal de aangepaste broncode worden vrijgegeven en zal het ook voor buitenstaanders worden toegestaan de zogenaamde 'MazaCoin' te *minen,* wat de vraag doet rijzen of de munt dan nog werkelijk in soevereine handen is.

Ten slotte kondigde[20] het kanaaleiland Alderney[21], het meest noordelijke eiland in het kanaal tussen Frankrijk en Engeland als onderdeel van de Britse Kroon, aan als eerste jurisdictie ooit tot nu toe fysieke Bitcoins te gaan produceren op basis van goud.

> "*The three-mile long British crown dependency has been working on plans to issue physical Bitcoins in partnership with the UK's Royal Mint since the summer, according to documents seen by the Financial Times. It wants to launch itself as the first international centre for Bitcoin transactions by setting up a cluster of services that are compliant with anti-money laundering rules, including exchanges, payment services and a Bitcoin storage vault. (…) David Janczewski, head of new business at the Royal Mint confirmed it had been approached by the finance minister of Alderney to "explore the possibility of manufacturing a physical commemorative coin with a Bitcoin theme".* "
>
> [22]

Het lijkt door de financiële crisis en de opkomst van revolutionaire middelen in valuta zoals Bitcoin dat er opnieuw gekeken wordt naar het concept van geld, en naar wat de rol van de overheid en het bankwezen daarin zou moeten zijn. Dit blijkt uit de voorbeelden uit Canada, het indianenreservaat en het kleine eilandje onder Brits bewind. In dit paper zullen de rollen ook opnieuw gewogen worden en wordt er onderzocht hoe Nederland een dergelijke verandering zou moeten ondergaan.

In de volgende sectie zullen we kijken waar een staatsmunt aan zou moeten voldoen volgens de beweging die pleit voor een transitie naar schuldvrij geld. Dan wordt de probleemstelling geformuleerd.

In het theoretisch kader zal er een introductie gegeven worden van het Bitcoinprotocol en de manier waarop het ons anders doet nadenken over de definitie van geld. Daarna wordt kort de mechaniek van het hedendaagse geldsysteem behandeld om een eerlijke vergelijking te kunnen maken met Bitcoin. Het theoretisch kader zal worden afgesloten met de daadwerkelijke vergelijking van de twee systemen, en een uitleg die expliceert waarom het wenselijk is dat een staatsmunt gebaseerd dient te worden op het Bitcoinprotocol. Het theoretisch kader is bedoeld om de context en technische concepten te schetsen voor het onderzoek, maar het onderzoek kan hier ook los van beschouwd worden.

1.1 Waar moet een nieuwe staatsmunt aan voldoen?

De eisen aan een nieuwe staatsmunt volgen grotendeels uit de voorstellen van leden van de IMMR, die zich op hun beurt baseren op het Chicago Plan. Zowel Positive Money[23] als Ons Geld[24] stellen dat geldcreatie (inclusief de geldscheppingswinst) in het algemeen belang moet dienen.

Zij stellen dat geldcreatie dient te gebeuren door een “transparant orgaan” en dat de beslissing 'hoeveel nieuw geld?' moet worden gescheiden van het besluit over de allocatie ervan. Stichting Ons Geld stelt:

> “*We willen graag de macht om geld te creëren overhevelen naar een democratisch, controleerbaar en transparant proces, waarbij iedereen weet wie de macht heeft om geld te creëren, hoeveel geld ze creëren, en hoe dat geld zal worden gebruikt. (...)*”

1.1.1 Transparantie van feitelijke statistieken

De nadruk ligt hier op de transparantie van het instituut en het proces. Het is voor het maatschappelijk vertrouwen belangrijk dat te allen tijde op aantoonbaar eerlijke wijze aangetoond kan worden wat de stand van zaken is. Het moet aantoonbaar duidelijk zijn hoeveel geld er op enig moment bestaat, en hoeveel er nieuw gecreëerd is/wordt. Dat is belangrijk voor democratische legitimiteit. Immers heeft de bevolking het recht te weten wanneer zaken uit de hand dreigen te lopen, te zien aan de hand van de data. Door een garantie te kunnen bieden op feitelijke juistheid worden ook critici als Boonstra tegemoet gekomen. De angst voor hyperinflatie die hij verwoordt kan deels worden ontnomen door de geldscheppende instantie de mogelijkheid te ontnemen feiten te verdraaien.

In het eerdergenoemde citaat (blz. 5) wordt genoemd dat het ook duidelijk moet zijn *wie* de macht heeft het geld te creëren. Wat hiermee bedoeld wordt is dat het instituut zó transparant moet zijn dat men weet welke mensen er in de verantwoordelijke commissie voor geldcreatie zitten. Deze doelstelling zal ik hier ietwat omvormen aangezien hier niet behandeld wordt hoe dat transparante geldscheppingsinstituut er uit moet zien. In dit paper zal het beoogde geldsysteem m.b.t. deze vraag dan ook slechts een garantie moeten kunnen geven dat het de

Staat is die daadwerkelijk de enige macht heeft het geld te doen ontstaan, en niets of niemand anders.

Dat de eis van operationele transparantie nog niet zo'n makkelijk streven is blijkt uit enkele voorbeelden. Het probleem dat er eigenlijk altijd geweest is, is dat uiteindelijk de verantwoordelijkheid voor het juist rapporteren van statistieken, zoals de geldhoeveelheid of de geldgroei, lag bij mensen. Deze mensen kunnen om wille van allerlei redenen vanuit het instituut besluiten de statistiek van feitelijke informatie op een andere manier te presenteren dan bedoeld, of helemaal niet meer publiceren. Dit wordt geïllustreerd door Milton Friedman, internationaal bekend econoom, die hierover spreekt:

> *"The difficulty of having people understand monetary theory is very simple—the central banks are good at press relations. The central banks hire people and the central banks employ a large fraction of all economists so there is a bias to tell the case—the story—in a way that is favorable to the central banks.*"[25]

Hier is een typerend voorbeeld voor. Op 10 November 2005 bracht de Federal Reserve, de private centrale bank van de Verenigde Staten, het volgende bericht naar buiten:

> "***Discontinuance of M3***
> *On March 23, 2006, the Board of Governors of the Federal Reserve System will cease publication of the M3 monetary aggregate. The Board will also cease publishing the following components: large-denomination time deposits, repurchase agreements (RPs), and Eurodollars. The Board will continue to publish institutional money market mutual funds as a memorandum item in this release.*
>
> *Measures of large-denomination time deposits will continue to be published by the Board in the Flow of Funds Accounts (Z.1 release) on a quarterly basis and in the H.8 release on a weekly basis (for commercial banks).*
>
> *M3 does not appear to convey any additional information about economic activity that is not already embodied in M2 and has not played a role in the monetary policy process for many years. Consequently, the Board judged that the costs of collecting the underlying data and publishing M3 outweigh the benefits.*"

Een senator stelde hier in 2005 vragen over aan Bernanke, de voorzitter van de Federal Reserve:

> "*The findings of the M3 report provide pertinent information to the public — from economists to investors and to industries which all use M3 report findings for economic forecasting, investing and business decisions. … Will you work to reverse this policy and commit to keeping the M3 report and its findings available and open to the public? What is the rationale and reasoning behind the Federal Reserve decision to keep the M3 information from the public?*"

En de voorzitter gaf de beweegredenen:

> *"(...) because the costs of collecting and processing the underlying data were judged to exceed the benefits. The Federal Reserve will not withhold the M3 data from the public; rather, it will no longer collect and assemble that information. The Federal Reserve will continue to collect data for and publish the monetary aggregates M1 and M2 and their components.*
>
> *The benefits of continuing to publish M3 appear to be minimal, because M3 has not been actively used in the formulation of U.S. monetary policy and, at least within the Federal Reserve, has not been found to have much value for economic forecasting. (...)"*[26]

Bernanke werkt hier slim om het kernpunt heen: de wens van het publiek tot transparantie over data van het geldsysteem, die in het huidige geldsysteem niet anders te achterhalen zijn dan via het portier van de Federal Reserve. Hij zegt niet dat het instituut data censureert of niet meer publiceert, wat in zou gaan tegen het idee van transparantie, maar dat de data simpelweg niet meer verzameld zullen worden, en daarmee niet gepubliceerd kúnnen worden. Dat de statistiek ondanks de woorden van de voorzitter waarschijnlijk toch van nut geweest zouden zijn blijkt uit het sentiment van auteur Jire Sekar, die in een artikel "*Death of M3: The Fifth Anniversary*" het volgende zegt:

"*If the Fed had been tracking repos in 2007–2008, what they would have seen was the unfolding of the financial crisis one full year before it went critical.*"[27]

Ook Tim McMahon, auteur op InflationData.com, denkt er zo over:

> "*In other words, M3 tracks what the big boys are doing with the money. (...) perhaps I'm just suspicious by nature but it begs the question, what are they trying to hide? (...) It is no coincidence that the M3 went up an annualized 9.4% in the last three months and an annualized 17.2% in December alone and now the FED wants to stop tracking it! (...) The writing is on the wall. When the Government starts hiding data the problem is big! If this trend continues, inflation is going to come roaring back big time.*"[28]

De voorbeelden zijn ook dichter bij huis te vinden. In de documentaire "*De Schuldvraag*" van TROS Radar die 17 December 2013 voor het eerst online vertoond werd komt hoogleraar Ewald Engelen erachter dat de Rekenkamer, "*een onafhankelijk orgaan dat controleert of de uitgaven van de Nederlandse rijksoverheid rechtmatig en doelmatig zijn*"[29], die boekhoudkundige controle moet uitoefenen op o.a. toezichthouders zoals De Nederlandsche bank, geen inzicht krijgt in dossiers van DNB vanwege een Europese geheimhoudingsbepaling.

Kortom, in een ideaal nieuw geldsysteem dient er geen *bottleneck* te zijn in de publicatie van essentiële statistieken en heeft iedereen dus toegang tot de data omtrent de geldhoeveelheid zonder een afhankelijkheid aan een instituut. Liever nog: zonder afhankelijkheid van menselijke tussenkomst.

1.1.2 Geld dient vrij van schuld te ontstaan

De doelstellingen van de International Movement for Monetary Reform zijn eerder al kort aan bod geweest in de inleiding. De IMMR beoogt dat in een nieuw geldsysteem het geld, in tegenstelling tot hoe dat nu gebeurt, vrij van schuld ontstaat. Later, in de sectie over de werking van het hedendaagse geldsysteem (3.2), zal in meer detail behandeld worden hoe het merendeel van het geld tegenwoordig ontstaat, waarom daar schulden bij komen, en waarom geld momenteel gelijk gesteld wordt aan schuld. Positive Money, bestaand sinds 2010, legt de eis voor geld dat niet gebaseerd is op schuld als volgt kort uit:

> "*Currently, banks create money when they make loans, which means that for every pound in your bank account, someone somewhere else will be a pound in debt. It means that almost all the money in the economy is effectively 'on loan' from the banking sector,*

and interest must be paid nearly every pound that exists. If we try to reduce our debts, money disappears from the economy, making it harder for others to repay their own debts. But if money was created by the state, in the public interest, and spent into the economy through government spending instead of being lent into the economy by banks, then that money would stimulate the real economy, create jobs, and make it possible for ordinary people to start reducing their own debts."

Het systeem dat zij beschrijft van private geldcreatie door wederzijdse schuldaanvaarding is internationaal de praktijk. In het citaat kan je de Ponden vervangen met menig andere valuta zonder af te doen aan de werkelijke situatie. Door een nieuwe staatsmunt niet te baseren op schuld zal het geldsysteem veel stabieler zijn.

1.1.3 Geld dient risicovrij te zijn

In het huidige geld- en banksysteem, mede doordat het hedendaagse geld is gebaseerd op schuld, is er voor de houders van geld op bankrekeningen geen mogelijkheid hun geld veilig te bewaren. Aangezien het bedrag op een rekening slechts een verplichting toont van de bank aan de rekeninghouder is er een risico verbonden aan het aanhouden van dat 'geld'. Dat risico is dat de aangehouden bankverplichting niet kan worden nagekomen door de bank, of dat een overheidsbesluit het saldo kan doen verminderen. Positive Money bespreekt dit op een pagina waar de mythe wordt ontkracht dat banken je spaargeld veilig in een kluis zouden bewaren:

"*But what are those numbers that appear in your account? Is that not money? In a legal sense, no. Those numbers in your account are just a record that the bank needs to repay you at some point in the future. In accounting terms, this is known as a liability of the bank. So the balance of your bank account doesn't actually represent the money that the bank is holding on your behalf. It just shows that they have a legal obligation – or liability – to repay you the money at some point in the future.*"[30]

Sinds het begin van de crisis zijn maatregelen in gang gezet om banken te redden, en daarbij is inmiddels gebruik gemaakt van de mogelijkheid om spaartegoeden (bankbeloftes) weg te strepen, ook wel een "*haircut*", of "*bail-in*" genoemd. In Cyprus bijvoorbeeld:

> "*(...) the Troika slammed large Cypriot depositors (...) with a "bail-in" template, soon coming to all insolvent European nations, that included not only a forced assignment of equity in broke Cypriot banks, but far more importantly a haircut that amounted to 37.5% of deposits over €100,000. Since then a few things have happened in Cyprus, neither of them good, i.e., (...) a record collapse in bank deposits despite capital controls and a record crash in the local real estate market.*"[31]

Aldus ZeroHedge.com, in een artikel genaamd "*Cyprus 37.5% Depositor Haircut Upgraded To 47.5% Brazilian Wax*". Om de banken in Cyprus te redden die op omvallen stonden werden spaartegoeden boven een ton met 37,5% verminderd. Het is moeilijk maatschappelijk draagvlak te vinden voor een geldsysteem waarin dit mogelijk is, zo stelt ook de schrijver van een kritische blogger 'Aziz' in een post getiteld "*There Is No Surer Way To Destroy A Banking System Than Giving Depositors A Haircut*":

> "*(...) I'm talking about the kind of haircut where depositors lose a portion of their money. This can destroy confidence in a fractional reserve banking system, as depositors in other banks and other countries fear that they too might be forced to take a haircut, leading to mass withdrawals, leading to illiquidity.*"[32]

Een geldsysteem van staatsgeld dient het in het belang van maatschappelijke stabiliteit, onmogelijk te maken voor houders van dat digitale geld het te kunnen verliezen per verordening; ondanks dat de Staat het in omloop zou brengen.

1.1.4 Een betrouwbare rem op geldschepping

Boonstra heeft gelijk dat er in de geschiedenis tijden zijn geweest dat er onverantwoordelijk is omgegaan met de geldschepping. De huidige crisis is dus geen uitzondering[1]. Zo wordt Boonstra geciteerd in de Volkskrant van 27 Juli 2013 in een artikel genaamd *"Geldcreatie is een gevaarlijk privilege, zowel in private als in publieke handen":*

> *"Wim Boonstra, hoofdeconoom van de Rabobank, stelt daar tegenover dat te veel overheidsbemoeienis juist de oorzaak is van veel financiële crises (Opinie, 3 juni), een recept voor inflatie. Politici zullen de geldpers laten draaien om kiezers te paaien met investeringen, oorlogen te voeren, uitbundige hofhoudingen te financieren of onverantwoorde belastingverlagingen. De geschiedenis is wat hem betreft op dit punt 'glashelder'. Van Duitsland in 1923 tot meer recentelijk in Zimbabwe kan vrijwel elke hyperinflatie 'rechtstreeks worden teruggevoerd op onbelemmerde gelddrukkerij door overheden of onder politieke invloed staande centrale banken'. "*[33]

Je kan je afvragen of het redelijk is Nederland te vergelijken met het politieke bestel in Zimbabwe, dan wel of onze democratische rechtstaat wel zou functioneren als het mogelijk is een "uitbundige hofhouding te vieren" wanneer de Staat weder een geldscheppingsmacht zou bezitten. Desalniettemin geeft het aan, of Boonstra gelijk heeft of niet, dat er bijna apolitieke garanties dienen te worden gegeven bij staatsgeldschepping, gelijkend aan de onafhankelijkheid van een hedendaagse centrale bank. Het is daarmee bij het ontwerp van een (geld)systeem verstandig gevaren alvast proberen in te dammen, en grenzen te stellen en te bewaken, met zoveel (systematische) garantie als mogelijk. Immers hoort een geldsysteem doorgaans decennia mee te gaan. Er zullen in die tijd vele bestuurders langskomen die niet allemaal dezelfde denkbeelden en perspectieven erop nahouden. Dat uit zich in beleidsvorming en beslissingen. Ook hier geldt dat het veel beter zou zijn als deze zekerheden op limieten van geldschepping gegeven konden worden zonder menselijke tussenkomst; d.w.z. dat de garanties op apolitieke wijze worden gegeven door de inrichting van het systeem zelf en niet afhankelijk zijn van menselijke toezichthouders die vaak aantoonbaar niet of te traag reageren[34].

Positive Money, Ons Geld, en andere leden van de IMMR houden er op dit punt een vrij klassieke visie op na. In de voorstellen van Positive Money bijvoorbeeld willen ze het

geldsysteem baseren in de boekhouding van hun centrale bank, de Bank of England. Concreter: ze willen het systeem zó veranderen dat al het digitale geld in de economie bestaat uit schuldvrije, renteloze risicovrije staatsuitgiften[10], en dat de inwoner dit type geld kan aanhouden *via* de commerciële banken. Dit zou een grote verbetering betekenen ten opzichte van het huidige systeem waarin geld ontstaat als, en met een, schuld. Echter wordt hier weer veel vertrouwen gelegd in een enkel instituut, een gecentraliseerde boekhouding en gecentraliseerde rapportage.

Gedrag en beheer in een geldsysteem kan nóg zo goed vastgelegd worden in de wet of in een protocol. Uiteindelijk zal de Staat de macht hebben de regels te veranderen. Dat is ook de bedoeling in een soevereine democratie, en kent legitieme gebruiken. Het geldsysteem heeft als uniek en krachtig instrument echter toch de neiging met de tijd misbruikt te worden, zoals Boonstra aangeeft. Het gevaar is dat een goed werkend systeem wordt omgevormd zonder dat daar maatschappelijk draagvlak voor zou zijn. Het is cruciaal dat de bevolking weet van fundamentele wijzigingen in het bestel dat hen per definitie allen raakt. De eerdergenoemde wens van complete transparantie in statistiek heeft hier veel mee te maken. Erkennende dat je een geldsysteem niet onveranderlijk kan maken zonder de soevereiniteit aan te tasten, is het daarmee nodig om genoeg systematische (technische) drempels in te richten. Deze drempels zullen (voor de Staat) overkoombaar moeten zijn, maar toch genoeg frictie en overhead in implementatie en transitie moeten leveren dat het aandacht genereert onder inwoners. Dankzij deze bewustwording kan men indien nodig tegen de verandering in protest gaan. We zullen zien dat we effectief de machten kunnen scheiden door de bankensector verantwoordelijk te maken voor de afdwinging van afgesproken regels op overheidsgeldschepping, middels een technische oplossing.

[10] de centralebankreserves uit het hedendaagse systeem zijn hier nog het best mee te vergelijken, behalve dat deze alleen in omloop kunnen komen door een lening, en dus, schuldcreatie.

2. Probleemstelling & Onderzoeksvraag

De International Movement for Monetary Reform pleit met o.a. de steun van IMF-onderzoekers Benes & Kumhof voor implementatie van nationaal[11] staatsgeld. Er heerst in het publiek debat echter een groot stigma over soevereine geldcreatie, vermoedelijk door de constant herhaalde maar vaak feitelijk onjuiste[12] voorbeelden van voorgaande hyperinflaties, vaak notabene in oorlogstijden, als resultaat van geldcreatie, volgens de narratief door de overheid. Een heruitvinding van echt[13] staatsgeld moet dus aan strenge eisen voldoen om democratische legitimiteit te genieten en vertrouwen te wekken. De mogelijkheden hiertoe worden verkend in onderzoeksvraag 2 (sectie 4.2).

Het Bitcoin-protocol bezit een aantal eigenschappen die wenselijk en bruikbaar zijn bij een toekomstig geldsysteem[14], waar het privilege op geldcreatie bij de Staat ligt, zoals dit voorgesteld wordt door de IMMR. Het protocol is in de huidige staat echter technisch gezien niet geschikt om deze in te zetten als nationale munt vanwege haar architectuur. Zo is het wenselijk om in een nationaal geldsysteem een publiek monopolie te hebben op (digitale) geldcreatie, terwijl geldcreatie in Bitcoin openlijk maar privaat gebeurt. De keuze voor deze manier van geldcreatie is een bewuste keuze geweest in het originele ontwerp, maar er zijn ook technische drempels die niet ontworpen zijn als 'feature'. In onderzoeksvraag 1 (sectie 4.1) wordt gekeken hoe dit aangepast kan worden.

Zo is het nog niet duidelijk of het Bitcoinsysteem het transactievolume aan kan indien zij genationaliseerd en geïnstitutionaliseerd wordt, en is het niet zeker of het in het belang is van een staatsmunt om gefundeerd te zijn op een systeem waarin de transactieprocessoren zijn verwikkeld in iets dat nog het meest lijkt op een ‘space-race’[35] maar dan met rekenkracht. Er is dan ook onderzoek nodig naar de mogelijkheid en/of haalbaarheid om het protocol zó aan te

[11] Dit kan eventueel ook in EU-verband gedaan worden, waarbij de ECB dan werkelijk als enige mogendheid de macht op geldschepping krijgt

[12] Een bekend voorbeeld hiervan is dat de hyperinflatie in Duitsland in 1923 ontstaan zou zijn wegens excessieve geldschepping door de overheid. De centrale bank was toen juist echter onder totale private contole gekomen: http://www.wintersonnenwende.com/scriptorium/english/archives/articles/hyperinflation-e.html

[13] d.w.z. met een verbod op private geldcreatie

[14] Dit is niet hetzelfde als een nationalisatie van het banksysteem. Het geldsysteem betreft in principe het systeem van geldcreatie, waar het banksysteem gaat over waarde-opslag en verdeling door middel van sparen en lenen. In het hedendaagse systeem zijn deze functies echter verwoven.

passen dat deze ingezet kan worden als staatsmunt. Men het Bitcoinprotocol als basis voor een staatsmunt beobserveren we enkele eigenschappen die de transparantie en credibiliteit van genationaliseerde geldcreatie ten goede komen. Dit gebeurt in onderzoeksvraag 3 (sectie 4.3).

Om een nationalisatie van geldcreatie voor elkaar te krijgen is een zo pragmatisch mogelijke insteek nodig. Om politieke acceptatie te verwerven voor een systematische verandering, zeker inzake het geldsysteem, is het nodig dat er ogenschijnlijk zo min mogelijk verandert. Mensen die 'het nieuwe systeem' gebruiken moeten zo min mogelijk herschoold worden om de vereiste *change management* te minimaliseren; het liefst merkt de bevolking letterlijk niet dat er systematisch intern iets veranderd is.

Dit vereist, ondanks dat nieuwe technieken zoals Bitcoin een revolutie in financiële vrijheid en privacy kunnen betekenen, dat ervoor gekozen moet worden deze in te perken ten faveure van de haalbaarheid van transitiemanagement. Daarom wordt in dit paper gezocht naar een manier om een digitale staatsmunt op basis van Bitcoin zó te modelleren dat deze zoveel mogelijk gelijkend is aan de infrastructuur *die er nu al is*, om makkelijk te kunnen passen binnen regelgeving die hedendaags nodig wordt geacht, zoals de WWFT[36]. Regelgeving die witwaspraktijken en terrorismefinanciering betrachten te identificeren[37] (en eventueel kunnen tegenhouden).

Ik doel hiermee met name op twee zaken: (a) rekeninggeneratie en (2) transactievalidatie. De verantwoordelijkheid voor beide ligt nu in de financiële sector, zij het gereguleerd. Wettelijke regulatie van rekeninggeneratie (het openen van een bankrekening) zorgt ervoor dat de overheid grip heeft op wie er precies een rekening opent en wie niet, en daarmee rekeninghouders kan identificeren; ook nuttig voor de belastingdienst. Dit belang staat op gespannen voet met het principe van vrijheid en privacy in Bitcoin waarin iedereen vrij adressen kan genereren zonder daarvoor geïdentificeerd te hoeven worden. Dit wordt besproken in onderzoeksvraag 4a.

De transactievalidatie gebeurt momenteel ook door banken. Zij hebben hiervoor over de jaren een grote investering in IT-structuur gedaan. Als we het principe aanhouden dat we procesmatig zo min mogelijk willen veranderen dan ligt het voor de hand de initiële lasten/baten van transactievalidatie ook door de bankensector te laten geschieden. Door hen de nieuwe

staatsmunt te laten valideren (*minen*) heb je tevens de initiële ondersteuning om het netwerk te beveiligen, gemeten in *hashpower*. Daar tegenover staat dat een oligarchie van een beperkt aantal banken, bij een hypothetische afwezigheid van andere publieke of private transactieprocessoren, het misschien mogelijk maakt het legitimiteitsprincipe te overtreden zoals we dat later introduceren, wat wél zou stroken met de huidige wetgeving omtrent witwaspraktijken, maar niet met de onze en die van Nakamoto. Dit wordt uitgezet in onderzoeksvraag 5 (sectie 4.5). Het onderzoekende deel van dit paper zal dus de volgende vragen beantwoorden:

Bitcoinimplementatie van staatsgeld (4.1)
Wat dient er veranderd te worden aan het Bitcoinprotocol om, in lijn met de principes van het Chicago Plan zoals gepropageerd door de International Movement for Monetary Reform, dit te gebruiken als basis voor een schuld- en rentevrije soevereine staatsmunt?

Protocollimiet op geldschepping & drempelvorming (4.2)
Welke garanties kan NLCoin geven die transparantie en democratische legitimiteit bieden, om op die manier kritiek op geldcreatie door de staat te ontladen en genoeg maatschappelijk vertrouwen te genereren dat dit systeem geïmplementeerd kan worden?

Schaalvergroting van Bitcoin naar Nederlandse proporties (4.3)
Wat dient er verbeterd te worden aan het Bitcoinprotocol om dit op nationale schaal te implementeren?

Inbedding in banksysteem & wetgeving (4.4)
Op welke manier dienen processen of principes binnen NLCoin te worden veranderd of te worden ingeperkt om op een zo pragmatisch mogelijke wijze een conservatieve drop-in replacement te kunnen zijn voor het geldsysteem met behoud van de infrastructuur van het huidige banksysteem?

Technische ondersteuning in het bankwezen (4.5)
Hoe kan de bankensector NLCoin zo goed mogelijk technisch ondersteunen om vanaf de introductie al een hoge mate van operationele veiligheid en functionaliteit te bieden, en daarmee

binnen het nieuwe geldsysteem m.b.t. het verwerken en valideren van transacties de rol te vervullen zoals zij die heeft in het hedendaagse geldsysteem?

In de volgende sectie zal eerst het theoretisch kader worden behandeld. De concepten van het geldsysteem zoals het nu is zullen worden verkend, evenals de achtergrond en technische werking van het Bitcoin-protocol. We zullen zien dat Bitcoin een aantal kwaliteiten omvat die van nut zijn bij de inrichting van een staatsmunt.

3. Theoretisch kader

3.1 Introductie van Bitcoin en het concept van geld

In 2008 publiceerde Satoshi Nakamoto een paper genaamd '*Bitcoin: A Peer-to-Peer Electronic Cash System*'[7]. Hierin introduceert hij of zij[15] een systeem van elektronisch cash geld dat voor het eerst het '*double-spending*'-probleem oploste zonder centrale authoriteit:

> "*A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network*"

Het systeem is essentieel een protocol gecodeerd in software dat openbaar wordt ontwikkeld en verspreid (open source). In 2009 is de eerste versie van dit protocol actief geworden, en het bestaat nog immer (November 2013). Het Bitcoin geldnetwerk functioneert thans als een complementaire munt[16] die dus bestaat naast valuta als de Dollar en de Euro. Bitcoin verschilt echter aanzienlijk van de hierboven genoemde valuta; ze wordt namelijk niet gecreëerd door een schuldbekentenis of wederzijdse schuldaanvaarding. Het concept van een complementaire munt (in tijden van crisis) is overigens niet nieuw en gaat ver terug[17].

Bitcoin prijst zichzelf als een globaal betalingsnetwerk, vrij van centrale autoriteit, met slechts zeer lage transactiekosten:

> "*Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the*

[15] Ondanks dat de auteur nog lange tijd na de publicatie van het paper in de openbaarheid heeft meegewerkt aan de broncode en veel technische uitleg heeft gegeven op het Bitcoin-forum, is de identiteit in nevelen gehuld. Het laatste wat van de auteur is vernomen is een bericht op het Bitcoin-forum op 12 December 2010. Er wordt online veel gespeculeerd over de ware identiteit, met name vanwege de vermoedens dat hij of zij eigenaar is van een aantal Bitcoins waarvan de waarde ten tijde van schrijven vele miljoenen Euro's overstijgt.

[16] "*A complementary currency (…) is an agreement to use something else than legal tender as a medium of exchange, with the purpose to link unmet needs with otherwise unused resources*" (Lietaer & Hallsmith (2006))

[17] zo is in het Oostenrijkse stadje Wörgl is in 1932 een experiment gedaan met complementair schuld- en rentevrij geld (Lietaer (2001)), en in Zwitserland in 1934, een systeem dat nog steeds bekend staat als de WIR

network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system." (Bitcoin.org (2013))

Het geldnetwerk is dus opgezet op basis van peer-to-peer technologie, zoals BitTorrent[18] dat ook is. Dit betekent dat het netwerk, net als BitTorrent, moeilijk zal zijn om neer te halen, iets wat bij BitTorrent al vele malen geprobeerd is door grote marktpartijen die zich bekommeren om copyright en 'illegaal' downloaden. Dit wordt geïllustreerd door een citaat van Nick Szabo, een blogger die schijnbaar een tijd vóór Satoshi met het idee 'BitGold' kwam:

"This technology will give us public records which can "survive a nuclear war", along the lines of the original design goal of the Internet. While thugs can still take physical property by force, the continued existence of correct ownership records will remain a thorn in the side of usurping claimants"[38]

Met het '*double spending*'-probleem (Nakamoto (2008)) dat werd genoemd in het eerste citaat wordt gerefereerd naar de situatie dat een gebruiker van een digitaal geldsysteem een token meer dan ééns kan uitgeven, omdat de aard van digitale data is dat zij eenvoudig gedupliceerd kan worden. Om deze reden is er voor digitale geldsystemen in het verleden vaak gebruik gemaakt van een centrale autoriteit die de boekhouding verzorgde en daarmee garandeerde dat het geld slechts één keer kon worden uitgegeven.

Jansen beschrijft het Bitcoinprotocol als volgt:

"*Bitcoin is designed to remove the centralized monetary policy crafted by bankers and instead use cryptography to control money creation and transfer by means of distribution. In other words, managing the money supply and transactions are carried out collectively by the network following a protocol*"[39]

Er wordt hier al geïmpliceerd dat de nood van Bitcoin is ontstaan uit een onvrede over gecentraliseerd financieel beleid van tegenwoordig. De politieke aard van deze innovatie wordt

[18] BitTorrent is een systeem om peer-to-peer (decentraal) gegevens uit te wisselen.

echter helemaal helder aan de hand van een bericht dat Nakamoto op de website van P2P Foundation plaatste op 11 Februari 2009:

> "*The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles*[19] *with barely a fraction in reserve*[20]*. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.*"[40]

Van Pelt impliceert een vergelijkbare reden:

> "*(...) commerciële banken vergroten de geldhoeveelheid wanneer ze geld uitlenen. Banken hebben maar een fractie van het uitgeleende geld werkelijk in kas als zogenaamde reserve. De term "fractioneel bankieren" komt hier vandaan. Banken verveelvoudigen elke munt in de vorm van deposito's. Een gevolg hiervan is dat een bankrun mogelijk is: een groot aantal klanten eist hun geld bij de bank maar de bank kan deze eisen niet beantwoorden en gaat failliet. Dat gebeurde bijvoorbeeld met DSB. In het Bitcoinsysteem is een bankrun niet mogelijk. Er is namelijk geen bank en daarbij is het niet mogelijk een veelvoud van bestaande bitcoins in omloop te brengen. Bitcoin hanteert in wezen 100% reserve bankieren*[21]*."*[41]

Tenslotte verklaarde David Chaum, een wijsgeer in de cryptografie die al in 1982 enkele protocollen beschreef voor elektronisch geld, in 1996[42] tijdens een interview voor een magazine:

---

[19] er wordt hier gerefereerd naar de kredietcyclus, zoals geanalyseerd door Hyman Minski in zijn Financial Instability Hypothesis (Minksy (1992))

[20] er wordt hier gerefereerd naar de praktijk van fractioneel bankieren, waarbij banken maar een fractie aan liquide middelen hebben ten opzichte van de uitstaande verplichtingen. m.a.w. voor al het krediet dat verstrekt wordt door wederzijdse schuldaanvaarding is er maar een fractie aan direct opvraagbare tegoeden beschikbaar. in dit paper wordt hier niet technisch op ingegaan.

[21] synoniem voor Full-reserve banking

"*The difference between a bad electronic cash system and well-developed digital cash will determine whether we will have a dictatorship or a real democracy*"

Het is dus duidelijk dat Bitcoin zich afzet van de vernomen onrechtmatigheid en instabiliteit van het huidige geld- en banksysteem door een technisch superieur alternatief te bieden. Hiermee hoeft er niet langer vertrouwen te zijn om de stabiliteit van het geldsysteem te garanderen en zijn de kosten voor gebruikers lager dan in het huidige systeem.

Ondanks dat het vanilla Bitcoinsysteem inderdaad wezenlijk een vorm is van Full-reserve banking, zoals van Pelt zegt, neemt dit niet weg dat er op basis van Bitcoin weer fractional bankieren[22] kan ontstaan door er een banksysteem op te baseren, aldus de wiki van bitcoin.org (Juli 2013):

"*There is no fundamental difference between classical currencies and Bitcoin as it applies to banking. Banks will still be free to take in bitcoins and present them to customers as "available for withdrawal" while still lending most of those bitcoins to a different customer for a profit. Some of those bitcoins will be held in reserves in case of a bank run. It will be up to the bank to hold a sufficient supply of reserves in order to prevent insolvency in the event of a bank run. Central banks were established to enforce reserve requirements and so, with Bitcoin lacking a central bank, some banks will almost surely collapse, taking their customers' deposits with them*"[43]

De situatie zoals hier beschreven doet denken aan het ideaal uit de leer van de Oostenrijkse school, waarin er stabiliteit ontstaat door de afwezigheid van overheidsregulatie en daarmee het *moreel risico*. Om echter een einde te maken aan de praktijk van fractioneel bankieren, zoals de International Movement for Monetary Reform dat beoogt, zal er dus meer moeten gebeuren dan slechts het invoeren van een cryptovaluta. De oplossing hiervoor zal moeten worden gezocht in regelgeving, maar dat is buiten de scope van dit onderzoek.

[22] zie voetnoot 13. fractioneel bankieren is de logische tegenhanger van Full-reserve banking en is de praktijk die tegenwoordig bijna overal ter wereld wordt toegepast ten behoeve van winstmaximalisatie.

Eerder is er al genoemd dat Bitcoin zich afzet tegen de 'onrechtmatigheid' van het huidige stelsel. Gezien er verderop ook nog naar de term gerefereerd zal worden is het belangrijk deze te definiëren. 'Rechtmatigheid' betekent hier:

- de garantie dat de valuta van het geldsysteem niet *arbitrair* ongebreideld gecreëerd wordt met mogelijke inflatie ten gevolge (*"The central bank must be trusted not to debase the currency*" (Nakamoto)),
- de zekerheid te kunnen hebben dat geld in jouw bezit niet zonder toestemming wordt uitgeleend met het risico dat het in onzekere tijden niet meer opvraagbaar is ("*Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles*[23] *with barely a fraction in reserve" (Nakamoto)* en "*Banken verveelvoudigen elke munt in de vorm van deposito's. Een gevolg hiervan is dat een bankrun mogelijk is: een groot aantal klanten eist hun geld bij de bank maar de bank kan deze eisen niet beantwoorden en gaat failliet."* (van Pelt))
- de garantie dat je transacties niet geblokkeerd worden

Door een digitaal financieel systeem te willen baseren op bovengenoemde rechtmatigheid is het dus nodig dat er niet een te grote macht ligt bij een enkele partij om bijvoorbeeld beleid te dicteren. Dit vereist de afwezigheid van een centrale autoriteit en hierdoor is het benodigd dat het systeem decentraal in elkaar steekt. Dit wordt bevestigd door Sompolinksy & Zohar (2013):

> *"A centrally controlled monetary system is open to intervention: Accounts can be frozen, money can be seized, and fees are high as the channels used for money transfer are controlled by a handful of entities that face little competition. Bitcoin's alternative, is to use the nodes in its large P2P network to verify each other's work and thus ensure that no single entity is able to misbehave."*

De decentralisatie zorgt echter voor een probleem in vertrouwen, met de mogelijkheid voor gebruikers om munten te '*double spenden*'. Dit misbruik wordt opgelost door het wantrouwen in te bouwen en de complete geschiedenis van alle transacties in de openbaarheid gedeeld te houden. Hiermee kan ieder onderdeel van het netwerk zelf verifiëren of het betalingsproces eerlijk verloopt. Deze transactieopenbaarheid zorgt voor een ongekende transparantie, zeker in

[23] er wordt hier gerefereerd naar de kredietcyclus, zoals geanalyseerd door Hyman Minski in zijn Financial Instability Hypothesis (Minksy (1992))

combinatie met de open staat van het protocol zelf, waarvan de code geheel *open source* is. Dit geeft op zijn beurt weer de nood aan op privacy bij het handelen, gezien alle handelingen herleid kunnen worden.

Samenvattend is Bitcoin gebouwd op de volgende principes (in systematische volgorde):

- rechtmatigheid (recht op saldobehoud, vrijheid van betaling en garantie van monetaire onvervalsbaarheid)
- onafhankelijkheid van centrale autoriteit
- decentralisatie
- wantrouwen
- transparantie
- recht op financiële privacy

Later zal er behandeld worden welke eigenschappen dit protocol zo wenselijk maken om als staatsmunt te gebruiken (sectie 3.6). Om af te sluiten nu eerst nog een woord over de waarde van Bitcoin en de definitie van geld.

3.1.1 Wat is geld?

Bitcoin verandert de manier waarop mensen nadenken over wat het concept 'geld' eigenlijk is. De getallen, de hoeveelheden Bitcoins, die in de transacties genoemd worden zijn geen representatie voor iets fysieks en hebben slechts en alleen monetaire[24] waarde omdat er mensen bereid zijn ze in betaling te accepteren; een impliciete afspraak. Er is immers (nog) geen overheid die de munt als belasting accepteert, het daarmee defacto als wettelijk betaalmiddel erkent, en daarmee ondersteunt door de bevolking te verplichten de munt te accepteren. Dit is wel zo met valuta als de Dollar en de Euro, die tevens nauwelijks intrinsieke waarde (de marktwaarde van de substantie waar het ruilmiddel van is gemaakt; in het geval van chartaal geld: papier en goedkoop metaal) bevatten maar toch als waardevol beschouwd worden. Veel mensen stellen dat Bitcoins om deze redenen, dat de munt geen representatie is van iets van waarde, niet gedekt wordt door waarde, en een verwaarloosbare intrinsieke waarde bevat, waardeloos zouden zijn en dat Bitcoin daarom een trend, ‘hype’, bubbel, of piramidespel

[24] aangezien Bitcoin zoals eerder gezegd de implementatie is van een geldsysteem op het systeem dat het mogelijk maakt decentraal bezit te erkennen heeft Bitcoin naast de monetaire waarde (gebaseerd op geloof en vertrouwen) ook praktische waarde, die je als ‘intrinsiek’ zou kunnen beschouwen: http://www.whyisntbitcoinworthless.com/

is. Een blogger genaamd Vitalik Buterin becommentarieert dit vraagstuk in een artikel "*An Exploration of Intrinsic Value: What It Is, Why Bitcoin Doesn't Have It, And Why Bitcoin Does Have It*":

> *"Unlike nearly all other goods which we interact with on a day-to-day basis, (...) bitcoins seem to have no value in and of themselves – they are simply entries on atn arbitrary database. And yet, at the same time, each one of these entries is now worth roughly $1000 on Bitstamp and even more on MtGox and BTCChina. This strange duality, the unique property of simultaneously being completely valueless in one sense and yet so exremely valuable in another, is perhaps the biggest psychological barrier for many individuals to accepting Bitcoin as a legitimate economic instrument; the feeling that one's wealth in BTC has no solid "floor" to stand on, aside from an ill-defined and foggy entity known as "the market", is notably difficult to overcome.*
>
> *Some economists even go so far as to say that Bitcoin cannot become a true currency for this reason, and is doomed to blow up and eventually permanently pop as a speculative bubble. But at the same time, others argue that Bitcoin does have intrinsic value, and still others claim that intrinsic value is not just unimportant, but is in fact a completely useless mental construction with no economically valid definition – all value is subjective"*[44]

Het vraagstuk raakt al snel de aard van geld en de vraag over wat geld eigenlijk is. Is het nodig dat geld een intrinsieke waarde heeft? Wat is een intrinsieke waarde? Heeft Bitcoin een intrinsieke waarde? Een mogelijk antwoord hierop werd onlangs mooi geïllustreerd door een artikel op de satirische weblog The Onion genaamd '*U.S. Economy Grinds To Halt As Nation Realizes Money Just A Symbolic, Mutually Shared Illusion*'[45].

> "*The U.S. economy ceased to function this week after unexpected existential remarks by Federal Reserve chairman Ben Bernanke shocked Americans into realizing that money is, in fact, just a meaningless and* ***intangible social construct.*** *(...) A few U.S. banks have remained open, though most teller windows are unmanned due to a lack of interest in transactions involving mere scraps of paper or, worse, decimal points and computer data signifying mere scraps of paper*"

De notie dat geld een maatschappelijk abstract construct is wordt ondersteund door de overschaduwde Aristoteliaanse definitie van geld:

> "*(...) all things that are exchanged must be somehow comparable. It is for this end that money has been introduced, and it becomes in a sense an intermediate; for it measures all things, and therefore the excess and the defect-how many shoes are equal to a house or to a given amount of food. (...). All goods must therefore be measured by some one thing, as we said before. Now this unit is in truth demand, which holds all things together (for if men did not need one another's goods at all, or did not need them equally, there would be either no exchange or not the same exchange); but money has become* ***by convention*** *a sort of representative of demand; and* ***this is why it has the name 'money' (nomisma)-because it exists not by nature but by law (nomos) and it is in our power to change it and make it useless.*** *(…) And for the future exchange-that if we do not need a thing now we shall have it if ever we do need it-money is as it were our surety; for it must be possible for us to get what we want by bringing the money. Now the same thing happens to money itself as to goods-it is not always worth the same; yet it tends to be steadier. (...)"* [46]

Geld is een abstracte meeteenheid die slechts bestaat door de afspraak dat het bestaat. 'Money' komt dan ook van '*nomisma',* dat afgeleid is van het Griekse '*nomos*': wet. Het behoeft geen intrinsieke waarde te hebben. De 'wet' hier is in Bitcoin de programmacode die definieert wat het geld is. De ontwikkelaars kunnen als wetgevers te allen tijde deze definitie aanpassen (al zal niet iedere Bitcoin *miner* per definitie een verandering accepteren). In NLCoin zou het de Nederlandse wet zijn die uiteindelijk bepaalt wat de programmacode is, om op die manier na lange tijd weer recht te doen aan de klassieke definitie van geld.

Ook Plato, een leerling van Aristoteles, definieert op deze manier 'geld' als 'bij wet'.

> "*Further, the law enjoins that no private man shall be allowed to possess gold and silver, but only coin for daily use, (...), whether slaves or immigrants, by all those persons who require the use of them. Wherefore our citizens, as we say,* ***should have a coin passing current among themselves, but not accepted among the rest of mankind****;*

with a view, however, to expeditions and journeys to other lands-for embassies, or for any other occasion which may arise of sending out a herald, the state must also possess a common Hellenic currency. If a private person is ever obliged to go abroad, let him have the consent of the magistrates and go; and if when he returns he has any foreign money remaining, let him give the surplus back to the treasury, and receive a corresponding sum in the local currency."[47]

Naast dat Plato het 'wetgeldsconcept' hier bestendigt door ruw edelmetaal als geld te verbieden beeld hij uit hoe in regio's met een soevereine geldcreatie omgegaan dient te worden met geld van buitenaf. In zijn beeld dient elke politieke regio (als staat of stadsstaat) een munt te bevatten die niet bedoeld is voor internationale handel, en daarmee complementair is aan dat wat tussen staten wordt geaccepteerd.

In het onderzoekende deel van het paper is het nodig de concepten achter Bitcoin te kennen om de voorgestelde aanpassingen te begrijpen. Om de value-proposition van Bitcoin in te zien zal eerst in het kort het hedendaagse geldsysteem worden uitgelegd ter referentie.

3.2 Hedendaagse geldsysteem

Voordat we in diepte het Bitcoinprotocol bespreken is het nuttig eerst een kort overzicht te geven van hoe het hedendaagse geldsysteem werkt. Op die manier kunnen de twee systemen vergeleken worden en is het aantoonbaarder duidelijk waarom Bitcoin zo'n goed systeem is, mede door de definitie van geld die ook hier zal spelen.

Er zijn meerdere concurrerende theorieën over hoe het geld- en banksysteem vandaag werkt. Ik houd hier de theorie aan van endogene geldcreatie zoals deze ook wordt aangehouden door Positive Money, Hyman Minsky, de New Economics Foundation, Benes & Kumhof en Frederick Soddy.

Er zijn drie soorten 'geld' (die hier voor ons van belang zijn[25]). Er zijn (1) centralebankreserves, digitale tokens van waarde die centrale banken creëren uit het niets en (2) het chartale geld zoals gecreëerd door nationale centrale banken op basis van een quotum van de ECB, en ten slotte (3) commerciële kredieten zoals gecreëerd door commerciële banken uit het niets (beter bekend onder de noemer ‘krediet’). Centralebankreserves worden gebruikt door commerciële banken om hun schulden naar elkaar mee te vereffenen en kunnen niet aangehouden worden door het publiek.

Het girale geld dat aangehouden kan worden door het publiek (het commerciële bankgeld (2)) wordt gecreëerd als er een 'lening' wordt aangegaan bij de bank. Dit geld[26] bestond eerder nog niet. Deze creëert het deposito voor de 'lening' uit het niets. Deze stelling wordt breed ondersteund, zo ook door Dirk Bezemer, professor monetaire economie aan de Rijksuniversiteit Groningen: "*Wanneer een bank een lening verstrekt wordt er nieuw geld gecreëerd*"[48]. Wanneer een 'lening' wordt afbetaald gebeurt het tegenovergestelde en wordt het geld vernietigd. Dit is mogelijk omdat commercieel bankgeld ‘krediet’ is; een belofte te betalen. Als een geleende bankbelofte wordt teruggegeven (bij het aflossen van een lening) kan deze in de boekhouding worden doorgestreept.

[25] M2 bestaat uit de hoeveelheid chartaal geld in handen van het publiek plus giraal geld. M3 bestaat uit M2 inclusief o.a. terugkoopovereenkomsten, aandelen en obligaties.

[26] het wordt hier ‘geld’ genoemd, maar het is in feite krediet: een belofte te betalen. Omdat dit krediet toch circuleert als ware het geld zal de distinctie verder niet expliciet gemaakt worden ter simplificatie

Betaalde rente wordt niet vernietigd, blijft bestaan en dient als winst voor de bank. Het geld dat wordt gecreëerd ontstaat als krediet en wordt 'gedekt' door de inspanningsbelofte van de lener. De belofte van de lener om het krediet terug te betalen komt aan de linkerzijde van de balans (en wordt door de bank gezien als een bezit met een waarde) en het krediet komt aan de rechterkant (een verplichting). Het krediet is in feite tevens een belofte, een belofte om te betalen. Dit proces van geldcreatie staat bekend als '*wederzijdse schuldaanvaarding*'. Aangezien de bank niet per se de liquide middelen nodig heeft om aan haar verplichtingen te voldoen (het krediet) heet dit systeem '*fractioneel bankieren*'. Het bankieren gebeurt namelijk op basis van een fractie van de beloofde reserves die daadwerkelijk aanwezig zouden moeten zijn. Dit is hetzelfde fractioneel bankieren waar van Pelt eerder naar refereerde, alsmede Nakamoto. Hier legt Wim Boonstra het proces nog eens kort uit in een artikel dat geplaatst is in het Financieel Dagblad (15 December 2012):

> "*(...) een bank verstrekt een krediet van zeg € 1000 en maakt dit uitgeleende bedrag over aan haar klant. Op de balans van de bank wordt aan de actiefzijde (bezitting van de bank, verplichting van haar klant) het krediet van € 1000 geboekt. Dit wordt bijgeschreven op de rekening van de klant (vanuit de bank gezien een verplichting). De balans van de bank is dus met € 1000 gestegen. De geldhoeveelheid is met € 1000 gegroeid, net als de uitstaande hoeveelheid krediet. Het lijkt er dus op dat ook gewone banken, net als centrale banken, op deze manier geld 'uit het niets' maken. Dat is een onterechte conclusie, want het door de bank gecreëerde geld is namelijk gedekt door de inspanningsverplichting van degene die het geld heeft geleend, de debiteur, om de lening weer terug te betalen. (...)*"[49]

Eerder heb ik het woord 'lening' tussen accolades geplaatst omdat er in het proces van geldcreatie door *wederzijdse schuldaanvaarding* feitelijk niets uitgeleend wordt, ondanks de bewering van Boonstra hierbovenstaande. Een lening impliceert dat de uitlener na het uitlenen het uitgeleende niet meer in bezit heeft. Dat is hier absoluut niet het geval aangezien de bank beide kanten van de balans ophoogt ('*double-entry bookkeeping*'). Frederick Soddy, nobelprijswinnaar in de chemie, erkent dit ook:

> "*Genuine and Fictitious Loans.—For a loan, if it is a genuine loan, does not make a deposit, because what the borrower gets the lender gives up, and there is no increase in*

the quantity of money, but only an alteration in the identity of the individual owners of it. But if the lender gives up nothing at all what the borrower receives is a new issue of money and the quantity is proportionately increased."[50]

Wat belangrijk is om hier (nogmaals) aan te merken is dat het gecreëerde 'geld' dus in feite een schuldbekentenis is, een belofte. Dit betekent dat 'geld' zoals we dat gebruiken in de economie dus gelijkstaat aan 'schuld' aangezien het slechts ontstaat door een schuldaanvaarding én ook een schuld representeert, die van de bank aan de lener. Bij een maatschappelijk grote economische afhankelijkheid van commercieel bankgeld is het dus zo dat er macro-economisch gezien hoe dan ook een schuld aangegaan moet worden om geld in de economie te hebben. Charlotte van Dixhoorn ondersteunt dit en schreef het volgende in haar extensieve masterscriptie 'The Nature of Money':

"The standard approach to this system, as discussed in almost all economic textbooks, is that central banks control the money supply by means of their base money, which banks can expand by means of the money multiplier model (Mishkin, 2009). However, new arguments claim money is based on credit, created by commercial banks and brought into the economy endogenously at the demand of the market (Wray, 1998). A greater demand for money hereby increases credit, of which debt is the flip-side. This strand of thought judges the money we utilize on a day to day basis, as bank debt, and thus for almost every Pound, Euro, or Dollar in existence someone has to go into debt with a bank."[51]

Het feit dat het geldsysteem is gebaseerd op schulden betekent dat de stabiliteit van de geldhoeveelheid afhangt van de gewildheid of mogelijkheid van mensen om te blijven lenen (zich nog verder in de schulden te steken), en de bereidheid van commerciële banken om kredieten te verstrekken. Daarnaast zijn er consequenties voor het systeem wanneer banken failliet gaan. Dan verdwijnt er namelijk geld dat (alleen) bestond in de boekhouding van deze specifieke bank[27]. Dit aspect, dat hedendaags 'geld' dus een schuldbekentenis representeert is belangrijk omdat we dit later zullen uitzetten tegenover Bitcoin (sectie 3.5).

[27] geld dat door bank A gecreëerd is verdwijnt bij een failissement niet als het eerder is overgemaakt naar bank B

Het '*multiplier model*' waar van Dixhoorn naar refereert is het model dat in de meeste tekstboeken economie wordt aangehouden. Dit model stelt dat het voor commerciële banken alleen mogelijk is geld uit te lenen als ze geld hebben afkomstig van de centrale bank. Het centralebankgeld dat ze als basis aanhouden wordt uitgeleend terwijl een klein deel in reserve gehouden wordt. Elke bank doet dit op haar beurt totdat er een multiplicatie heeft plaatsgevonden van een bepaalde ratio. De theorie is dat de centrale bank hierbij kan sturen op de geldhoeveelheid door meer of minder basisgeld uit te geven en door de rentelasten te beïnvloeden. De praktijk werkt echter anders en dit model is achterhaald zoals ook blijkt uit het volgende citaat:

> *"It is argued by some that financial institutions would be free to instantly transform their loans from the central bank into credit to the non-financial sector. This fits into the old theoretical view about the credit multiplier according to which the sequence of money creation goes from the primary liquidity created by central banks to total money supply created by banks via their credit decisions. In reality the sequence works more in the opposite direction with banks taking first their credit decisions and then looking for the necessary funding and reserves of central bank money."*
> - Vitor Constancio, vicepresident van de ECB (2011)

Het '*money multiplier model*' zoals van Dixhoorn het benoemde wordt hierboven als de '*credit multiplier*' aangemerkt. Ook de kredietbeoordelaar Standard & Poor's onderkent dat de geldhoeveelheid primair afhankelijk is van commerciële banken in het rapport "*Economic Research: Repeat After Me: Banks Cannot And Do Not "Lend Out" Reserves*" (13 Augustus 2013): "*Banks don't lend out of deposits; nor do they lend out of reserves. They lend by creating deposits.*"

De onderzoekers van het IMF die onafhankelijk van het instituut het '*Chicago Plan revisited*' (2012) schreven en het voorstel van Irving Fisher uit de jaren dertig om het bank- en geldsysteem te hervormen onder de loep namen, Benes & Kumhof, verwoordden het ook mooi:

> "(...) *In other words, at all times, when banks ask for reserves, the central bank obliges. Reserves therefore impose no constraint. The deposit multiplier is simply, in the words*

of Kydland and Prescott (1990), a myth. And because of this, private banks are almost fully in control of the money creation process."[52]

Helaas maar niet verwonderlijk wordt de fout nog steeds vaak gemaakt en daarmee het proces van geldcreatie verkeerd omschreven. Zo ook Jansen, in '*Bitcoin: the political 'virtual' of an intangible material currency*', het werk waar al eerder uit geciteerd werd:

"*After central banks have created 'base money', commercial banks are also allowed to create money by means of the so-called 'money multiplier' enacted by the fractional reserve ratio imposed by the central bank. This means that commercial banks maintain money reserves that are a fraction of its customer's deposits. The fraction is called the reserve ratio, which is the percentage of deposits that the bank keeps as reserve. For every deposit of money at the bank, the bank keeps a percentage as reserve and may loan out the rest of the amount*"

Het hierbovenstaande is dus incorrect. In de praktijk werkt het andersom. Banken verstrekken éérst krediet en zoeken later pas de benodigde reserves al dan niet bij de centrale bank om te voldoen aan de regelgeving van de liquiditeitseis[53]. Dit proces van geldcreatie ligt soms gevoelig en wordt niet wijd begrepen. Een citaat van Soddy (1926) illustreert dit:

"*No doubt there are still many people, if not the majority, who will be frankly incredulous that money vastly exceeding in amount the total national money can be, and is created and destroyed by the moneylender with a stroke of the pen. How frequently does one still read in the Press that the banks can only loan their customers spare money! Most people still think of what money once was, "a public instrument owned and controlled by the State*"[54]

Tot slot een woord over de samenhang van het bankwezen. Wanneer een bank geld creëert door kredietverstrekking bestaat dat geld in principe slechts in de boekhouding van de betreffende bank. Als je het gecreëerde krediet als geld ziet betekent dit dat elke commerciële bank dus haar eigen geld creëert, dat alleen bij de betreffende bank kan worden gebruikt bij het afbetalen van leningen. Vergelijk dit met de situatie in Engeland van vóór de invoering van de '*Bank Charter act*' van 1844. Voordat de overheid de vrije productie van bankbiljetten door

banken monopoliseerde door het alleenrecht aan de Bank of England te verschaffen wemelde het van de verschillende bankbiljetten die allemaal afkomstig waren van andere banken. Elke bank had haar eigen geldsysteem. De mogelijkheden tot ongebreidelde creatie van bankbiljetten had tot enkele crises geleid en was bovendien erg onhandig in gebruik:

> "*(...) the opening up of South America and the Industrial Revolution sparked a wave of speculation in company start-ups, leading to increasingly reckless lending (and so banknote creation) and the inevitable wave of bank failures and crises from 1825 to 1839 (...). Blame for the collapse was placed at the time on over-issue of banknotes by the country banks*" [55]

Tegenwoordig zitten we met dezelfde situatie[28], ware het niet dat de private bankbiljetten nu digitaal zijn en gerepresenteerd worden door de getallen van ons saldo. Doordat het geld dat banken creëren slechts bestaat in hun eigen boekhouding is er een complex mechanisme voor nodig geweest om deze banksystemen zó aan elkaar te rijgen dat deze kredieten ook overgemaakt kunnen worden naar andere banken. Dit gebeurt door een techniek genaamd '*inter-bank settlements*'. Hierbij wordt er aan het eind van de dag (letterlijk) berekend hoeveel elke bank schuldig is aan elkaar door alle onderlinge transacties bij elkaar op te tellen en betalen ze elkaar slechts het benodigde resultaat van alle transacties van die dag in reserves, voornamelijk centralebankreserves.

Het punt dat ik hier mee wil maken is het volgende: de werking van het hedendaagse geldsysteem is onnodig complex en hangt als een lappendeken van individuele systemen en boekhoudingen aan elkaar. Onthoud dit, gezien we dit later (sectie 3.5) uit systeemperspectief zullen vergelijken met het Bitcoinsysteem op basis van het KISS-principe.

[28] Niet alleen in de bankensector, maak ook in de non-bancaire sector. Iedere dag worden er nieuwe valuta gestart op basis van de Bitcoin-code. In die zin maken we op het moment ook een vergelijkbare wildgroei mee als toentertijd in Engeland.

3.3 Overzicht van de werking van Bitcoin

Om aan het eind van het theoretische framework een overzicht te kunnen geven van de systematische verschillen tussen Bitcoin en het hedendaagse geldsysteem is het nodig om de eerstgenoemde eerst technisch te begrijpen.

3.3.1 Protocol

Bitcoin is de naam van het protocol dat wordt gebruikt om decentraal monetaire transacties mee te verwerken. Dit protocol bestaat in de programmacode[56] en beschrijft de regels waar alle agenten aan dienen te voldoen om het systeem te laten werken. Het protocol is in grote mate afhankelijk van wiskunde. Je kan het protocol vergelijken met het HTTP-protocol van het internet. Een set van regels om interactie mogelijk te maken. Bitcoin is essentieel een internetprotocol dat beschrijft hoe een systeem op een decentrale manier tot een eenduidige besluitvorming kan komen wat betreft eigendom. Dat Bitcoin puur en alleen een geldsysteem zou zijn is daarmee onwaar. De functie als geldsysteem is echter de eerste toepassing of applicatie die erop gebaseerd is. Stefan Molyneux, een blogger/auteur van Canadese afkomst, legt dit uit:

> *"Bitcoin is not just a money construct. It's one of the components and it's what gives it a great value, but Bitcoin is not just money transfer. (...)*
>
> *Bitcoin is a publicly ordered ledger of what has occurred for you. Financially, in terms of property, (...) ownership, (...) contracts… and all these things can be publicly audited, and verified. (...) It eliminates labour in conflict resolution. (...)*
>
> *Bitcoin is a revolutionary protocol for information synchronization. It can precisely and chronologically order all database entries and check their validity without central authority."*[57]

Hierop volgend zullen we Bitcoin alleen nog bespreken als zijnde een geldsysteem.

In het protocol staat gedefinieerd dat het geld, de Bitcoins, worden gecreëerd als beloning voor het verifiëren van transacties en dat dient elke tien minuten eenmalig te gebeuren. Een

verzameling transacties die gevalideerd is staat bekend als een '*block*' (hierna ook wel *'transactieblok'* genoemd), en de beloning van Bitcoins die erbij hoort als '*block reward*'. Het verifiëren van transacties staat bekend als '*minen'* en de computers die dat doen staan bekend als '*miners*'.

3.3.2 Geldcreatie & geldhoeveelheid

Er kunnen niet meer dan ~21 miljoen[58] van deze Bitcoins in omloop komen doordat de hoeveelheid Bitcoins die als beloning wordt toegekend ongeveer elke 4 jaar halveert, en uiteindelijk op nul zal uitkomen. Het halveren gebeurt na elke 210.000 verwerkte transactieblokken en heeft dus géén vaste link aan tijd, ondanks dat dat gesuggereerd wordt door te stellen dat er elke tien minuten zo'n blok gevalideerd dient te worden. Het startbedrag van de beloning bedroeg in 2009 vijftig Bitcoin en is op heden één keer gehalveerd; in 2013 werd de beloning gehalveerd naar 25 Bitcoin per *block*.

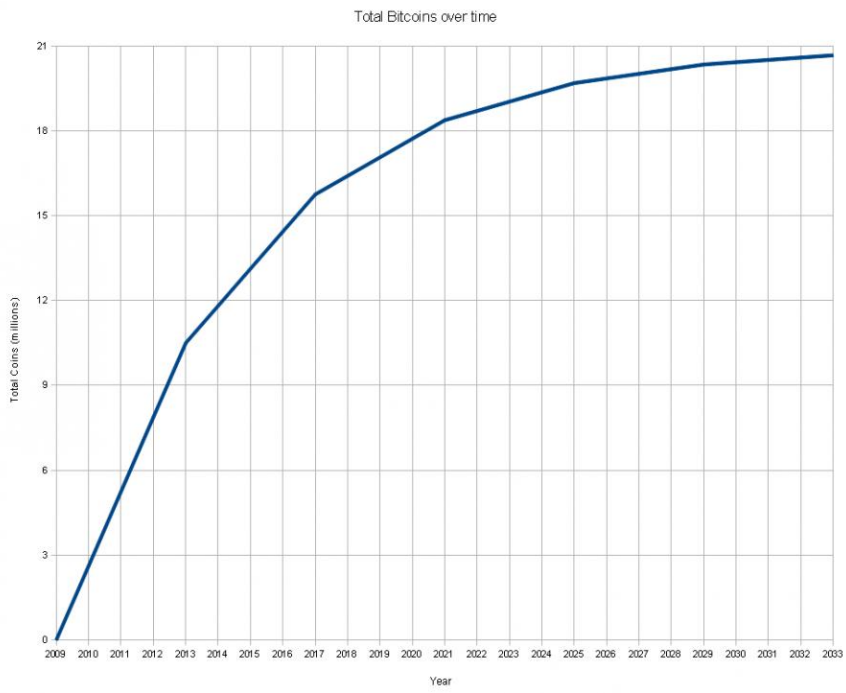
De vraag[59] waarom er maar 21 miljoen Bitcoins in totaal in omloop zullen zijn wordt dus beantwoord door simpelweg de som in te vullen van de gegeven startparameters. Als na elke 210.000 transactieblokken de grootte van de beloning voor het verifiëren van transacties gehalveerd wordt (naar beneden afgerond), en je met een beloning van 50 Bitcoin begint, dan kan je in een tabel mooi de progressie en het verloop zien. Aangezien een Bitcoin deelbaar is door 100.000.000 wordt hier gerekend met het meest elementaire deeltje van een Bitcoin: een '*Satoshi*' $(\frac{1}{100.000.000})$. Een *Satoshi* kan je vergelijken met de ondeelbaarheid van een eurocent.

~Jaar	Block reward (x100.000.000)	Gegenereerde aantal Satoshi deze periode
2009	50	1.05e+15
2013	25	525.000.000.000.000
2017	12.5	262.500.000.000.000
2021	6.25	131.250.000.000.000
2025	3.125	65.625.000.000.000
...	...	...
2137	1e-8 (1 Satoshi)	210.000
		Totaal: ~2.100.000.000.000.000

De totale geldhoeveelheid is dus de uitkomst van twee waarschijnlijk arbitraire keuzes: het besluit het geldnetwerk te beginnen met een *block reward* van 50 Bitcoin, en de wens om deze elke 4 jaar te laten halveren. Door dit elke 210.000 blokken te laten gebeuren kom je ongeveer uit op een cyclus van 4 jaar: 6 blokken per uur, 144 per dag, 52560 per jaar, en 210.240 per 4 jaar.

Het besluit om het totaal aantal Bitcoins uit te laten komen op een schaalgrootte van miljoenen in plaats van miljarden is waarschijnlijk psychologisch van aard geweest[60]. Ter vergelijking: volgens de ECB[61] was er in het jaar 2013 in de maand Oktober 9882 miljard Euro (M3), en dus $9882\,x\,10^{11}$eurocenten. Er zijn meer Satoshi's dan dat ($21\,x\,10^{14}$), maar die zouden lange tijd tijdens de opstartfase van Bitcoin werkelijk niets waard geweest zijn als we ze op die schaalgrootte hadden aangehouden. Door Bitcoins in miljoenen te rekenen lijkt de totale hoeveelheid schaarser dan die eigenlijk is en komt de marktprijs sneller hoger te liggen dan die van hedendaagse fiatvaluta, wat de media-aandacht en adoptie ten goede komt.

De laatste Bitcoins zullen naar schatting vóór het jaar 2140 gedolven worden. Dat resulteert in de volgende curve voor de geldhoeveelheid:

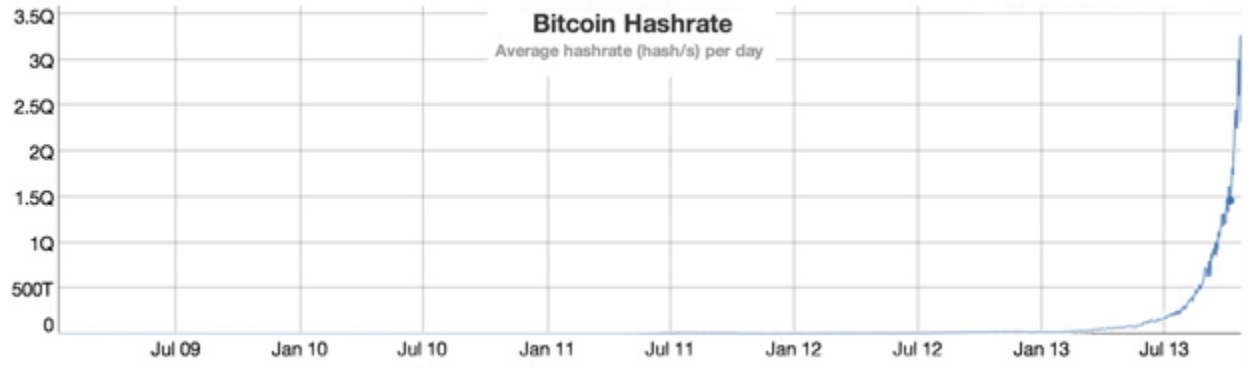


De curve lijkt erg op de curve van het delven naar goud. Dat is ook waar de terminologie van *mining*[29] en *miners* vandaan komt. Immers is goud ook schaars, is er tot nog toe slechts 171,300 ton goud gedolven sinds het begin der mensheid en neemt ook de goudproductie gestaag af (die is afhankelijk van de winstgevendheid van het delven). Dit is waar de analogie ophoudt. Waar goud namelijk bij een gegeven kostenniveau niet meer gedolven zal worden zullen er toch (minimaal) elke tien minuten nieuwe Bitcoins blijven ontstaan om de bedoelde curve in stand te houden. Het netwerk past gezamenlijk de kosten aan van het virtuele delvingsproces om te garanderen dat er ongeveer elke tien minuten gedolven zal worden. Dit gebeurt door collectief de zogeheten '*difficulty*' of *moeilijkheid* aan te passen van de

[29] deze analogie is echter niet door Satoshi voorgesteld. Nakamoto had het in de eerste implementaties van de applicatie gelabeld als "generate coins". De oorsprong ligt in de volgende passage uit het paper: "*The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended*." Hier werd bijvoorbeeld nog gesproken over 'minting': https://bitcointalk.org/index.php?topic=721.0 voordat de conses door de gemeenschap toch op 'mining' kwam te liggen.

cryptografische puzzels die *miners* dienen op te lossen. Deze *difficulty* wordt ongeveer elke 2 weken (elke 2016 *blocks*) aangepast.

Ondanks dat het de bedoeling is dat er ongeveer elke tien minuten nieuwe Bitcoins gedolven worden is de praktijk iets anders. Het delvingsproces is afhankelijk van de hash-functie (HashCash) die Bitcoin gebruikt om *miners* te kunnen laten bewijzen dat ze een bepaalde moeite hebben gedaan voor het valideren van de transacties. Inmiddels zijn er een aantal producenten die computers op de markt zetten die bekend staan onder de term 'ASIC' (Application-Specific Integrated Circuit). Deze computers kunnen een specifieke berekening extreem efficiënt uitvoeren. In dit geval: de hashfunctie die *miners* uitvoeren (zie 3.3.11). Sinds er een hoop van deze ASICs in korte tijd in gebruik zijn genomen is de efficiëntie van het *minen* exponentieel toegenomen.



In bovenstaande grafiek is de gezamenlijke rekenkracht van het Bitcoinnetwerk uitgezet. De *difficulty*, de moeilijkheid van de cryptografische puzzels bij het valideren van transacties, past zich vanzelf aan aan deze influx van nieuwe rekenkracht. Dit gebeurt echter maar elke *twee weken*. Als er een aantal sterke ASICs in gebruik worden genomen kan het gebeuren dat er een periode te snel nieuwe Bitcoins worden ontdekt, en dat er sneller transacties gevalideerd worden dan elke tien minuten zoals de bedoeling is. Dit heeft ook ten gevolge dat er een steeds scherpere centralisatie plaatsvindt van het delven, omdat het steeds hogere investeringen vereist om rendabel te blijven, die loodrecht staat op een van de principes van Bitcoin, namelijk decentralisatie. Morgen E. Peck, blogger op de website IEEE Spectrum zei dit erover in een artikel genaamd "*Bitcoin's Computing Crisis*":

"*The change has occurred as enriched bitcoin miners have reinvested their profits into new, sophisticated hardware, a trend that's likely to continue until companies manufacturing this equipment bump up against the state of the art in computer-chip technology. In the meantime, smaller operations, the little guys who once had a decent chance of earning some bitcoins on their laptop PCs, are being edged out by the competition, leaving the stability and security of Bitcoin in the hands of fewer people and threatening the reputation of a currency that was designed to distribute power among the masses.*"[62]

3.3.3 Decentralisatie

Gezien een van de principes waar Bitcoin op is gebouwd de 'rechtmatigheid' is zoals die eerder gedefinieerd is, *de onmogelijkheid voor een partij je transactie te weigeren of jou je geld afhandig te maken buiten je wil om*, is het nodig dat de *blockchain* decentraal wordt opgeslagen en verwerkt. D.w.z. iedereen is vrij een computer aan te sluiten op het netwerk en de rol van betalingsverwerker te spelen en om zo te '*minen'.* Diens handelingen worden dan alleen door de rest van het netwerk geaccepteerd als je hetzelfde protocol gebruikt. Enkel op die manier is er de garantie dat er niet een enkele autoriteit een onrechtmatigheid pleegt, want er is in dit systeem méér dan één autoriteit die transacties verwerkt, en deze autoriteiten moeten het met elkaar eens worden over de versie van de boekhouding die ze delen. Deze autoriteiten worden '*miners'* genoemd. Het beslissingsproces van overeenstemming over de juiste versie van de *blokketen* is de revolutionaire kern van het protocol. De aangaande centralisatie van het delvingsproces, gedreven door technische ontwikkelingen van *mining*-hardware, is echter mogelijk een gevaar voor de decentrale aard van het protocol. (zie ook sectie 4.5.2)

Alle *miners* gebruiken dezelfde software, en dat garandeert dat ze de regels uitvoeren naar behoren, en daarmee je transactie verwerken zonder sjoemelen. Als *miners* de regels (van het protocol) anders uitvoeren dan bedoeld (door bijvoorbeeld een aangepaste variant van de software te draaien) dan worden hun acties niet geaccepteerd door de rest van het netwerk. Het hele netwerk moet in consensus zijn over de gedane zaken, anders worden bepaalde transacties niet verwerkt in de centrale boekhouding en niet vereeuwigd.

3.3.4 Adressen / rekeningnummers

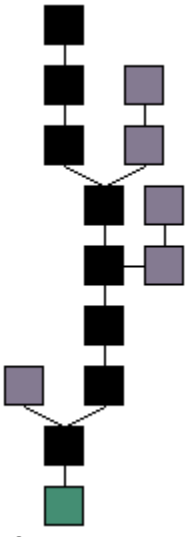
Het Bitcoinsysteem bevat 'accounts' waar geld op te ontvangen is. Dit zijn de zogeheten Bitcoinadressen. In tegenstelling tot de adressen in het reguliere banksysteem, die bestaan uit getallen, is het in Bitcoin mogelijk zomaar nieuwe adressen te genereren om geld op te ontvangen zonder dat iemand daar toestemming voor hoeft te geven. Een Bitcoin-adres ziet er als volgt uit: '`12qsmag851PVGQsmqPayCgNABS3mbc2tgL`'. Een vrij willekeurige tekenreeks dus die op zichzelf niet gekoppeld is aan een menselijke identiteit. Elk Bitcoinadres bestaat uit twee delen: een private sleutel en een publieke sleutel. De publieke sleutel is het Bitcoinadres dat wordt gebruikt bij het ontvangen van transacties[30]. De private sleutel wordt gebruikt om te kunnen bewijzen dat een publieke sleutel aan jou toebehoort. Het is vanwege het grote aantal mogelijke sleutels statistisch onwaarschijnlijk een sleutelpaar te genereren dat iemand anders al bezit.

3.3.5 Wallet

De private sleutels van Bitcoinadressen in je beheer worden opgeslagen in een zogeheten '*wallet*'. Dit is een klein bestand, vaak versleuteld. Als je deze *wallet* kwijtraakt of de toegang ertoe verliest ben je daarmee de toegang tot de Bitcoins kwijt die in de *blockchain* staan. De Bitcoins zijn dan niet weg, slechts de sleutels om te bewijzen dat ze van jou waren. Van een *wallet* is makkelijk een back-up te maken voor de veiligheid. Vaak worden de digitale portemonnees echter niet meer op de computers van consumenten gehouden maar op een website die je *wallet* beheert om te voorkomen dat je portemonnee gestolen wordt wegens beveiligingslekken in een computersysteem[31].

3.3.6 Boekhouding

De kern van het systeem is een enkel bestand waar alle transacties (ooit) in worden bijgehouden. De unieke centrale boekhouding; een transactielogboek. Hier staan slechts transacties in; het is geen lijst van accounts met saldi. Dit bestand heet de *'blockchain',* of '*blokketen'* omdat het bestaat uit een keten van blokken met gevalideerde transacties (zie illustratie rechts). Van dit bestand is het de bedoeling dat er maar één



[30] dit is een versimpelde weergave. Om enkele redenen wordt er voor Bitcoinadres aakt van *een hash van de publieke sleutel*

[31] Het is al vele malen voorgekomen dat er Bitcoins zijn gestolen door beveiligingslek https://bitcointalk.org/index.php?topic=83794.0

enkele versie van is in het hele netwerk. Vergelijk dit enkele bestand met de systematische complexiteit van de collectieve boekhouding in het hedendaagse geldsysteem; een samenhangsel van de boekhoudingen van élke commerciële bank én de centrale bank. Als commerciële banken geen geld zouden kunnen creëren en burgers reserves aan konden houden bij de centrale bank[32], dan had je de *blockchain* kunnen vergelijken met het transactielogboek op de server van de centrale bank, en dat is ongeveer wat leden van de IMMR ook proberen te bereiken. Het verschil is dat er in de boekhoudingen van banken vooral wordt bijgehouden hoeveel saldo er staat op accounts. In Bitcoin is niet aan te wijzen waar een Bitcoin zich precies bevindt. Bitcoins bestaan alleen omdat ze worden genoemd in transacties. Daarom is het ook nodig de hele *blokketen* terug te kijken om precies te weten wat het saldo van een bepaald Bitcoinadres is. Een artikel op Coindesk.com legt dit goed uit:

> *"Here's the funny thing about bitcoins: they don't exist anywhere, even on a hard drive. We talk about someone having bitcoins, but when you look at a particular bitcoin address, there are no digital bitcoins held in it, in the same way that you might hold pounds or dollars in a bank account. You cannot point to a physical object, or even a digital file, and say "this is a bitcoin". Instead, there are only records of transactions between different addresses, with balances that increase and decrease. Every transaction that ever took place is stored in a vast general ledger called the block chain. If you want to work out the balance of any bitcoin address, the information isn't held at that address; you must reconstruct it by looking at the block chain."*[63]

3.3.7 Veiligheid

Het netwerk blijft in theorie relatief veilig zolang meer dan 51% van de *miners* (meer dan de helft van de rekenkracht van het netwerk) eerlijk is. Wanneer dat niet langer het geval is, is het in theorie mogelijk voor degene die meer dan de helft van de rekenkracht bezit om Bitcoins vaker dan ééns uit te geven ('*double-spending*'). In de praktijk zal een dergelijke aanval echter al met een kleinere rekenkracht plaats kunnen vinden gezien de binomiale aard van de verdeling (Rosenfeld (2012)). De kosten voor het bemachtigen van meer dan 51% (of de minimale ratio die volgens Rosenfeld slechts benodigd zou zijn voor een bepaalde duur) van de totale rekencapaciteit, én het succesvol uitvoeren van een *double-spend attack* worden echter

[32] zoals het voorstel van Positive Money

zó hoog geschat dat het (in theorie) financieel aantrekkelijker zou moeten zijn om met een dergelijke rekenkracht eerder nieuwe Bitcoins te genereren dan deze in te zetten om reeds geverifieerde transacties aan te passen in je voordeel.

3.3.8 Transparantie

Doordat de boekhouding decentraal gedeeld wordt zijn dus alle transacties van iedereen openbaar. Alleen op deze wijze is het mogelijk voor alle partijen (*miners*) om de validiteit van transacties te controleren. Dit betekent dat je gemakkelijk via het internet verbinding kan maken met het Bitcoinprotocol en kan 'meeluisteren' naar wat er gebeurt. Je kan de *blokketen* opvragen en er berekeningen op uitvoeren (die niet op het netwerk van invloed zijn; voor privé-gebruik), maar het belangrijkste aspect: het is mogelijk als derde partij te kunnen volgen *hoeveel nieuw geld er in het netwerk gecreëerd wordt, hoe snel, en door 'wie'*. Dit zal later van pas komen bij de wens van transparantie bij geldschepping van digitaal staatsgeld (sectie 4.2).

Het kunnen opvragen van de *blokketen* stelt je verder in staat om een applicatie te schrijven die je (bijvoorbeeld) live per email laat weten wanneer je saldo verandert, of wanneer iemand je geld stuurt. Vergelijk dit met het huidige banksysteem, waar je je saldo alleen kan zien bij het internetbankieren waar je als persoon moet inloggen, en geen notificaties kunt krijgen voor nieuwe inkomende en uitgaande betalingen. Er zijn in het kader van veiligheid doorgaans geen mogelijkheden om applicaties te schrijven die interacteren met je bankrekening. Het hedendaagse geld- en bankprotocol is privé.

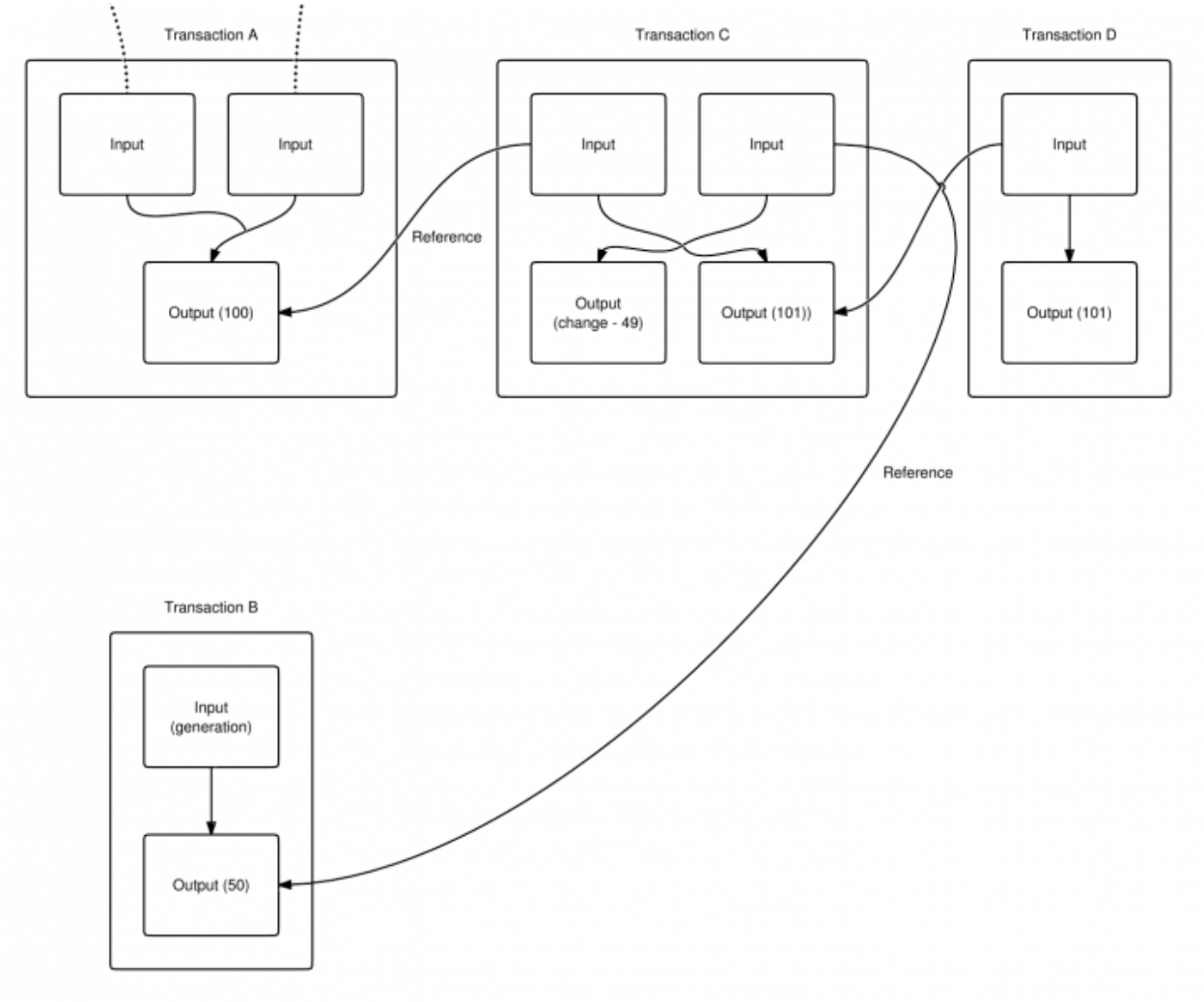
Dit wordt nog eens duidelijk gemaakt aan de hand van een project dat dit ook beoogt te veranderen: het 'Open Bank Project'[64]. Het Open Bank Project ontwikkelt een applicatie-interface waarmee banken op een veilige manier de klantdata kunnen vrijgeven zodat die gebruikt kunnen worden in applicaties. Dit zeggen ze erover:

> *"The Open Bank Project provides an open source developer friendly "API for banks" that developers and companies can use to build innovative applications and services based on the account holders transaction data. It uses a secure, enterprise ready technology stack and supports secure Internet protocols such as OAuth.*
>
> *The Open Bank Project exposes transaction data in a simple and consistent structure by abstracting away the peculiarities of each banking system. This is achieved by "connectors" that interface between the OBP API and each core banking system. This enables application developers to write an app once, and use it for many banks."*

Met dit project proberen ze nu dan eindelijk innovatie aan te brengen bij banken. Met de API van het Open Bank Project zal het mogelijk zijn om met banken te interacteren op de manier dat dat nu al mogelijk is met het Bitcoinnetwerk. De enige tekortkoming is dat je nog steeds geen toegang zal kunnen krijgen tot de statistieken van geldcreatie.

3.3.9 Transacties

Om een betaling te doen verstuur je een bericht naar de andere computers in het netwerk die een versie van de boekhouding, de *blockchain*, bijhouden. In dit bericht stel je dat je een aantal Bitcoins verstuurt van jouw Bitcoinadres naar een ander adres. Het is hierbij een eis dat er in het bericht gerefereerd wordt naar eerdere transacties die Bitcoins hebben overgemaakt naar een of meer adressen die aantoonbaar van jou zijn, en die nog niet zijn uitgegeven. De transacties waar naar gerefereerd wordt heten '*inputs*', de transactiehoeveelheid i.c.m. het adres van de ontvanger wordt een '*output*' genoemd. Hier is een schematisch overzicht van dit concept:


Transaction A
Input
Input
Output (100)
Reference
Transaction C
Input
Input
Output
(change - 49)
Output (101))
Transaction D
Input
Output (101)
Reference
Transaction B
Input
(generation)
Output (50)

3.3.10 Transactievalidatie

Wanneer een transactie verstuurd wordt betekent dit nog niet dat de transactie ook gevalideerd is. Het zou bijvoorbeeld nog steeds kunnen voorkomen dat de transactie bij nadere inspectie geweigerd moet worden. Nadat een gebruiker een transactie naar de rest van het netwerk stuurt zullen de *miners* het met elkaar eens moeten worden over welke transacties wél geaccepteerd zullen worden en welke niet. De *miners* voeren hiervoor o.a. een aantal checks uit: (a) ze kijken terug in hun eigen boekhouding (de *blokketen*) om er zeker van te zijn dat het adres van waaruit je Bitcoins probeert te versturen een toereikend saldo heeft, (b) ze doen een veiligheidscheck om er zeker van te zijn dat jij als persoon de echte eigenaar bent van het gestelde Bitcoinadres, en (c) ze onderzoeken de afwezigheid van andere transacties die dezelfde Bitcoins proberen te gebruiken (*double-spend*[33]).

Als aan deze eisen wordt voldaan kan de transactie in principe collectief in de boekhouding bijgeschreven worden. Dan rest er nog een probleem. De computers in het netwerk moeten overeenkomen over een volgorde van de transacties die ze gevalideerd hebben. Aangezien ze dit decentraal moeten doen is het onwaarschijnlijk dat ze de gevalideerde transacties op dezelfde manier in hun boekhoudingen zouden verwerken zonder daarbij op een manier te overleggen. Immers krijgen ze allen op andere tijdstippen te horen welke nieuwe transacties er gedaan worden, vanwege de structuur van de netwerkverbinding. In welke volgorde wordt overeengekomen dat de transacties gedaan zijn en op welk precieze tijdstip zijn deze gevalideerd? Dit proces, het doen van een tijdsbepaling van data, wordt *timestamping* genoemd. Om dit te faciliteren is er, zoals eerder gezegd, in het protocol ingebouwd dat *miners* eerst een cryptografische puzzel dienen op te lossen.

3.3.11 Proof-of-work (PoW)

Het concept van de puzzel is dat deze moeilijk is om op te lossen, maar dat de oplossing makkelijk te verifiëren is wanneer deze eenmaal bekend is. Dit wordt een '*Proof-of-work*' genoemd, omdat je met de oplossing kan bewijzen dat je een bepaalde hoeveelheid werk hebt verricht. Bitcoin gebruikt hiervoor het eerdergenoemde HashCash-algoritme.

[33] Voor een illustratieve uitleg van de *double-spend* aanval, zie Rosenfeld (2012)

Miners verzamelen de transacties en valideren deze. Terwijl ze dit doen proberen ze ook de moeilijke HashCash-puzzel op te lossen. Als een *miner* de oplossing van de puzzel vindt stuurt hij deze samen met de door hem gevalideerde transacties naar de andere computers in het netwerk. Die kunnen de zogenaamde oplossing van de puzzel valideren. Als deze correct is valideren zij op hun beurt alle transacties die door de ene *miner* gevalideerd zijn en schrijven ze die collectief in hun boekhoudingen. Als de eerste *miner* transacties verkeerd gevalideerd heeft en zich daarmee niet aan de regels gehouden, dan zullen de andere *miners* zijn werk niet accepteren, wordt de *blokketen* niet met zijn *blok* verlengd en ontvangt hij geen *block reward*.

Door in het proces van validatie een kunstmatig moeilijk werk te vereisen zorgt het protocol ervoor dat alle *miners* decentraal toch kunnen overeenstemmen over *timestamps* van transacties. Nogmaals, de moeilijkheid van de puzzel, de *difficulty*, wordt decentraal bepaald en is afhankelijk van hoe snel de afgelopen 2016 puzzels (wat de voorgaande twee weken zouden moeten zijn als er daadwerkelijk elke tien minuten een *blok* wordt gecreëerd) zijn opgelost. Het is de bedoeling dat er elke tien minuten een wordt opgelost. Als er veel computers in het netwerk zijn die de puzzel proberen zal de moeilijkheid van de puzzel omhoog gaan, en andersom, om weer naar deze streeftijd te accomoderen.

3.3.12 Samenvattend

Het moge duidelijk zijn dat Bitcoin niet makkelijk simpel te beschrijven is. Molyneux zegt dat Bitcoin een protocol beschrijft van eigendomsoverdrachten. Een Bitcoin bestaat eigenlijk niet. Er zijn alleen vastgelegde berichten over veranderingen van eigendom. Als je een Bitcoin 'bezit' heb je in feite een eigendomstitel, en die eigendomstitel is wat je weggeeft als je met Bitcoins 'betaalt'. Daarom zegt Molyneux ook dat Bitcoin primair een protocol is dat eigendomsoverdracht beschrijft, en pas in tweede plaats ook een valuta is.

Dit concept, een protocol dat de overdracht van eigendomsrechten faciliteert, is doorgaans moeilijk uit te leggen omdat er maar zo weinig dingen zijn die we gebruiken waar het mee te vergelijken is. Een auteur die bekend staat als George Ettinger liep ook tegen dit probleem aan, dat het moeilijk is de kern van het protocol eenvoudig uit te leggen:

> *Bitcoin does not lend itself to casual explanation or to convenient metaphor. In fact, very few comparisons even suit it! It's a currency but it works like a commodity. It's mined in*

> *limited quantities, so… it's almost like gold! …except it's created at an exact, fixed rate and will end at an exact, fixed point. So, not like gold. The work of 'mining' doesn't really 'accomplish' anything, either. Bitcoin is a trainwreck of anachronisms to have to dump on any unsuspecting novice, and horrible pseudo-words like 'blockchain' and 'hashcash' just make it sound more like a scam.*

Hij zocht vervolgens naar een narratief om Bitcoin mee te kunnen vergelijken. Deze heeft hij ook gevonden[65]. In de stille oceaan, in Micronesië, ligt het Eiland van Yap. Hier werd geen geld gebruikt zoals we het nu kennen. De inwoners maakten hier enorme muntvormige rotsen die ze naar hun eiland verplaatsten. De 'munten' werden er neergelegd maar waren te groot om bij iedere transactie te verplaatsen. Bij een transactie dienden de beide partijen in het openbaar, in het bijzijn van een groot deel van de bevolking, te verklaren dat de munt van eigenaar wisselde. Op deze manier was je geen eigenaar van een munt totdat een meerderheid van de bevolking je het eigendom toekende.

> "*Ownership was a matter of public declaration. By spreading the word to others, it became verification. You didn't own currency unless you got the majority of the community to agree you did. You did this by conducting your business transparently, and announcing all transactions to the world at large. A deal made in secret or made dishonestly was impossible; transparency was part of the protocol.*"

Het verhaal is opgenomen in de bijlagen.

In het volgende deel zal er dieper worden ingegaan op de techniek van het protocol. Hier zullen ook de haken en ogen worden uitgelegd die ontstaan bij dit proces van transactievalidatie.

3.4 Technische werking van Bitcoin

In de volgende sectie volgt een uitleg over de technische werking van het protocol. Deze raakt eerlijk gezegd nog maar de oppervlakte. Er zijn meer specificaties, technische aspecten, vraagstukken en axioma's die hieraan ten grondslag liggen, maar wat volgt kan gezien worden als de basis en dus een basale explicatie van de werking. Het is van essentie deze werking toe te lichten om in volgende secties het belang van wijzigingen en overwegingen te begrijpen.

Enkele basisbegrippen waar de technische werking van afhankelijk is, zoals asymmetrische cryptografie en hash-functies, zal ik hier niet in detail uitleggen.

3.4.1 Een transactie opstellen

Wanneer persoon Aeen x aantal Bitcoin wil verzenden naar persoon B dan is het nodig dat A het publieke adres van B weet. Dit adres kan B vrijelijk delen en bekend maken. Laten we zeggen dat B een nieuw adres maakt[66] voor deze transactie met A. Het nieuw gegenereerde adres bevat een publieke sleutel en een private sleutel. De publieke sleutel wordt aan A bekend gemaakt. Dit is effectief het rekeningnummer.

A stelt vervolgens een bericht op[67] waarin ze verklaart een x aantal Bitcoin te versturen naar het adres van B. In dit bericht vermeldt ze ook de identificatienummers (hashes) van één of meer eerdere transacties naar één of meer adressen waar ze de private sleutels van beheert. Door dit te doen laat ze zien dat ze (a) in het verleden een hoeveelheid Bitcoins heeft ontvangen, en (b) dat die nog niet zijn uitgegeven en dus gebruikt kunnen worden in deze transactie. *Miners* zullen bij het verifiëren terug moeten kijken in de *blokketen* om te zien of A de waarheid heeft gesproken en geen Bitcoins heeft geprobeerd te gebruiken die ze niet had.

Geld spenderen in Bitcoin kan je vergelijken met het betalen van een bedrag in cash, waarbij je je voor moet stellen dat je een bedrag van bijvoorbeeld €1,- betaalt met een briefje van €20,- en daarbij een aantal biljetten als wisselgeld terugkrijgt. Het verschil met Bitcoin is dat je wisselgeld een enkel briefje is met precies de denominatie van het bedrag aan wisselgeld.

Zoals eerder vermeld worden transacties die als geldbronnen in nieuwe transacties worden aangehaald '*inputs'* genoemd. Een *input* kan je vergelijken[68] met het biljet van €20,- waarmee

je in bovenstaand voorbeeld het bedrag van €1,- betaalt. Dit zegt de officiele wiki[67] over een *input*:

> "*An input is a reference to an output in a different transaction. Multiple inputs are often listed in a transaction. The values of the referenced outputs are added up, and the total is usable in the outputs of this transaction.*"

Zo ziet een *input* er uit:

Previous tx	f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index	0
scriptSig	304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Hier zie je in de eerste rij het identificatienummer staan van een eerdere transactie waar naar gerefereerd wordt. In de gerefereerde transactie zijn Bitcoins overgemaakt naar een adres en die gaan nu gebruikt worden. Het indexgetal in de tweede rij geeft aan welke *output* in die transactie hier gebruikt moet worden als geldbron. Laten we zeggen dat er 20 Bitcoin (BTC) in deze *input* staat, op een adres waar A de private sleutel van beheert. In de laatste rij staat o.a. de handtekening van A gedaan met haar private sleutel die bewijst dat de Bitcoins in *output* #0 van de gerefereerde transactie van haar zijn.

Het Bitcoinadres van de ontvanger (B) in combinatie met de hoeveelheid te versturen Bitcoins heet een '*output*'. Dit zegt de wiki over een *output:*

> *"An output contains instructions for sending bitcoins. (...). There can be more than one output, and they share the combined value of the inputs. Because an output can only ever be referenced by a single input, the entire combined input value needs to be sent in an output if you don't want to lose it. If the input is worth 50 BTC but you only want to send 25 BTC, Bitcoin will create two outputs worth 25 BTC: one to the destination, and one back to you (known as "change", though you send it to yourself). Any input bitcoins*

not redeemed in an output is considered a transaction fee; whoever generates the block will get it."

Hier wordt een belangrijk axioma uitgelegd. Wanneer je een *input* refereert in een nieuwe transactie zal je die in het geheel moeten benutten (voor de volle waarde) omdat de restwaarde gezien wordt als transactiefooi, en je *outputs* uit eerdere transacties maar één keer kunt gebruiken. De manier om in een transactie geld te wisselen is dus om restwaarden in een tweede *output* weer naar jezelf (een adres in jouw beheer) te sturen. Als A dus een *input* gebruikt waar 20BTC op staat van haar, en ze die wil gebruiken om een betaling mee te verrichten van 1BTC, dan dient ze twee *outputs* te maken. Één van 1BTC naar het adres van B, en een van 19BTC naar een adres in eigen beheer (dit kan hetzelfde adres zijn van waaruit de munten in eerste instantie verzonden worden). Dit kan je zien als wisselgeld ('*change*').

Zo ziet een *output* eruit:

Value	1000000000
scriptPubKey	OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d OP_EQUALVERIFY OP_CHECKSIG

De eerste rij geeft aan hoeveel *Satoshis* (de atomaire rekeneenheid) er overgemaakt dienen te worden aan de ontvanger met het publieke adres zoals vermeld in de tweede rij. In de tweede rij staat het stukje programmacode dat uitgevoerd moet worden door de persoon die de Bitcoins in de *output* van deze transactie wil claimen.

De opgestelde transactie zoals hier beschreven ziet er in zijn geheel schematisch als volgt uit:

Transactie #0 van $? -> A$ van 20 Bitcoin
[hash: 8888b0191a55a1c4da2993ef780ca38f767ab92455b15f0621047074ec64c226**]**

inputs	outputs
(...)	**Value** 20000000000 **scriptPubKey** <adres A> <code> (...)

Transactie #1 van $A -> B$ van 1 Bitcoin

inputs	outputs
Previous tx 8888b0191a55a1c4da2993ef780ca38f767ab92455b15f0621047074ec64c226 **Index** 0 **scriptSig** <pub sleutel A> <handtkng A>	**Value** 1000000000 **scriptPubKey** <adres B> <code> **Value** 19000000000 **scriptPubKey** <adres A> <code>

De eerste transactie (**#0**) is een transactie die 20 Bitcoin heeft overgemaakt op het adres van A. In de transactie naar Bwordt deze gebruikt als geldbron door deze te noemen in de *inputs*. Zie dat de hash in het veld '**Previous tx**' overeenkomt met de hash van **transactie #0**. Deze link vormt een keten van transacties die het mogelijk maakt de bronnen van betalingen te traceren tot aan de eerste in 2009. De eerste *output* is de betaling aan B, de tweede *output* is de restwaarde van de gerefereerde *input*, de *change* die terug wordt gestuurd naar het adres van A.

3.4.2 De transactie signeren[69]

Ten slotte dient A de transactie te ondertekenen met haar handtekening om aan te tonen dat het publieke adres in de *outputs* van de gerefereerde transactie (**transactie #0**) aan haar toebehoort. Voor elke *input* in **transactie #1** zal ze haar handtekening moeten zetten.

Onthoud, bij het genereren van een Bitcoinadres worden er twee sleutels gegenereerd door middel van asymmetrische versleuteling[70]. De private sleutel is in feite het wachtwoord voor het Bitcoinadres (die je als bankrekening kan zien), maar deze kan natuurlijk niet openlijk gedeeld worden. Dan zou iedereen de sleutel kunnen kopiëren en gebruiken om toegang te krijgen tot de Bitcoins van A. Er moet dus bewezen worden dat Abeschikt over de private sleutel die hoort bij het publieke adres, zoals gespecificeerd in de *output* van de transactie waar ze de Bitcoins uit wil halen. Dit dient bewezen te worden *zonder* dat deze private sleutel wordt prijsgegeven.

In plaats van het prijsgeven van de private sleutel wordt de nieuwe transactie (**#1**) zoals die net is opgesteld (min de al gegenereerde handtekeningen voor *inputs*[34]) voor iedere gerefereerde *output* gecodeerd met de corresponderende private sleutel. Kortom, een handtekening voor een *input* bestaat uit een hash van de nieuwe transactie (zonder handtekeningen), gecodeerd met de private sleutel die hoort bij de publieke sleutel in de gerefereerde *output*. Bij iedere *input* komt een handtekening te staan om (a) te bewijzen dat alle gerefereerde publieke adressen in de *outputs* van vorige transacties aan A toebehoren en dat ze daarmee gerechtigd is de Bitcoins erin uit te geven, en (b) de essentiële data in de transactie te beveiligen tegen modificatie van derden.

[34] Het is nodig dat de handtekening voor de transactie wordt gedaan over de gehele opgestelde transactie, exclusief handtekeningen voor *inputs*. Dit moet omdat de handtekening na elke gesigneerde *input* anders in een andere waarde zou resulteren.

Voor het gemak is eerder gesteld dat Bitcoinadressen simpelweg de publieke sleutel zijn van een gegenereerd sleutelpaar. In feite is een Bitcoinadres om enkele redenen een *hash* van de publieke sleutel[67]. Dit betekent dat de handtekening die bij het signeren wordt gezet voor elke input niet gedecodeerd kan worden met het Bitcoinadres van de ontvanger. Hiervoor is de originele publieke sleutel nodig. Om deze reden worden *inputs* naast de handtekening ook ondertekend met de originele publieke sleutel van waaruit het Bitcoinadres gegenereerd is. In het schema staat de originele publieke sleutel vermeld als '`pub sleutel`', en het derivate Bitcoinadres als '`adres`'.

Derde partijen kunnen bij het ontvangen van het transactiebestand niet zomaar het ontvangstadres in de *output* wijzigen omdat dat haar handtekeningen voor de *inputs* zou invalideren.

3.4.3 Bitcoins claimen

In iedere transactie staat in de *output* een veld '**scriptPubKey**'. Eerder is vermeld dat hier het Bitcoinadres wordt vermeld als bestemming van de betaling. Het veld behelst eigenlijk meer dan dat. Het Bitcoinprotocol gebruikt een scriptingsysteem voor het claimen van transacties. Bij het opstellen van *outputs* in transacties kan de opsteller condities in scripttaal coderen. Een agent kan de waarde in een ongespendeerde *output* van een bestaande transactie vervolgens alléén claimen door in het veld '**scriptSig**' in de *input* van een nieuwe transactie de benodigde parameters te geven die resulteren in goedkeuring van de scriptfunctie, wanneer deze wordt uitgevoerd. Scripts zijn functies die in het transactieproces controleren of de agent die Bitcoins probeert uit te geven daar ook daadwerkelijk toestemming voor heeft. Deze functies worden uitgevoerd door de *miners.*

Alhoewel de mogelijkheden groot zijn is er in de praktijk (nog) maar één type script prevalent. Dat is het script zoals het eerder is uitgelegd; iemand die Bitcoins claimt dient aan te leveren:

- de publieke sleutel aan te leveren waarvan de hash gelijk is aan het adres in het script
- een handtekening van de hash van de nieuwe transactie, gedaan met de private sleutel, die met de publieke sleutel gedecodeerd kan worden en daarmee bewijst dat de claimer in bezit is van de vereiste private sleutel

3.4.4 Bitcoins *minen*

Miners, de computers die transacties valideren en het netwerk beveiligen tegen fraude, voeren een iteratief stappenplan uit (versimpeld):

- verstuurde transacties worden verzameld uit het netwerk
- transacties worden gevalideerd op basis van wat regels, en staan geen conflicten toe
- gevalideerde transacties worden gebundeld in een *blok*
- er wordt een SHA256-hashwaarde gezocht van het *blok* dat voldoet aan de eis van de *difficulty* (HashCash)
- het *blok* wordt met de gevonden hashwaarde verstuurd naar het netwerk

De *miners* krijgen als onderdeel van het peer-to-peer netwerk constant nieuwe transacties toegezonden terwijl ze op zoek zijn naar een *Proof-of-work* die de rest van het netwerk zou accepteren. Zoals eerder gesteld is de *PoW* nodig om te laten zien dat een bepaalde *miner* een bepaalde hoeveelheid werk heeft voltooid, waarmee hij zich differentieert van andere *miners.* Zonder dit differentiatieproces zou elke *miner constant* transacties valideren en zouden transacties niet meer eenduidig gevalideerd worden.

De nieuwe transacties moeten ingesloten worden in het *blok* dat op dát moment gemaakt wordt, en dit betekent dat de data waar het *blok* uit bestaat constant verandert, wat het proces van het genereren van hashes nog verder randomiseert. Om deze reden wordt het genereren van Bitcoins ook wel gezien als een loterij[71].

3.4.5 Transacties valideren

De transacties die ontvangen worden, worden o.a.[72] op een aantal zaken gecontroleerd, en worden vergeleken met twee bronnen van andere transacties. De eerste is de *blokketen* (BK) waar eerdere transacties al in vereeuwigd zijn. De tweede is de collectie van ontvangen transacties (O) die nog niet gevalideerd zijn. De inkomende transacties worden gecontroleerd op het volgende (versimpeld):

- de transactie dient nog onbekend te zijn in O, en niet te bestaan in BK
- de *outputs* die gebruikt worden in de *inputs* van de transactie dienen niet gebruikt te worden door andere transacties in O
- de handtekeningen met de private sleutels in het script dienen te kloppen

- de *outputs* die gebruikt worden in de *inputs* van de transactie dienen nog niet gespendeerd te zijn in BK
- de transactiefooi dient hoog genoeg te zijn om ingesloten te worden

De laatst genoemde regel behandelt de transactiefooi. Bitcoin prijst zichzelf als een betalingsnetwerk dat vrijwel gratis in gebruik is. Echter is het in de praktijk vaak toch vereist fooien toe te voegen aan transacties om deze tijdig geaccepteerd te doen krijgen.

3.4.6 Transactieblok creëren

Zoals gezegd moeten *miners* de ontvangen transacties valideren en dan insluiten in een *blok* dat ze aan het maken zijn. Wat is een *block* precies?

> *"Data is permanently recorded in the Bitcoin network through files called blocks. A block is a record of some or all of the most recent Bitcoin transactions that have not yet been recorded in any prior blocks. They could be thought of like the individual pages of a city recorder's recordbook (where changes to title to real estate are recorded) or a stock transaction ledger. (...) new blocks are added to the end of the record (known in Bitcoin as the block chain), and once written, are never changed or removed. Each block memorializes what took place immediately before it was created."*[73]

Blokken zijn dus collecties van transacties die elke 10 minuten gevalideerd worden. Een *blok* ziet er als volgt uit.

Blocksize	[grootte van blok in bytes, max 1MB (2013)]
Blockheader	

Version	1
hashPrevBlock	00000000000004ddbb71c6f49ea5324dadbe11a41e00ae590d670e3115b81dc6
hashMerkleRoot	f1bbf9be40010a8e43696ef4dbd692cbab76853274ab850bcaae39dad14eec58
Time	1317220624
Bits	436858461
Nonce	3382188868

Transaction counter	2
Transactions	

Transactie #0 [hash: (...)**]**

inputs	**outputs**
(...)	(...)

Transactie #1 [hash: (...)**]**

inputs	**outputs**
(...)	(...)

Zoals je hierboven ziet is een *blok* niets meer dan een collectie transacties, en wat metadata daarover, inclusief het bewijs dat de HashCash-puzzel gedaan is (daar komen we zo op). Wat een *miner* doet is het creëren van dit soort blokken met transacties.

Vooralsnog is er een limiet aan de grootte (in bytes) dat een block mag zijn, zoals te lezen is in het veld **Blocksize**; een *blok* mag voorlopig niet groter zijn dan 1MB. Satoshi heeft dit maximum ingesteld in 2010 als tijdelijke maatregel tegen spam d.m.v. te grote *blokken* die het netwerk zouden vertragen.

Belangrijk voor de *miner* is dat hij er een transactie bijdoet waarin hij de *block reward* aan zichzelf toekent. Een dergelijke transactie wordt een '*coinbase transactie*' genoemd omdat daar uiteindelijk alle Bitcoins uit ontstaan zijn. Zo'n transactie bevat geen *inputs*.

> *"A special kind of transaction, called a coinbase transaction, has no inputs. It is created by miners, and there is one coinbase transaction per block. Because each block comes with a reward of newly created Bitcoins (e.g. 50 BTC for the first 210,000 blocks), the first transaction of a block is, with few exceptions, the transaction that grants those coins to their recipient (the miner). In addition to the newly created Bitcoins, the coinbase transaction is also used for assigning the recipient of any transaction fees that were paid within the other transactions being included in the same block. (...)"*[74]

Omdat de *outputs* in een *coinbasetransactie* (er zijn geen *inputs*) specifiek naar het Bitcoinadres van de *miner* verwijzen zal de transactiepool die iedere *miner* gebruikt verschillen, en dus andere hashes opleveren.

In de **Blockheader** zie je de hash staan van het vorige *blok* dat geaccepteerd is in de *blokketen*. De link naar het vorige *blok* maakt de *blokketen* een keten. In het veld **hashMerkleRoot** staat de hash van alle hashes van de transacties die in het blok zijn opgenomen. Wanneer de *miner* nieuwe transacties ontvangt worden deze dan wel in het blok opgenomen, maar het kost nauwelijks meer rekenkracht om ze bij het berekenen van het *blok* te betrekken omdat er slechts een hash gemaakt wordt van de hashes, en niet elke keer van alle transactiedata zelf. Dit zegt de wikipagina[75] erover: "*Because transactions aren't hashed directly, hashing a block with 1 transaction takes exactly the same amount of effort as hashing a block with 10,000 transactions.*" Dit veld (**hashMerkleRoot**) is een van de velden die tijdens het zoeken naar de *PoW* constant zal veranderen.

3.4.7 Het hashalgoritme voor de Proof-of-Work (HashCash)

Wat dan nu is de *Proof-of-Work* waar elke miner naar op zoek is*?* Het vinden van een geldig *PoW* behelst het volgende: De gehele inhoud van het **Blockheader** veld wordt tweemaal[35] gehashed met het SHA-256 algoritme. De uitkomst van de berekening kan je uitdrukken in een getal. Als dit getal kleiner of gelijk is aan de *difficulty*, de moeilijkheid van de puzzel zoals die collectief bepaald wordt om ervoor te zorgen dat er slechts elke tien minuten ongeveer een oplossing wordt gevonden, dan 'wint' de *miner* de 'loterij' en zal deze een aantal Bitcoins toegekend krijgen als hij precies dat blok naar de rest van het netwerk verstuurt. Nogmaals, de data als invoer voor de hashfunctie verandert doorgaans. Immers komen er vaak tijdens het proces nieuwe transacties binnen[36] die aan de collectie in het *blok* moeten worden toegevoegd en moet het **time** veld afentoe geactualiseerd worden met de juiste tijd. Uiteindelijk zal er echter niets nieuws meer zijn om te hashen. Om ervoor te zorgen dat de *miner* toch constant meer combinaties kan blijven uitproberen is er het veld **nonce**. Dit veld omvat een betekenisloze teller die oploopt om de *miner* genoeg mogelijke inputdata te geven zodat er altijd verschillende hashes gegenereerd kunnen worden. Dit zegt de wiki:

> *"Any change to the block data (such as the nonce) will make the block hash completely different. Since it is believed infeasible to predict which combination of bits will result in the right hash, many different nonce values are tried, and the hash is recomputed for each value until a hash containing the required number of zero bits is found. As this iterative calculation requires time and resources, the presentation of the block with the correct nonce value constitutes proof of work."*[76]

Wanneer de *miner* een juiste **nonce** gevonden heeft voor het *blok* dat hij aan het construeren was verstuurt hij deze naar de rest van het netwerk. De andere nodes zullen vervolgens het

[35] Het tweemaal uitvoeren van de SHA256-hashfunctie is voorgesteld door Ferguson & Schneier in hun boek "*Practical Cryptography*" en in "*Cryptography Engineering*" als middel om een zogeheten "length-extension"-aanval uit te sluiten.

[36] De *miners* hebben er belang bij zoveel mogelijk transacties in hun *blok* te verwerken. De Bitcoinsoftware is immers zo ingesteld dat clients bij een keuze het nieuwe *blok* prefereren dat de meeste transacties omvat. Hierdoor heeft de *miner* een financiële motivatie, wegens het risico dat zijn *block* mogelijk niet wordt geaccepteerd bij een gelijktijdige creatie van een ander *blok* van een andere *miner,* met meer transacties.

ontvangen *blok* ook valideren. Ze zullen de **Blockheader** met de gegeven **nonce** ook twee keer met SHA-256 hashen om te verifiëren dat de *Proof-of-Work* klopt.

3.5 Vergelijking van Bitcoin en het hedendaagse geldsysteem

Nu de technische uitleg is behandeld zal tot slot van deze sectie een kort overzicht gegeven worden van de wezenlijke verschillen tussen het huidige geldsysteem en het Bitcoin-geldsysteem waarin de definitie van geld een grote rol speelt.

3.5.1 Het concept van het geld

Zoals we eerder hebben besproken is electronisch commerciëel bankgeld een verplichting van de bank aan de lener of rekeninghouder, een belofte. Omdat het geld een belofte voorstelt draagt deze een risico, namelijk, dat deze niet kan worden ingelost. Bitcoin daarentegen is geen belofte, noch een verplichting. Het is het geld zelf, het beloofde. Dat betekent dat Bitcoin risicovrij[37] geld betreft omdat er net als met cash geld geen inherent risico bestaat dat het zomaar kan ophouden te bestaan (wanneer de uitgever insolvabel is), net zoals Aristoteliaans geld dat gezeteld is in de wet. Dit verschil wordt mooi geïllustreerd door de kamervragen van Nijboer (PvdA) aangaande het toezicht op de munt, op 19 December 2013. Er werd gevraagd om een bevestiging dat *"virtuele geldeenheden die inwisselbaar zijn tegen echte valuta geen vordering op de uitgever vertegenwoordigen en niet onder de definitie van (elektronisch) geld vallen"*[77], teneinde te weten te komen of en hoe er belasting over Bitcoin geheven kon worden. Minister van Financiën Jeroen Dijsselbloem antwoordde bondig:

> *"De Bitcoin valt niet onder de definitie van (elektronisch) geld in de zin van de Wft onder meer omdat de Bitcoin geen vordering op de uitgever vertegenwoordigt."*

De Bitcoin valt dus niet onder de Nederlandse definitie van electronisch geld. Die is namelijk als volgt:

> "***elektronisch geld****: geldswaarde die elektronisch of magnetisch is opgeslagen die een vordering op de uitgever vertegenwoordigt, die is uitgegeven in ruil voor ontvangen geld om betalingstransacties te verrichten (...), en waarmee betalingen kunnen worden verricht aan een andere persoon dan de uitgever;*" (Wet Financieel Toezicht (WFT) Hfd. 1.1 Afd. 1.1.1 Art. 1:1)[78]

[37] Natuurlijk bestaan er nog wel risico's, maar die zijn ook present met contant geld. Het risico dat je het kwijtraakt in de locatiezin bijvoorbeeld.

Opvallend is dat het concept 'geld' waar naar wordt gerefereerd in bovenstaande definitie, in zijn geheel niet is gedefinieerd in de wet (deze, of in welke dan ook), wat ook ICT-jurist Arnoud Engelfriet opviel[79]. Elektronisch geld is dus per definitie een krediet, een vordering, maar wat wettelijk dan écht het concept van geld behelst, is onbekend. Zarlenga zei het volgende over de oprichting van de Bank of England (~1700), waarbij schuldvrij risicovrij staatsgeld voorgoed vervangen werd met vorderingen op de centrale bank:

> "*This has promoted a confusion between credit, and money, to this day. But they are different things. Credit depends on the creditor remaining solvent. Real money does not promise to pay something else. Credit can legally be improperly made into money, but it's not itself money. Money is on a higher order than Credit.*"[80]

Dit citaat sluit aan bij het verschil dat hier aan de orde is. Het verschil in geldsconcept van hedendaags geld en Bitcoin kan als volgt getypeerd worden: Bitcoin kan gezien worden als Aristoteliaanse/Platonische vorm van geld, dat géén vordering representeert op de uitgevers ervan (*miners*) en alleen bestaat doordat het is afgesproken dat het bestaat (al dan niet door een staat). M.A. Jansen bevestigt dit ook, in zijn werk '*Bitcoin: the political 'virtual' of an intangible material currency*' (2012):

> *"Thus, Bitcoin has a functional likeness to the identifier to money, cash, rather than that it has a functional likeness to contemporary money itself; the intangible abstract numbers administrated by banks that quantify the concept of debt. Therefore, Bitcoins main difference is that contrary to contemporary currencies such as the euro, Bitcoins are not created as debt relations between legal entities. Instead, Bitcoins are created 'debt-free', meaning that once Bitcoins have been created (verified) there is no requirement of Bitcoins to be paid back to the issuer as is the case with contemporary money."*

Het elektronische 'geld' waar wij voor meer dan 94%[81] van afhankelijk zijn in onze maatschappij betreft wél een vorm van een vordering, en bestaat níet door de wet, maar

doordat het gecreëerd wordt door private instellingen. Zarlenga, Aristoteles en Plato zouden stellen dat Bitcoin waarlijker[38] geld is dan het bankkrediet in ons systeem.

3.5.2 Boekhouding

De boekhouding in het hedendaagse geldsysteem is een gefragmentariseerde intransparante samenstelling bestaande uit de centrale bank (DNB+ECB) en alle private banken. Het is hierbij niet mogelijk om aan de statistieken van het geldsysteem te komen zonder te vertrouwen op de rapportage van instituten, met een *single point of failure*. In constrast zijn in Bitcoin alle transactiedata en statistieken over de geldgroei- en hoeveelheid openbaar en is er geen vertrouwen nodig in een enkele partij om aan betrouwbare informatie te komen.

3.5.3 Autoriteit

In het hedendaagse geldsysteem waar het 'geld op je rekening' slechts een tegoed betreft is het mogelijk voor banken en overheden in te grijpen in dit tegoed, door het te verlagen wanneer dat nodig wordt geacht. In Bitcoin is het niet mogelijk dat er wordt ingegrepen in de gelden onder jouw beheer, tenzij de private sleutels worden gedeeld of meer dan de helft van de kracht in het netwerk wordt aangewend om een deel van de *blokketen* te vervalsen. De aard van het verschil ligt in de organisatie van de systeemstructuur, waarbij deze in Bitcoin decentraal verdeeld is en in 'ons' systeem gecentraliseerd binnen een oligarchie van een aantal banken en een overheid. Dit verschil is ook te vergelijken met het contrast tussen het gedachtengoed van Thomas Hobbes en Jean-Jacques Rousseau[82].

3.5.4 Instapmogelijkheid

Er is in Bitcoin geen authorisatie nodig van een derde partij voordat gelden ontvangen kunnen worden. In ons systeem gaat er een goedkeuring vooraf aan het proces van rekeninggeneratie.

3.5.5 Settlements

In het hedendaagse geldsysteem worden uiteindelijke verrekeningen verlaat uitgevoerd. Banken verrekenen interne transacties zelf, strepen redundante interbancaire transacties tegen elkaar weg en doen de uiteindelijke verrekening vaak aan het eind van de dag in centralebankreserves. In Bitcoin vindt de verrekening zo snel plaats als dat de transactie voorkomt in een *block*.

[38] Aristoteles sprak ook over dat het handig is dat geld (dat bij wet bestaat) over het algemeen vaster in waarde was. Dit kan helaas nog niet gezegd worden over Bitcoin. Op dit punt zou je kunnen beargumenteren dat ook Bitcoin geen écht geld is.

3.5.6 Anonimiteit

Alleen jij en jouw bank weten van jouw transacties. De overheid kan transactiegegevens wel opvragen. De koppeling van je rekeningnummer aan je identiteit is quasi-privé[39]. Het is niet mogelijk voor het publiek om mee te kijken met je transactiegeschiedenis en het is ook niet mogelijk achter je balans te komen. Bitcoin is pseudoniem waarbij identiteiten niet inherent gekoppeld zijn aan adressen. Transacties en balansen zijn echter openbaar en geven veel informatie weg wanneer identitieiten gekoppeld worden aan adressen.

	Hedendaags digitaal bankkrediet	**Bitcoin**
Geldsconcept	Vordering op de uitgever	Aristoteliaanse token van waarde
Bestaansrecht	Private uitgever	Wet
Boekhouding	Gefragmenteerd verdeeld over centrale bank en alle private banken	Eenduidige boekhouding
Transparantie	Intransparant. Afhankelijkheid van toezichthouder	Openbare onpartijdige informatievoorziening
Autoriteit	Private uitgever / overheid bij wet	Adreshouder
Anonimiteit	Informatie ontoegankelijk voor derden behalve eigen bank en overheid (op verzoek).	Ongelinkte identiteit. Transactiegeschiedenis en balanstotaal openbaar
Verrekening	Instantaan indien intern, anders in meeste gevallen (twee)dagelijks	~elke 10 minuten

[39] Bij het doen van een overboeking corrigeren veel banken de ingevulde naam van de rekeninghouder met een suggestie.

3.6 Waarom een staatsmunt op basis van Bitcoin?

De financiële crisis heeft duidelijk gemaakt dat er een structurele instabiliteit zit in het geld- en bankensysteem zoals we dat kennen. De International Movement for Monetary Reform en haar leden verklaren dat de oorzaak ligt in de manier waarop geld door banken wordt gecreëerd. Zij pleiten voor de introductie van schulden- en rentevrij staatsgeld. Vanuit de financiële sector wordt als reactie geuit dat het riskant zou zijn om staten de controle (terug) te geven op een eigen munt wegens het 'imminente' gevaar op hyperinflatie. Innovaties als Bitcoin scheppen echter nieuwe mogelijkheden om verantwoordelijkheden af te bakenen en machten te scheiden. Uit het decentrale ontwerp van Bitcoin vloeit de mogelijkheid regulatie door middel van apolitieke wiskunde af te dwingen. Dit staat een geldsysteem toe dat beide partijen tegemoet komt in hun wensen.

Door middel van een decentraal betalingsprotocol kan er geheel zoals gewenst (IMMR) schuldvrij geld gecreëerd worden middels een transparant voorgedefinieerd proces waarbij de voordelen van geldschepping aan het algemeen belang ten goede komen. Aan de andere kant kunnen er door de decentraliteit en wiskunde aard limieten worden geregeld die voorkomen dat de Staat te ver zou gaan met haar terugverworven rechten. De bankensector die haar twijfels uit over de uitvoering van deze praktijk zal in effect de verantwoordelijkheid kunnen gaan dragen om deze limieten kracht bij te zetten, en te garanderen dat de regels naar behoren worden nageleefd.

4. Onderzoek

4.1 Bitcoinimplementatie van staatsgeld

Er zijn in Bitcoin een aantal concepten die veranderd zullen moeten worden om het protocol een monopolie op geldcreatie toe te staan, zoals de IMMR dat vereist. Ten eerste zal de *block reward* naar nul veranderd moeten worden, zodat *miners* geen coins meer kunnen creëren. Er moet een mechanisme komen voor de Staat om op een of andere manier het netwerk kenbaar te maken dat zij geld wenst te creëren. De code voor het accepteren van berichten of transacties zal waarschijnlijk gewijzigd moeten worden om dit type bericht te accomoderen en te accepteren. Ten slotte moet het netwerk gestart worden op basis van een nieuwe *genesis block*, het eerste *blok* in de keten. In dit *blok* zal de initiële geldhoeveelheid gedefinieerd[40] worden. De code is gebaseerd op de 0.8.6-tak.[83]

Parameters

De *block reward* wordt in tegenstelling tot andere startparameters gedefinieerd in de functie **GetBlockValue** in *main.cpp:1076*. Standaard staat deze op 50 omdat Bitcoin bij het begin van een *blokketen miners* nog 50 Bitcoins subsidie geeft.

```
    int64_t nSubsidy = 50 * COIN;

    // Subsidy is cut in half every 210,000 blocks which will occur
approximately every 4 years.
    nSubsidy >>= (nHeight / Params().SubsidyHalvingInterval());
```

Deze zal met nul vervangen moeten worden. Dan rest er nog de maximum *blokgrootte* (zie sectie 4.3.4). Deze vinden we in *main.h:28*.

```
/** The maximum allowed size for a serialized block, in bytes (network rule) */
static const unsigned int MAX_BLOCK_SIZE = 1000000;
```

Deze zal verhoogd moeten worden naar een waarde die het toestaat dat het netwerk geen limieten zal ondervinden. Één of twee gigabyte zou (voorlopig) genoeg moeten zijn, zoals Satoshi het zich had voorgesteld. Dan moeten we ter onderscheiding de poorten veranderen waar de client connectie mee zoekt, in *protocol.h:19* en *bitcoinrpc.cpp:46*

[40] Volgens de procedure van het Chicago Plan

```
static inline unsigned short GetDefaultPort(const bool testnet = fTestNet)
{
    return testnet ? 18333 : 8333;
}
```

Ook de limiet op de geldhoeveelheid moet worden opgehoogd: *(main.h:52)*

```
/** No amount larger than this (in satoshi) is valid */
static const int64 MAX_MONEY = 21000000 * COIN;
```

Dit is de absolute limiet van het geldsysteem en kan gerust op een waarde worden gezet tussen 1.5 en 2x van de initiële geldhoeveelheid. In het ergste geval zou de limiet bereikt worden en zou er gedraaid worden op een vaste inflatieloze geldhoeveelheid (als de limiet dan niet wordt opgehoogd). In een publiek geldsysteem is dan geen inherente groeidwang en zal een vergroting van de geldhoeveelheid optioneel worden, al is dit natuurlijk een politieke keuze.

De blockchain initialiseren

Tenslotte moeten we de software instrueren *niet* de *blokketen* van de officiële Bitcoin op te vragen. De hash van de *genesis block* is in de Bitcoin-code geëtst zodat de client er altijd zeker van kan zijn dat hij de goede keten ontvangt. Als de Bitcoinsoftware voor het eerst gestart wordt zonder dat er *blokken* in de database staan zal hij de *genesis block* zelf opnieuw genereren.
We moeten de generatie van dit *genesis block* aanpassen om ervoor te zorgen dat we een nieuwe keten creëren. We veranderen het veld *pszTimestamp*, waar Satoshi het bericht: *"The Times 26/Dec/2013 Chancellor on brink of second bailout for banks"* in had gezet als bewijs van publicatiedatum. Tevens veranderen we de eerste *block reward* van 50 naar 800 miljard, wat in 2012 ongeveer de toevoeging[81] (M3 ex. contant) van Nederland aan de monetaire aggregaten in Europa was. Deze initiële *block reward* moet claimbaar zijn door het adres dat de Staat zal gebruiken, en dit zal het 'oude' kredietgeld vervangen. We genereren dus eerst een Bitcoinadres om een public key te verkrijgen, en de public key voeren we in de parameters van de *genesis block*. Dan moet de code gecompileerd worden. De eerste keer dat het programma vervolgens wordt uitgevoerd zal deze stoppen met de volgende foutmelding:

> "*nlcoin-qt: src/main.cpp:2783: bool InitBlockIndex(): Assertion `block.hashMerkleRoot == uint256("0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b")' failed.*"

Dit geeft aan dat de hash van het door ons gegenereerde *genesis block* niet overeenstemt met de hash die in de code staat aangeven als de hash van het enige echte Bitcoin *genesis block*. We moeten ons eigen *block* eerst nog minen op de laagste *difficulty.* Na het minen[84] moet in de code de *nNonce* vervangen worden, de *nTime*, en moet de orginele hash vervangen worden met de onze en dan is het NLCoin *genesis block* geïnitieerd. *(main.cpp:34)*

```
uint256
hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f"
);
```

Na het vervangen van alle voorkomingen van het woord 'bitcoin' met 'nlcoin' en 'BTC' met 'NLC' kan de code nogmaals gecompileerd en gestart worden.

Een staatsgeldcreatietransactie creëren

Er zijn een aantal mogelijkheden om een staatsgeldcreatiebericht te ontwerpen. Het kan via een netwerkbericht dat verspreid wordt, via een *block*, of via een transactie. De staat zou een eigen blok kunnen vervaardigen met maar een enkele coinbase-transactie, maar dat zou het minen van partijen wel in de weg zitten omdat het de blokken zou invalideren waar op dat moment aan gewerkt wordt (Sompolinsky (2013)). Het is het makkelijkst om de geldgeneratie te laten gebeuren door een op zichzelf staande *Coinbase*-transactie over het netwerk te versturen die normaal gesproken alleen in *blokken* mag voorkomen. Er staat expliciet in de code vermeld dat het niet de bedoeling is *Coinbase*-transacties los te accepteren, zonder dat ze in een *block* zitten. Dat zal veranderd moeten worden om een uitzondering toe te staan. *Coinbase*-transacties moeten geaccepteerd worden als de handtekening van de Staat eronder staat. Het enige dat de Staat hoeft te doen is een transactie te maken zonder *inputs*, en die versturen met het gewenste bedrag naar haar rekening.

Een staatsgeldcreatietransactie accepteren

Miners dienen deze transactie ten eerste niet te weigeren in de verwerking van hun *blok*. Dit is het eerste probleem, aangezien dit geen standaardgedrag is. (*main.cpp:687*)

```
    // Coinbase is only valid in a block, not as a loose transaction
    if (tx.IsCoinBase())
        return state.DoS(100, error("CTxMemPool::accept() : coinbase as individual
tx"));
```

Hier moet een uitzondering gemaakt worden voor *coinbases* van de Staat. Even later zullen ook de *input*-checks omzeild moeten worden. (*main.cpp:733-743*) De check of er wel genoeg fooi betaald is zal ook genegeerd moeten worden:

```
        // Don't accept it if it can't get into a block
        int64 txMinFee = tx.GetMinFee(1000, true, GMF_RELAY);
       if (fLimitFree && nFees < txMinFee)
            return error("CTxMemPool::accept() : not enough fees %s,
      %"PRI64d" < %"PRI64d, hash.ToString().c_str(), nFees, txMinFee);
```

Als we het zouden toestaan dat de Staat net als gewone gebruikers een fooi zou moeten betalen, dan zet dat de mogelijkheid open tot non-compliance, omdat banken dan zouden kunnen stellen dat de hoogte van de fooi de kosten niet dekt, wat moeilijk is om te verifiëren. Het verwerken van staatsgeldcreatietransacties dient gratis[41] te gebeuren.

We zullen moeten kiezen tussen of we meerdere *coinbases* in een *blok* gaan toestaan, of dat we de *staatscoinbase* samenvoegen met de unieke *coinbase* per *block*. In het tweede geval moeten we op een of andere manier de handtekening van het Staatsadres erbij voegen om te voorkomen dat de hoeveelheid nieuw geld niet gewijzigd wordt. Als we voor optie 1 gaan zal de volgende code moeten worden veranderd. (*main.cpp:2113*)

[41] Uiteindelijk zullen veel gecreëerde gelden bij banken gedeponeerd worden die daar dan weer beschikking tot hebben, dus zo erg is het niet.

```
    // First transaction must be coinbase, the rest must not be
    if (vtx.empty() || !vtx[0].IsCoinBase())
        return state.DoS(100, error("CheckBlock() : first tx is not coinbase"));
for (unsigned int i = 1; i < vtx.size(); i++)
if (vtx[i].IsCoinBase())
            return state.DoS(100, error("CheckBlock() : more than one coinbase"));
```

De tweede keus is makkelijker. Dan bewaren we de handtekening van de transactie in het *coinbase*-veld dat arbitraire data-opslag ondersteunt.

Een staatsgeldcreatietransactie minen

Wanneer de staatstransactie in de transactiepool is toegelaten zal deze in het *miningsproces* verwerkt moeten worden. Er is doorgaans maar één *coinbase* transactie die in een *blok* terecht komt, en dat is die, die door de *miner* zelf gemaakt wordt om de *block reward* en fooien mee uit te keren (naar zichzelf). Nu moet er rekening gehouden worden met twéé *(main.cpp:4201).* Het is dan ook het makkelijkst voor de *miner* om de waarden uit de staatscoinbasetransactie over te nemen en in zijn eigen *coinbase* te stoppen. Waar een *miner* normaal de *block reward* definieert zal hij nu de hoogte van de geldcreatie definieren in een *output*. In een tweede *output* kunnen de transactiefooien van normale transacties verwerkt worden voor zichzelf. Het is hier belangrijk dat het ontvangstadres van de staatsgelden het adres van de Staat **moet** zijn. Dit zullen andere *miners* dan ook moeten valideren wanneer zij *blokken* ontvangen, om te voorkomen dat *miners* van deze synergie gebruik maken om zichzelf torenhoge *coinbases* uit te keren.

```
// Create coinbase tx
CTransaction txNew;
txNew.vin.resize(1);
txNew.vin[0].prevout.SetNull();
txNew.vout.resize(1);
CPubKey pubkey;
if (!reservekey.GetReservedKey(pubkey))
    return NULL;
txNew.vout[0].scriptPubKey << pubkey << OP_CHECKSIG;
```

In de laatste regel wordt de *output* naar de *miner* zelf gemaakt. Hier moet een *output* aan toegevoegd worden voor de Staat.

Al met al blijkt het in Bitcoin nog niet al te complex om naar onze wensen aan te passen. Het veranderen van het protocol is goed te doen om staatsgeldcreatie te accomoderen.

4.2 Protocollimiet op geldschepping & drempelvorming

In een systeem van staatsgeldcreatie moeten systematische limieten worden ingebouwd om te voorkomen dat de geldscheppende macht het recht misbruikt. Of het redelijk is om aan te nemen dat dit misbruik zou voorkomen of niet is hier niet belangrijk. Het belangrijke is dat er partijen zijn in de samenleving die het voorstel zouden aanvechten op grond van de mogelijkheid. We zoeken dus een technische limiet die garantie kan bieden om deze partijen gerust te stellen, en het liefst verantwoordelijk te maken voor de naleving van de afspraken. Door de verantwoordelijkheid van de naleving van de limieten te leggen bij de bankensector die het voorstel afwijst op grond van de initiële afwezigheid van deze limieten wordt er een constructie neergezet die te vergelijken valt met het concept van de Trias Politica, of 'de scheiding der machten', maar dan in geldschepping. Op welke manieren kan er in het protocol een limiet worden ingebouwd op geldschepping? Het moet hier gaan om een puur technische limiet die door het protocol (eventueel dynamisch) zelf bepaald moet kunnen worden, onafhankelijk van omgevingsvariabelen die menselijke input vereisen om in te voeren. Laten we eerst eens kijken naar de beschikbare[42] variabelen in een gedecentraliseerd cryptografisch geldsysteem:

Variabele	beschrijving
Geldhoeveelheid	hoeveelheid NLCoins in het systeem
Transactievolume	hoeveelheid transacties per *block*
Outputhoogte	gecombineerde hoogte van *outputs* per *block*
Omloopsnelheid*	snelheid waarmee coins van adres wisselen
Tijd	tijd, gemeten in *blocks*
Geldcreatie	hoeveelheid coins die gegenereerd zijn door de Staat (in een bepaalde periode)
Staatsinkomsten	hoeveelheid coins die zijn ontvangen op het staatsadres (in een gegeven periode)
Staatsuitgaven	hoeveelheid coins die zijn uitgegeven vanaf het staatsadres
Adressen*	hoeveelheid adressen / het verloop (activatie / deactivatie)
Zakelijke adressen*	Hoeveelheid zakelijke adressen, balansen, in/uitstromen
Difficulty	Moeilijkheid van de HashCash-puzzel

* zie sectie 4.4

[42] Deze data zijn af te leiden uit de *blockchain*, die openbaar beschikbaar is

Deze metrieken spreken redelijk voor zich na de technische uitleg zoals eerder gegeven, op één na: de omloopsnelheid. Het is makelijk te zien hoe snel Bitcoins van private sleutel wisselen, maar dat zegt op zichzelf niets. In Bitcoin zijn de meeste adressen namelijk pseudoniem en weet je niet hoeveel transacties er ook daadwerkelijk gedaan worden tussen adressen die niet dezelfde eigenaar hebben. Om inzicht te kunnen verkrijgen over de daadwerkelijke omloopsnelheid zal je eerst moeten weten of elk adres toebehoort aan een unieke persoonsidentiteit. In sectie 4.4 wordt de adresgeneratie gekoppeld aan identificatie van personen (of instellingen), dus afhankelijk van hoeveel rekeningen het men dan wordt toegestaan te bezitten kan er een aanname gedaan worden over hoeveel adressen in het NLCoin-systeem dan toebehoren aan unieke identiteiten. Als er een protocol wordt gebruikt voor het toekennen van rekeningnummers voegt het de mogelijkheid toe zakelijke rekeningen van particulieren te onderscheiden. Op dat moment is er waarschijnlijk iets nuttigs te zeggen over de omloopsnelheid.

De Staat creëert geld door een *Coinbase*-transactie zonder *Proof-of-work* naar haar eigen adres *aan* het netwerk kenbaar te maken (zie 4.1). De miners moeten nakijken of dit de gespecificeerde limiet niet zou overschrijden. De *miners* zijn hier effectief het bankwezen, dus op die manier kunnen zij in zekere zin zelf garanderen dat de Staat zich aan de afspraken houdt. Om de 'transactie' te verifiëren zullen ze een vooraf vastgestelde periode terug moeten kijken in de *blockchain*. Dat kan een maand zijn, een jaar of een electorale periode van 4 jaar, afhankelijk van de gedefinieerde termijn waarover de geldcreatielimiet waakt.

Er zijn per limiet een aantal systeemvariabelen die vastgesteld moeten worden bij de implementatie: *limietsperiode* (LP), *maximum* (M). Run-time variabelen zijn *tijd* (T), *nieuw geld* (NG) en de som van *reeds gecreëerde gelden* (∑) in een bepaalde periode van T. De *limietsperiode* en de *tijd* worden gerekend in blokaantallen, waarbij T de blokteller is. Een geldcreatietransactie is geldig zolang (∑([T, T-1, T-2 … T-LP]) + NG) <= M.

Statische limiet (a)

De meest eenvoudige limiet die te implementeren is om een hyperinflatie te voorkomen is om een statische limiet in te bouwen in een bepaalde tijdsperiode. Zo zou je een limiet kunnen stellen van een x miljard NLCoin per maand, waarbij de initiële bepaling een bepaald

percentage van de geldhoeveelheid op dat moment is. Een concrete waarde is hier niet relevant gezien dat een politieke keuze is.

Stel dat we de Staat toestaan elke maand 100 NLCoins te creëren. Er worden gemiddeld 4380 *blokken* per maand gecreëerd. De *limietsperiode* LP = 4380, *maximum* M = 100. Geld mag gecreëerd worden zolang (S(T-4380) + NG) <= 100. In de volgende tabel is bij wijze van illustratie te zien na wat voor verloop van *blokken* de formule niet langer zou toestaan dat er elk *blok* geld bijgecreëerd wordt.

T	∑([T, T-1, T-2 … T-LP])	NG	Toegestaan
1	0	0	1
2	0	10	1
3	10	10	1
4	20	10	1
...			
12	100	0	0
13	100	13*	0
14	100	40*	0

* geweigerde gecreëerde gelden = 0

Limiet als percentage[43] van de geldhoeveelheid (b)

Een limiet waarbij de limiet wordt bepaald door de geldhoeveelheid. Ter illustratie voor een waarde kan er gekeken worden naar de '*Hanke-Krus Hyperinflation Table*' (Hanke & Krus (2012)).[85] Als er een limiet wordt ingesteld die onder het minimum zit zoals te zien in de kolom '*highest monthly inflation rate*' (50%) dan voorkom je al een hyperinflatie[44]. In de praktijk zal het wenselijk zijn een veel lager getal te kiezen. Wijlen Milton Friedman zou affiniteit hebben gehad met deze vorm van een limiet. In een interview gaf hij aan de functie van de Federal Reserve te willen vervangen door een computer:

> "*I've always been puzzled by why they insist on using the interest rate rather than the quantity of money. If you really carried out the logic concerning the quantity of money,*

[43] Dit resulteert uiteindelijk in een exponentiële curve. Ik heb de functie opgenomen omdat het een mogelijkheid is maar zou deze vorm van limiet niet aanraden uit duurzaamheidsoverwegingen.

[44] De definitie van hyperinflatie is arbitrair. In het gerefereerde onderzoek is er gekozen voor een ration van 50% inflatie per maand.

you deprive the Federal Reserve of anything to do. Suppose the Federal Reserve said it was going to increase the quantity of money by 4 percent a year, year after year, week after week, month after month. That would be a purely mechanical project. You could program a computer to do that."

Stel dat we de Staat toestaan elke maand 4% NLCoins te creëren van de geldhoeveelheid. Er worden gemiddeld 4380 *blokken* per maand gecreëerd. De *limietsperiode* LP = 4380, *maximum* M = ∑(T-LP) * 0.04. Geld mag gecreëerd worden zolang (S(T-4380) + NG) <= ∑(T-4380) * 0.04.

Limiet afhankelijk van de omloopsnelheid van geld (c)

In deze limiet is de maximumhoogte van geldcreatie in een periode afhankelijk van hoe snel geld wordt uitgegeven. Het is dan de vraag welke relatie deze twee variabelen tot elkaar dienen te hebben. Moet er meer geld gecreëerd kunnen worden als geld snel wordt uitgegeven? (dit is vaak het geval bij hoge inflatie, in welke tijd het juist niet handig is de geldhoeveelheid te vergroten) Of juist niet?

Implementatie

De implementatie voor deze checks moet gemaakt worden in de functie **AcceptToMemoryPool(...)** die te vinden is in *main.cpp:678*. In deze functie voert een Bitcoin-node (niet per sé een *miner*) een aantal checks uit op transacties die ontvangen worden. Bij het overschrijden van de gedefinieerde limieten kunnen geldcreatietransacties van de Staat simpelweg genegeerd worden. Wegens de open aard van het protocol zal het tevens mogelijk zijn voor derden om te zien of de nodes in het protocol zich ook daadwerkelijk aan de regels houden en niet bijvoorbeeld teveel geldcreatietransacties van de Staat negeren, zonder dat de limiet echt bereikt wordt.

4.3 Schaalvergroting van Bitcoin naar Nederlandse proporties

Om te weten of de Bitcoin-technologie schaalbaar is naar een niveau zoals dat vereist is in Nederland zullen we moeten weten wat de situatie is in Nederland, en zullen we moeten weten wat het is dat Bitcoin op het moment tegenhoudt te groeien naar die grootte.

4.3.1 Transactievolume

Hoeveel transacties worden er jaarlijks gedaan binnen Nederland? Om dit in te schatten maken we gebruik van het meest recentelijke rapport over het betaalverkeer van DNB, '*Rapportage Maatschappelijk Overleg Betalingsverkeer 2012*'[86]. We willen hier de meest atomaire transactie weten die te vergelijken valt met een overschrijving in Bitcoin. In Bitcoin staat bij een overschrijving het 'geld' direct op de rekening van de ontvanger nadat de transactie gevalideerd is. In het hedendaagse bankwezen is dit te vergelijken met het overschrijven[45] van bankgeld van de ene binnenlandse girale betaalrekening naar de andere. Dit staat ook wel bekend als een '*settlement*'.

Er zijn nog veel meer statistieken[87] bekend, zoals over de hoeveel er met bepaalde betaal*methoden* betaald wordt als iDEAL en AcceptGiro, maar uiteindelijk zijn dat slechts middelen voor het doen van een transactie van één rekening naar een ander. In de volgende tabel zie je de jaarlijkse statistiek zoals gerapporteerd door DNB. We zijn hier geïnteresseerd in het volume voor alle niet-cash banktransacties. De eerste rij **'Giraal'** is eenduidig en behelst het volume van directe overboekingen. De tweede, '**Online betaalmethoden**', zorgt al voor problemen. Het is namelijk zo dat het geld bij een iDEAL-transactie dat bestemd is voor de verkoper éérst terecht komt op de bankrekening van de zogenaamde '*Payment Service Provider*' (PSP). De PSP maakt het bedrag vervolgens in batch met alle andere transacties over naar de betreffende verkopers. Het is niet duidelijk waar de tweede transactie hier dan in wordt ingedeeld, maar vermoedelijk in de eerste rij. Eenzelfde probleem is er met creditcardbetalingen. Wat gebeurt er precies bij een betaling met creditcard? Indien het proces

[45] Hier dient een kritische noot gemaakt te worden: het is afhankelijk van hoe je naar dit proces kijkt om te kunnen zeggen dat het hier echt om een *settlement* gaat of niet. Ofschoon het voor ons aanvoelt dat het 'geld' dat op onze rekening stond is 'overgemaakt' naar een andere rekening, in werkelijkheid wordt slechts de verplichting van de bank aan de eerste rekeninghouder verlaagd, en bij de tweede rekeninghouder verhoogd. Echter gaat het nog steeds om een verplichting van de bank. Er is dan wel een *settlement* gedaan in verplichtingen, maar die verplichtingen zelf zijn nog niet ge-*settled.* Om de *settlement* in de schuld van de bank aan de rekeninghouder te doen plaatsvinden dient die cash uitbetaald te worden.

zo werkt dat de bank of de creditcardmaatschappij je aankoop voorschiet, waarna jij je krediet aan het eind van de maand afbetaalt, dan is het aantal bankoverschrijvingen te benaderen door het maandelijke transactievolume te nemen per persoon en er voor iedere maand (minstens) één bij op te tellen.

Voor het gemak zal ik het transactievolume in Nederland zien als de optelsom van de secties **'Giraal'**, **'Online betaalmethoden'** en **'Toonbank** -> pinnen', omdat die representatief zijn voor banktransacties. Ik neem hier aan dat banktransacties als resultaat van betalingen met creditcard, zoals de maandelijkse afbetaling van de rente en de overboeking van de creditcardmaatschappij naar de koper bij een betaling, zijn opgenomen in de eerste sectie.

Tabel B1

Miljoenen	2003	2004	2005 [1]	2006	2007	2008	2009	2010	2011	2012
Giraal (betalen op afstand) *1*	**2.272**	**2.316**	**2.374**	**2.557**	**2.644**	**2.751**	**2.830**	**2.950**	**2.976**	**3.075**
overschrijvingen (excl. iDEAL)	1.271	1.264	1.315	1.413	1.452	1.498	1.512	1.571	1.541	1.589
wv acceptgiro	*231*	*217*	*231*	*209*	*209*	*205*	*195*	*194*	*188*	*182*
incasso-opdrachten	1.001	1.051	1.059	1.139	1.177	1.226	1.272	1.310	1.340	1.369
Online betaalmethoden			0	4	**14,9**	**27,9**	**45,4**	**68,8**	**93,9**	**117,2**
iDEAL transacties			0	4	14,9	27,9	45,4	68,8	93,9	117,2
Toonbank (niet-contant)	**1.296**	**1.407**	**1.510**	**1.647**	**1.797**	**1.969**	**2.158**	**2.368**	**2.496**	**2.660**
pinnen	1.157	1.247	1.334	1.451	1.588	1.756	1.946	2.154	2.285	2.474
chippen	109	127	147	165	175	176	177	178	172	148
creditcard *2*	30	33	30	32	34	37	35	35	39	38
cheques	0	0	0	0	0	0	0	0	0	0
Totaal niet-contant betalen	**3.568**	**3.723**	**3.884**	**4.204**	**4.442**	**4.721**	**4.988**	**5.317**	**5.471**	**5.735**
Chartaal										
opname geldautomaat *3*	494	484	471	475	469	473	455	434	437	447
opname balie *1*			*16*	14	13	12	10	7	6	5

Bron: DNB, banken, Currence, creditcardmaatschappijen en toonbankinstellingen

Het transactievolume van het jaar 2012 in Nederland komt dan uit op $5.666.200.000$ transacties. Dat is $5666,2$ miljoen, of $5,6662$ miljard.

Bitcoin heeft door een technische keuze (zoals eerder genoemd), de maximumgrootte van een *block*, een harde transactielimiet per seconde, genoteerd in TPS (‘*Transactions Per Second’*). Dit zegt de wiki:

> *“Today the Bitcoin network is restricted to a sustained rate of 7 tps by some artificial limits. These were put in place to stop people from ballooning the size of the block chain before the network and community was ready for it.”*[88]

Het hedendaagse geldsysteem heeft daar minder last van, dus zullen we de twee vergelijken in TPS. Bitcoin kan op het moment Om het Nederlandse transactievolume te vergelijken met het huidige maximumtransactievolume per seconde van Bitcoin delen we deze door het aantal seconden in een jaar. $5.666.200.000 \ / \ 31.556.926 = \pm 180 TPS.$ In Nederland vinden dus (over het jaar) *gemiddeld* 180 transacties per seconde plaats. Vergelijk dit met het betaalsysteem van bijvoorbeeld PayPal (58TPS, 2011)[89] dat internationaal opereert.

Natuurlijk is $180TPS$ slechts het gemiddelde voor Nederland over een heel jaar. In sommige perioden zal dit hoger liggen en in sommigen lager. Zo wordt de periode voor kerst vaak aangemeten als de drukste periode van het jaar. We moeten dus eigenlijk ook het maximum weten. Stel[46] dat we een maximum hebben van $400TPS$, wat is er dan voor nodig om Bitcoin dat te kunnen laten halen?

4.3.2 Limiterende factoren voor TPS

De TPS-limiet in Bitcoin wordt door twee zaken gedefinieerd: de *block creation time* van ~10 minuten en de maximum blokgrootte. Er zouden meer transacties verwerkt kunnen worden als er of sneller *blokken* gecreëerd zouden worden, of als er meer transacties per blok opgenomen zouden kunnen worden. De *block creation rate* kan best omhooggeschroefd worden, zoals veel wordt gedaan in alt-coins[47] zoals Litecoin & Fastcoin, maar deze experimentele munten tonen dan ook aan dat de gevestigde *rate* er niet voor niets is. Wanneer er veel vaker dan eens in de tien minuten een *blok* gemaakt wordt gaat het risico omhoog dat er op een zeker moment

[46] Ik doe hier een aanname op basis van de tabel. In werkelijkheid zou het maximum nog veel hoger kunnen liggen

[47] alternatieve cryptovaluta gebaseerd op de code van Bitcoin, vaak met slechts minimale verschillen in parameters

tegelijkertijd concurrerende *blokken* gemaakt worden. Hierdoor vergroot de onzekerheid in het netwerk omdat het dan niet meer duidelijk is welk van de twee *blokken* de hoofdketting van de *blockchain* vertegenwoordigt. Dit verhoogt het risico op een *double spend-attack*. De 10-minuten creatierichtlijn is er dus vanwege de veiligheid van het protocol en wordt uiteindelijk bestendigt door de propagatiesnelheid van het netwerk[90]. Immers is de kans klein dat er *blokken* zouden concurreren als het netwerk altijd in één (hypothetisch) seconde op de hoogte zou zijn van de nieuwe ontwikkelingen. De blokcreatietijd moest net genoeg ruimte geven om *blokken* van een bepaalde grootte naar het merendeel van het netwerk te verspreiden[7].

4.3.3 Blokcreatetijd

Zoals gezegd is de gestelde blokcreatetijd van 10 minuten een functie van de propagatiesnelheid van het netwerk. De tijdspanne van 10 minuten moet voldoende ruimte geven voor nieuwe *blokken* om te propageren zodat de kans op een race van concurrerende blokken uitblijft. Deze tijdslimiet is een limiterende factor voor de TPS, en een lagere waarde (van de blokcreatietijd) zou leiden tot een hogere TPS, maar komt ten koste van de veiligheid. Veel alt-coins experimenteren met snelle blokcreatiesnelheden en de bijkomende problematiek van *orphaned blocks* en een verlaagde veiligheid. Er is volgens Sompolinksy & Zohar echter een aanpassing te doen aan het protocol waardoor de TPS verhoogt zonder dat hiervoor de veiligheid van het netwerk in het geding komt. Ze stellen voor de *blokketen* te veranderen naar een *blokboom*. Als meerdere *miners* concurrerende *blokken* uitbrengen vanwege een lage blokcreatetijd zullen deze allebei meetellen ter validatie van het *blok* waarop ze gebouwd zijn. Op deze manier tellen *blokken* die niet in de hoofdketen terecht komen alsnog mee voor de veiligheid (*block rewards voor secundaire blokken blijven* uit).

> "*Since high transaction rates imply many conflicting blocks are created, it would be quite useful if these blocks were not really lost. In fact, each block can be seen as supporting not just transactions inside it, but also those embedded in previous blocks. Even if a block is not in the main chain, we can still count the confirmations it gives previous blocks as valid. This is the basis of our proposed modification, which we call the "Greedy Heaviest-Observed Sub-Tree" chain selection rule.*"

Dit betekent helaas wel dat er meer *blokken* gegenereerd zullen worden die niet in de hoofdketen terecht zullen komen, en dat daarmee de transacties erin niet als valide gemarkeerd

worden. Dit gaat echter niet ten koste van de veiligheid, en als de veiligheid gewaarborgd kan worden kan de blokcreatetijd versneld worden om zodoende alsnog een hogere TPS te behalen.

> *"In high transaction rates, GHOST builds slightly less blocks in its main-chain (because it doesn't always extend the longest chain), thus slightly lowering the number of transactions accepted per second, but it does so more securely! Delays and many off-chain blocks no longer make it more susceptible to 50% attacks. This implies that we can increase the block creation rates and block size to levels that were previously too risky and easily make up for the loss in transaction volumes. In fact, we estimate that 1 second blocks can be easily combined with rates of over 200 TPS."*

4.3.4 Blokgrootte

Blokken die geproduceerd worden door *miners* mogen momenteel niet groter worden dan 1MB, anders zullen ze door de rest van het netwerk geweigerd worden. Op 15 Juli 2010[91] is deze limiet in werking gesteld, verlaagd vanuit de 32MB zoals die daarvóór[92] bedroeg. Dit is gedaan om te voorkomen dat enkele *miners* extreem grote blokken zouden produceren die congestie zouden veroorzaken in het netwerk, wegens tekort schietende netwerk- of processorkracht in de prille begintijd. Oleg Andreev, een Bitcoin software-architect die een Bitcoin-implementatie in Objective-C heeft geschreven, verklaart dit:

> "*The limit was set in place initially to make sure that the network is not spammed with huge blocks with useless transactions when people were just starting playing with Bitcoin and mining blocks was possible on personal computers. Huge blocks could lead to excessive use of bandwidth which could lead to higher percentage of orphaned blocks*[48] *due to higher synchronization delays. There was no empirical proof for this limit, it was mostly an intuitive safety mechanism, "good enough" in the short run. Satoshi, the initial developer, suggested that the limit is temporary and should be raised or removed once the network becomes more powerful and could sustain larger amount of transactions.*"[93]

[48] een *orphaned block* is een *blok* dat met een juiste *Proof-of-Work* door een *miner* is vervaardigd, maar niet door het netwerk is geaccepteerd. Dit komt voor wanneer er bijna gelijktijdig door een concurrerende *miner* een ander *blok* wordt gevonden dat sneller of eerder door het netwerk propageert en eerder geaccepteerd wordt.

De limiet zoals die bedoeld was van 32MB zou per *block* bij een gemiddelde transactiegrootte van 500bytes[94] een transactievolume van ~$107TPS$ aankunnen. Voor een transactievolume zoals dat van Nederland zou de blokgrootte echter minimaal (om aan de veilige kant te zitten) het vierdubbele moeten bedragen. Voor $400TPS$ bij een gemiddelde transactiegrootte van 0.5KB moet de maximum blokgrootte dus liggen op ($0.5KB * 400TPS * 60s * 10m =$) 120.000KB (120MB), of op oneindig (nonexistent).

De maximumblokgrootte kan verhoogd worden om meer transacties toe te staan. Het probleem is echter dat volgens sommige partijen met belangen in Bitcoin het verhogen van de blokgroottelimiet zou resulteren in de vernietiging van het netwerk, door een situatie uit de speltheorie die bekend staat als '*Tragedy of the Commons*'[95] (TOTC) of '*Tragedie van de Meent*'.[96] De theorie beschrijft een situatie waarin actoren die in hun ogenschijnlijk rationeel eigenbelang handelen toch op den duur tegen het belang van de gemeenschap inwerken. De beredenering is als volgt: wanneer de ruimte in een *blok* niet langer schaars is zullen gebruikers geen motivatie hebben om een fooi aan hun transactie toe te voegen. Hierdoor zou *minen* op den duur (aangezien de *block reward* elke vier jaar halveert) onhoudbaar worden gezien de winstgevendheid zonder (of met lage) fooien naar nul dreigt te gaan, wat vervolgens zou resulteren in een verlaging van de *hash rate* omdat *miners* stoppen met transactievalidatie. Anders bekeken, wanneer elke transactie in een *blok* zou passen, en *miners* ook waardeloze transacties zouden verwerken, dan zouden volgens de kosten van verwerking enorm omhoog gaan. Immers zou de *blockchain* enorm in grootte groeien en zijn *miners* dan een grotere investering kwijt om de systeemeisen bij te benen van processor- en geheugenkracht. Dit zou leiden tot een principieel ongewenste centralisatie waarbij alleen de kapitaalkrachtige *miners* nog solvabel kunnen opereren, gelijkend aan centrale instituten zoals de commerciële banken die ze nu proberen te bevechten; kortom een ideologisch falen. Andreev:

> *"Some people fear that if block size will become unlimited, miners will include a lot of spammy transactions, eat everybody's bandwidth, fees will get lower (thus undermining sustainability of the blockchain in the future) and some miners with poorer connection will be forced out of the market which is supposedly unfair to them."*

Dit vernomen probleem is bij Bitcoin op het moment (2013/2014) nog niet eens een dergelijk groot probleem, er is immers de *block reward*, de geldcreatie uit het niets als betaling voor *miners*, die wordt toegekend. Echter, in een systeem zoals dat hier wordt voorgesteld, zal geen *block reward* aanwezig zijn aangezien alle geldcreatie dient te gebeuren op verantwoordelijkheid en toekomen van de Staat. Een Bitcoin-staatsgeldsysteem dient te kunnen overleven op slechts fooien[49]. Dat betekent dat dit vernomen probleem, het debat over de maximumblokgrootte, meteen bij aanvang een relevant onderwerp zou zijn.

Dat dit een van de meest politiek verhitte debatten binnen de Bitcoingemeenschap is wordt geïllustreerd door de hoeveelheid[97] [98] aan discussie[99] erover[100]. De tegenstanders van bovengenoemde redeneringen beweren namelijk precies het tegenovergestelde, dat het houden van de blokgroottelimiet resulteert in een financiële corpocratie:

> "*(...) [it] will simply cause a monopoly on blocksize space that can be controlled by entities with enough money to drive out transactions that have more modest transaction fees, thus prioritising who can use the Bitcoin network and primarily favouring the richer users that can afford to pay for the artificially high fees*.[101]
>
> (...) *Once the blocks becomes really scarce and serious competition to get transactions into a block happen, the transaction negotiation dynamic will change. It will change from a negotiation to an auction. This is really bad since it moves power to miners in an unnatural fashion, it means that miners are literally forced to favour the highest transaction fees. We no longer have a free market on transaction fees and this will eventually result in only those that can afford to pay the exorbitant fees to use the Bitcoin network. It will mean there will be a two tiered system, ultrasafe transfers of value for the privileged and monied institutions and everyone else is driven to less secure intermediaries that will be the next western union. Even worse, this will stunt Bitcoin growth (or even destroy Bitcoin) because one of the biggest selling points of the Bitcoin protocol will be nullified making it scarcely better than banks. Intermediaries will be the new banking system that can force you to reveal your identity, charge exorbitant*

[49] Al is er ook wat voor te zeggen dat als je al een staatsgeldsysteem hebt, deze ook ondersteund kan worden vanuit de organisatie die er staat voor het algemeen belang.

fees for the pleasure of moving your money, freeze your funds, and tell you who you can/can't send money to.[102]"

Het debat is zelfs zó verhit geworden[103] dat er een "propaganda"[50] video gemaakt is om het publiek te overtuigen dat de artificiële tijdelijke blokgroottelimiet behouden moet worden, zoals de video "*Why the blocksize limit keeps Bitcoin free and decentralised*" afkomstig van de site http://keepbitcoinfree.org/.

Dit kamp, zij die pleiten voor een artificiële begrenzing van transacties om de motivatie voor fooien niet teniet te doen, lijkt echter een ding over het hoofd te zien. Ze heeft het idee dat er zonder blokgroottelimiet geen enkele economisch limiterende factor is die fooien zo legitimeren. Er wordt hier vergeten dat er een natuurlijke grens is: de netwerksnelheid en de kosten van het zowel opslaan van de *blokketen* als het verifiëren van transacties. Zonder limiet op de blokgrootte is het in principe voor elke transactie mogelijk een plek te vinden in een *blok* om geverifiëerd te worden. Hierdoor zullen (bij veel transacties met lage fooien) de groottes van *blokken* enorm opzwellen, wat de verwerkingskosten zal doen oplopen. Een groter *blok* betekent tevens dat het langer duurt voordat deze in de begrensde tijd van ~10 minuten door het netwerk gepropageerd zal zijn. Hierdoor neemt het risico toe dat het *blok* wordt ingehaald door een concurrerend *blok* van een kleinere grootte, gecreëerd door een andere *miner,* dat zich sneller door het netwerk kan verplaatsen[104]. Het is dus in het economisch belang van de *miner* zelf niet te grote trage *blokken* te produceren. Andreev is opvallend genoeg een van de weinigen[105] die dit lijkt in te zien:

"Is there any natural limit on the block size? Sure there is: it is network bandwidth and the costs of storage and transaction verification. The more transactions you need to verify and transmit, the higher your operating costs and (most importantly) the higher the risk of orphaning a block. If the block is too big to be distributed and verified by other peers, the risk of somebody else creating a shorter block in parallel gets higher. If the shorter block gets validated by majority faster than the longer one, the latter will become

[50] "*unfortunately rather than accept that the majority are in support of Gavin et al. have instead been rather petulant and have tried to undermine via propaganda to sway the general public that anything but the current implementation is "bad"*"
http://www.reddit.com/r/Bitcoin/comments/1owbpn/is_there_a_consensus_on_the_blocksize_limit_issue/ccwe3s7

orphaned. Orphaned blocks mean immediate loss of time and money for miner, and since transactions are rescheduled and delayed, frequently orphaned blocks undermine market value of miner's savings."

Echter, Decker & Wattenhofer tonen in hun werk '*Information Propagation to the Bitcoin Network*' (2013) aan dat de genoemde economische risico's van *orphaned blocks* verminderd kunnen worden door de interconnectiviteit tussen nodes in het netwerk te verhogen, en/of de berichtgeving over het bestaan van een nieuw *blok* te laten plaatsvinden direct vóór of na de validatie van de *Proof-of-Work* van het nieuwe *blok*, in plaats van ná de bijkomende validatie van alle transacties. Dit heeft wel intenser netwerkgebruik ten gevolg (tot 100MB/s) en zou onpraktisch kunnen zijn voor veel kleine *miners*.

4.3.5 Opslaglimitaties & Efficiëntere blokketenverwerking

In de geuite zorgen over oplopende kosten voor verwerking en opslag van de *blockchain* wordt nauwelijks rekening gehouden met nieuwe technieken binnen Bitcoin die ervoor kunnen zorgen dat deze, ook zonder blokgroottelimiet, beperkt blijven. Zo wordt er op het moment (2013/2014) veel tijd gestoken in de mogelijkheid de *blokketen* te kunnen *'prunen';* het weggooien van oude *blokken* transactiedata om opslagruimte te besparen. Veel nodes in het netwerk zouden een groot deel van de *blokketen* dan niet meer bewaren, slechts een lijst van ongespendeerde *outputs*. Deze nodes zouden zogenaamde 'SPV'-nodes, of '*Simple Payment Verification'*-nodes zijn en kunnen transacties alleen op validiteit controleren door na te gaan hoe diep die zich in de *blokketen* bevinden. Ze kunnen dan niet meer weten of een *output* nog gespendeerd kan worden of niet. Het probleem hieraan is dat de SPV-nodes ontvankelijker zouden zijn voor *double-spend attacks* (gezien ze geen historie meer bijhouden om alles zelf mee te kunnen verifiëren) en dat er centralisatie in het netwerk zou plaatsvinden, namelijk van de enkele nodes die het zich kunnen permitteren de *blokchain* met de complete historie van het netwerk te bewaren[7].

De basis van deze functionaliteit lijkt sinds Oktober 2012 (stilletjes) onderdeel te zijn van de Bitcoin-code[106], aldus Peter Wuille, ontwikkelaar in het kernteam:

> *"I've just merged my "ultraprune" branch into mainline (...). (…) The idea behind ultraprune is to use an ultra-pruned copy (only unspent transaction outputs in a custom compact format) of the block chain for validation (as opposed to a transaction index into the block chain). It still keeps all blocks around for serving them to other nodes, for rescanning, and for reorganisations. As such, it is still a full node. So, despite the name, it does not implement any actual pruning yet, though pruning would be trivial to implement now. (...)"[107]*

De implementatie van het *pruning*smechanisme is er dus al. Volgens Pieter Wuille wordt de implementatie vooral nog tegengehouden doordat het nog niet makkelijk is om de netwerkfunctionaliteit eraan te accomoderen. Er moet bijvoorbeeld op macroniveau voorkomen worden dat nodes massaal hun oude data zullen gaan weggooien. Er moet een decentrale consensus zijn over waar bepaalde stukken van de geschiedenis van de *blockchain* te vinden gaan zijn: "*The biggest roadblock is making sure new and old nodes that start up are able to find nodes to synchronize from (...)*"

De ontwikkeling van het *prunen* van de *blockchain* lijkt erg op een ander idee dat wacht op implementatie: de '*finite blockchain*'. In dit voorstel[108] worden de drie functies[51] van de *blokketen* van elkaar gescheiden zodat er een *blokketen* van een eindige lengte overblijft, een collectie van accountbalansen, en een tweede keten waarin alle *Proof-of-Work*s worden opgeslagen, die niet getrimd dient te worden:

> *"Each time a new block is solved the oldest block is trimmed from the end of the mini-blockchain so that it always has the same number of blocks. It is argued that the loss of security this trimming process incurs can be solved with a small "proof chain" and the loss of coin ownership data is solved with a database which holds the balance of all non-empty addresses, dubbed the "account tree". The proof chain secures the mini-*

[51] het coördineren van de transactieverwerking, het bewaren van de *Proof-of-Work* ter beveiliging van het netwerk, en het bijhouden van accountbalansen om na te kunnen gaan wat de tegoeden van adressen zijn

blockchain and the mini-blockchain secures the account tree." (Bruce (2013))

Ten slotte kan er worden bekeken hoe houdbaar het is alsnog de hele *blockchain* op te slaan en te verwerken als deze niet efficient gemaakt wordt. Dit is ook waar Satoshi rekening mee hield. Op basis van de Wet van Moore die stelt dat de hoeveelheid transistors of logische schakelingen op een chip elke 2 jaar zal verdubbelen ging hij ervan uit dat de stand van de techniek in processorkracht, netwerksnelheid en opslaggrootte de systeemeisen van de *blockchain* zullen opvangen tegen de tijd dat deze een omvang zal aannemen die we op dit moment onhoudbaar zouden vinden. Dit werd gesteld in de mailinglist met de originele aankondiging:

> "*The bandwidth might not be as prohibitive as you think. A typical transaction would be about 400 bytes (...). Each transaction has to be broadcast twice, so lets say 1KB per transaction. Visa processed 37 billion transactions in FY2008, or an average of 100 million transactions per day. That many transactions would take 100GB of bandwidth, or the size of 12 DVD or 2 HD quality movies, or about $18 worth of bandwidth at current prices. If the network were to get that big, it would take several years, and by then, sending 2 HD movies over the Internet would probably not seem like a big deal.*"[109]

4.3.6 Capaciteiten IT-infrastructuur bankwezen in Nederland

Uit de interviews met architecten bij banken bleek dat het bijna niet haalbaar zou zijn om een immer uitdijende *blockchain* bij te houden. Gigabytes moeten namelijk minstens vier keer gerepliceerd worden, en de data moet ongeveer tien jaar bewaard blijven voor de autoriteiten. De dataretentie-eisen zijn nochtans een mooie limiet die je op de *blockchain* zou kunnen toepassen. Als de technieken van *pruning* verder vorderen moet het mogelijk worden een soort eindige *blockchain* te hebben rouleren die een stabiele grootte zal benaderen waar op gerekend kan worden.

4.4 Inbedding in banksysteem & wetgeving

Eerder is besproken dat een aanpassing van het geldsysteem zoals hier wordt voorgesteld de meeste kans van slagen heeft als deze zo min mogelijk verandering vereist. Dit houdt in dat een nationaal geldsysteem gebaseerd op Bitcoin gemodelleerd moet worden naar de processen van het huidige systeem. Het belangrijkste proces hiervoor is de manier waarop een rekening geopend wordt waarmee transacties gedaan kunnen worden, en de regelgeving die daarbij komt kijken.

4.4.1 Een rekening openen

Bij het openen van een rekening in Nederland is men veelal verplicht de identificatie mee te sturen. Er is een kopie van een identiteitskaart of paspoort nodig. Dit is om twee redenen. Het burgerservicenummer dient ten eerste doorgegeven te worden aan de belasting opdat de belastingdienst inzicht heeft in de balans op je rekening, ter voorkoming van belastingfraude[110] De bank dient ten tweede onder de '*Wet Identificatie Dienstverlening*' (WID)[111] de klant te identificeren zodat ze kunnen voldoen aan de '*Wet ter voorkoming van witwassen en financieren van terrorisme*' (WWFT): "*In de WID is geregeld dat een bank de identiteit van alle cliënten moet vaststellen en de verkregen gegevens moet vastleggen.*" (Rijksoverheid.nl[112]). De WWFT verplicht banken melding te maken van transacties die verdacht zijn op basis van een aantal vastgestelde objectieve en subjectieve indicatoren[113]. Deze melding komt dan binnen bij de '*Financial Intelligence Unit-Nederland*' (FIU-Nederland), een onderdeel van de nationale politie.

Het moge duidelijk zijn dat het voor de Staat nodig (volgens de huidige wetgeving) is de rekeninghouder te kunnen identificeren. Hoe zou de Staat dit moeten doen in een valuta gebaseerd op Bitcoin? In Bitcoin is het immers slechts nodig dat er een cryptografisch sleutelpaar gegenereerd wordt waar vervolgens Arestoteliaans geld mee ontvangen en verstuurd kan worden. Er is geen enkele afhankelijkheid van autoriteit die in het proces van rekeninggeneratie kan inhaken om de WID als verplichting in te voeren. Helaas zal deze afhankelijkheid dus moeten worden ingebouwd om te voldoen aan de wetgeving. Het zou natuurlijk gemakkelijker zijn om de wetgeving aan te passen zodat dit vraagstuk geen probleem meer is, maar dat is buiten de scope van dit onderzoek. Het zou ook mogelijk zijn de wetgeving juist ín te bouwen in het protocol.[114]

4.4.2 Verantwoordelijkheid voor rekeninggeneratie[52] & distributie

Het lijkt dat de gebruiker 'Democraatus' daar al rekening mee had gehouden in zijn of haar 'Dutchcoin'-voorstel (zie Inleiding): "(...) *Bij lancering geeft de Staat iedereen via zijn Digi-ID een vast bedrag aan Dutchcoins (bijvoorbeeld DTC 10.000). Eventueel wordt in de software ingebakken dat de Staat per jaar 1% nieuwe Dutchcoins krijgt voor het jaarlijkse overheidsbudget. Ook is denkbaar dat over dit jaarlijkse percentage wordt gestemd ieder jaar, ook weer via de Digi-ID*". Wat is het 'Digi-ID' waar hier naar gerefereerd wordt? De Rijksoverheid geeft antwoord:

> "*DigiD staat voor Digitale Identiteit en is een persoonlijke combinatie van een gebruikersnaam en een wachtwoord. U gebruikt DigiD om u te legitimeren op internet. Zo weten organisaties dat ze ook echt met u te maken hebben.*"[115]

Er wordt in de citatie van Democraatus geïmpliceerd dat er via een DigiD-autorisatie aan een Dutchcoin-adres (in ons geval NLCoin) gekomen kan worden. Dit zou goed te doen zijn. De overheid genereert de adressen voor de cryptovaluta en distribueert die op voorwaarde dat deze gekoppeld worden aan persoonsgegevens door middel van DigiD. Aangezien ieder adres in een cryptovaluta in feite een bankrekening voorstelt maakt dat het onnodig nog naar een bank te hoeven voor het openen van een rekening. (a)

Aan de andere kant kunnen we de verantwoordelijkheid voor de identificatie (volgens de WID) ook bij de bankensector laten. Dan hebben we de keus tussen adresgeneratie door de overheid, waarbij banken de rekening'nummers' slechts distribueren (b), of adresgeneratie door de bankensector, waarbij banken de adressen genereren en naar de overheid slechts de terugkoppeling doen met de persoonsidentificatie. (c)

[52] In het volgende deel zullen de begrippen 'rekening', 'adres', 'rekeningnummer' en 'bitcoinadres' door elkaar heen gebruikt worden. Ik doel met deze begrippen op het concept van een bankrekening, wat in Bitcoin een enkel Bitcoinadres is, en in de bankensector een rekeningnummer.

We identificeren hier een matrix van keuze binnen het vraagstuk van het enerzijds *genereren* van rekeningadressen, en het anderzijds *distribueren* ervan:

- rekeninggeneratie door de overheid, distributie door de overheid (a)
- rekeninggeneratie door de overheid, distributie door de bankensector (b)
- rekeninggeneratie door de bankensector, distributie door de bankensector (c)
- rekeninggeneratie door de bankensector, distributie door de overheid (d)

Beide partijen zouden voor beide functies aangewezen kunnen worden, al is optie (d) erg onlogisch. De enige eis is dat de overheid (FIU-Nederland) melding krijgt van verdachte transacties wanneer die plaatsvinden, en dat het bij een dergelijke melding duidelijk is welke identiteit gekoppeld is aan de betrokken rekening(en). Wat hierbij een erg belangrijk gegeven is, is dat in de huidige situatie *de overheid niet sowieso de gegevens over identiteiten en transacties bezit.* De situatie die Democraatus schetst, waarbij de overheid via een DigiD-koppeling de rekeningnummers van iedere inwoner kent, sluit dus niet aan bij de huidige situatie. Dit wordt bewezen door een passage uit de WWFT (artikel 2): "*Bij een melding als bedoeld in het eerste lid verstrekt de instelling de volgende gegevens: a. de identiteit van de cliënt en, voor zover mogelijk, de identiteit van degene ten behoeve van wie de transactie wordt uitgevoerd; (...)*"[116]. De identiteit hoeft dus pas worden prijsgegeven door een financiële instelling wanneer een transactie verdacht is, en dit impliceert (maar bewijst niet) dat de koppeling van rekeningnummer en persoonsgegevens bij de FIU-Nederland vóór de melding nog niet bekend is. Het is onduidelijk of er bij een melding volgens de WWFT überhaupt melding wordt gemaakt van het rekeningnummer.

Het lijkt mij evident dat het onwenselijk is om de verantwoording van rekeninggeneratie te implementeren volgens schema (a), waarbij de overheidsinstantie defacto de koppeling kent tussen rekeningnummer en persoonsidentiteit, wat enkelen zouden associëren met een vorm van totalitarisme. Dit maakt schema (b) overbodig en gezien de irrelevantie van mogelijkheid (d) blijft schema (c) over. De implementatie van schema (c) strookt mooi met het voorgenomen principe van pragmatisme om procesmatig zo min mogelijk te veranderen

De bankensector zal dus, net zoals nu het geval is, de verantwoording moeten krijgen over het genereren van rekeningnummers terwijl ze voldoen over de eisen van de WID.

4.4.3 Bitcoin & geautoriseerde adresgeneratie

In de technische uitleg is al naar voren gekomen dat Bitcoinadressen in principe zonder tussenkomst gegenereerd kunnen worden; een Bitcoinadres is immers slechts een combinatie van een assymmetrisch sleutelpaar. Dit vormt een probleem voor de zojuist gestelde eis dat de bankensector de verantwoording zal moeten dragen voor het genereren van adressen om aan de '*Wet Identificatie Dienstverlening'* te kunnen voldoen. Er zal een manier moeten worden gevonden om het open principe van adresgeneratie in Bitcoin zó aan te passen dat adressen alleen bruikbaar zijn wanneer deze gegenereerd of goedgekeurd zijn door een financieel instituut zoals een bank. Dit zal een spanning opleveren met het vereiste principe van legitimiteit zoals dat eerder gedefinieerd is: *de onmogelijkheid voor een derde partij om je saldo te kunnen beïnvloeden of ontoegankelijk te maken*. Als de bankensector de verantwoordelijkheid heeft adressen vrij te geven is het denkbaar dat ze dat dan ook ongedaan kan maken, al is dat natuurlijk afhankelijk van hoe dit schema geïmplementeerd wordt. (zie 4.4.4) Verder zal het gedrag van de adresgeneratoren ook nog consistent moeten blijven om geen conflicten te creëren tussen banken onderling; het moet niet mogelijk zijn bij verschillende banken hetzelfde adres te verkrijgen. Tot op heden zorgt het bedrijf Equens daarvoor, een pan-Europees bedrijf dat alle pin- chipknip- en acceptgirobetalingen afhandelt.

4.4.4 Rol voor banken: adresgenerator of stempeldrukker?

In de situatie zoals hierboven is een ontwerpbeslissing nog niet opgenomen. Er zijn namelijk twee mogelijkheden om een adres te authoriseren. Een bank kan een adres genereren en goedkeuren zoals hierboven gesteld (I). Dit stelt de bank echter in staat de bijkomende private sleutel te bewaren. De private sleutel maakt het weer mogelijk voor de bank een aantal acties uit te voeren in naam van de gebruiker, wat niet strookt met het legitimiteitsprincipe. Zeker in combinatie met het monopolie op adresgeneratie in de sector is dat een grote machtspositie. Een tweede mogelijkheid is dat banken slechts dienen als stempelorganisaties die goedkeuringen verspreiden en adressen een “stamp of approval” geven (II). Gebruikers genereren dan zelf een adres en laten deze slechts goedkeuren door de sector zonder ooit de private sleutel over te dragen.

Een bedrijf in de Verenigde Staten, CoinValidation, doet al iets dat hiermee te vergelijken is:

> *"When a user interacts with a participating business, we would like to verify that an address belongs to an individual analogous to the way that compliance companies currently verify that a bank account belongs to a specific individual. We are working with regulators to standardize policy."*[117]

4.4.5 Ultieme overstapservice

Er is een keuze. Het is mogelijk wettelijk te verplichten dat banken van alle adressen de private sleutels ook beheren (zoals nu), maar dit systeem schept juist de spannende mogelijkheden van het alternatief: de keuze zelf. In een gedistribueerd betalingssysteem waarbij slechts de initiële rekeninggoedkeuring door een aangestelde autoriteit dient te gebeuren heeft de rekeninghouder de keuze waar diens *wallet* beheerd moet worden. De gebruiker kan ervoor kiezen zijn *wallet* zelf in beheer te nemen, of in beheer te geven bij een bank (zonder de private sleutel prijs te geven). Wanneer de dienst niet bevalt verplaatst hij zijn *wallet*, vaak een enkel bestand, naar een andere bank.

Voordat we naar een implementatie zullen kijken waarbij we Bitcoin aanpassen om adresgeneratie toch onder te brengen onder een autoriteit moeten we eerst een ander aspect onder de loep nemen dat erg belangrijk zal blijken in dit licht, anonimiteit namelijk.

4.4.6 Anonimiteit

We hebben gezien dat er bij transacties in Bitcoin geen koppelingen worden gemaakt met identiteiten. Dit suggereert voor velen dat Bitcoin anoniem is. Dat is echter niet waar. Bitcoin is 'pseudoniem'. Alle transacties en adressen zijn openbaar, wat betekent dat zodra er ergens een koppeling gemaakt wordt met een identiteit, zoals tijdens het doen van een aankoop bijvoorbeeld, de complete financiële historie van dat adres te achterhalen is. Dit zegt de Bitcoin website (2013) erover onder het kopje '*Bitcoin is not anonymous*':

> *"Some effort is required to protect your privacy with Bitcoin. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address. However, the identity of the user behind an address remains unknown until information is revealed during a purchase or*

in other circumstances. This is one reason why Bitcoin addresses should only be used once. Always remember that it is your responsibility to adopt good practices in order to protect your privacy."[118]

Een probleem dat in het systeem op deze manier kan voorkomen wordt geïllustreerd door een hypothetische situatie zoals gesteld door een gebruiker van het officiële discussieforum[119]. Het is in Bitcoin de bedoeling voor elke betaling die je ontvangt een nieuw Bitcoinadres aan te maken zodat men niet kan achterhalen wat je collectieve balans is door slechts te kijken naar de balans van het gegeven adres waarop ze je moeten betalen. Echter kan een persoon die een betaling ontvangt wél zien wat de balans was van de *output* waaruit hij betaalt kreeg. Als je je salaris gestort krijgt op een enkel nieuw gegenereerd Bitcoinadres weet iedereen hoeveel salaris je krijgt of hoeveel spaargeld je hebt wanneer je vanuit dat adres een betaling doet.

Enkele onderzoekers van het Johns Hopkins Information Security instituut erkennen de tekortkoming in ware anonimiteit:

"(...) Bitcoin transactions are conducted in public. The Bitcoin protocol and clients address this in two ways: (1) all Bitcoin transactions are conducted using public keys as identifiers, and these public keys are not linked to individual names. And (2) Bitcoin clients are capable of generating many public keys ("identities") to help users resist tracking. Unfortunately, a growing body of research indicates that these protections are insufficient. This information may allow data miners to link individual transactions, identify related payments, and otherwise trace the activities of Bitcoin users."[120]

In het gebruik van Bitcoin wordt het dus (voor de 'anonimiteit') aangeraden om voor iedere transactie een nieuw adres te genereren. Dit zal dan echter op gespannen voet staan met de eis dat adressen alleen gegenereerd mogen kunnen worden door de bankensector. Het kan namelijk een onhandig proces vereisen om iedere keer je identiteit te moeten bewijzen (WID) wanneer je een nieuw adres zou willen genereren. Dat heeft ook invloed op het legitimiteitsprincipe zoals eerder besproken, een bank kan dan namelijk makkelijk weigeren een nieuw adres te genereren, wat ten koste gaat van de privacy. Het is dus in ons belang zo min mogelijk adressen te hoeven genereren (en daarmee de identificatielast te minimaliseren) terwijl we wel de anonimiteit voor de buitenwereld willen maximaliseren.

Matthew Green, een van de onderzoekers aan het John Hopkins instituut, heeft '*Zerocoin*' ontwikkeld. Zerocoin is een extensie voor het Bitcoinprotocol dat ervoor zorgt dat transacties anoniem blijven, zo wordt beschreven in het paper '*Zerocoin: Anonymous Distributed E-Cash from Bitcoin* ':

> "*Zerocoin, a distributed e-cash system that uses cryptographic techniques to break the link between individual Bitcoin transactions without adding trusted parties* "

De toevoeging van Zerocoin aan het betaalsysteem zorgt er effectief voor dat er geen link meer zal zijn te vinden tussen transacties (in identiteit). Dit biedt werkelijke anonimiteit in het protocol en ontdoet de nood om voor iedere transactie een nieuw adres te genereren (aldus Green[121]), zoals dat in het pseudonieme Bitcoin het geval is. Door Zerocoin te gebruiken in NLCoin is het mogelijk de verantwoordelijkheid op adresgeneratie op een efficiente manier toe te kennen aan financiële instituten, gezien de identificatienood (WID) miniem of slechts eenmalig zal blijken. In de praktijk zullen er dan minimaal per persoon twéé adressen gegenereerd dienen te worden. Een publiek ontvangstadres en een spaaradres. Gezien de aard van het protocol zal het nog steeds mogelijk zijn de balans van een adres op te vragen. Als je geld zou willen ontvangen zal je je publieke sleutel van het adres moeten vrijgeven. De betaler zal met de publieke sleutel (het adres) kunnen zien wat de balans van het adres is. Voor ware anonimiteit zullen alle ontvangen gelden dus doorgestuurd moeten worden naar het spaaradres. De toevoeging van Zerocoin zorgt ervoor dat het tweede adres dan privé blijft.

Door de implementatie van Zerocoin kunnen we op een efficiente manier voldoen aan de WID. Het protocol zal echter de eis aan de WFFT weer vermoeilijken. Zonder de toevoeging van Zerocoin kan een bank makkelijk aan de FIU-Nederland rapporteren wat de bestemming is van een bitcointransactie, namelijk, het ontvangende adres zoals genoteerd in de *blockchain (*de identiteitsgegevens daarachter kunnen dan weer worden opgevraagd bij de desbetreffende bank*).* Met de toevoeging van Zerocoin is dat niet inherent meer mogelijk. Gelukkig (?) schijnt de auteur hier rekening mee te hebben gehouden:

> "*But Zerocoin can be used however we, as a democracy, decide it should be used. Once the technology exists, we as citizens can have a discussion about what degree of privacy is appropriate. For example, we might decide that transactions should be hidden*

from your neighbors — as they already are in traditional payment systems — but that the government should have access upon obtaining a valid warrant. If we make this decision, Zerocoin can easily be configured to accommodate that access. But such decisions should be made by the people through their legislatures and courts. They should not be made by government agencies acting on their own."[122]

Naast Zerocoin is er recentelijk (6 Januari 2014) een nieuw voorstel verschenen[123] voor het implementeren van privacy bij transacties dat tot veel enthousiasme heeft gezorgd: *'Stealth addresses'.*

"(...) an anonymity-enhancing address generation scheme (...) Dubbed "Stealth Addresses", the system allows an individual/merchant to provide a single address to their debtors/customers that can be used to make recurring payments without sacrificing anonymity. The payee/merchant can reuse that address forever (...) Payments to the stealth address are not recorded in the blockchain because it is only used as an input to an algorithm that generates a fresh address (and private key) for every incoming transaction"[124]

Deze techniek zou het mogelijk maken anoniem betalingen ontvangen middels slechts een enkel publiek adres. Dit zou maar een kleine aanpassing vereisen aan het Bitcoinprotocol, en men zou nog steeds betalingen ontvangen op unieke adressen, zoals dat nu de bedoeling is. Dit maakt Zerocoin nog niet overbodig: 'stealth addresses' lossen de link op tussen de identiteit van de betaler en het daadwerkelijk gebruikte Bitcoinadres. Het pad is er echter nog steeds: als het ergens wél bekend wordt welke identiteit verbonden is aan een bepaald adres, dan kan je een aantal stappen terug krijken. Met Zerocoin wordt de betekenis van dit pad onbruikbaar gemaakt en kan er geen informatie over identiteit worden verkregen door te kijken naar de verloopsgeschiedenis van een Bitcoin. Als deze techniek gecombineerd wordt met Zerocoin los je het probleem op dat er minimaal twee adressen benodigd zouden zijn. Immers kan je dan je *stealth address* gebruiken voor het ontvangen van gelden op je spaarrekening zonder dat de betaler je saldo te weten kan komen.

4.4.7 Systeemeisen

De uiteindelijke eisen van het systeem zoals dat zo zal worden beschreven zijn als volgt:

1. Het moet niet meer mogelijk zijn adressen te kunnen gebruiken zonder toestemming van de daarvoor aangewezen instellingen. Hierdoor wordt er een artificiële afhankelijkheid gecreëerd die het mogelijk maakt NLCoin-adressen te koppelen aan identiteiten, in voldoening met de WID.
2. Deze instellingen moeten adressen kunnen activeren, maar ook kunnen deactiveren. Bij deactivatie mag het legitimiteitsprincipe niet worden overtreden; het mag niet mogelijk zijn rekeninggebruik zomaar te bemoeilijken of onmogelijk te maken.
3. Er dienen geen afhankelijkheden te bestaan buiten het protocol en de blockchain.
4. De autorisatiestructuur dient modulair te zijn opgebouwd. Toewijzingen in autorisatie dienen te bestaan door protocoloperaties, en niet doordat ze hard zijn gecodeerd in de broncode.

4.4.8 Techniek

We zullen nu bekijken wat er aan het Bitcoinprotocol gedaan zou moeten worden om het bankwezen autoriteit te geven over het genereren van adressen. De (complexe) implementatie van Zerocoin wordt achterwege gelaten, daar dat voor het concept niet uitmaakt.

Laten we eerst een voorstelling maken van hoe het proces zou moeten werken vanuit de actoren. Wanneer iemand een rekening wil openen gaat hij of zij naar een bank. De bank is door de overheid of door DNB aangemerkt als instituut dat adresgeneratie is toegestaan, en dient te voldoen aan de WID. Een inschrijving voor een rekening wordt gedaan en de bank voert haar identificatieplicht uit volgens de WID. De persoonsgegevens worden opgeslagen, zoals tegenwoordig gebeurt. De bank stuurt een bericht naar het op Bitcoin gebaseerde NLCoin-netwerk en laat het netwerk weten dat vanaf dat moment een gegeven[53] adres, door de bank of

[53] In sectie 4.2 waar er gezocht wordt naar een technische limiet op geldcreatie wordt er gesproken over de variabele 'omloopsnelheid' die niet waardevol is. Deze metriek kan waardevoller gemaakt worden door adressen volgens een bepaald protocol te genereren. Bijvoorbeeld, adressen die een even getal representeren zijn voor particulieren, waar adressen van een oneven getal zakelijke rekeningen vertegenwoordigen. Voor de buitenwereld blijft het geheim welke bedrijven het beheer hebben over welke zakelijke rekening. Het protocol kan hiermee wel betekenisvollere uitspraken doen over de omloopsnelheid of de staat van de economie. Er kan berekend worden welk percentage van de geldhoeveelheid in handen is van het bedrijfsleven, en welk in particuliere handen. Er kan bekeken worden of en hoe snel particulieren hun geld uitgeven en of bedrijfsomzetten over een tijd verbeteren of verslechteren.

door de klant gekozen, bruikbaar dient te zijn. Het adres moet eerder nog niet in gebruik genomen geweest zijn[54]. Wanneer de bank het netwerk een bericht heeft gestuurd dat het adres geactiveerd dient te worden kan de gebruiker[55] de rekening gebruiken. Eventueel zou de rekening bij sterfte, verlies van staatsburgerschap of andere uitzonderlijke voorvallen gesloten kunnen worden. Doordat het Zerocoin-protocol is geïmplementeerd is het niet nodig meer dan twee adressen te verkrijgen.

Het gebruik van adressen in het Bitcoinprotocol is op het moment niet schaars. Ze zijn gemakkelijk te genereren en te gebruiken. Om de toegang tot adressen schaars te maken zullen de miners een check moeten gaan doen op transacties. Ze zullen moeten nakijken of adressen die voorkomen in transacties volgens het protocol geactiveerd zijn door een bank (met een *adresauthorisatie*). Transacties van of naar adressen die niet geactiveerd zijn zullen worden geweigerd. In de beginstaat zullen er nog geen geactiveerde adressen zijn. De informatie over de activatiestatus van adressen zal in de blockchain transparant moeten worden opgeslagen zodat miners volgens protocolprocedures aan deze informatie kunnen komen. Om een bepaald adres te activeren zal een bank een speciaal bericht het netwerk in moeten sturen. Dit bericht bevat de informatie over welk(e) adres(sen) geactiveerd moet(en) worden. Het bericht zal moeten worden opgenomen in een block, en daarna in de blokketen. Wanneer het blok met het bericht is opgenomen in de blokketen kunnen de miners gebruik maken van de informatie van de activatie bij het valideren van transacties.

Hoe weten de miners (in de praktijk zullen dit bankclusters zijn) dat de afzender van een *adresauthorisatie* wel echt de autoriteit heeft om adressen te activeren? Een naïeve manier zou zijn om de publieke sleutels in de protocolbroncode te zetten, van de banken en instellingen die ten tijde van de invoering van het systeem de verantwoordelijkheid moeten dragen. De instellingen zouden dan op voorhand de private sleutels van de hun toebedeelde adressen moeten krijgen. Zij zouden hun *adresauthorisatieberichten* moeten ondertekenen met hun private sleutel om te bewijzen dat ze de eigenaar zijn van de publieke sleutel in de broncode,

[54] Gezien adressen worden geregistreerd in de *blockchain* is dit gemakkelijk te verifiëren

[55] Ik zeg hier specifiek geen 'klant' omdat het proces van rekeninggeneratie praktisch niet kostendragend zou moeten zijn. De dienst die hier wordt afgenomen bestaat alleen om een overheidsbelang te behartigen en is nauwelijks een product van de sector te noemen. Pas als de gebruiker zou besluiten het adres ook door de bank te laten beheren zou het een klant zijn van die dienst.

die daar zou staan omdat het vooraf bepaald was dat ze de verantwoordelijkheid toebedeeld hadden gekregen. Wanneer een bank dan een *adresauthorisatie* het netwerk in stuurt zal een miner kijken of de ondertekening ervan gedecodeerd kan worden met een van de publieke sleutels uit de broncode. Dit stelt ons echter voor een probleem. Als er in deze situatie een bank failliet gaat, een nieuwe bank ontstaat, of een bank de licentie voor adresgeneratie verliest, dan is er geen mogelijkheid die bank dynamisch het privilege van adresgeneratie d.m.v. *adresauthorisaties* toe te kennen of af te nemen. Elke verandering in de verantwoording voor adresgeneraties zou een protocolupdate vereisen. Dit is iets wat zo goed mogelijk vermeden dient te worden. Naast dat het waarschijnlijk een lastig proces zou zijn om de protocolsoftware een update te geven (stel je voor dat alle banken en enkele pensioenfondsen hun software allemaal moeten aanpassen), zou dat de mogelijkheid geven voor de Staat om bij een dergelijke update óók de ingebouwde limieten op de geldcreatie te veranderen. De updates aan de software moeten zó beperkt worden dat, wanneer het dan gebeurt om eventueel de limiet op geldcreatie te veranderen, dit fenomeen groot zal worden uitgemeten in de media, dat de maatschappelijke verantwoording en transparantie ten goede zou komen. De toekenning van adresgeneratierechten dient dus dynamisch te gebeuren.

Om de privileges van *adresgeneratierechten* dynamisch te kunnen toekennen hebben we een nieuwe autoriteit nodig die daar boven staat. Deze autoriteit moet door middel van berichten in het netwerk bepaalde adressen rechten van adresgeneratie kunnen geven of afnemen, zodat deze adressen niet in de broncode vermeld hoeven worden. De autoriteit hiervoor zou de Staat kunnen zijn, of DNB. Welk instituut uiteindelijk die controle in handen krijgt is voor het concept hier niet belangrijk. De publieke sleutel, of sleutels, die zullen toebehoren aan de autoriteit op *adresgeneratierechten* zal wél in de broncode kunnen worden opgenomen.

Hoe moet de autorisatiestructuur van dit netwerk in gang worden gezet? Er wordt om te beginnen een sleutelpaar gegenereerd. Deze wordt met de publieke sleutel in de broncode gedefinieerd als *autoriteit op adresgeneratierechten*. De private sleutel wordt in beheer gegeven van de Staat, DNB, of een regulerend instituut. Dit instituut bepaalt vervolgens welke financiële instellingen de mogelijkheid moeten krijgen om adressen te activeren (ze zullen moeten voldoen aan de WID). Het instituut zal een of meer *adresgeneratierechttoekenningsberichten* het netwerk in moeten sturen. Deze berichten zijn simpele *adresauthorisaties*, met als enige verschil dat deze adressen het recht zullen krijgen zelf ook *adresauthorisaties* te ondertekenen.

De private sleutels van de geactiveerde adressen dienen terecht te komen bij de verantwoordelijke banken en financiële instellingen. Die kunnen dan op hun beurt met *adresauthorisaties* rekeningen aanmaken voor klanten, voldoenend aan de WID.

Adresgeneratierechttoekenningsbericht:

Address	12qsmag851PVGQsmqPayCgNABS3mbc2tgL
scriptSig	304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4

Adresauthorisatiebericht:

Address[]	12qsmag851PVGQsmqPayCgNABS3mbc2tgL (...)
PrevAuthHash	ca361787e999bb4fa62005d7332ab0f53c268ca3bca250587f1bbebdbee6326e
scriptSig	304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4

De handtekeningen van beide type berichten kunnen (eventueel) gedaan worden met de '*multi-signature'*-techniek om de organisatiestructuur van het instituut tegemoet te komen. Op die manier kan een 'single point of failure' worden voorkomen; de onfortuinlijke mogelijkheid dat een ambtenaar de enkele private sleutel zou kwijtraken of verspelen bijvoorbeeld.

We hebben gezien dat instituten geautoriseerd kunnen worden om adressen te activeren, en dat deze adressen actief zullen zijn op het moment dat ze in de *blokketen* zijn opgenomen. Er is nog een ontwerpkeuze over, en dat is de reversibiliteit van deze processen: het sluiten van rekeningen (adressen) en het voorkomen of terugdraaien van transacties.

4.4.9 Incasso en machtigen in NLCoin

Een van de meest voorkomende (legitieme) ongedaanmakingen van transacties zit in het betaalproduct 'Incasso', dat nu vervangen wordt door een Europese variant.[125] Met Incasso kan een bedrijf, met goedkeuring van de klant, met een bepaalde frequentie een beperkt variërend bedrag (denk aan maandelijke vaste lasten) claimen van de rekening van de klant. Het speciale hieraan is dat de klant 8 weken krijgt (56 dagen) om een periodieke incasso vrij gemakkelijk ongedaan te maken. Het bedrijf dat de gelden ontvangt kan die meteen gebruiken ondanks dat deze nog 8 weken teruggeclaimd kunnen worden door de bank van de klant. Om ervoor te zorgen dat bedrijven deze altijd weer kunnen terugbetalen zijn er strenge regels verbonden aan het versturen van verzoeken tot incasso.

De incassofunctie kan (naïef) worden nagebouwd door de financiële instituten die verantwoordelijk zijn voor adresgeneratie te verplichten[56] de goedgekeurde *private sleutels* van een adres te bewaren, zodat zij kunnen ingrijpen in de rekeningen en per definitie zonder tussenkomst van de eigenaar een bedrag kunnen storneren. Dit is de meest simpele en meest vrijheidsoverdragende mogelijkheid, die het meest gelijkend is aan de hedendaagse situatie.

Een andere mogelijkheid is om de functionaliteit in het protocol in te bouwen met een techniek die bekend staat als '*distributed contracts''*[126], een vorm van *'smart contracts'*[127]. Een beschrijving van de Bitcoin-wiki:

> "*A distributed contract is a method of using Bitcoin to form agreements with people via the block chain. Contracts don't make anything possible that was previously impossible, but rather, they allow you to solve common problems in a way that minimizes trust. Minimal trust often makes things more convenient by allowing human judgements to be taken out of the loop, thus allowing complete automation.*"

Nick Szabo vertelt in zijn paper *'Formalizing and Securing Relationships on Public Networks'* (1997)*'*[128] mooi hoe de maatschappij een ontwikkeling heeft doorgemaakt in het formaliseren en contractualiseren van menselijke relaties, en de media die daar met de tijd bij zijn komen kijken om het formaliseren te bewerkstelligen, eindigend met het (digitale) papier van tegenwoordig.

> "*Business is now dominated by paper and institutions of written literacy. Security measures have included chops, seals, and written signatures. Value has been transfered via bills of exchange (which evolved into checks), bearer certificates, and accounts using the double-entry bookeeping system. Most importantly, we take for granted that contracts and law are written on this static medium, to be interpreted and enforced by human authorities."*

Hij beargumenteerde zeven jaar geleden dat de volgende stap in de evolutie van geformaliseerde contractering een electronische is, vastgelegd in '*smart contract protocols'.* Er zijn volgens hem een aantal zaken waar slimme contracten aan moeten voldoen om opgesteld te kunnen worden in (electronische) protocollen:

---

[56] In het geval dat de incassofunctie onderdeel zou moeten zijn van het algehele geldsysteem

> "*Economists stress two properties important to good contract design:* ***observability by principals*** *and* ***verifiability by third parties*** *such as auditors and adjudicators. From the traditions behind contract law and the objectives of data security, we derive a third objective, privity.*"

Zoals eerder is aangehaald is Bitcoin niet alleen een valuta, maar (vooral) een systeem voor decentrale besluitvorming. Ik haal nog eens het citaat aan van Stefan Molyneux om dat te illustreren: "*Bitcoin is a publicly ordered ledger of what has occurred for you. Financially, in terms of property, (...) ownership, (...)* ***contracts****… and all these things can be* ***publicly audited****, and* ***verified****. (...) It eliminates labour in conflict resolution. (...)* ". De mogelijkheid om decentraal en vertrouwenloos slimme contracten te kunnen formuleren en bestendigen is dus de revolutionariteit van het Bitcoin-protocol. Laten we eens kijken of we de incassofunctie kunnen implementeren als *smart contract* op het Bitcoinprotocol.

Het incasserende bedrijf stuurt via het protocol een verzoek naar de klant voor een periodiek claimrecht op diens adres. Hierbij zullen alle limieten en voorwaarden gedefinieerd moeten worden, zoals de toegestade frequentie van claims, de toegestane variatie van het te claimen bedrag, de vervaldatum van het contract, de eventueel toegestane opzegtermijn, en de formule voor de berekening van 'administratiekosten' of boetes[129] in het geval van wanbetaling. Tijdsbepalingen kunnen worden gesteld in een aantal *blokken* of in een absolute tijd[57]. De klant bevestigt dit door het voorstel te onderschrijven met diens private sleutel en het netwerk in te sturen. Aan de contracttransactie wordt een fooi voor het netwerk gehangen die geacht wordt de gestelde regels na te leven. De claimer (en niemand anders) zal, nadat het contract in een *blok* is terecht gekomen, zonder tussenkomst van de klant een transactie kunnen opstellen vanuit de klant naar het bedrijf, waarbij de *miners* de transactie alleen zullen goedkeuren als deze binnen de afgesproken limieten vallen. Er kan hier geen garantie gegeven worden dat de klant op het moment van incasso genoeg saldo heeft.

[57] In hoeverre dat bestaat. (Einstein (1920)) Een 'absolute' tijdsbepaling hoeft hier niet zo precies te zijn. Het moet bij contracten duidelijk zijn wanneer deze zijn verlopen, en secondes zoals in Bitcoin voldoen.

Periodiek claimrechtsvoorstel (op basis van Bitcointransactie):

Incassant	12qsmag851PVGQsmqPayCgNABS3mbc2tgL
Klant	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
PrevCKHash	ca361787e999bb4fa62005d7332ab0f53c268ca3bca250587f1bbebdbee6326e
Frequentie	4380
Stor. Per.	8064
Dwaling	[formule voor incassokosten]
CostRange	1-700
Renewal	52560
ScriptSig I	304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4
ScriptSig K	

Om stornering mogelijk te maken zal de klant ook een claimcontract aan moeten gaan met de claimer, waarbij ze in feite aan *wederzijdse claimerkenning* doen. In dit contract zal echter staan[58] dat de klant binnen een tijdsperiode van 56 dagen (8064 *blokken*) en de tijd van de laatste claim van de claimer, een bedrag kan claimen zoals dat de laatste keer van hem is geclaimd. Ook hier geldt dat er geen garantie kan gegeven worden dat de claimer dit bedrag terug kan uitkeren, gezien het bedrag na ontvangst direct overgeboekt kan worden. Als contracten binnen het protocol rechtsgeldig zijn zal de garantie niet per sé nodig zijn; daar zijn incassobureau's voor. Indien dat niet zo zal zijn zullen de geclaimde NLCoins toch bij ontvangst volgens het protocol vastgezet[59] moeten worden voor de duur van de periodieke storneringsperiode, wat de functionaliteit teniet doet.

[58] "*Every transaction can have a lock time associated with it. This allows the transaction to be pending and replaceable until an agreed-upon future time, specified either as a block index or as a timestamp (the same field is used for both, but values less than 500 million are interpreted as a block index). If a transaction's lock time has been reached, we say it is final.*" (Bitcoin wiki (2014))

[59] Wanneer *miners* Bitcoins genereren beginnen zij met het opstellen van een *Coinbase*-transactie waarin de gegenereerde Bitcoins uit het niets ontstaan. Bij het oplossen van een *block* krijgt de *miner* de verzonnen coins (in overeenstemming met het protocol). Deze kunnen echter pas na een x aantal *blokken* gespendeerd worden om te voorkomen dat deze verzilverd worden door uitgifte wanneer het nog niet duidelijk is in het netwerk of het gegenereerde *blok* ook daadwerkelijk op de langere termijn in de *blokketen* zal komen. Een dergelijke constructie kan ook worden ingezet voor incassogelden, die dan niet kunnen worden uitgegeven voor de duur van de vastgelegde storneringsperiode.

In het geval dat de geïncasseerde gelden volgens het protocol vastgezet zullen worden ten duur van de storneringstermijn kan de functionaliteit net zo goed vervangen worden door een periodieke betaling vanuit de klant. De rekeninghouder behoeft iedere maand alleen nog zijn of haar goedkeuring te geven middels de private sleutel. Hiervoor zou het incasserende bedrijf een transactie opstellen waarbij de rekening van de klant als *input* wordt gebruikt en de rekening van het bedrijf als *output*. Het bedrijf specificeert het gewenste bedrag en ondertekent de transactie met een private sleutel die de klant kan garanderen dat het incasserende bedrijf daadwerkelijk de beheerder is van het ontvangende adres. Vervolgens zal de klant deze transactie moeten ondertekenen met de private sleutel die aan de *input* toebehoort. Het zal voor de klant in dit geval echter niet mogelijk zijn het bedrag te storneren.

Er is nog een derde mogelijkheid, en dat is een hybride vorm. Banken zouden de incassofunctie als product kunnen aanbieden. Zakelijke gebruikers die graag gelden zouden incasseren dienen dan (naast hun eventuele non-bankbeheerde adres) een rekening te openen bij een bank, waarbij de bank de private sleutels in beheer houdt. Voor klanten die de incassoverzoeken ontvangen is dit optioneel. Immers kan je de softwareclient die je *wallet* en daarmee je *private keys* beheert instrueren in te gaan op het periodieke incassoverzoek. Voor een stornering zal de klant contact op moeten nemen met de bank van het bedrijf van de claimer. Te allen tijde kan de klant de periodieke authorisatie weigeren en voorkomen dat er nog gelden zullen worden overgeboekt, gezien de softwareclient iedere maandelijkse transactie met de private key dient te ondertekenen. Bedrijven die incassogelden ontvangen zullen contracten met de klanten willen afsluiten om te voorkomen dat deze zomaar hun authorisatie op incasso stopzetten terwijl ze nog gebonden zijn aan betaling. In dit scenario functioneert de bank als contractbemiddelaar.

Kortom, de incassofunctie kan op enkele manieren worden benaderd:

1. Er wordt wettelijk verplicht dat de private sleutels van alle rekeningen in beheer zijn van een bank, zodat banken van iedereen bedragen kunnen storneren (bedrijven) en afschrijven (klanten)
2. Authorisatie voor het claimen van rekeninggelden wordt ingebouwd in het protocol (een *smart contract*). De limieten en periodes waar de klant de incasserende rekeninghouder voor machtigt worden vastgelegd in de *blockchain*. We noemen het *wederzijdse claimaanvaarding*[60].

[60] Dit zou je ook *wederzijdse claimaanverkenning* kunnen noemen

3. 'Incasso' wordt een product dat banken kunnen aanbieden. Bedrijven nemen een incassorekening waarbij de bank de private sleutel in beheer heeft, wat het toestaat om bedragen te storneren. Een incassorekening voor de machtiger is optioneel.

4.4.10 Erfrecht, belasting en misdaad

In enkele gevallen is het soms wenselijk een rekening te bevriezen of te sluiten. Een van die gevallen is bij overlijden. In de praktijk wordt een rekening (ook gedeelde rekeningen) bevroren wanneer de bank melding krijgt van het overlijden van een rekeninghouder. Erfgenamen dienen vervolgens een dure 'verklaring van erfrecht' te bemachtigen bij een notaris om te bewijzen dat ze (een) recht hebben op het geld dat werd beheerd alvorens het weer wordt ontdooid. Voordat de erfgenamen het geld uitgekeerd krijgen dient er eerst ook nog erfbelasting betaald te worden. Een complexe procedure. Voor *wallets* die bij een bank beheerd worden (met toegang voor de bank) is dit geen groot probleem. Voor zelfstandige (NLCoin) rekeninghouders is er de mogelijkheid dat de private sleutel verloren gaat als deze niet is overgedragen. Financiële instellingen kunnen het rekeningauthorisatieproces omgekeerd afspelen om een rekening te bevriezen. In het protocol kan eventueel een bloklimiet ingesteld worden die als buffer zou dienen voordat een dergelijke de-authorisatie van kracht wordt om institutioneel misbruik tegen te gaan, maar gezien de aard van het bevriezen van rekeningen (om grootschalige leeghaling te voorkomen) is dit misschien niet wenselijk. Om te voorkomen dat er een regeling opgenomen dient te worden die banken in staat stelt beslag te leggen op rekeninggelden van overledenen, zelfs *zonder* dat ze de private sleutels zouden hebben, dient er een resolutiemechanisme te worden ingebouwd dat de afwikkeling hiervan zou faciliteren. Zo kan er in het protocol worden opgenomen dat bij de rekeninggeneratie een adres gekoppeld dient te worden van de notaris, aan wie de rekeninggelden automatisch worden overgemaakt nadat er aan enkele condities zijn voldaan. Het technisch nakijken van die condities is moeilijk aangezien het hier gaat om een sterfgeval. Hoe weet het protocol met zo min mogelijke menselijke tussenkomst dat een rekeninghouder is overleden? Dit is in het bijzonder een moeilijke kwestie waar uiteindelijk toch ergens menselijke input vereist zal zijn. Hier is voorlopig geen makkelijk antwoord op.

4.5 Technische ondersteuning in het bankwezen

De premisse in dit paper is geweest dat het voorgestelde systeem ondersteund zou moeten worden door het bankenwezen en de financiële sector, om pragmatische redenen. Door het hart van het financiële systeem te vervangen en daarna vernieuwd terug te plaatsen op de plek waar het al zat wordt beoogd zo min mogelijk procesmatig te veranderen, om daarmee de maatschappelijke acceptatie te verhogen. In deze sectie zal exploratief gekeken worden hoe de bankensector NLCoin zou kunnen ondersteunen, op basis van gesprekken met enkele software-architecten van de SNS, ING en Rabobank, die hun visie op persoonlijke titel, en niet verbonden aan hun werkgever, gedeeld hebben.

4.5.1 Decentralisatie

De reden dat het banksysteem NLCoin zou moeten *minen* is om ervoor te zorgen dat de afgesproken regels van het protocol worden nageleefd, en dan specifiek de regels betreffende de geldcreatie. Zoals we eerder hebben vastgesteld heerst er een (bankiers-)stigma op schuldvrije geldschepping door de Staat wegens een veelal irreële angst op een hyperinflatie (Boonstra (2013)). Deze angst kunnen we ontladen door het toegestane gedrag van de overheid vast te leggen in het protocol. Om ervoor te zorgen dat het protocol niet alsnog wordt overschreden zal deze zo decentraal mogelijk ondersteund moeten worden.

Minen is effectief het verifiëren van transacties en het naleven van de regels van het protocol. In Bitcoin is de primaire reden voor het *minen* het leveren van veiligheid tegen aanvallen zoals de 51%-aanval. In NLCoin is de primaire reden van het gedecentraliseerd *minen* het opwerpen van drempels tot protocolwijziging; de beveiliging tegen de 51%-aanval is secundair. Er dienen genoeg verschillende partijen te *minen* zodat als de Staat toch een verandering van het protocol zou willen doorvoeren, en daarmee wellicht de regels op geldschepping zou veranderen, dat zou resulteren in een dergelijk grote transitie- en implementatielast dat dit groot nieuws (moet) zijn waarbij de bevolking wordt ingelicht over de geplande verandering.

Om de transactiefooien eerlijk over de *miners* te verdelen (elk *block* zullen n-1 *miners* toch hun tijd verspild[61] hebben met het proberen van het vinden van een *block*) is het handig één nationale *mining pool* te maken waar *miners* voor *minen*. Een *pool* is een server die bijhoudt

[61] Zolang het GHOST-protocol niet wordt geïmplementeerd.

hoeveel rekenkracht een aangesloten *miner* levert en de winsten bij het collectief creëren van een *block* naar prestatie verdeelt over de deelnemers:

> "*Bitcoins are ordinarily only ever created in chunks of 25 at a time, with the whole 25 paid to a single person. Furthermore, the race to get the 25 BTC prize in a given block is highly competitive. If you set out mining on your own, it may be a long time before you can make a return. Pooled mining allows you to receive smaller, more frequent, steadier payouts instead. If you have a slower computer, or a CPU miner, then pooled mining may be the only way that you will ever mine any bitcoins at all.*"[130]

Voor NLCoin is de waarde hier natuurlijk 0. Door de *miners* aan te sluiten bij een *pool* zullen ze frequenter uitbetaald worden in de verwerkte transactiefooien. Als ze zich niet zouden aansluiten wordt elke *miner* die geen *blokken* genereert niet betaald. Er is gelukkig *pooling*-software van decentrale aard gelijkend aan Bitcoin, genaamd '*P2Pool*'[131]. Door deze te gebruiken wordt iedere deelnemer op frequente basis betaald zonder dat daar gecentraliseerde besluiten aan vooraf gaan. Dit systeem is dus niet makkelijk te misbruiken, zoals een gecentraliseerde *pool* geleid door een stel bestuurders dat wél zou zijn. Dat het toch echt niet allemaal om de transactiefooien zal gaan wordt geschat door Jeff Garzik, een van de kernontwikkelaars:

> *"Second, in a successful Bitcoin future, financial institutions are not all going to be into mining for the profits of mining, but also for the digital equivalent of a bank spending half a million on a bank vault. For the security this contributes for their own membership. Nor will all these institutions be banks, as credit unions and non-profit institutions exist now and therefore it's reasonable to expect them to exist in the future. These institutions will participate in the Bitcoin infrastructure for their clients' comfort and benefit moreso than the possibility of (direct) profits. And these same institutions are likely to develop interlinking agreements to process the transactions of each other's clients for free even if they were to refuse to process free transactions in general."*[132]

4.5.2 Openheid van de markt voor het *minen*

Ondanks de eis van decentraliteit zal het helaas niet toegestaan kunnen worden de buitenlandse markt voor het *minen* van NLCoin open te laten. Dit heeft te maken met jurisdictie. Als de (buitenlandse) vrije markt een groter aandeel in het *minen* van NLCoins zou hebben dan partijen waar we jurisdictie over hebben, dan betekent dat alsnog een verlies van soevereiniteit. Het moet gezegd worden dat zelfs als het openlijk toegestaan werd NLCoin te *minen* (internationaal), dat *miners* dan ten eerste alsnog éérst een adres voor de uitbetaling van transactiefooien moeten verkrijgen bij de Nederlandse *adresgeneratoren*. Daar komt bij dat als die *miners* regels in het protocol zouden toepassen (of laten) op een manier dat het ons (als democratie) niet bevalt, of dat de Nederlandse bankensector geen overhand meer zou hebben in het *minen,* het de Staat altijd vrij staat een triviale protocolverandering door te voeren die resulteert in een harde splitsing[62] *(hard fork)* van de *blokketen* tussen Nederland en de rest. Een geldsysteem is (op Bitcoin na) in de regel verbonden met een politieke regio, wat ook hier uit blijkt.

Het verlenen van licenties en authorisaties op minen zal op een vergelijkbare manier moeten gebeuren als de *adresauthorisaties* in de vorige sectie. De staat stuurt een bericht het netwerk in dat het een bepaald adres is toegestaan om *blokken* te produceren. Vanwege het *bootstrapping*-probleem zal de Staat bij het starten van het netwerk wellicht zelf ook het tweede (na het *genesis blok*) moeten *minen* om ervoor te zorgen dat de *minerauthorisatie* voor de eerste bank in een *blok* terecht komt, waarna de geautoriseerde kan beginnen met *minen*. De *adresauthorisaties* en *minerauthorisaties* kunnen van elkaar verschillen. Op die manier zouden er twee typen financiële instituten kunnen ontstaan. De instituten die *adressen* goedkeuren en aan WID-identificatie doen, en de instituten die de transacties valideren. Een *minerauthorisatie* zal te vergelijken zijn met een type banklicentie dat nu verleend wordt aan Payment Service Providers (PSP). Elk NLCoin *blok* zal in de *blokheader* twee velden moeten opnemen, voor respectievelijk de publieke sleutel van de *miner* en de handtekening waarmee de *miner* het gegenereerde *blok* met zijn private sleutel heeft ondertekend.

[62] Dit houdt in dat delen van het netwerk er andere regels op na houden en dat er in feite verschillende versies van de *blockchain* ontstaan, en dus verschillende geldnetwerken

Zolang alle banken qua *hashrate* en rekenkracht die ze leveren aan het netwerk elkaar in balans houden is er niks aan de hand. Als de krachten verdeeld worden hoeven de *hashrates* ook niet hoog te zijn. Er is geen kans dat er *miners* met krachtige ASIC's uit het buitenland mee zouden doen, want zonder de juiste *minerauthorisaties* zullen hun *blokken* niet worden geaccepteerd. Het is wel mogelijk dat de instellingen in Nederland zelf op een zeker moment plotseling meer rekenkracht zouden kunnen aanleveren om daarmee de balans te verstoren. Een ander 'gevaar' is dat de overheid een aantal ASIC's achterhoudt om in tijden van economische tegenspoed zélf mee te doe met *minen.* Als haar capaciteit dan bij activatie meer zou behelsen dan 51% van de rekenkracht van het zelf toegestane bankwezen, dan is het mogelijk de limieten op geldcreatie te omzeilen. Een eenvoudigere manier zou echter zijn om kortstondig alle *minerauthorisaties* in te trekken, als daar geen incubatietijd voor wordt ingebouwd. Om te voorkomen dat de decentralisatie scheef zou gaan lopen kan de overheid een mandaat van verhoudingen vaststellen waar banken zich aan zouden moeten houden.

4.5.3 Kunnen banken het protocol uitvoeren?

De software voor het protocol kan in de IT-structuur van banken gedraaid worden. “Geen probleem” (Rabobank). Banken hebben een veelvoud aan systemen; o.a. voor het verwerken van het betalingsverkeer, voor het verwerken van de administratie en voor het genereren van rapportages voor de toezichthouders. Hieronder bevinden zich '*Host Security Modules*' (HSM), dure kleine machines die cryptografische berekeningen uitvoeren (helaas zijn ze te specifiek voor een reeks SHA-256-hashes), maar ook standaardmachines met gangbare besturingssystemen zoals Linux waar het inderdaad niet moeilijk op zou zijn het *mining* protocol uit te voeren. De performance zou desalniettemin erbarmelijk zijn. Zolang de geleverde rekenkracht van de *miners* in balans blijft is dat niet erg, op voorwaarde dat het *minen* binnen Nederland wordt afgeschermd.

4.5.4 Hoe moet het *mining*-algoritme aangepast worden?

Een vraag die hier mee te maken heeft betreft de keuze van het algoritme. Bitcoin maakt gebruik van SHA-256 bij het *minen*. Hier zijn speciaal mooie ASIC's voor gemaakt die een uitstekende prestatie kunnen leveren, gemeten in *GigaHash*, en *TeraHash*. Een van de eerste alternatieve munten naast Bitcoin, “*Litecoin*”, gebruikt een ander algoritme: 'SCrypt'. Welk algoritme is het meest geschikt voor de IT-structuurin het bankwezen?

> "*scrypt (…) --in contrast with Bitcoin's SHA-256d-- serves to inhibit hardware scalability by requiring a significant amount of memory when performing its calculations. This change reduces the efficiency gain and economic incentive to develop custom hardware such as Application Specific Integrated Circuits (ASIC). While ASICs can be adopted for any purpose and are likely to be introduced for Litecoin, the use of scrypt should delay this change, and preserve the decentralization in mining that brings a decentralized currency so much of its value and resiliency.*"[133]

Het SCrypt algoritme maakt de hashberekening dus arbitrair moeilijk en gebruikt zoveel mogelijk geheugen. Dit maakt het lastig(er) voor dit algoritme een ASIC te produceren. Dit betekent dat Litecoin nog makkelijker gedolven kan worden op gewone CPU's en videokaarten, wat de decentralisatie ten goede komt. Welk algoritme zou beter passen bij onze doelstellingen? Het klinkt initiëel aantrekkelijk om het SCrypt-algoritme te gebruiken uit de waardering voor het hooghouden van de decentralisatie. Dat is hier alleen niet zo heel belangrijk omdat er niet veel spelers zullen zijn. Tevens zal SCrypt onnodig inefficiënt zijn voor de servers van banken. Het teleurstellende antwoord is uiteindelijk dat het niet zal uitmaken. Banken zullen toch moeten investeren in ASIC's, omdat er nauwelijks echte rekenkracht beschikbaar zal komen in hun IT-infrastructuur om hier aan te besteden.

4.5.5 Besparingen?

Het klinkt alsof NLCoin veel processen irrelevant zou maken. Het verwerken van transacties, het bijwerken van sommige typen administratie, het beveiligen van rekeningen en rekeningnummers. Een educated guess van een systeemarchitect bij de Rabobank wist desondanks te vertellen dat de meeste servers toch praktisch constant blijven draaien voor het genereren van complexe rapporten die ze verplicht zijn te maken voor de toezichthouders. Ook de administratie vereiste een hoop rekenwerk, en dat is administratie buiten de transactiegeschiedenis om. Er zullen dus nauwelijks besparingen zijn. In tegendeel. De eerste transitieperiode zal het veel kosten om alle bankprocessen opnieuw aan te sluiten aan de nieuwe betalingsstandaard. Banken zullen in de praktijk enkele off-the-shelf ASIC's aanschaffen en bij elkaar zetten in een gedeeld netwerkcentrum. Op die manier wordt de *propagation time* van de grote *blokken* drastisch verlaagd. Er werd gesteld dat het verwerken van transacties dan weer bijna de methodiek van betalingsverwerker Equens zou benaderen, uit de tijd dat het nog Interpay heette.

Er is te beargumenteren dat de kosten die de banken maken voor het genereren van rapportages onnodig zijn. De data waar alle rapportages op gebaseerd zijn zullen met NLCoin voor iedereen vrij en toegankelijk zijn. De toezichthouders kunnen zelf in de *blockchain* kijken. Dit is verder te rationaliseren. Onderdelen van de Wet van Financieel Toezicht (WFT) en de belastingdienst kunnen worden ingebouwd in het protocol, om rapportage te automatiseren. Er kan automatisch belasting worden afgedragen over bepaalde typen transacties en er kunnen automatisch meldingen wordengemaakt van verdachte transacties. De mogelijkheden gaan erg ver, en in principe kan alle digitale data die beschikbaar is gebruikt worden. Er wordt hier verder niet diep op ingegaan, maar het concept van automatische wetsverwerking verdient een apart onderzoek op zich.

4.5.6 Transitieperiode

Het is moeilijk een inschatting te maken hoe veel tijd het zou kosten voor een bank om de overstap te maken naar een nieuw systeem als dit. Er wordt hier een grote verandering voorgesteld die waarschijnlijk structureel meer verandering in processen zou vereisen dan de invoering van de ChipKnip. Ter illustratie, het overleg tussen banken over de invoering van de ChipKnip heeft anderhalf jaar geduurd. Een professionele schatting beraamde dat het tussen de 10 en 15 jaar zou kosten om een dergelijk cryptografisch muntsysteem te implementeren. Dit is een *educated guess* van een systeemarchitect. Het PIN-systeem kon waarschijnlijk zonder al te veel problemen worden aanehouden.

5. Conclusie

Leden van het collectief genaamd de 'International Movement for Monetary Reform' pleiten voor een implementatie van staatsgeld volgens het Chicago Plan. Ze geven te kennen dat te willen installeren bij een publiek orgaan of de centrale bank. Er zijn vanuit de financiële sector kritische geluiden te horen. Zo waarschuwen enkele economen voor een hyperinflatie als we de Staat het geld zouden laten scheppen.

Het innovatieve betalingsnetwerk Bitcoin bezit enkele eigenschappen die we goed zouden kunnen gebruiken in een staatsgeldsysteem. Deze eigenschappen zijn duidelijk geworden door de werking van Bitcoin te vergelijken met de werking van het hedendaagse geldsysteem. Hierbij zijn we ook gestuit op de aard van het concept van geld. Zo blijkt Bitcoin meer gelijkend aan de Aristoteliaanse en Platonische definitie van geld, 'bestaande door afspraak', waar het elektronische geld in het hedendaagse systeem slechts een vordering op de uitgever betreft, bestaande door de markt. De aard van het tweede type geld is verantwoordelijk voor de algemene instabiliteit van het huidige systeem, en het eerste type is wat de internationale beweging beoogt te installeren om de crisis op te lossen.

Bitcoin kan op een technische manier enkele garanties geven die overmatige geldcreatie kunnen voorkomen dankzij de decentrale aard van het protocol, en biedt een ongekende statistische- en procesmatige transparantie, die tevens van pas zal komen voor de maatschappelijke legitimering en vertrouwenswekking van een staatsgeldsysteem. In dit paper is verkennend onderzoek opgenomen dat ruwweg bekijkt of het mogelijk is de goede eigenschappen van Bitcoin te gebruiken in een nieuw systeem van staatsgeld. Dit blijkt goed mogelijk te zijn. Het is mogelijk binnen Bitcoin een enkele autoriteit te definieren die de bevoegdheid heeft geld te creëren, waar het de huidige *miners* ontnomen zal worden. Door *miners coinbases* te laten accepteren en verwerken die afkomstig zijn van de staat wordt er geld gecreëerd.

Door de verantwoordelijkheid van het verifiëren van transacties te leggen bij de bankensector die juist zo kritisch is over een systeem van overheidsgeld, is het mogelijk een scheiding van machten te realiseren betreffende geldschepping. Er kunnen regels opgesteld worden omtrent de limieten van de geldschepping. Deze regels zullen vooraf gedefinieerd worden en achteraf

nageleefd. Samen met de nieuwe transparantie van het geldscheppingsproces zullen ze het bancaire en maatschappelijke vertrouwen scheppen dat nodig is om het systeem van staatsgeld te ondersteunen, op voorwaarde dat het niet te gemakkelijk zal zijn voor de Staat om protocolaanpassingen te verordenen. Het zal moeilijk zijn kritiek te leveren op dit systeem voor de sector die zelf verantwoordelijk zal zijn voor de strikte handhaving van de wiskundige apolitieke regels. We hebben hiervoor een aantal mogelijke regels besproken: een statische limiet, en een dynamische op basis van de geldhoeveelheid, of de omloopsnelheid. Er zijn er ongetwijfeld meer te ontwerpen gezien de hoeveelheid beschikbare meetbare variabelen.

Er wordt op basis van enkele variabelen aangenomen dat Bitcoin in de toekomst nog redelijk zal kunnen schalen tot het niveau dat hier gewenst zou zijn, naar ~400TPS. De maximumblokgrootte kan, ondanks felle tegenstand uit angst voor afnemende tot onmogelijke profitabiliteit en de daarmee resulterende onveiligheid, verhoogd worden tot vele malen van het huidige niveau. Eventuele problemen kunnen ondervangen worden met een voorstel voor conservatieve protocolwijziging: het GHOST-protocol dat verlaging van de blokcreatietijd zou toestaan (zonder daarbij de beveiliging te compromitteren) en de TPS-waarde nog verder zou verhogen. Nieuwe voorziene innovaties zullen de grootte van de *blokchain* in toom houden, maar zullen leiden tot meer centralisatie van *miners* die als enige de volledige historie van de keten bij zullen (kunnen) houden. Dat is in het licht van het voorstel in dit onderzoek minder een probleem dan bij Bitcoin. Hier wordt immers onderzocht hoe de taak van *minen* in een staatsmuntvaluta op basis van Bitcoin kan worden toegespitst op het Nederlandse bankwezen, wat al als een hoge mate van centralisatie gezien kan worden. We zouden graag zien dat we in het ergste geval wat betreft het vraagstuk van schaalbaarheid afhankelijk zouden zijn van de notie dat met tijd, en de immer-uitdijende grootte van de *blockchain* die bijgehouden moet worden, nieuwe technieken ons, op basis van de Wet van Moore, zouden toestaan efficienter deze *blokketen* te beheren, zoals Satoshi zich dat voorstelde. Helaas is de realiteit dat dit voor het bankwezen in haar huidige vorm bijna onhaalbaar is. De kosten voor het opslaan en meerdermaals dupliceren van data zijn reeds hoog. Het is van belang dat er een *prunable*, dan wel *finite blockchain* komt om de kosten van verwerking tot een eindig niveau te beperken. De implementatie hiervoor is onderweg, maar het zal nog een tijd duren voordat de technieken zo beproefd zijn dat er met een zekerheid te zeggen is dat het zal werken als gedacht. Wanneer de techniek er is zal de *blockchain* een maximumlengte hebben die grenst aan de dataretentie-eis.

Om de stap naar een dergelijk systeem zo klein mogelijk te maken wordt een pragmatisch principe aangehouden. De implementatie van het NLCoin-systeem dient zoveel mogelijk te lijken op het systeem zoals het nu is, qua taakverdeling. Door de adresgeneratie op een kunstmatige manier te beperken is het mogelijk een Bitcoinproces te koppelen aan de wettelijke eisen van de *Wet Identificatie Dienstverlening* en de *Wet ter voorkoming van Witwassing en Financiering van Terrorisme*. Op deze manier kunnen rekeninghouders geïdentificeerd worden bij het openen van een rekening, terwijl er nog wel de keus is hen het eigendom op het beheer van de rekening toe te kennen. Het zal mogelijk zijn een ultieme vrijemarktwerking te laten bestaan in rekeningbeheer, doordat rekeninghouders met het grootste gemak kunnen kiezen wie hun *wallet* dient te beheren.

Het besluit over welke bank op welk tijdstip de licentie krijgt om adressen het netwerk in te brengen wordt een protocol-feature die dynamisch kan worden gebruikt. Het staat de wetgever toe in de tijd verschillende instanties adresgeneratierechten toe te spelen of af te nemen zonder dat het protocol daarvoor hoeft worden aangepast. Hetzelfde geldt voor de licentie om te *minen*. Er is een moeilijke ontwerpkeuze te maken omtrent de rechten van adressen in het beheer van overledenen, omdat de keuze inhaakt op het legitimiteitsprincipe en de mogelijkheid tot institutioneel misbruik.

Wanneer we banken de adressen laten genereren of goedkeuren komen we in de knel met privacy. Hiervoor zijn enkele protocollen als toevoeging ontwikkeld die dit probleem kunnen verhelpen. Zo is er Zerocoin ontwikkeld dat het mogelijk maakt de link tussen identiteiten van partijen in een Bitcoinbetaling te anonimiseren. Zerocoin staat een 'backdoor' toe die de toezichthouders kunnen laten meekijken, al is er nog geen duidelijkheid over hoe dit technisch zou moeten werken. Ook wordt er werk gemaakt van de implementatie van *stealth addresses*, adressen die oneindig gebruikt kunnen worden en voorkomen dat betalers de balans kunnen opmaken van de betaalde aan de hand van het rekeningnummer. Deze twee technieken samen zorgen voor een anonimiteit in het betaalsysteem zoals we dat nu kennen, en houdt de mogelijkheden open voor toezichthouders om hun werk te blijven doen.

De meeste betaalproducten zijn nog steeds mogelijk en toepasbaar in een NLCoin-systeem. Alleen het product 'incasso' levert problemen op. Zo wordt er inbreuk gemaakt op het principe van legitimiteit doordat gelden zonder tussenkomst af- of teruggeboekt kunnen worden. We hebben een theoretische voorbeeldimplementatie gegeven van hoe het toch mogelijk is de

incassofunctie te implementeren, binnen de grenzen van het systeem. Dit is gedaan door een proces dat we *wederzijdse claimaanvaarding* noemen.

Tegen verwachting in beschikken banken niet over de verwachte IT-architectuur. Bij implementatie zouden banken ASIC-machines moeten aanschaffen om te voldoen aan het quotum aan *hashrates*. De technische veranderingen aan het protocol zelf zijn nog niet zo veel werk. Het meeste werk zal liggen bij de bankensector. Er is te kennen gegeven dat het minimaal tussen de 10 en 15 jaar zou duren voordat een transitie als een die hier wordt voorgesteld voltooid zou kunnen zijn. In dit werk is initieel verkennend onderzoek gedaan. Er moet nog veel meer specifiek onderzoek gedaan worden om in te kunnen schatten wat precies de effecten voor de maatschappij en de bankensector zouden zijn.

Ook in de technische ondersteuning wijken de processen van de digitale munt sterk af van Bitcoin. Waar Bitcoin (nog) echt een vrije munt is die door iedereen vrij verhandeld en gegenereerd kan worden zonder drempels zal NLCoin in alle waarschijnlijkheid slechts nationaal gevalideerd worden om in veilige wateren te zitten betreffende de politieke jurisdictie. Het is nodig de munt decentraal te *minen* om een drempel op te werpen die de gevaren van ingrijpende protocolwijzigingen zou vertragen. Om een balans te garanderen tussen de *miners* kan er een mandaat worden ingesteld. De IT-structuur van banken is voor wat we beogen teveel gericht op de complete efficiëntie van verwerking van transacties in het 'klassieke' geldsysteem: het hedendaagse. De hoop dat banken genoeg serverparken zouden hebben staan om cryptografische validaties mee te kunnen uitvoeren is vervlogen, en banken zullen in de transitieperiode waarschijnlijk een behoorlijk aantal ASIC-pakketten moeten aanschaffen, die samen met de machines van andere banken op een centrale verwerkingsplek gestald zullen worden. Het is nog onduidelijk hoeveel ASIC's iedere bank zou (kunnen) kopen. Ook is er geen goede kwantitatieve meting voor de hoogte van de *hashrate* die veilig zou zijn om het netwerk mee te beginnen. De keuze voor een specifieke hashfunctie is irrelevant geworden. In plaats van eventuele besparingen die dit systeem zou opleveren wegens bedrijfstakken die met de invoering irrelevant geworden zullen zijn, zal de invoering de eerste fases behoorlijk wat geld kosten. Veel nieuwe apparatuur en een enorme omslag van bedrijfsprocessen en change-management in mensen.

Al met al, een technische Bitcoinimplementatie die een monopolie op geldcreatie aan de Staat garandeert is mogelijk, en niet te moeilijk. Er kunnen heldere limieten voor gevonden worden die vertrouwen zullen wekken. Of het mogelijk is het netwerk te schalen tot Nederlandse proporties is waarschijnlijk, maar is nog in afwachting van beloofde techniek. Om aan regelgeving te voldoen en het systeem een drop-in replacement te maken kan het proces van rekeninggeneratie dynamisch worden toevertrouwd aan banken die daarmee kunnen toezien op de WID en de WFFT. De anonimiteit kan gewaarborgd blijven door de implementatie van twee protocol-addenda. Banken zullen de munt moeten minen in een decentrale nationale pool, maar dat zal aanzienlijke investeringen kosten die ze waarschijnlijk niet terugzien in besparingen.

6. Discussie

Het is goed mogelijk gebleken een Bitcoinvariant te maken die gebruikt kan worden als Staatsmunt. Een dergelijke munt in Nederland inzetten zou niet zonder kosten zijn. Om het netwerk in te bedden in gegeven wetgeving moeten er veel concessies gedaan worden aan functionaliteiten in Bitcoin, die juist de aantrekkingskracht vertegenwoordigen. NLCoin zoals het hier is uitgelegd is geen Bitcoin meer. Het heeft enkele pure principes van vrijheid en gemak verloren aan bijvoorbeeld de identificatieplicht en eventuele reversibiliteit. Wat NLCoin zou zijn is een nieuwe munt in een oud jasje waarbij het systeem zo min mogelijk moet veranderen, maar juist ook fundamenteel veel is veranderd. Ondanks dat NLCoin zich inpast in regelgeving om het hedendaagse systeem te imiteren is het een verbetering. Dat let niet dat er nog grote ontwerpkwesties open staan. Zo is het nog onduidelijk wat er gedaan zou kunnen worden wanneer een rekeninghouder sterft. Deze kwestie vereist meer gespecificeerd onderzoek.

Dit paper ging uit van de hypothetische implementatie van Zerocoin. Ondanks dat Zerocoin de tekortkomingen in privacy tegemoet lijkt te komen zijn er wel wat kanttekeningen bij te zetten die de implementatie vermoeilijken. Zo zouden de handtekeningen voor de transacties nog steeds teveel data vereisen: meer dan 40KB. Vergelijk dit met de gemiddelde transactiegrootte in Bitcoin: 400 bytes. Tevens zou het computationeel intensiever worden de validatie van een Zerocoin uit te voeren, waardoor er met de huidige techniek niet sneller dan 1 á 2 transacties per seconde gevalideerd zouden kunnen worden. Aldus Greg Maxwell[134], kernontwikkelaar[135]. Zerocoin zal binnenkort als eigen munt verschijnen. Dit zal aantonen of de prestatieproblemen met de munt echt zo erg zijn als wordt verwacht. Het zal goed mogelijk zijn dat NLCoin bij een uiteindelijke implementatie van Zerocoin gelimiteerder gaat zijn in TP/S dan hier wordt aangenomen.

Het werk is in eerste instantie geschreven om een technische garantie te kunnen geven tegen de angst voor hyperinflatie. Vaak in interviews werd ik erop gewezen dat het decentrale systeem toch wel heel erg redundant en inefficiënt zou zijn om zo te implementeren. 'Het zou veel makkelijker zijn om één centrale bank te laten *minen. Dat is efficiënter*'. Dit mag zo zijn, maar hiermee wordt tevens weer een groot voordeel opgegeven. Efficiëntie is de prijs voor veiligheid. Het zou hoe dan ook een win-win situatie zijn. Als de centrale bank NLCoin verwerkt

krijgt de IMMR haar zin, en anders zal het protocol decentraal moeten zijn om bankiers gerust te stellen, waarbij de IMMR óók wint.

7. Toekomstig onderzoek

Er zijn veel aspecten behandeld. Toch zijn er ook veel zaken aan bod gekomen die hier niet tot hun recht komen. Zo zou het interessant zijn onderzoek te doen naar een echte implementatie van de Incasso-techniek op basis van Bitcoin. Tevens vereist het een heel nieuw veld van onderzoek om te zien of het belastingrecht niet vereenvoudigd kan worden door deze op te nemen in het protocol. Tot slot is er onderzoek nodig naar de maatschappelijke haalbaarheid om rekeninghouders de vrijheid te geven hun eigen rekeningen te mogen beheren. Welke kill-switches zullen in het protocol worden opgenomen om rekeningen alsnog van hun saldo te ontdoen?

8. Bibliografie

1: Carmen M. Reinhart & Kenneth S. Rogoff (2009), *This Time Is Different: Eight Centuries of Financial Folly*

2: Centraal Bureau voor de Statistiek, *Definitie: Geldscheppende financiële instelling*, http://www.cbs.nl/nl-NL/menu/methoden/begrippen/default.htm?ConceptID=3095

3: Douglas, Paul H.; Fisher, Irving; Graham, Frank D.; Hamilton, Earl J.; King, Willford I.; Whittlesey, Charles R (1939), *A Program for Monetary Reform*

4: Wim Boonstra (2013), *Geld speelt (g)een rol*

5: Stephen A. Zarlenga (2002), *The Lost Science of Money*

6: Stichting Ons Geld (2013), *Weerlegging van Wim Boonstra*, http://onsgeld.nu/weerlegging/wim-boonstra-3/weerlegging-wim-boonstra-deel-1-schuldgeld-vs-echt-geld/

7: Satoshi Nakamoto (2009), Bitcoin: A Peer-to-Peer Electronic Cash System

8: Bitcoin.it (2013), *Trust and Integrity*, http://bitcoin.org/en/innovation

9: Zaplog.nl – Democraatus (2013), *Dutchcoin - let's do it*, http://zaplog.nl/zaplog/article/dutchcoin_lets_do_it/

10: Financial Post (September 2013), *Canadian Mint ready to test its own digital money project*, http://business.financialpost.com/2013/09/19/canadian-mint-pushes-ahead-in-murky-world-of-crypto-currency-with-mintchip-project/

11: Financial Post (September 2013), *Q&A: MintChip boss Marc Brûlé on getting into the digital currency business*, 2013, http://business.financialpost.com/2013/09/19/q-a-interview-with-mintchip-boss-marc-brule/

12: ChallengePost (2012), *Is MintChip the next evolution of cash?*, http://blog.challengepost.com/post/20777146688/is-mintchip-the-next-evolution-of-cash

13: Mintchip Developer Resources, http://developer.mintchipchallenge.com

14: Bitcoin Magazine (2012), *The MintChip: The Canadian Government's Answer to Bitcoin*, http://bitcoinmagazine.com/776/the-mintchip-the-canadian-governments-answer-to-bitcoin/

15: Forbes (2012), Mintchip misses the point of digital currency, http://www.forbes.com/sites/jonmatonis/2012/04/12/mintchip-misses-the-point-of-digital-currency/

16: Kimitsu Asset Management, *BTC Oyate Project Concept*, http://www.hyjinxentertainment.com/kam/oyate.htm

17: Wikipedia, *Lakota (volk) - Onderverdeling van de Lakota*, http://nl.wikipedia.org/wiki/Lakota_(volk)#Onderverdeling_van_de_Lakota

18: Wikipedia, *Pine Ridge Indian Reservation*, http://nl.wikipedia.org/wiki/Pine_Ridge_Indian_Reservation

19: Altwire (2013), *Mazacoin press release 1*, http://altwire.utne.com/rt/buddhism_v3/mazacoin-press-release-1--pastebincom/55492b744b4a4d76794f646156762b344c73446175773d3d

20: Financial Times (November 2013), *Alderney looks to cash in on virtual Bitcoins with Royal Mint reality*, http://www.ft.com/intl/cms/s/0/4903fc9a-591f-11e3-a7cb-00144feabdc0.html

21: Wikipedia, *Alderney*, http://en.wikipedia.org/wiki/Alderney

22: Financial Times (2013), Alderney to cash in on Bitcoins with Royal Mint

23: Positive Money (2013), *Our Proposals*, http://www.positivemoney.org/our-proposals/

24: Stichting Ons Geld (2013), *Onze voorstellen*, http://onsgeld.nu/oplossing/

25: Library of Economics and Liberty (2006), *An interview with Milton Friedman*

26: The Wall Street Journal (2005), *Response by Dr. Ben S. Bernanke to written questions received from Senator Bunning in connection with the hearing before the Committee on Banking, Housing, and Urban Affairs on November 15, 2005*, http://online.wsj.com/public/resources/documents/bernankebunning11212005.pdf

27: Ludwig von Mises Institute (2010), *Death of M3: The Fifth Anniversary*, http://mises.org/daily/4859/

28: Tim McMahon (2006), *Goodbye M3 – What is the Government hiding?*, http://inflationdata.com/articles/2006/03/16/goodbye-m3-what-is-the-government-hiding/

29: Wikipedia, *Algemene Rekenkamer*, http://nl.wikipedia.org/wiki/Algemene_Rekenkamer

30: Positive Money (2013), *The Money Multiplier and Other Myths about Banking*, http://www.positivemoney.org/how-money-works/advanced/the-money-multiplier-and-other-myths-about-banking/

31: Zerohedge (2013), *Cyprus 37.5% Depositor Haircut Upgraded To 47.5% Brazilian Wax*, http://www.zerohedge.com/news/2013-07-29/cyprus-375-depositor-haircut-upgraded-475-brazilian-wax

32: Aziz (2013), *There Is No Surer Way To Destroy A Banking System Than Giving Depositors A Haircut*, http://azizonomics.com/2013/03/16/there-is-no-surer-way-to-destroy-a-banking-system-than-giving-depositors-a-haircut/

33: Klaas van Egmond, Francis Weyzig, Rens van Tilburg (2013), *Geldcreatie is een gevaarlijk privilege, zowel in private als in publieke handen*

34: Rudie Kagie en Map Oberndorff (2009), *Nout Wellink: 'We hebben gezien dat er grote gaten zitten in het toezichtsysteem.'*, http://www.vn.nl/Standaard-Media-Pagina/Nout-Wellink-We-hebben-gezien-dat-er-grote-gaten-zitten-in-het-toezichtsysteem..htm

35: Adam Clark Estes (2013), *To Win the Global Bitcoin Arms Race, Crypto Miners Are Building Custom Microchips*, http://motherboard.vice.com/blog/bitcoin-mining-creating-cottage-industry-custom-microchips

36: Wikipedia, *Wet ter voorkoming van Witwassen en Financieren van Terrorisme*, http://nl.wikipedia.org/wiki/Wet_ter_voorkoming_van_witwassen_en_financieren_van_terrorisme

37: Nederlandse wet, *Wet ter voorkoming van Witwassen en Financieren van Terrorisme*

38: Nick Szabo (2008), *Bit gold*, http://unenumerated.blogspot.nl/2005/12/bit-gold.html

39: M.A. Jansen, *BITCOIN: THE POLITICAL 'VIRTUAL' OF AN INTANGIBLE MATERIAL CURRENCY*,

40: Satoshi Nakamoto (2009), *Bitcoin open source implementation of P2P currency*, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

41: Tim van Pelt (2013), *Bitcoin - een decentrale munteenheid*

42: Next! Magazine (1999), *How DigiCash Blew Everything*, http://cryptome.org/jya/digicrash.htm

43: Bitcoin.it, *Fractional Reserve Banking and Bitcoin*, https://en.bitcoin.it/wiki/Fractional_Reserve_Banking_and_Bitcoin

44: Vitalik Buterin (2013), *An Exploration of Intrinsic Value: What It Is, Why Bitcoin Doesn't Have It, And Why Bitcoin Does Have It*, http://bitcoinmagazine.com/8640/an-exploration-of-intrinsic-value-what-it-is-why-bitcoin-doesnt-have-it-and-why-bitcoin-does-have-it/

45: The Onion (2010), *U.S. Economy Grinds To Halt As Nation Realizes Money Just A Symbolic, Mutually Shared Illusion*

46: Aristoteles (350 v.C), *Ethica Nicomachea*

47: Plato (360 v.C), *Laws*

48: Dirk Bezemer (2013), *DEBT episode 1: a great invention*, http://www.youtube.com/watch?v=F_7HIxCg4is

49: Wim Boonstra (2012), *Geld scheppen is een fluitje van een cent*

50: Frederick Soddy (1934), *The Role of Money*

51: Charlotte van Dixhoorn (2013), *The Nature of Money*

52: Benes & Kumhoff (2012), *The Chicago Plan Revisited*

53: mkbservicedesk.nl, *Wat zijn de financiële ratio's?*, http://www.mkbservicedesk.nl/2335/wat-zijn-financiele-ratio.htm

54: Frederick Soddy (1926), *Wealth, Virtual Wealth, and Debt*

55: Jackson & Dyson (2013), *Modernizing Money*

56: Github, *Bitcoin*, https://github.com/bitcoin/bitcoin

57: Stefan Molyneux, *The True Value of Bitcoin: What You Really Need To Know*, http://www.youtube.com/watch?v=Cs6F91dFYCs

58: Stackoverflow.com (2013), *Why was 21 million picked as the number of bitcoins to be created?*, http://bitcoin.stackexchange.com/questions/8439/why-was-21-million-picked-as-the-number-of-bitcoins-to-be-created

59: bitcointalk.org (2013), *Why is there only 2,100,000,000,000,000 (2.1 quadrillion) units in BTC?*, https://bitcointalk.org/index.php?topic=137096.0

60: Stackoverflow.com (2013), Why was 21 million picked as the number of bitcoins to be created?, 2013, http://bitcoin.stackexchange.com/questions/8439/why-was-21-million-picked-as-the-number-of-bitcoins-to-be-created/8444#8444

61: ECB, Monetary Aggregates, , http://sdw.ecb.europa.eu/reports.do?node=1000003478

62: Morgen E. Peck (2013), *Bitcoin's Computing Crisis*, http://spectrum.ieee.org/computing/networks/bitcoins-computing-crisis

63: CoinDesk.com (2013), *How do bitcoin transactions work?*, http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

64: Open Bank Project, *home page*, http://openbankproject.com/

65: George Ettinger, *The Island of Stone Bitcoins*, http://letstalkbitcoin.com/the-island-of-stone-bitcoins/#.Uu-MrD15NBI

66: bitcoin.it, *Technical background of version 1 Bitcoin addresses*, https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses

67: bitcoin.it, *Transactions*, https://en.bitcoin.it/wiki/Transactions

68: bitcoin.it, *Change*, https://en.bitcoin.it/wiki/Change

69: Stackoverflow.com (2011), *How would I hand code a Bitcoin transaction*, http://bitcoin.stackexchange.com/questions/808/how-would-i-hand-code-a-bitcoin-transaction

70: bitcoin.it, *Elliptic Curve Digital Signature Algorithm*, https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm

71: Cryptome (2011), *The Bitcoin Lottery*, http://cryptome.org/0004/bitcoin-lottery.htm

72: bitcoin.it, *Protocol Specification*, https://en.bitcoin.it/wiki/Protocol_specification#tx

73: bitcoin.it, *Blocks*, https://en.bitcoin.it/wiki/Blocks

74: bitcoin.it, *Transaction Verification*, https://en.bitcoin.it/wiki/Protocol_specification#Transaction_Verification

75: bitcoin.it, *Block Hashing Algorhythm*, https://en.bitcoin.it/wiki/Block_hashing_algorithm

76: bitcoin.it, *Nonce*, https://en.bitcoin.it/wiki/Nonce

77: J.R.V.A. Dijsselbloem (2013), *Betreft Vragen van het lid Nijboer (PVDA) aan de minister van Financiën over de opkomst van Bitcoin als digitale betaaleenheid*

78: stab.nl, WET OP HET FINANCIEEL TOEZICHT, http://www.st-ab.nl/wetten/1064_Wet_op_het_financieel_toezicht_Wft.htm

79: Arnoud Engelfriet (2013), Inkomsten in Bitcoins zijn gewoon belastbaar

80: Stephen Zarlenga (2003), *Stephen Zarlenga's speech at the U.S. Treasury (Dec. 4, 2003)*

81: DNB, *Binnenlands bankbedrijf (monetair) - Bijdrage van Nederland aan monetaire aggregaten in het eurogebied; niet gecorrigeerd voor securitisaties*, http://www.statistics.dnb.nl/usr/statistics/excel/t5.3nk.xls

82: Brett Scott (2013), *If you want to know what money is, don't ask a banker. Take a leap of faith and start your own currency*

83: Github, *Bitcoin 0.8.6 branch*, https://github.com/bitcoin/bitcoin/commit/03a7d673876dc8fbae876290b455c02b0cac80bd

84: bitcointalk.org (2013), *[ANN] Genesis Block Generator*, https://bitcointalk.org/index.php?topic=181981.0

85: Steve H. Hanke & Nicholas Krus (2013), The Hanke-Krus Hyperinflation Table

86: DNB (2012), *Rapportage Maatschappelijk Overleg Betalingsverkeer 2012*

87: Currence (2012), *Jaarverslag 2012*

88: bitcoin.it, *Scalability*, https://en.bitcoin.it/wiki/Scalability

89: TechCrunch (September 2011), *PayPal Now Processing $315 Million In Payments Per Day*

90: Sompolinsky & Zahar (2013), *Accelerating Bitcoin's Transaction Processing (Fast Money Grows on Trees, Not Chains)*

93: Oleg Andreev (2013), *Economics of block size limit*

94: bitcoin.it, *Transaction Fees*, https://en.bitcoin.it/wiki/Transaction_fees

95: Wikipedia.org, *Tragedy of the Commons*, http://en.wikipedia.org/wiki/Tragedy_of_the_commons

96: Wikipedia.org, *Tragedie van de Meent*, http://nl.wikipedia.org/wiki/Tragedie_van_de_meent

97: bitcointalk.org (2010), *[PATCH] increase block size limit*, https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366

98: bitcointalk.org (2010), *Block size limit automatic adjustment*, https://bitcointalk.org/index.php?topic=1865.msg23226

99: Reddit.com (2013), *Is there a consensus on the blocksize limit issue?*, http://www.reddit.com/r/Bitcoin/comments/1owbpn/is_there_a_consensus_on_the_blocksize_limit_issue/

100: bitcointalk.org (2010), *What will keep transaction fees up?*, https://bitcointalk.org/index.php?topic=1847.0

101: Reddit.com (2013), *Is there a consensus on the blocksize limit issue?*, http://www.reddit.com/r/Bitcoin/comments/1owbpn/is_there_a_consensus_on_the_blocksize_limit_issue/ccwe3s7

102: Reddit.com (2013), *Is there a consensus on the blocksize limit issue?*, http://www.reddit.com/r/Bitcoin/comments/1owbpn/is_there_a_consensus_on_the_blocksize_limit_issue/ccwesbl

103: bitcointalk.org (2011), *[If tx limit is removed] Disturbingly low future difficulty equilibrium*, https://bitcointalk.org/index.php?topic=6284.0

104: Decker & Wattenhofer (2013), *Information propagation in the Bitcoin network*

105: bitcointalk.org (2013), *Re: Once again, what about the scalability issue?*, https://109.201.133.195/index.php?topic=249147.msg2758597#msg2758597

106: Peter Wuille (2013), *Ultraprune: use a pruned-txout-set database for block validation #1677*

107: Peter Wuille (2012), *Pruning in the reference client: ultraprune mode*, https://bitcointalk.org/index.php?topic=91954

108: J.D. Bruce (2013), *Purely P2P Crypto-Currency With Finite Mini-Blockchain*

109: Satoshi Nakamoto (2009), *Re: Bitcoin P2P e-cash paper*

110: SNS, *Juridische informatie - BSN*, http://www.snsbank.nl/zakelijk/over-sns-bank/juridische-informatie/burgerservicenummer.html#

111: wetten.overheid.nl, *Wet identificatie bij dienstverlening (WID)*, http://wetten.overheid.nl/BWBR0028490/geldigheidsdatum_13-12-2011

112: Rijksoverheid (2008), *Identificatie door banken*, http://www.rijksoverheid.nl/nieuws/2008/07/21/identificatie-door-banken.html

113: FIU-Nederland (2008), *Wetgeving algemeen*

114: J Camenisch, S Hohenberger, A Lysyanskaya (2006), *Balancing accountability and privacy using e-cash*

115: Rijksoverheid, *Wat is DigiD?*, http://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-digid.html

116: wetten.overheid.nl, *Afdrukvoorbeeld artikel 16 (WWFT)*, http://wetten.overheid.nl/BWBR0024282/Hoofdstuk3/32/Artikel16/geldigheidsdatum_07-01-2014/afdrukken/redirect_BWBR0024282%252FHoofdstuk3%252F32%252FArtikel16

117: coinvalidation.com, *CoinValidation*, http://www.coinvalidation.com/resources/

118: bitcoin.it, *Some things you need to know*, https://bitcoin.org/en/you-need-to-know

119: bitcointalk.org (2013), *FAQ on the payment protocol*, https://bitcointalk.org/index.php?topic=300809.msg3225143#msg3225143

120: zerocoin.org, *Zerocoin website*, http://zerocoin.org/

121: Matthew Green (2014), *tweet from 8 Januari*

122: Matthew D. Green, Christina Garman, Ian Miers and Aviel D. Rubin (2014), *Bitcoin research is no sop to organized crime [Letter]*, http://www.baltimoresun.com/news/opinion/readersrespond/bs-ed-bitcoin-letter-20131204,0,3966705.story#ixzz2sGj4qfy5

123: Peter Todd (2014), *[Bitcoin-development] Stealth Addresses*, http://sourceforge.net/mailarchive/message.php?msg_id=31813471

124: Chandler Wyatt (2014), *Anonymity Meets Convenience in Bitcoin "Stealth Address" Proposal*, http://coinconsultancy.com/2014/01/16/anonymity-meets-convenience-bitcoin-stealth-address-proposal/

125: Incasso/machtigen, *Ontvangen van betalingen met behulp van Incasso*, http://www.incassomachtigen.nl/Zakelijk/Incassoaccepteren/Pages/default.aspx

126: bitcoin.it, *Contracts*, https://en.bitcoin.it/wiki/Contracts

127: bitcoin.it, *Smart Contracts*, http://en.wikipedia.org/wiki/Smart_contract

128: Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, http://szabo.best.vwh.net/formalize.html

129: schuldinfo.nl, *Incassokosten*, http://schuldinfo.nl/?id=50

130: bitcoin.cz, *BitcoinCZ - Slush's Pool*, http://mining.bitcoin.cz/

131: bitcoin.it, *P2Pool*, https://en.bitcoin.it/wiki/P2Pool

132: bitcointalk.org, *Re: [If tx limit is removed] Disturbingly low future difficulty equilibrium - bericht 95264*, , https://bitcointalk.org/index.php?topic=6284.msg95264#msg95264

133: litecoin.info, *Litecoin homepage*, https://litecoin.info/Litecoin

134: bitcointalk.org, *CoinJoin: Bitcoin privacy for the real world*, https://bitcointalk.org/index.php?topic=279249.0

135: bitcointalk.org, *Zerocoin when?*, https://bitcointalk.org/index.php?topic=216982.msg2279321#msg2279321

Tot slot zou ik nog enkelen willen bedanken zonder wiens hulp dit niet gelukt zou zijn:

SNS

Gerald Lankamp (sr. Architect)

Marinus Bier (sr. Architect)

Johan van der Sman (systeemarchitect Cards-keten)

Bonne van Dijk (sr. Architect)

ING

Arjen Heida

Marnix den Otter

Rabobank

Harrie Vollaard

ABN-Amro

Floris Kleemans

Universiteit Utrecht

Gerard Tel

Marco Spruit

9. Bijlage(n)

9.1 The Island of Stone Bitcoins

(...) Bitcoin does not lend itself to casual explanation or to convenient metaphor. In fact, very few comparisons even suit it! It's a currency but it works like a commodity. It's mined in limited quantities, so… it's almost like gold! …except it's created at an exact, fixed rate and will end at an exact, fixed point. So, not like gold. The work of 'mining' doesn't really 'accomplish' anything, either. Bitcoin is a trainwreck of anachronisms to have to dump on any unsuspecting novice, and horrible pseudo-words like 'blockchain' and 'hashcash' just make it sound more like a scam.

(...) I made mention of a story that helped to finally introduce me to the world of Bitcoin, and the more I've learned the more apt the story has become. There is a strong allegory for Bitcoin in a currency that has already been used before. That currency is hundreds of years old, and there isn't anything else quite like it. Off in the Pacific Ocean, among the Caroline Islands, is a particular trio of small islands known together as the Island of Yap. Its native residents form several communities among the islands and number in the thousands. (...) Yap was lush in vegetation and fairly sustainable but had no precious metals or minerals to be found. So, for function of currency they made stone coins. The people of Yap, keen on not half-assing this 'coin' thing, decided to go big AND to go home. They sailed up to four hundred miles to other islands with vast limestone quarries so that they could carve out enormous stone discs three to twelve feet in diameter, wheel them over to rafts, and sail them back to Yap. The men who carved the stone rolled it into a convenient place (even if it took a dozen extra hands to do so) and it was ready for trade. After they 'mined' and moved the coin, its journey really was done. When time came for a large trade, something on par with livestock or a dowry, the coin changed hands. By 'changed hands' I mean the two involved parties loudly and publicly declared that this particular coin here was now property of so-and-so, and proceeded to leave it right where it was. Nobody could be arsed to move the bloody things. They were massive, and the community was tight-knit; so why bother? So generations passed and the stones never moved. Tallies were never marked or recorded on the stones- it wasn't necessary. Business was conducted and announced publicly, and the rightful owner of any given stone was common knowledge to anyone living near it. So these stone coins weren't traditional "coins." You could not fit them in the pockets of anything but the most clownly of pants. You did not even put them in a vault for safekeeping. They simply existed, and the community kept the knowledge of who owned which

at any given time. (...) For at least three generations, there was a particular family in a particular home whose wealth was well-known across the islands. The family had long been owners of what might have been one of the biggest stone coins in circulation … and not one person on those islands had ever seen it. Those aforementioned generations earlier, this enormous coin was carved out and loaded up for transport by an expedition of incredibly ambitious Yap residents. Their prodigious haul slipped from import manifests and into mytho-history when a harsh storm battered their rafts just a little ways from home shores. The raft carrying King Coin (...) was cut loose, and their newfound wealth plummeted to the seafloor. In a boring, physicality-obsessed, fiat economy, this would be the tragic end of an otherwise uplifting tale of heroic (and Homeric) avarice. (...) The people of Yap, however, didn't see what the fuss was about. The men of the expedition all vouched for the proportions of the coin and its general location. Adding to this the fact that it was 'lost' only in the tangible sense and not in the fiscal one, there was no reason not to go on using it. After all, they lost their millions to a storm, not to the craps table. Just like "that coin between those two trees," or "that coin next to Jim's house," (...) this coin entered circulation based on reputation. It was "that coin at the bottom of the ocean," and this family had clutched it for years before spending it on God-knows-what. The stone coins already existed in a decentralized, community-enforced 'ledger.' By this precedent, they no longer needed even to be tactile objects. Stone coins were simply a unit on the Stonecoin Blockchain, tracked by group-verified transactions. With only so many coins in circulation, the community kept fairly consistent tabs on who owned what. Whether or not Yap investors lived in fear of a 51% attack is beyond the scope of this allegory; the point itself should be abundantly clear by now … the point is that the stone coins are an allegory for Bitcoin. (...)
Ownership was a matter of public declaration. By spreading the word to others, it became verification. You didn't own currency unless you got the majority of the community to agree you did. You did this by conducting your business transparently, and announcing all transactions to the world at large. A deal made in secret or made dishonestly was impossible; transparency was part of the protocol. Bitcoin and stone coin changed hands almost identically. Whether limestone or crypto, these aren't the typical 'coins' one rustles from sofa cushions or the pockets of your playground extortion victims. We don't lay eyes on these coins- we just all agree on where they are and who they belong to. All our Bitcoins are on the metaphorical ocean floor, safely away from prying eyes and sticky fingers, and every member of the community is sitting on a hard copy of the ledger. We don't simply 'trust,' however- our ledger is produced, updated, and thoroughly encrypted by the same software protocol that makes it possible. Prying eyes

aren't left totally in the dark, either; the same blockchain that tracks this ledger is protected from being altered, but is visible to any who want to see what coins have moved where. What Yap enforced by culture we enforce by encryption (...). Its these traits that made their stones and our bitcoins commodities instead of reserve notes; false value could not be simply printed off a press. Bitcoins and stone coins weren't empty promises generated on a whim. They are the product of investment, whether its time spent sailing or time spent mining a processor. The story of Yap, the stone coins, and the system they used is a great teaching tool, certainly- but it's not just for the outsiders. See, the story of stone money doesn't simply end there; all of us within the community can learn from what happened to Yap's stone coins when the Tax Man came calling. After Germany got over the novelty of having their own tiny preindustrial island, it decided to move in and get unpacking. They mercifully weren't insistent on displacing or bothering the native culture too much, but they wanted room for military stations around the islands and needed the infrastructure to connect them. The simple gravel walking trails connecting all of Yap's villages were awesome for bare feet and batcave-sized novelty coins, but were less than ideal for German road vehicles. The German government sent word out to all the village leaders that wider, modern stone roads needed to be implemented across the islands. It isn't in doubt whether or not the elders got the message- it just seems unlikely that any of them gave a damn what their absentee foreign overlords wanted. There was very little incentive to appease these strangers, and months upon months went by without any sign of the tropical expressway the military was looking for. German officials, recognizing that no progress was being made, resorted to other means of motivating the locals. (...) A few officials went around the Island, spray-painting sizable black X's on the biggest stone coins they could find. They then proclaimed, for all to hear, that these stones were now confiscated funds of the German government. The people of Yap had been fined. Durable, modern-sized roads appeared in very, very short order. Upon completion, friendly German officials were dispatched once again- this time with solvents to clean the marks off the stones. The levied fines had been refunded.

The people of Yap were manipulated, of course- but was their money manipulated, or was their belief? The Germans never took a thing away from the residents of the Island; they simply preyed on the peoples' willingness to play by their rules. In their graciousness to be part of the larger world their European 'masters' presented, the people of Yap mistakenly believed that those paint-wielding officials' rules held real power over them. Forgetting that they themselves -the community- held power over their money, they let the ILLUSION of authority give a few bureaucrats REAL authority. (...)