Naar een nieuw monetair systeem met nieuw monetair beleid

Kees van Hee
Jacob Wijngaard

WHITE PAPER

Vaart-Dommel-Rotte Collectief, november 2016

Naar een nieuw monetair systeem met nieuw monetair beleid

Kees van Hee

Jacob Wijngaard

Inhoud

Voorwoord

Naast een gezamenlijke achtergrond als promovendi aan de Technische Universiteit Eindhoven, op het gebied van de stochastische beslissingstheorie, delen we belangstelling voor monetaire economie. Bij de één is die ontstaan via consultancy voor financiële instellingen en bij de ander via supply chain finance en betrokkenheid bij STRO, de stichting in Utrecht die zich bezig houdt met complementair geld.
Die interesse zou nooit tot meer geleid hebben dan wat hemelbestorming tijdens de borrel als de financiële crisis zich niet had voorgedaan. Zo'n crisis is uitdagend. Voldoende uitdagend om de aarzeling te overwinnen die ook wij als wetenschappers hebben om ons met een ander gebied dan het onze te bemoeien. Vandaar dit white paper over een nieuw monetair systeem met nieuw monetair beleid. Dat we geen economen zijn willen we hier graag nog een keer benadrukken en is ook te zien aan de beperkte inbedding in de literatuur.
De economische wetenschap is vooral gericht op het verklaren en voorspellen van economische verschijnselen. Wij hebben een duidelijke ontwerpers attitude. Hoewel wij niet denken dat de wereld maakbaar is denken we wel dat een goed monetair systeem maakbaar is.

Het uitwerken van onze voorstellen vereist nog heel wat werk en natuurlijk veel politieke besluitvorming. Wij denken dat het echt anders kan en moet. Hopelijk leidt dit white paper tot de exploratie van nieuwe mogelijkheden.

Kees van Hee en Jacob Wijngaard

Het derde lid van het "collectief" werd node gemist. We dragen daarom het stuk op aan onze vriend en oud-collega Jo van Nunen. Hij zou zeker aan dit stuk hebben meegewerkt als hij het had mogen beleven

Naar een nieuw monetair systeem met nieuw monetair beleid

Kees van Hee en Jacob Wijngaard

1 Inleiding

Sinds de financiële crisis is er een heftig debat los gebarsten over de rol van banken in het financiële en monetaire systeem. Kunnen banken niet te gemakkelijk geld scheppen? Werken banken per definitie felle schommelingen in de economie in de hand? Zijn de banken "schuldig" aan de hoge schuldenlast in de particuliere sector? Is het niet beter het scheppen van geld over te laten aan de overheid? Deze vragen zijn door de Stichting Ons Geld, gesteund door een voldoende groot deel van de Nederlandse burgers, ook voorgelegd aan de Tweede Kamer. Die heeft de minister gevraagd zich daarover nader te informeren. Daar heeft de minister de WRR bij betrokken. Deze notitie is bedoeld om bij te dragen aan dit debat.

Wij hebben thans een mengsel van *chartaal* geld (munten en bankbiljetten) en *giraal* geld (digitale tegoeden bij banken). Het chartale geld maakt deel uit van het *basisgeld*. (*base money*[1]). Het andere basisgeld is digitaal en onzichtbaar voor burgers en bedrijven. Het omvat de *reserves* van (commerciële) banken en van de overheid bij de Centrale Bank (CB). Het geld op een rekeningcourant, het *banktegoed,* is (slechts) een *claim* op basisgeld. Zo'n claim wordt wel door ieder geaccepteerd. Omdat men meer en meer gebruik maakt van dit girale geld, wordt een claim minder en minder vaak geëffectueerd (in cash omgezet). Dat geeft de banken steeds meer vrijheid met betrekking tot het scheppen van nieuw geld. Daarbij speelt ook dat de CB de banken helpt via het verstrekken van basisgeld als dat toch nodig blijkt te zijn.

Het meest fundamentele element van het debat betreft de vraag of we de banktegoeden als betaalmiddel moeten blijven gebruiken. In plaats daarvan kun je burgers en bedrijven ook toegang geven tot het basisgeld en alleen dat geld als betaalmiddel faciliteren. De voorstellen van Positive Money in de UK en van het Burgerinitiatief Ons Geld komen hier op neer. Deze notitie sluit daar op hoofdpunten bij aan.

[1] Zie bijvoorbeeld Ryan-Collins, Greenham, Werner and Jackson, "Where does Money come from", NEF, 2011

Wij stellen drie fundamentele veranderingen voor: (1) de keuze voor basisgeld als enig wettig betaalmiddel en afschaffing van chartaal geld, (2) een nieuw betalingssysteem en (3) het monetair beleid aanpassen.

De eerste verandering betreft de afschaffing van betalen met banktegoeden en de afschaffing chartaal geld. Dit voorkomt het bestaan van zwart geld en dus ook ten dele belastingontduiking. De tweede verandering betreft het faciliteren van betalingen. In het huidige systeem wordt dat logischerwijs door de banken gedaan, omdat het om claims op de banken gaat. Als basisgeld het betaalmiddel wordt, is dat niet meer zo. Dan ligt meest voor de hand dat er een centrale, aan de CB gerelateerde instantie is die dat regelt. In Paragraaf 3 komt dit aan de orde. In de derde plaats leidt basisgeld als betaalmiddel tot een heel ander monetair beleid. Dat komt aan de orde in Paragraaf 4. In Paragraaf 5 gaan we in op de transitie van het huidige stelsel naar het nieuwe.

Voor we met deze drie veranderingen aan de gang gaan, wordt in Paragraaf 2 een wat bredere reflectie gegeven op de problematiek. Waarom er toch werkelijk wel een groot probleem is, ons perspectief daarop en hoe wij positie kiezen wat betreft mogelijke oplossingen. In Paragraaf 6 geven we conclusies en aanbevelingen.

2 Waarom het huidige financiële systeem aan revisie toe is

Na de Tweede Wereldoorlog is een tijd lang het akkoord van Bretton Woods gevolgd. Daarbij werden vaste wisselkoersen voorzien. En alleen de dollar kon ingewisseld worden tegen goud. Er was toen dus nog een (indirecte) verbinding met werkelijke waarde. Dat ging goed zolang het vertrouwen er was dat dollars inderdaad ingewisseld konden worden tegen goud. Toen de Amerikaanse overheid, o.a. in verband met de Vietnam oorlog, nogal royaal extra dollars ging scheppen, verdween dat. Centrale banken buiten de VS gingen werkelijk goud claimen en het systeem verviel. Sinds die tijd (1971) is de hoogste vorm van geld in een land het geld dat de CB heeft uitgegeven: chartaal geld en reserves van banken en overheid bij de CB. De CB is de bankier van de banken en van de centrale overheid. Die hebben dus reserves bij de CB. Dat totaal van chartaal geld en reserves wordt wel de *monetary base* genoemd. De monetary base bestaat uit *base money*. Wij zullen spreken van *basisgeld*.

Wij betalen elkaar in de regel niet met basisgeld, maar met banktegoed. Een banktegoed is een claim op basisgeld. Het alternatief voor betalen met een banktegoed is het gebruik van cash. Maar dat gebruik neemt af, althans relatief. Men gebruikt het vooral nog voor kleine uitgaven[2]. En een behoorlijk, maar redelijk stabiel deel ervan wordt opgepot. De behoefte aan cash is al met al zo klein dat de banken gemakkelijk claims kunnen creëren zonder dat er basisgeld tegenover staat. Ze hoeven niet bang te zijn voor het massaal cashen van die claims.

Bij betalingen van burgers of bedrijven binnen dezelfde bank is er geen effect op de reserves van die bank bij de CB. Bij een transactie van burgers of bedrijven die bij een verschillende bank hun tegoeden hebben, wordt het banktegoed van de één verhoogd en het banktegoed van de ander met hetzelfde bedrag verlaagd. En tussen de banken vindt ook precies zo'n overdracht plaats van hetzelfde bedrag. De banken hebben onderling rekeningen lopen: de banken hebben een schuld of tegoed bij elkaar. Op gezette tijden vereffenen de banken hun onderlinge rekeningen: *clearing* (het vaststellen wat er overgedragen moet worden) en *settlement* (het feitelijk overdragen van reserves bij de CB van de ene bank naar de andere). Dat kan op zich problematisch zijn voor een bank, maar er zijn allerhande manieren om de reserves aan te vullen: onderling lenen of lenen van de CB.

Ook de CB is er op gericht om het betalingsverkeer ongestoord te laten verlopen. Eventuele tekorten aan reserves kunnen door de CB aangevuld worden. Dat geldt ook als de betalingen het gevolg zijn van verstrekte kredieten. Als een bank een goede mogelijkheid ziet om een krediet te verstrekken, zal ze dat gewoon doen. Eventuele problemen met betrekking tot

[2] Zie bijvoorbeeld het "Cash Report 2016, Europe", G4S, 2016

betalingen aan andere banken worden opgelost. De beslissing om krediet te geven en zo geld te scheppen, wordt genomen door de banken, samen met de krediet nemers. Banken kunnen burgers en bedrijven geld (claims op basis geld) ter beschikking stellen zonder dat daar basisgeld tegenover staat. Er zijn wel spelregels met betrekking tot reserves en liquiditeit in het algemeen (Basel I, II en III). Maar de beoordeling van de verschillende categorieën van assets is niet altijd helder en de geldigheid van de opeenvolgende reeks van Basel regels is niet altijd duidelijk[3]. Daardoor hebben de banken feitelijk een grote vrijheid in het scheppen van geld: de claims die daarmee weg gegeven worden bijna nooit geclaimd (gecasht).

Banktegoeden zijn dus een merkwaardige vorm van geld. Niettemin, vanaf 1971, na de opheffing van Bretton Woods heeft het een tijd lang goed gefunctioneerd. Met het aanpassen van de rente voor het lenen van bankreserves werd de beschikbaarheid van kredieten gestuurd en zo de hele economie. En gedurende de periode 1985 – 2005 leek men dat sturen aardig onder de knie te krijgen. Die periode wordt daarom wel “the great moderation” genoemd. Inmiddels echter zijn er, vooral vanwege de financiële crisis, ernstige twijfels gerezen. Het is duidelijk dat de banken bij het ontstaan van die crisis een grote rol gespeeld hebben. Met name via overkreditering van de Amerikaanse huizenmarkt. In combinatie met te ingewikkelde financiële producten, die ten koste gingen van de transparantie van markten en producten.[4] En de structurele vrijheid van de banken die hoort bij het huidige monetaire systeem wordt daarbij vaak als diepere oorzaak gezien. Er worden allerlei oplossingen aanbevolen. Hogere eisen wat betreft liquiditeit en solvabiliteit[5], beter toezicht, narrow banking (banken die zich concentreren op de activiteiten rond betalen en sparen en die slechts uitlenen voor zover dat volledig en veilig gegarandeerd kan worden) [6].

De Positive Money beweging (PM) geeft de meest fundamentele en heldere aanbeveling[7]. Hun advies houdt in dat het basisgeld ook beschikbaar komt voor burgers en bedrijven en dat er niet meer vrijelijk gehandeld kan worden in claims op basisgeld. Basisgeld wordt het enige wettige betaalmiddel in de hele economie. Banken kunnen dus geen geld meer scheppen. Banken kunnen alleen geld uitlenen leningen afsluiten als ze basisgeld beschikbaar hebben. Ze kunnen wel basisgeld lenen van de CB. Dus de enige geldscheppende instantie is de CB Het voorstel sluit aan bij het veel oudere Chicago plan[8]. Daarbij ging het om *full reserve banking.* Daarbij zijn het per definitie nog banken die het geld beschikbaar stellen, maar er moet wel 100% dekking

[3] Zie bijvoorbeeld Admati and Hellwig, “The Bankers New Clothes”, Princeton University Press, 2013
[4] Zie bijvoorbeeld Roubini and Mihm, “Crisis Economics”, Penguin Books, 2010
[5] Zie bijvoorbeeld Admati andHellwig, “The Bankers New Clothes”, Princeton University Press, 2013
[6] Zie bijvoorbeeld Kay, Narrow Banking; The Reform of Banking Regulation, Centre for the Study of Financial Innovation, 2009
[7] Zie Jackson en Dyson, “Modernising Money”, Positive Money, 2012
[8] Fisher, I. “100% Money and the Public debt” Economic Forum, Spring Number, April-June 1936, 406-420.

met basisgeld zijn[9]. PM trekt terecht de conclusie dat het dan logischer en helderder is om iedereen maar met basisgeld te laten betalen. Ze gaan er nog wel van uit dat banken de betreffende rekeningen faciliteren, maar dat is niet meer per definitie zo. In Nederland is het initiatief overgenomen door het Burgerinitiatief Ons Geld. Dat burgerinitiatief heeft uiteindelijk geleid tot het verzoek van de minister van Financiën aan de WRR om een advies te geven over de wenselijkheden en mogelijkheden m.b.t. geldschepping.

De voorstellen van PM zijn voor ons een belangrijk referentiepunt in deze notitie. Daarom is het belangrijk de pro's en contra's van PM, vergeleken met het huidige systeem nog eens goed op een rijtje te zetten. Daarbij helpt het recente special issue van De Cambridge Journal of Economics[10]. Dat is helemaal gewijd aan alternatieve monetaire systemen, met daarin ook veel aandacht voor PM.

Instabiliteit is het belangrijkste argument van PM. Dat wordt nog een keer bevestigd in de bijdrage van PM in genoemd special issue[11]. Het belangrijkste product van banken zijn leningen. Die verkopen ze graag. Echter, te gemakkelijk krediet verlenen leidt tot overwaardering van de betrokken assets. En tot nieuwe kredieten. Tot die vicieuze cirkel een keer breekt. Competitie en fancy financiële producten verergeren die instabiliteit: het gaat er niet meer om of de bank vertrouwen heeft in een bepaald financieel product, zolang de potentiele klant er maar vertrouwen in heeft. Het deposito garantiestelsel geeft nog een zetje in dezelfde richting: doe maar, als puntje bij het paaltje komt, is er wel soelaas. Die neiging tot instabiliteit wordt ook niet echt omstreden door de criticasters. Wel wat vergoelijkt. Er wordt aangegeven dat er allerhande maatregelen mogelijk zijn om instabiliteit te reduceren en er wordt op gewezen dat er ook bij toepassing van PM nog wel instabiliteit zal zijn. Allemaal argumenten die we hier niet willen bestrijden. Maar ze tellen pas als er belangrijke bezwaren tegen PM in te brengen zijn.

De twee belangrijkste bezwaren die genoemd worden zijn:

- Vermenging van fiscaal beleid en monetair beleid
- Te inflexibele kredietverlening

Het eerste bezwaar is zonder meer terecht. In de PM voorstellen wordt tamelijk gemakkelijk gesuggereerd het scheppen van geld ook te gebruiken om overheidsuitgaven te bekostigen. En dat kun je beter niet doen. De overheid heeft velerlei functies. Eén daarvan is het faciliteren van een goed monetair systeem. Die functie is belangrijk, hoe je verder ook denkt over de rol van

[9] Dat plan was al afgestoft door Benes and Kumhof, "The Chicago Plan Revisited" IMF, 2012
[10] Cambridge Journal of Economics, 2016, **40**
[11] Dyson, Hodgson and Van Lerven, "A response to Critiques of 'Full Reserve Banking'", Cambridge Journal of Economics, 2016, **40**, 1351 - 1361

de overheid. Die functie moet je dus zo goed mogelijk regelen, onafhankelijk van verdere beslissingen inzake de rol van de overheid. Dan moet je het scheppen van geld dat eventueel nodig is voor het functioneren van het monetaire systeem niet gebruiken om overheidsuitgaven te faciliteren die anders niet mogelijk zouden zijn. In de PM voorstellen gebeurt dat wel, maar het positive money concept als zodanig impliceert die koppeling niet[12]. Positive money kan best gecombineerd worden met een strakke splitsing van monetair beleid en fiscaal beleid. Je kunt bijvoorbeeld bepalen dat als er nieuw geld geschapen wordt, het effect daarvan op de overheidsbegroting gecompenseerd wordt. Bij voorbeeld via een korting op de BTW. Of te eisen dat het overheidstekort kleiner, respectievelijk het overheidsoverschot groter moet worden. In feite is dit bezwaar dus niet een bezwaar tegen positive money, maar alleen tegen een bepaalde wijze van uitwerking ervan.

Het tweede bezwaar is misschien terecht. Het gaat terug op een publicatie van Schumpeter, die kredietverlening van banken koppelt aan innovatie[13]. De noodzakelijke flexibiliteit die daarvoor nodig is, stelt hij, is alleen beschikbaar via het creëren van nieuw geld door banken, gesteund door de mogelijkheid basisgeld te lenen van de CB. Dyson c.s. stellen daar tegenover dat ook in het PM voorstel, banken basisgeld kunnen lenen van de CB en op die manier nieuw geld in de economie kunnen pompen en dat het PM voorstel wat dat betreft dus niet minder flexibel hoeft te zijn. De monetaire autoriteit die daarover gaat, moet daar dan wel weer beperkingen aan opleggen, dat het alleen voor productieve doeleinden is[14]. Onze observatie daarbij is dat als die beperkingen gemakkelijk te omzeilen zijn, de banken weer net zoveel vrijheid hebben als in het huidige systeem en dan is het de vraag of de overgang de moeite waard is. Als de beperkingen hard zijn, zou het toch kunnen dat overgang naar PM ten koste gaat van belangrijke kredietflexibiliteit.

De conclusie is dat positive money een interessant monetair concept is. Maar dat het belangrijk is bij de uitwerking ervan strak de hand te houden aan de fiscale neutraliteit ervan. En dat nader bekeken moet worden of er wel voldoende flexibiliteit van kredietverlening is. Gedetailleerde monetaire regels m.b.t. waar banken wel voor kunnen lenen (van de CB) en waar niet, zijn ongeschikt. Hoe robuuster de monetaire regels zijn, ook de regels voor het lenen van basisgeld door banken, hoe beter dat is. Die nadere uitwerking gebeurt in de volgende twee paragrafen.

---

[12] In die zin verschilt het principieel van MMT (Modern Monetary Theory). Daarin is functional finance essentieel. Dat wil zeggen dat er geld gecreëerd wordt door de CB, namens de staat, ten behoeve van vooral de werkgelegenheid. Zie bijvoorbeeld Juniper en Mitchell, “There is no financial crisis so deep that cannot be dealt with by public spending”, University of Newcastle, Australia, 2008.

[13] Schumpeter, “The Theory of Economic Development”, Harvard University Press, 1912 [1934]

[14] Zie Dyson, Hodgson and Van Lerven, “A response to Critiques of ‘Full Reserve Banking’”, Cambridge Journal of Economics, 2016, **40**, 1351 - 1361.

Daarbij gaan we uit van een monetaire zone, een land of de eurozone, waarbinnen monetair beleid geldt. De structuur van opslag en transport van basisgeld wordt behandeld in de volgende paragraaf. In de PM voorstellen wordt er van uitgegaan dat het betalen gefaciliteerd wordt door de banken. Dat laten we vallen. We gaan er vanuit dat de kern daarvan gefaciliteerd wordt door een overheidsorganisatie. Het is een nieuw, digitaal geldsysteem dat zich beperkt tot het bewaren en overdragen van basisgeld. Aan dit systeem kunnen allerlei functies worden toegevoegd, zowel in de private sfeer als voor monetair beleid.

In Paragraaf 4 gaan we in op het monetaire beleid. Door het koppelen van de basisgeld bedragen op de betaalrekeningen aan het (nominale) BBP, in combinatie met een belasting erop, kan de inflatie absoluut beheerst worden. Het PM voorstel veronderstelt een nogal activistische monetaire autoriteit, die bovenop het economische gebeuren zit en die zo ook de inflatie binnen de perken wil houden. Dat wordt op deze manier rustiger en afstandelijker.

In beide paragrafen houden we geen rekening meer met het bestaan van cash. In het PM voorstel hoort cash nog bij basisgeld, net als in het huidige systeem. We stellen voor dat los te laten en binnen het monetaire systeem ook geen alternatieve vormen van cash te ontwerpen, maar *cashless* te gaan werken. De voordelen van cashless (veiligheid, minder zwart geld, etc.) zijn sowieso al groot, ook in het huidige systeem. In Paragraaf 5, waar ingegaan wordt op transitie naar het door ons voorgestelde systeem, wordt ook aandacht besteed aan de complicaties van overgang naar cashless.

3 Monetair Systeem

In deze paragraaf gaat het met name over opslag en transport van basisgeld. Deze basisfuncties vormen de infrastructuur voor het hele monetaire systeem. In tegenstelling tot het huidige systeem, ligt nu niet meer voor de hand dat opslag en transport geregeld worden door de banken. Het gaat nu om basisgeld rekeningen die onafhankelijk van de banken bestaan. De benadering van Kay[15] spreekt ons aan. Het beschikbaar stellen van deze infrastructuur is een nutsfunctie, zo cruciaal. dat de overheid er een enorme controle op zou moeten zetten wat betreft beschikbaarheid, prijs, veiligheid en kwaliteit. Daarom is het efficiënter als de overheid deze functies zelf gaat vervullen of overlaat aan een door de staat gecontroleerde autoriteit. Er kan dan ook meer snelheid en veiligheid gerealiseerd worden[16]. Banken spelen wel een rol, maar staan eerder naast de andere rekeninghouders dan tussen rekeninghouders en CB. Als de infrastructuur eenmaal goed geregeld is, is er natuurlijk alle ruime voor banken en andere private organisaties om daar omheen een schil van financiële services aan te bieden.

De belangrijkste actoren in het monetaire systeem zijn:

- Centrale bank
- Houders van *A-accounts* (*betaalrekeningen)*
- Banken

Daarnaast is er de centrale, administratieve actor die we het Monetair Systeem (afgekort tot MS) zullen noemen. De CB creëert het basisgeld. Het komt op de één of andere manier terecht op de betaalrekeningen van de economische actoren in de monetaire zone die het betreft. De hoeveelheid basisgeld op een betaalrekening is altijd positief. Je kunt niet meer betalen dan er beschikbaar is. Overheden hebben ook betaalrekeningen en ook daarvoor geldt dat ze niet negatief kunnen staan. Banken hebben voor hun eigen huishouding ook zulke betaalrekeningen. Economische actoren die basisgeld voor een bepaalde termijn “over” hebben, kunnen dat uitlenen aan een bank. De contracten daarvoor zullen in de regel een termijn en een vergoeding (rente) bepalen. De administratie ervan wordt door de banken zelf bijgehouden. PM gebruikt daarvoor de term *investment account*. Het basisgeld wordt overgemaakt op een *B-account*. Die B-account komt overeen met de *investment pool* van PM. Vanuit die B-account kan basisgeld geleend worden aan alle (A-)rekeninghouders Het kan nodig zijn om meer flexibiliteit m.b.t kredietverlening te realiseren (het “Schumpeter-argument”, zie vorige paragraaf). Daartoe is er voor banken de mogelijkheid om basisgeld te lenen van de CB.

[15] Zie Kay,: “Narrow Banking; The Reform of Banking Regulation”, Centre for the Study of Financial Innovation, 2009

[16] Het is in dit verband interessant op te merken dat het eerste girale systeem in Nederland een staatsbedrijf was, nl. de Postcheque en Girodienst.

Daarvoor hebben de banken de *C-account* bij de CB. Het geleende bedrag wordt overgemaakt van de C-account naar de B-account van de bank. Het bedrag aan basisgeld op de C-account is dus altijd *negatief.* Het totaal aan basisgeld op alle rekeningen (A, B en C) blijft dus *constant* bij overboeking van de ene rekening naar de andere, wat voor overboeking dan ook.

Dat het beschikbaar stellen van de infrastructuur van opslag en transport van basisgeld, en dus met name het faciliteren en beheren van betaalrekeningen, een taak van de overheid wordt, hoeft niet te impliceren dat die overheid een "vertrouwde derde" wordt bij het beheer van de rekeningen. Er zijn allerlei mogelijkheden om via encryptie de informatie die de beheerder van het MS krijgt, te beperken. De keuzen die daarin gemaakt kunnen worden, zullen hierna aan de orde komen.

3.1 Het betalingsverkeer

Iedere actor heeft één of meer betaalrekeningen (accounts), altijd met een niet-negatief bedrag. Elk account heeft een eigen internet adres (url, uniform resource locator). Er is een *asymmetrisch encryptie* systeem geïnstalleerd (zie Appendix 1). Bij elk account hoort een eigen paar van een *secret key* en een *public key.* Alle gegevens van een account zijn versleuteld met de secret key van de eigenaar en kunnen dus niet gemanipuleerd worden door de beheerders of eventuele hackers. Wel kunnen de beheerder en dus ook hackers, met de public key de informatie in het account zien.
Het MS houdt twee soorten *records* bij: (1) *saldo-records* en (2) *transactie-records*:

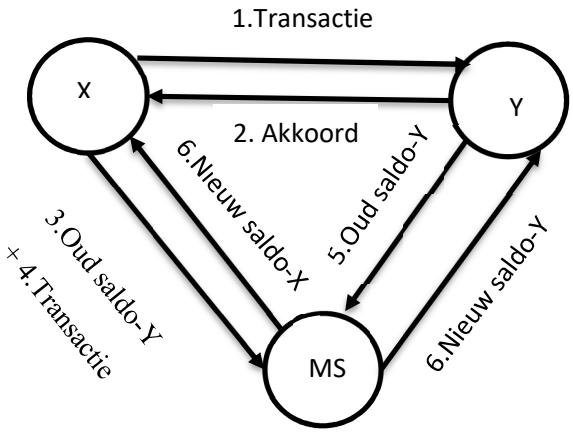
- Saldo-record: [acnr: X, saldo: A, vlgnr: M, $S_{MS}(X,A,M)$]
- Transactie-record: [van: X, bedrag: B, naar :Y, trnr:N, $S_X(X,B,Y,N)$]

Een record wordt hier tussen […] geplaatst en een record bevat velden gescheiden door komma's. De meeste velden hebben een attribuut en een waarde, gescheiden door een ':'. De laatste velden hebben alleen een waarde. Het attribuut acnr is het accountnummer van een actor, vlgnr het volgnummer van updates bij MS en trnr het transactie-volgnummer van het account dat betaalt. Hier zijn X en Y accounts van actoren. De velden aangeduid met $S_{MS}(X,A,M)$ en met $S_X(X,B,Y,N)$ zijn met de secret key van MS respectievelijk X, versleutelde waarden van de er voor vermelde waarden. Ze zijn met de public keys te lezen, maar niet te veranderen. Het doel is de rest van het record te beschermen tegen manipulatie: een kwaadwillende kan bijvoorbeeld in een saldo record X, A en M veranderen, maar alleen het MS kan $S_{MS}(X,A,M)$ veranderen dus als een actor vals speelt is dat in het record te zien. Er zijn natuurlijk variaties op deze record structuur mogelijk, maar die komen in essentie op hetzelfde neer.
De saldorecords geven dus de opeenvolgende saldi van het account aan. De transactierecords geven de overboekingen aan.
Een actor kan een *overboeking* doen, van maximaal het hele bedrag van het account, naar een ander account, dus ook naar een ander eigen account. Accounts worden dus nooit negatief. De

actoren bieden *transacties* met hun *actuele saldorecord* aan het MS aan en het MS voert de updates uit en stuurt de nieuwe saldo-records terug. Het enige dat het MS echt hoeft te onthouden zijn de actuele volgnummers horend bij de accounts, d.w.z. de volgnummers van saldi die actueel zijn.
Het MS moet de volgnummer updates van de saldi onthouden om te voorkomen dat een actor twee maal hetzelfde saldo record kan aanbieden. In het bitcoin alternatief (zie Appendix 3) is het twee maal uitgeven van dezelfde bitcoin het grote probleem waarvoor men de publieke blockchain heeft bedacht. Onze oplossing is veel simpeler en net zo anoniem. De overige records kunnen bij de actoren zelf opgeslagen worden! In dat minimale geval onthoudt het MS dus alleen de volgnummers van updates van saldi bij en niet de saldi en de transacties zelf en heeft dus geen weet van de geldstromen.

3.2 Protocol voor een standaard overboeking.

We beschrijven het protocol voor een betaling van bedrag B van actor X naar actor Y. Dit is ook referentiepunt voor andere overboekingen in het monetaire systeem.
Eerst moeten X en Y akkoord zijn met de betaling. In onderstaande figuur zien we het protocol in de minimale variant, waarbij de actoren X en Y eerst tot overeenstemming komen en dan beiden hun actuele saldo records naar het MS sturen. De betaler, X, stuurt ook het geaccordeerde transactierecord mee. (Dit is een willekeurige keuze: het zou ook door de ontvanger kunnen gebeuren.) Het MS doet de updates, d.w.z. het MS verlaagt het saldo van X met het bedrag uit het transactierecord en verhoogt het saldo van Y met datzelfde bedrag. Ook verhoogt het MS de volgnummers van de saldi en dan stuurt het MS de saldo records weer terug en onthoudt alleen de volgnummers van deze saldi.



In bovenstaande figuur staan deze acties in een diagram. De nummers geven de volgorde van de stappen aan. (Als twee acties hetzelfde nummer hebben mogen ze tegelijk of in een willekeurige volgorde worden uitgevoerd. Acties 3, 4 en 5 mogen ook in willekeurige volgorde). In Appendix 2 wordt dit protocol in detail beschreven.

Er zijn (dalende) *niveaus van privacy* mogelijk, waarbij het MS steeds meer gaat onthouden van de transacties, maar dan ook meer *service* biedt. Het MS communiceert met de actoren via een application program interface (API) en Internet. Dus kunnen actoren alle mobiele en vaste computersystemen gebruiken.

1. MS onthoudt alleen het laatste saldo-volgnummer van elke actor. Zo wordt voorkomen dat een actor een saldorecord met een hoger saldo opnieuw aanbiedt. Verder houdt MS ook een lijst bij van accountnummers, public keys en url's van de actoren. Actoren hebben hun eigen systemen voor opslag van saldo- en transactierecords en zij maken alleen gebruik van de API voor stappen 4, 5 en 6 van het protocol. Private ondernemingen (bijvoorbeeld banken, betaalinstellingen of administratiekantoren) kunnen dit soort systemen voor actoren opzetten en beheren.
   In deze variant heeft het MS dus alleen te maken met stappen 3 t/m 6 van het protocol.
2. MS onthoudt ook een *hash* (zie Appendix 1) van de *saldo-records* van de actors. Zo kan gecontroleerd worden of de actoren hun saldorecords niet achteraf aanpassen voor boekhoudkundige of fiscale verslaglegging . Actoren kunnen checks opvragen bij het MS.
3. MS onthoudt de saldo-records, bijvoorbeeld in een blockchain (zie Appendix 3). Zo kunnen stappen 3 en 5 van het protocol overgeslagen worden. Actoren hoeven hun saldo niet zelf bij te houden en dit steeds via een API opvragen bij het MS.
4. MS houdt naast de saldorecords ook de transactierecords bij in een blockchain. Zo kan de hele historie gereconstrueerd worden. Actors hoeven in principe zelf geen records meer bij te bij te houden en kunnen alle gegevens nodig voor hun boekhouding middels een API opvragen.
   In deze variant ondersteunt het MS alle stappen van het protocol, maar dit is een big brother variant, wat op zich niet gevaarlijk hoeft te zijn als het MS deze gegevens maar niet aan derden versterkt of zich laat hacken.

We pleiten voor niveau 3 omdat daarmee de actoren meer beschermd zijn tegen verlies en omdat het MS dan goed gebruikt kan worden om het beoogde monetair beleid te realiseren (zie Paragraaf 4).

3.3 Functionaliteit en performance van het MS

In de praktijk zijn er allerlei speciale transacties, zoals de *uitgestelde betaling* en *de doorlopende machtiging.* De eerste doet zich voor bij transacties waar het bedrag nog niet bekend is aan het begin van de transactie, zoals bij tanken of parkeren. Het protocol verschilt dan alleen in de eerste twee stappen van het protocol: het bericht van X naar Y heeft nog geen ingevuld bedrag en het antwoord van Y naar X wel. In de eerste drievarianten gebeurt dit dus buiten het MS om.

Pas als de transactie gereed is wordt deze naar het MS gestuurd. De doorlopende machtiging doet zich voor als er een contract is waarbij partij Y van X mag afboeken, zoals bij nutsbedrijven gebruikelijk is. In dit geval begint het protocol met een bericht van X zonder bedrag en dit wordt, net als bij de uitgesteld betaling gevolgd door een bericht van Y met een bedrag. Maar nu kan Y dit soort berichten onbeperkt blijven sturen, totdat X een bericht stuurt waarmee de machtiging wordt ingetrokken. Ook dit betreft de eerste twee stappen van het protocol en blijft dus bij de eerste drievarianten buiten het MS. In de praktijk van het betalingsverkeer zijn er meer betalingsvarianten. Maar wij zijn er van overtuigd dat deze goed inpasbaar zijn in het voorgestelde MS.

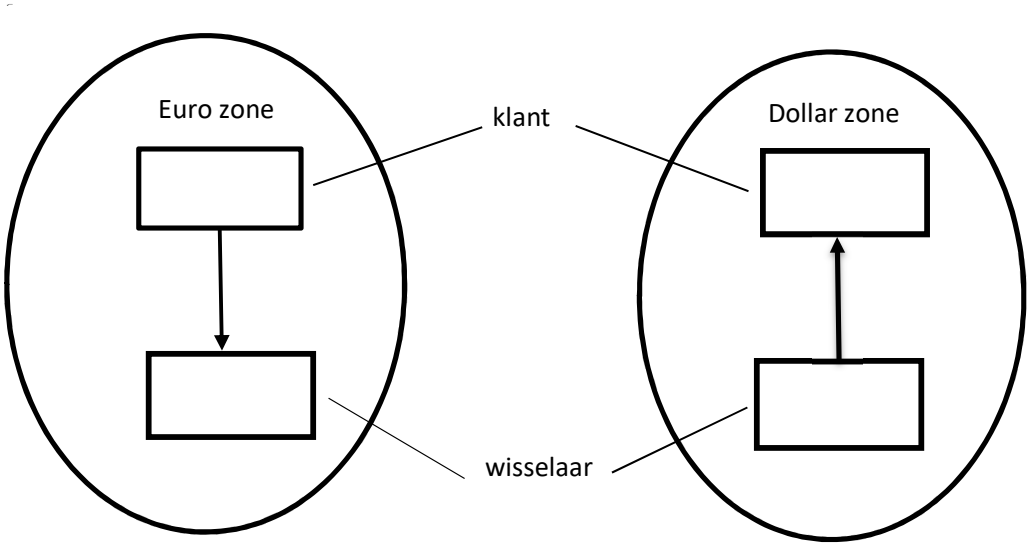
Naast deze transactie gerelateerde functies heeft het MS ook *beheersfuncties*. Bijvoorbeeld voor het aanmaken, samenvoegen, splitsen en verwijderen van accounts. Om de security te verhogen is het nodig de sleutelparen, public en private key van de accounts regelmatig te verversen. Ook hiervoor zijn functies nodig, vergelijkbaar met het huidige DigiD systeem.

Er leven ca 300 miljoen personen in de eurozone, dus met de bedrijven en instellingen er bij is 1 à 2 miljard een goede schatting voor het aantal accounts. Voor andere zones zal het vergelijkbaar zijn. Met een totale opslag van een paar MB per account heeft de infrastructuur een opslagcapaciteit nodig van 1 Peta Byte. De hoeveelheid computertijd per transactie is klein (tienden van een seconde): de gegevens per account moeten opgezocht worden (de public key en het saldo volgnummer en het saldo-record bij de laatste twee varianten). Het rekenwerk bestaat uit het ontcijferen en versleutelen van de berichten en daartussen de minieme berekeningen voor de update van het saldo. Het is heel goed mogelijk om deze services door een gedistribueerd netwerk van servers (cloud) van het MS te laten uitvoeren. Denk hierbij aan 100 tot 1000 servers voor de euro zone. Eén van de mogelijke oplossingen is die waarbij de accounts over de servers verdeeld zijn en de transactie bij de server van de betaler wordt uitgevoerd. De server waar de betaler geregistreerd is vraagt dan het saldo-record bij de server van de ontvanger op en stuurt de geupdate versie terug. Met *load balancing* worden de accounts zo verdeeld dat elke server van het MS ongeveer even veel werk krijgt. Hierdoor is het systeem heel goed schaalbaar en zullen er geen performance belemmeringen zijn. Uit veiligheidsoverwegingen is het verstandig dat de gegevens van elk account op één server beheerd worden, terwijl op een groot aantal andere servers steeds de actuele kopie van het saldo-record wordt bewaard. Zo is de kans dat een actueel saldo-record verdwijnt in de orde van grootte van de kans dat de aarde door een meteoriet vernietigd wordt.

3.4 Handel met andere monetaire zones

Er is natuurlijk ook handel met andere monetaire zones. Die kan gefaciliteerd worden door actoren die als valuta handelaar optreden. Zo'n valuta handelaar heeft een A-account in deze

zone, bijvoorbeeld de eurozone, en in een andere zone, bijvoorbeeld een dollarzone, een dollarrekening. Een valuta handelaar ontvangt van een euro-actor een bepaald bedrag op zijn A-account en geeft deze actor, die ook een dollar rekening heeft, een overeenkomstig bedrag in dollars. Dat haalt de valuta handelaar van zijn dollar rekening. Voor deze wissel ontvangt de valuta handelaar een vergoeding. Hij heeft voldoende grote buffers van euro's en dollars nodig om dit spel met succes te kunnen spelen. De valuta handelaren zullen in de regel banken zijn.



3.5 'Vrij' spel in de serviceschil

Rechtstreeks op de MS infrastructuur zullen aanbieders van nieuwe diensten komen die zich afspelen in de zogeheten *serviceschil* om het MS Voorbeelden zijn boekhouddiensten waarmee transacties van meer informatie voorzien worden, zodat ze rechtstreeks als journaalposten geboekt kunnen worden en men alleen voor het feitelijke geldtransport nog het MS gebruikt. Een ander voorbeeld van een toegevoegde dienst is de automatische BTW afdracht. Dit zou ook in het MS zelf ingebouwd kunnen worden, via toevoeging van een transactie label dat BTW-plicht aangeeft, maar het is waarschijnlijk 'netter' dit in de service schil onder te brengen.
Er zullen ook diensten uit het huidige systeem verdwijnen, want de debit card transacties worden sterk gestroomlijnd. Nu lopen deze transacties via payment service providers (PSP) en worden uiteindelijk, uren of dagen later, via banken afgewikkeld. Deze PSP ontlenen hun bestaansrecht aan de onmacht van het bancaire systeem om real-time betalingen te verrichten, zeker als er andere banken bij betrokken zijn. Dit betekent ook dat de functies die SWIFT vervult deels zullen verdwijnen. Nu maken de banken een lijst van wat zij over en weer moeten

betalen (clearing) en periodiek is er een afrekening van de verschillen (settlement). Deze functies verdwijnen.
Natuurlijk moet er toezicht zijn op de diensten in de serviceschil. Maar het mooie van de MS infrastructuur is dat het veel makkelijker is voor aanbieders van nieuwe services in die schil. Vergelijkbaar met de app stores voor smart phones en tablets.

4 Monetair beleid

Bij monetair beleid gaat het om het realiseren van stabiliteit en economische ontwikkeling. Stabiliteit van koopkracht en stabiliteit van wisselkoersen. Zonder die stabiliteit is het geld moeilijk als ruilmiddel te gebruiken. Het voornaamste monetaire instrument in het huidige systeem is de rente die de banken moeten betalen voor een lening (van basisgeld) van de CB (refinancing rate). Binnen de eurozone ligt op het ogenblik de nadruk op stabiliteit van koopkracht. De ECB heeft wat dit betreft als expliciet doel de inflatie onder, maar dicht bij de 2% te houden. De veronderstelling is dat dat goed is voor de economische ontwikkeling. Omdat de rente al rond de 0% ligt, is er aanvullend beleid nodig om de kredietverlening te faciliteren en zo de economie te stimuleren, het opkopen van staatsobligaties en andere obligaties, quantitative easing (QE). Ook daarmee lukt het op het ogenblik niet dat inflatiedoel te bereiken. Kennelijk is het niet zo gemakkelijk de economie aan te jagen op deze manier. Wij willen dat inflatiedoel op een hele andere manier bereiken.

Het monetaire beleid wordt gescheiden van het fiscale beleid, ook in onze voorstellen . Ook het fiscale beleid is deels gericht op economische ontwikkeling. Dus wat doelstelling betreft is er wel overlap. Maar de gereedschappen van monetair beleid zijn heel anders dan die van fiscaal beleid. Bij het monetaire beleid gaat het, naast het realiseren van stabiliteit, hoogstens om het stimuleren van gretigheid tot kopen en ondernemen in het algemeen en facilitering van kredietverlening in de breedte. We gaan er vanuit dat het monetaire beleid gevoerd wordt door de CB.

Voor de PM beweging is het direct aanpassen van de hoeveelheid basisgeld het hoofdinstrument van monetair beleid. Binnen PM worden monetair beleid en fiscaal beleid minder strak gescheiden. Bij de doelen van geldschepping staan het mogelijk maken van overheidsuitgaven en belastingverlaging naast het faciliteren van bancaire kredieten via het uitlenen van extra basisgeld[17]. En het beleid is nogal bemoeierig. Veel meer dan het huidige systeem. Bij het uitlenen van extra basisgeld aan banken wil men bijvoorbeeld onderscheid maken naar soorten van bancaire kredieten. PM wil een ruimer kredietbeleid voor nieuwe productie dan ten behoeve van handel in bestaande assets en financiële producten. Zo verwacht men dan ook de inflatie te kunnen beheersen. Dat bemoeierige lijkt ons gevaarlijk. Ook in onze visie is de rol van de overheid belangrijk. Maar i.h.a. is de overheid niet erg goed in het in detail stimuleren van economische activiteit. En het is de vraag of de inflatie zo beheerst

[17] Zie Dyson, Hodgson and Van Lerven, “A response to Critiques of ‘Full Reserve Banking’”, Cambridge Journal of Economics, 2016, **40**, 1351 - 1361.

kan worden. Je kunt banken aan de ene kant kort houden, maar ze zijn vast creatief in het schuiven met geld van de ene bestemming naar de andere.

Hoe moet je hier verder? Het huidige systeem is kennelijk niet in staat de inflatie goed te beheersen. PM dreigt te bemoeierig te worden. Als eenmaal geaccepteerd is dat basisgeld volledig digitaal is, ligt de oplossing in feite voor het grijpen. Het gaat erom dat de waarde ontwikkeling van basisgeldbedragen op de individuele rekeningen beheerst wordt. Dat doen we door die bedragen te koppelen aan het BBP[18].

4.1 Koppeling en belaste koppeling aan BBP

Ga er van uit dat er dagelijks een schatting beschikbaar is van het (nominale) BBP. Verderop komen we er op terug hoe er geschat kan worden. Laat B^tde BBP schatting zijn aan het begin van dag t. Aan het begin van die dag wordt het basisgeld bedrag op elke rekening, dus A-,B- en ook C-accounts vermenigvuldigd met B^t/B^{t-1}. Dat betekent dat de koopkracht ervan in lijn blijft met het BBP. En de totale hoeveelheid geld op A- en B-accounts blijft dan steeds: $M(t)=\boldsymbol{f}.B^t$. Hierbij is $\boldsymbol{f}$ een nader te bepalen grootheid. Als er alleen prijsstijgingen zijn en er geen reële groei van het BBP is, blijft de koopkracht op deze manier ongewijzigd. Als er ook nog reële BBP groei is, groeit de koopkracht net zo snel. Hoewel deze aanpassingen van de accounts tot 100-sten van procenten beperkt blijven, zouden de bezitters van basisgeld in de verleiding kunnen komen om het niet uit te geven en beleggers zouden kunnen overwegen om te beleggen in basisgeld. Vandaar dat we er van uitgaan dat er een *anti-oppot belasting* nodig is, zeg τ per jaar. De parameter $\boldsymbol{\tau}$ is vergelijkbaar met de inflatie van 2% waar de ECB naar streeft. Het is een vorm van belasting zoals voorgesteld door Gesell en met enige waardering genoemd door Keynes[19]. De belasting komt bovenop eventuele andere belastingen op vermogen. Deze anti-oppot belasting, in combinatie met de eerder genoemde koppeling, houdt in dat elk basisgeld bedrag dagelijks wordt vermenigvuldigd met $(B^t/B^{t-1}) - \boldsymbol{\tau}/365$.[20] Ook deze dagelijkse aanpassingen zijn zo klein dat men dat men dit nauwelijks merkt. De totale waarde van het basisgeld, getotaliseerd over alle A- en B-accounts, als fractie van het BBP kan constant gehouden worden door het totaal van die belasting via een basisgeld rekening van de overheid terug in de economie brengen. Zie Appendix 4 voor een nadere toelichting van de koppeling.

[18] In een eerdere versie van dit paper hebben we het BNP gebruikt. Dat was een vergissing. Bij het BNP gaat het om ingezetenen, bij het BBP om plaats van productie. We zouden het liefst het totaal van alles wat met "onze" munt wordt betaald gebruiken. Dat is ook niet helemaal identiek aan het BBP, maar dat komt er dichter bij dan het BNP.

[19] J.M. Keynes, "The General Theory of Employment, Money and Interest", Book VI, Chapter 23

[20] Dat delen door 365 is natuurlijk niet helemaal precies goed. Maar bij een laag belastingpercentage is die fout verwaarloosbaar.

Door de hoeveelheid basisgeld die terug gebracht wordt in de economie af te laten wijken van de totale belasting, is het natuurlijk ook mogelijk de basisgeld hoeveelheid, als fractie van het BBP, te laten stijgen of dalen.

4.2 Schatten van het BBP

Er zijn meerdere mogelijkheden om tot een dagelijkse schatting van het BBP te komen. Een voor de hand liggende wordt hier uitgewerkt. Periodiek komt er een officiële schatting beschikbaar van het BBP. Daar tussendoor kan de totale transactiesom gedurende het afgelopen jaar (365 dagen) voor transacties die betrekking hebben op reële goederen en diensten, gebruikt worden om de BBP schatting te updaten. Die kan bijgehouden worden door MS (zie Paragraaf 3), als aan de transacties een label wel/niet reëel meegegeven kan worden.

Stel, $P_r(t)$ is de som van alle reële transacties (goederen en diensten) gedurende het af gelopen jaar, aan het begin van dag t. Het grote verschil tussen B^t en $P_r(t)$ is dat in de laatste grootheid ook alle transacties *in* voortbrengingsketens worden geteld. De fragmentatie van de voortbrenging heeft dus veel invloed. Maar als die niet al te snel wijzigt, en dat mag je verwachten, geldt dat $B(t) = \beta(t)P_r(t)$, met $\beta(t)$ een evenredigheidsconstante die maar heel langzaam met t verandert. Aan het begin van dag t wordt de BBP schatting vermenigvuldigd met· $(P_r(t)/P_r(t-1))$. Dus

$$B^t = B^{t-1} \cdot (P_r(t)/P_r(t-1))$$

Dat is de hoofdregel. En zodra er weer een nieuwe schatting van het BBP beschikbaar komt, vindt er correctie plaats. Zie daarvoor Appendix 4. Daar wordt ook ingegaan op de aanloopproblemen en op de mogelijkheid om correcties nog glad te strijken.

4.3 Alternatieven voor basisgeld

Het monetaire beleid grijpt aan op door iedereen gebruikte basisgeld. Dat is het wettige betaalmiddel. Het aantrekkelijke ervan is de koppeling aan het BBP. De belasting erop zal minder positief worden ervaren. Er zal ongetwijfeld gezocht worden naar alternatieven. Voor de hand liggende mogelijkheden zijn: dollars, goud en bitcoins. Maar zowel bij dollars en goud als bij bitcoins geldt het bezwaar van mogelijke wisselkoers fluctuaties. Bij dollars wellicht het minst. Het voordeel van de koppeling aan het BBP zal bij het vergelijken met deze mogelijkheden al gauw het bezwaar van wat belasting compenseren.

Een interessante mogelijkheid is dat een bank, of eventueel de gezamenlijke banken, claims op basisgeld gaan uitgeven. Uiteindelijk kan iedereen een claim op zichzelf uitgeven en die claim kan door alle “gelovigen” gebruikt worden als betaalmiddel. Bij banken, zeker bij de gezamenlijke banken, zullen er best veel gelovigen zijn. Het voordeel ervan is dat er geen belasting over betaald hoeft te worden. De banken zouden nog een stap verder kunnen gaan en

die claims ook kunnen koppelen aan het BBP, hoewel het voor een bank lastig zal zijn zo'n koppeling te garanderen. En het uitgeven van zulke claims wordt sowieso bemoeilijkt doordat de overheid betaling ermee niet zal accepteren. Er moet dus wel relatief veel dekking zijn, omdat actoren die de overheid moeten betalen, hun tegoed zullen willen converteren naar basisgeld. Eventueel kan het de banken ook verboden worden. De toegang tot basisgeld krediet kan dan ontzegd worden. Niet-banken zouden het dan nog kunnen doen, maar die hebben sowieso geen toegang tot basisgeld krediet en zullen niet gemakkelijk voldoende dekking kunnen creëren.

Het is zaak de belasting op basisgeld zodanig te beperken dat het voordeel van de waardevastheid het nadeel van de belasting erop meer dan compenseert. Geen belasting kan het te aantrekkelijk maken om het niet meer uit te geven, bij een te hoge belasting wil een eventuele ontvanger er zijn vingers niet meer aan branden.

4.4 Monetaire beleidsparameters

De belangrijkste monetaire parameters zijn de totale basisgeld hoeveelheid als fractie $\boldsymbol{f}$ van het BBP en de belasting op basisgeld, $\boldsymbol{\tau}$ (zie boven). Daarnaast zijn er dan nog de limiet op basisgeld krediet van de CB en de rente daarop. Die komen verderop nog aan de orde.

De monetaire autoriteit zal af en toe kleine wijzigingen aanbrengen in $\boldsymbol{f}$**.** Dat kan door de belasting op bezit van basisgeld niet helemaal te compenseren (fractie wordt kleiner) of meer dan te compenseren (fractie wordt groter). Het is belangrijk voorzichtig te zijn met het sturen op $\boldsymbol{f}$**.** Hoe meer stabiliteit hoe beter. Heel gemakkelijk creëer je anders zelf allerhande schommelingen. Daarnaast moet $\boldsymbol{f}$ niet onnodig groot zijn. Teveel geld in de economie leidt gemakkelijk tot instabiliteit. In een gretige economie is niet veel geld nodig. Men vindt gemakkelijk allerhande manieren om transacties af te ronden, desnoods via ruilen. Hoe kun je dan verwachten dat de economie gretiger wordt door de geld hoeveelheid te verruimen? Dat is net zoiets als hopen dat boksers actiever worden door de ring te vergroten.

Er is (basis)geld nodig als werkkapitaal en huishoudgeld. Er is basisgeld nodig op de kapitaalmarkt, om het switchen van de ene asset naar de andere in een beleggingsportefeuille gemakkelijk te maken. En er is geld nodig voor het financieren van investeringen. In Appendix 4 wordt geschetst hoe je een schatting kunt maken van wat er voor elk van die functies nodig is aan geld. Zo kom je tot een eerste schatting van wat er totaal nodig is. Dat zal wel lager zijn dan wat er nu totaal beschikbaar is op de betaalrekeningen. En bij de overgang naar dit systeem, begin je daarmee als basisgeld (zie de volgende paragraaf). Daarna volgt een trial-and-error proces van voortdurende verkleining van $\boldsymbol{f}$. Tot je merkt aan het gedrag van de banken inzake het lenen van basisgeld dat je aan de grens komt. Namelijk als banken het van de CB geleende

basisgeld ook gaan gebruiken voor het aanvullen van werkkapitaal. De schatting van wat er nodig is blijft daarbij ook een nuttig referentiepunt.

Naast de keuze van $\boldsymbol{f}$, is er de keuze van $\boldsymbol{\tau}$. Voor de hand ligt die zo groot mogelijk te kiezen. Zo groot dat er net niet gezocht wordt naar alternatieven voor basisgeld (zie boven). Hoe groter $\boldsymbol{\tau}$, hoe minder de actoren geneigd zijn basisgeld vast te houden, hoe kleiner $\boldsymbol{f}$ gemaakt kan worden en hoe stabieler het systeem wordt. Het voordeel van dit monetaire systeem is de *waardevastheid* van basisgeld. Stel de verwachte nominale stijging van het BBP is 2%. En neem aan dat de helft daarvan inflatie is en de andere helft stijging van productiviteit. Dan kun je $\boldsymbol{\tau}$ ook minstens gelijk aan 1% maken. Bij $\boldsymbol{\tau}$ gelijk aan 1% blijft de koopkracht van het basisgeld bedrag op een rekening nog constant. En je kunt nog wel iets verder gaan, omdat het niet gemakkelijk zal zijn liquide alternatieven te vinden die ook 100% koopkracht behoud geven. Ook inflatie helpt dus om de keus voor basisgeld aantrekkelijk te maken. En je mag wel enige inflatie verwachten in dit systeem. In het gevecht om de koek, het BBP, zal niemand snel geneigd zijn de eigen bijdrage te devalueren en gaan de prijzen dus gemakkelijker naar boven dan naar beneden. Dat zal wel zo blijven. Enige inflatie is dus normaal. Daarnaast wat productiviteitsstijging. Er is dus wel ruimte om $\boldsymbol{\tau} > 0$ te kiezen.

De kritiek op het Positive Money voorstel, dat er ook bankkrediet nodig is om voldoende flexibel investeringen en innovaties te kunnen financieren, zal ook dit voorstel gelden. Dat zou terechte kritiek kunnen zijn. Daarom wordt in het Positive Money voorstel al voorzien dat banken basisgeld kunnen lenen. Dat geldt hier ook: banken kunnen negatief staan op hun C-account en zo hun B-account aanvullen. Het voorstel is dat te relateren aan het totaal van de tegoeden aan basisgeld van andere actoren op die B-account. Het maximum aan basisgeld dat geleend kan worden van de CB, wordt bepaald op een vaste fractie $\boldsymbol{g}$ van dat gemiddelde totale tegoed. Dat is de derde monetaire parameter. Het is een vorm van fractional reserve banking. Belangrijk is dat de $\boldsymbol{g}$ niet onderhandelbaar is. Er is ook hier weer trial-and-error nodig om die g vast te stellen. De bedoeling is $\boldsymbol{g}$ zo te kiezen dat het totaal wat beschikbaar is via de B-accounts voldoende is om banken in de gelegenheid te stellen investeringen voor te financieren. De hoeveelheid basisgeld die daarvoor nodig is kan wel geschat worden. Zie Appendix 4.

De vierde monetaire parameter is de rente $\boldsymbol{r}$ die verschuldigd is voor zo'n basisgeld lening. Dat is o.i. de enige parameter die wat actiever aangepast mag worden. Als bijvoorbeeld blijkt dat de ruimte op de C-accounts toch gebruikt wordt voor het financieren van transacties op de kapitaalmarkt, kan men de rente verhogen. Wat de andere parameters betreft is het een kwestie van zorgvuldig inregelen en daarna vooral zo laten. Het systeem rustig zijn gang laten gaan.

4.5 Wisselkoers stabiliteit

Monetair beleid gaat ook over wisselkoers stabiliteit. Er zijn natuurlijk allerhande redenen om reële goederen en diensten te willen kopen of verkopen in een andere monetaire zone. En om daar in aandelen, obligaties of andere financiële producten te willen handelen. Dat is niet anders dan in het huidige systeem. En het is niet de bedoeling te suggereren dat de door ons voorgestelde koppeling dat nu ook allemaal stabieler en helderder maakt.

Maar enige extra stabiliteit is er wel. De ontwikkeling van de koopkracht van een gekoppeld basisgeld bedrag is goed voorspelbaar want de ontwikkeling van het BBP is goed voorspelbaar. En inflatie risico's hoeven niet afgedekt te worden. Dat voordeel wordt groter naarmate er meer zones zijn waarin de koppeling wordt toegepast. De koppeling brengt wel met zich mee dat men er rekening mee moet houden dat het betreffende basisgeld een aantrekkelijk beleggingsproduct wordt op de internationale kapitaalmarkt. Zeker als er een hoge verwachte groei van het BBP is en een lage belasting. Dan zou het kunnen gebeuren dat een groot deel van het beschikbare basisgeld wordt gekocht door internationale beleggers en vervolgens niet meer wordt gebruikt. Het is daarom belangrijk daar rekening mee te houden bij het instellen van de belasting.

Het koppelen aan het BBP impliceert ook een interessante extra mogelijkheid voor de eurozone. Meest voor de hand ligt de eurozone te zien als één monetaire zone. Dan worden de basisgeld bedragen in euro's gekoppeld aan het BBP van de totale eurozone. In plaats daarvan zou je ook met verschillende monetaire zones kunnen werken, wel allemaal met de euro als munteenheid, maar met koppeling aan het eigen BBP. Dat geeft enige vrijheid binnen de eurozone, zonder de ene euro los te laten. Ook dan geldt weer dat het belangrijk is de verwachte groei van het reële BBP minus de belasting ongeveer gelijk te houden over de verschillende zones. Anders wordt, bij vrij betalingsverkeer, ieders liquiditeit opgeslagen in de zone waar dit verschil het grootst is.

5 Implementatie en migratie

Het is belangrijk dat de overgang van het huidige systeem naar het nieuwe soepel verloopt. Een incrementele veranderingsstrategie, waarbij een grote verandering in kleine stapjes wordt gerealiseerd, is te prefereren boven een big-bang strategie waarbij het nieuwe systeem in één klap ingevoerd wordt. In dit geval is een incrementele strategie mogelijk. De invoering van de euro was een vergelijkbare operatie, die ook incrementeel verliep.

Bij de implementatie moet onderscheid gemaakt worden naar een monetair systeem (MS) en monetair beleid. Wat het monetair systeem betreft gaat het vooral om het organiseren van de betaalrekeningen (A-accounts). We beginnen met de minimale variant van het MS waarbij het MS voor elke account alleen het laatste saldo-volgnummer, dus het nummer van de laatste mutatie, bijhoudt. Dit moet in elk geval gebeuren en andere functies van het MS kunnen later toegevoegd worden. Er is ook een andere reden waarom het goed is met de minimale variant te beginnen: de banken kunnen aanvankelijk een groot deel van hun functie behouden en daarna gaan concurreren met andere aanbieders van betaalfuncties, zoals betaalinstellingen, ict-bedrijven, aanbieders van clouddiensten, telecom providers en administratiekantoren. Hoewel de echte operatie een uitgebreide planning vereist, schetsen we hier alleen de belangrijkste stappen die gezet moeten worden.

1. Voor alle actoren moeten betaalrekeningen (A-accounts) gecreëerd worden. Bijna alle actoren hebben al betaalrekeningen bij banken en die rekeningen hebben al een uniek nummer. Het ligt dus voor de hand om die te gebruiken. Het MS moet de elementaire functies kunnen bieden: dus één transactierecord en twee saldi-records kunnen ontvangen, de nodige verificaties doen en de saldi-records updaten en terugsturen.
2. Girale transacties zullen in eerste instantie door de banken worden uitgevoerd: zij zullen voor hun cliënten de saldo-records bewaren en als een actor een betaalopdracht geeft zal de bank het transactierecord samenstellen en de twee saldi-records opzoeken en dit alles naar het MS sturen en de saldi-records die terugkomen weer bewaren. Als het een overboeking tussen twee accounts binnen één bank is, dan kan dat gemakkelijk, als het verkeer tussen twee banken is dan zal de bank van de betaler het saldo-record van de ontvanger bij diens bank moeten opvragen. Door de encryptie is hier geen risico voor malversaties, maar de banken moeten natuurlijk wel de privacy van zowel ontvanger als betaler beschermen.
   Dit vergt een software inspanning voor de banken, maar de cliënten merken er nog niets van. Als dit is gerealiseerd dan kunnen ook andere partijen deze functies voor actoren gaan vervullen. In principe kan iedereen het zelf doen en grotere bedrijven zullen dat dan ook zelf gaan doen.

3. Als de minimale variant eenmaal ingevoerd is, kan het MS uitgebreid worden met het registreren van de saldo-records en zal een aantal actoren voor betalingen de banken gaan omzeilen.
4. Voor de winkeltransacties moeten we onderscheid maken tussen *cash* en *card* transacties. (Onder winkels verstaan we alle organisaties waar consumenten betalen, dus naast 'echte' winkels ook horeca, bioscopen, pretparken etc). De cash transacties moeten op termijn uitsterven. Dus een actor mag nog een nader te bepalen periode met cash betalen, maar hij krijgt in winkels, horeca en dergelijke wisselgeld in girale vorm terug. Ook bij banken kan men cash storten en laten bijwerken in het saldo, maar niemand kan meer cash opnemen bij de banken. Zo sterft het cash geld vanzelf uit. Merk op dat de totale hoeveelheid basisgeld dus in het begin stijgt doordat cash in basisgeld wordt geconverteerd.
5. Voor card transacties kunnen de bestaande systemen aangepast worden. Nu gebruikt men meestal het C-TAP protocol, waarbij de transacties via de debit card organisaties verlopen (Master Cad, met Maestro, Visa met V-pay). Betalen met de card en een betaalterminal in de winkel kan ook. Bij de minimale variant, waarbij de actor zelf zijn saldo bewaart moet de card aangepast worden en eigenlijk iets van de functionaliteit van de chipknip terugkrijgen: de card bevat het saldo-record van de consument en wat ondersteunende gegevens. De betaalautomaat maakt het transactierecord uit de registratie in de kassa en verzendt de saldi-records van de consument en de winkel tezamen met het transactierecord naar het MS en zet na afloop het saldo-record van de consument weer op zijn card. Als variant 3 geïmplementeerd is, hoeven de saldo-records niet op de cards en kan de volstaan worden met het versturen van de transactiegegevens. (Merk op dat we doorgaans veronderstellen dat de betaler de tranasctie naar het MS verstuurt, terwijl dat hier de ontvanger is.) Ook nu al kan men met een smartphone in winkels betalen door deze in de buurt van de betaalterminal te houden (near field communication). Maar dan fungeert de smartphone als een card en geeft alleen de identiteit van de consument en zijn vaste gegevens door, gegevens die ook op de card staan. Debit card organisaties verdwijnen dus.
6. Voor transacties tussen consumenten onderling en ook in winkels komt er een nieuwe smartphone app, waarmee men zijn saldo op de smartphone bewaart (in een wallet) en waarmee men kan communiceren met een ander en samen de saldi-records en het transactie-record naar het MS kan sturen die de geupdate saldo-record weer terug stuurt. (In variant 3 is het bewaren en versturen van de saldo record niet meer nodig)
   Hoewel de debit card organisaties overbodig worden, kan de credit card gewoon blijven bestaan. De consument betaalt dan niet zelf maar de credit card organisatie doet dit en de consument bouwt een claim op bij de credit card organisatie, net als nu het geval is.

Natuurlijk zal in de praktijk blijken dat het minder eenvoudig is dan het zo lijkt, maar in principe is het niet ingewikkelder dan hier geschetst. Zo zal de vraag beantwoord moeten worden wat er gebeurt bij een hevige stroomstoring. Natuurlijk zullen alle saldo-records goed opgeslagen moeten zijn dus op meerdere plaatsen in een cloud.(In variant 3 is dat reeds voorzien.) Dan kan men weer verder als de storing voorbij is en zijn hoogstens een paar transacties verloren

gegaan die dan opnieuw moeten worden uitgevoerd. Tijdens de storing is dan beperkt betalingsverkeer mogelijk, namelijk tussen mobiel systemen en systemen met power back ups. Dit is niet anders dan in de huidige situatie.
Tenslotte zal men willen weten wat transacties in dit MS kosten. Het ligt voor de handkosten per transactie en kosten van opslag in rekening te brengen, maar een vast abonnement kan ook aantrekkelijk zijn.

Wat monetair beleid betreft begint de implementatie met het aanbrengen van de koppeling van de bedragen op de A-accounts met het BBP. Daartoe moet er een BBP schattingsprocedure ontwikkeld worden (zie Appendix 4). Bij die koppeling moet ook meteen een eerste keus gemaakt worden voor de toe te passen belasting ($\boldsymbol{\tau}$). De koppeling hoeft niet meteen beschikbaar te zijn bij de overgang van de betaalrekeningen naar het MS (zie stap 1 hierboven), maar wel als het MS de saldo records gaat bijhouden ende rol van de banken kleiner gemaakt kan worden (zie stap 3 hierboven)[21] Vanaf het moment van de koppeling zijn de tegoeden op de betaalrekeningen basisgeld. De bestaande tegoeden op alle betaalrekeningen gaan compleet op in het basisgeld. Er zal dus eerst wel teveel basisgeld zijn ($\boldsymbol{f}$ te hoog). Vanaf dat moment ook hebben de verschillende actoren de gelegenheid om basisgeld uit te lenen aan banken. Het basisgeld komt dan terecht op de B-account van een bank. Die B-account moet dan dus ook beschikbaar zijn, en gekoppeld worden aan het BBP.

Bij de koppeling worden de tegoeden op de bestaande betaalrekeningen basisgeld. De tegoeden op die rekeningen zijn deels gebaseerd op bankleningen. Die leningen stelt de bank nu dus beschikbaar in basisgeld. Zoveel basisgeld zal de bank niet zelf hebben. Dat betekent dat er een lening van de CB nodig is, via de C-account. Die C-account moet dus ook vanaf het begin operationeel zijn (en gekoppeld worden aan het BBP). Er wordt eerst een voldoende hoge limiet ($\boldsymbol{g}$) gehanteerd en een lage rente gevraagd ($\boldsymbol{r}$). Pas daarna worden de monetaire parameters beter ingeregeld. Zie Sectie 4.4 en Appendix 4.

[21] Het bijhouden van de saldo records door het MS is essentieel voor de voorgestelde wijze van koppeling (elke nacht het bedrag aanpassen). Als de minimale variant gekozen wordt, kan er ook wel gekoppeld worden, maar dat vergt een wat complexer vorm van aanpassing van de bedragen, n.l. alleen bij transacties.

6. Conclusie

Deze notitie bedoelt bij te dragen aan het debat over de rol van banken in het financiële en monetaire systeem. Door de Stichting Ons Geld, geïnspireerd door de Positive Money (PM) beweging in de UK, is dat debat verscherpt naar de vraag of het niet beter is het scheppen van geld over te laten aan de overheid. De minister van Financiën heeft daarover het advies van de WRR gevraagd. We hopen dat deze notitie daarbij betrokken kan worden.

De meest natuurlijke manier om het scheppen van geld weg te halen bij de banken is om de money base, die nu bestaat uit munten, bankbiljetten en reserves van de banken bij de Centrale Bank, anders in te richten en dit “basisgeld” te verheffen tot voor ieder toegankelijk betaalmiddel. Dat spoort met de voorstellen van PM en Stichting Ons Geld. De voordelen hiervan (meer stabiliteit en een beter gegarandeerde nutsfunctie van opslag en betalen) worden breed erkend. Maar dat heeft nog niet geleid tot acceptatie ervan in bankwereld en politiek. Wij hebben dat principe in deze notitie gevolgd en in de volgende drie richtingen uitgewerkt:

- Schaf chartaal geld af. De beschikbare informatietechnologie maakt dat mogelijk en aantrekkelijk.
- Creëer een nieuw MS waarmee basisgeld kan worden opgeslagen en overgedragen Banken gaan zich weer concentreren op hun primaire diensten: krediet verstrekken met spaargeld en bij de CB geleend geld.
- Ontwikkel monetair beleid waarbij de basisgeld bedragen op individuele rekeningen gekoppeld worden aan het BBP. Op die manier kan de koopkracht gegarandeerd blijven zonder dat er voortdurend ingegrepen hoeft te worden door de CB.

Daarbij hebben we rekening gehouden met de bezwaren die wel worden ingebracht tegen zo’n systeem: Te weinig flexibiliteit m.b.t. kredietverlening en vermenging van fiscaal beleid en monetair beleid.

De belangrijkste paragrafen zijn de Paragrafen 3 en 4. In Paragraaf 3 hebben we een monetair systeem ontwikkeld waarbij alle actoren één of meer betaalrekeningen hebben met basisgeld. Er is een betalingsprotocol met vrijwel absolute privacy voor de actoren (zie Appendix 2). De noodzakelijke cryptografie wordt toegelicht in de Appendices 1 en 3. Banken hebben daarnaast een rekening met basisgeld dat deels geleend is van actoren die dat tijdelijk over hebben en deels van de Centrale Bank. Die rekening komt overeen met de investment pool in de voorstellen van PM. In Paragraaf 4 hebben we een viertal monetaire beleidsparameters ontwikkeld. Daarbij uitgaand van koppeling van de basisgeld bedragen op de individuele rekeningen met het BBP. De monetaire parameters staan voor (1) de evenredigheid van de

totale geldhoeveelheid met het BBP, (2) de belasting op basisgeld, (3) de limiet op de kredietruimte van de CB en (4) de bijbehorende rente. In Appendix 4 wordt ingegaan op de mogelijkheid om goede keuzen wat deze parameters betreft te bepalen. Dat leidt tot rust in het monetaire beleid. Op de problematiek van implementatie en migratie wordt in Paragraaf 5 ingegaan. Daar wordt een stapsgewijze implementatie van het monetaire systeem beschreven, met een geleidelijke tuning van de beleidsparameters.

De conclusie is dat er zo een robuust monetair systeem ontworpen en ingevoerd kan worden. Het SFL (Sustainable Finance Lab) heeft kort geleden een enquête laten houden, waarbij o.a. gevraagd werd of men weet wie het meeste geld creëert en ook wie men vindt dat dat zou moeten creëren. Het is absoluut niet verbazend dat de overgrote meerderheid denkt en vindt dat de overheid dat doet en moet doen. Kennelijk is het huidige systeem vreemd: een systeem gebaseerd op claims die nauwelijks meer geeffectueerd worden. Dat het kan functioneren wordt alleen begrepen door experts. Dat is op zich niet erg, maar er zijn kennelijk voortdurend drastische maatregelen nodig om het geheel een beetje binnen de perken te houden. En desondanks vliegt het af en toe volledig uit de bocht. Voor elke ingenieur riekt dit naar slecht ontwerp. De tegenwerping zal zijn dat het geen ontwerp is, maar een gegroeid systeem. Wel, wordt het dan geen tijd om de verdere groei richting te geven via een ontwerp?

Wij hebben zo'n ontwerp geschetst hier. Uitgangspunt daarbij was dat geld *objectief* moet zijn, "positief", en *hard*. Dat kan. In het hier beschreven monetaire systeem is bezit van geld onafhankelijk van de rol van de banken. En het is hard, want gekoppeld aan het BBP.

Over de auteurs

Kees van Hee en Jacob Wijngaard zijn beiden gepromoveerd in de wiskunde en emeriti hoogleraren, in respectievelijk informatica (TU/e) en bedrijfskunde (TU/e en RUG). De eerste auteur is ook 16 jaar consultant geweest, onder andere als partner bij Deloitte.
E-mail adressen: k.m.v.hee@tue.nl en j.wijngaard@rug.nl
Website: www.robuustgeld.nl

Appendix 1: Cryptografie in een notendop

Een *asymmetrisch encryptiesysteem* heeft twee sleutels, een *secret key* S, die geheim gehouden wordt en een *public key* P die openbaar is. Een sleutel is een groot getal (in de orde van 100 cijfers) en het encryptie-systeem omvat een algoritme waardoor de sleutel zich gedraagt als een *functie* die een willekeurige getal omzet in een ander getal. We zullen de sleutels S en P dan ook als functies beschouwen. Dus als we S toepassen op een getal A dan krijgen we een getal B en dit noteren we als S(A)=B. De sleutels S en P zijn elkaars *inverse,* hetgeen wil zeggen dat als we S op een getal A toepassen met als resultaat B en we daarna P toepassen op B dan krijgen we A weer terug. Dus voor elke string A geldt: P(S(A))=A en ook S(P(A))=A. Als je maar één van de twee sleutels hebt is het praktisch onmogelijk deze te inverteren. Met 'praktisch onmogelijk' wordt bedoel dat het meer dan 100 jaar rekenen op het grootste beschikbare computernetwerk kost om A te vinden als je B hebt en weet dat S(A)=B. Het meest beroemde asymmetrische encryptie systeem dateert uit 1977 en heet RSA, naar de ontwerpers Rivest, Shamir en Adleman.[22]

Men kan met zo'n sleutelpaar een *digitale handtekening* zetten: een actor X stuurt een bericht naar actor Y en wil dat Y weet dat het van hem. Dan stuurt X het bericht: [van:X, Sx(X), inhoud, naar:Y] want alleen X kent S_X. De ontvanger Y kan dan de public key van X opzoeken (immers X staat in het bericht) en $P_X(S_X(X))=X$ verifiëren. Maar dit bericht kan onderschept worden en zo kan een ieder dit lezen en zien dat het van X komt. Als je wilt dat het bericht alleen door Y gelezen kan worden dan versleutel je het met de public key van Y:
P_Y([van:X, Sx(X), inhoud, naar:Y]) en dan kan Y het lezen door:
$S_Y(P_Y$([van:X, Sx(X), inhoud, naar:Y]))=[van:X, Sx(X), inhoud, naar:Y]

Een ander instrument in de cryptografie is een *hash functie*. Zo'n functie wordt ook gerealiseerd door een algoritme. Een hash functie H maakt van een heel grote rij van letters en cijfers een kortere rij. Dus H toegepast op een rij A geeft een kortere rij B: H(A)=B. Het doel is een om een compactere representatie van de eerste rij te krijgen, dus om via een kortere rij de langere te *identificeren.* Maar dat kan natuurlijk niet, want er bestaan verschillende lange rijen die door H tot dezelfde kortere rij . getransformeerd worden. Het interessante van hash functies is dat dit in de praktijk zelden voorkomt, omdat het aantal grote rijen die we in de praktijk gebruiken 'verwaarloosbaar' klein is ten opzichte van het totaal aantal rijen waar we de hash functie op zouden kunnen toepassen en dat de hash functie de geproduceerde rijen goed 'verspreidt'. Hash functies zijn dus niet injectief en dus ook niet inverteerbaar, zoals de sleutels van een asymmetrisch encryptie systeem. Maar het kost heel veel computertijd om een string A te

[22] Rivest, R.L. ,A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM (1978); Handbook of Applied Cryptography CRC Press (2001)

vinden als je B kent en weet dat H(A)=B. Een veel gebruikte hash functie heet SHA-256 (Secret Hash Algorithm 256)[23] ontwikkeld door NSA.

Daarom worden hash functies ook gebruikt om de *authenticiteit* van gegevens te beschermen. Bijvoorbeeld als men een string A wil versturen en wil garanderen dat tijdens het transport A niet veranderd wordt in B dan stuurt men A en separaat H(A). Als de ontvanger dan B krijgt ziet hij dat H(B) niet gelijk is aan de ontvangen H(A) en weet dus dat er gefraudeerd is. Het zelfde systeem past men toe op bestanden. Op het moment dat een bestand A opgeslagen wordt berekent men H(A) en slaat dat elders op. Zodra men het bestand weer ophaalt en dit mogelijk in B is veranderd, berekent men H(B) en vergelijkt het met H(A). De kans dat zo'n manipulatie niet ontdekt wordt, dus dat H(A)=H(B), is verwaarloosbaar. Een klassiek voorbeeld van een heel elementaire hash functie is de *check sum.* Als je een groot getal moet oversturen dan voeg je de som der cijfers toe en als de ontvanger de cijfers van het getal optelt en zet dat dit verschilt van de check sum dan weet hij dat er iets fout is gegaan. Garantie dat het goed is gegaan kan men niet krijgen.

[23] H.Gilbert, H. Handschuh, "Security analysis of SHA-256 and sisters", Selected areas in cryptography 2003, pp175-193

Appendix 2: Betalingsprotocol

Hier geven we het protocol dat beschreven is in paragraaf 3.2 in detail weer. Er zijn natuurlijk variaties mogelijk, maar hier staan de essentiële stappen.

1. X stuurt bericht naar Y, versleuteld met de public key van Y en voorzien van zijn eigen 'handtekening' d.w.z. de met zijn secret key (S_X) versleutelde informatie is toegevoegd. Er is een uniek eigen transactienummer N van X :
   P_Y([van: X, bedrag: B, naar Y: trnr: N, S_X (X,B,Y, N)])
   a. Y ontcijfert dit bericht door zijn secret key S_Y er op los te laten en krijgt dan:
      [van: X, bedrag: B, naar: Y, trnr: N, S_X (X,B,Y,N)]
   b. Door de public key van X, P_X , te gebruiken kan Y de handtekening verifiëren:
      $P_X(S_X(X,B,Y,N))=(X,B,Y,N)$
2. Y moet nu beslissen of het de betaling zal aanvaarden. Zo ja, dan stuurt Y een bevestiging in de vorm van $P_X([van:Y, S_Y(X,B,Y,N)])$ en anders een reject bericht en stopt het protocol.
3. X stuurt nu deze bevestiging van Y met twee handtekeningen door naar MS:
   P_{MS}([van: X, bedrag: B, naar:Y, trnr: N, $S_X(X,B,Y,N],),S_Y(X,B,Y,N),]$),
   die het kan lezen met S_{MS} , P_Y en P_X. Zo ziet MS dat X en Y de transactie geautoriseerd hebben.
4. X stuurt nu zijn laatste saldo-record dat door de MS is vastgesteld en versleuteld met de secret key van MS:
   $P_{MS}([acnr:X, saldo: A_X, vlgnr: M_X, S_{MS} (X,A_X,M_X)))$.
   M_X is het unieke volgnummer dat de MS heeft gegeven bij de laatste update van X.
5. Idem voor Y: $P_{MS}(acnr:Y, saldo: B_Y, vlgnr: M_Y, S_{MS} (Y,A_Y,M_Y)))$.
6. MS leest deze records met zijn secret key en met ontcijfert met zijn eigen public key de saldi. MS controleert of de saldi actueel zijn d.w.z.de volgnummers de laatsten zijn. Dan verhoogt MS het saldo van Y met B en verlaagt het saldo van X met B, versleutelt dit en stuurt ze naar X resp. Y:
   $P_X([acnr:X, saldo: A_X-B, vlgnr:M_X+1, S_{MS}(X, A_X-B,M_X+1])$ en
   $P_Y([acnr: Y, saldo: A_Y+B, vlgnr: M_Y+1, S_{MS}(Y,A_Y+B,M_Y+1])$

De saldo nummers worden met één opgehoogd en door MS bewaard. Merk op dat X en Y hun eigen saldo kunnen lezen met P_{MS} maar niet zelf kunnen wijzigen en ook de transactienummers niet.

In de variant die wij voorstellen (niveau 3) onthoudt het MS ook de saldi van de accounts. Stappen 4 en 5 zijn dan overbodig en eigenlijk hoeven de volgnummers niet bewaard te worden, maar die geven toch wat extra zekerheid.

Appendix 3: Bitcoin en blockchain

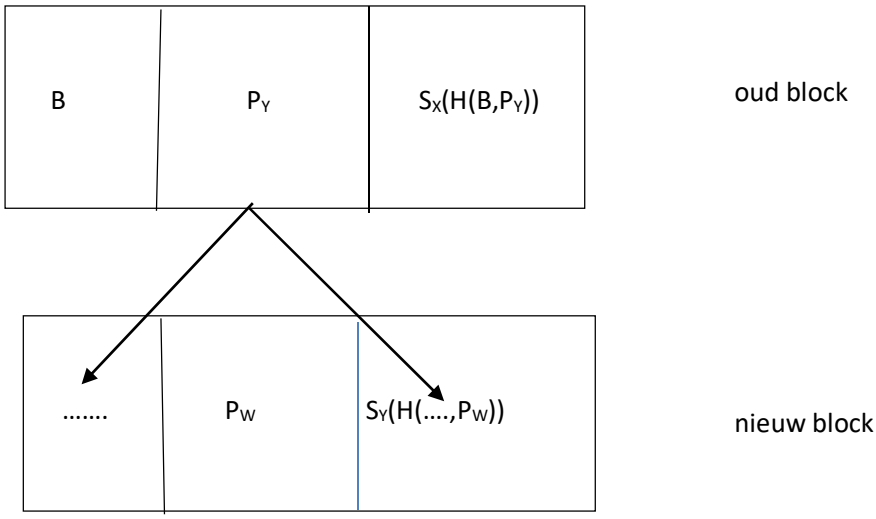
De bitcoin[24] is een alternatieve virtuele munt. In het verleden waren munten gemaakt van een schaars materiaal zoals zilver of goud en kwam de waarde van dit materiaal overeen met de muntwaarde. Later is men munten en bankbiljetten gaan maken die moeilijk te vervalsen zijn, in de hoop dat de moeite die het kost om de munt te vervalsen niet opweegt tegen de waarde van de munt. Bij de bitcoin is een vergelijkbare waarde gekozen: het kost veel jaren rekenen op een gigantisch computernetwerk om een nieuwe bitcoin te berekenen. Alleen al de energie die dit rekenwerk kost weegt op den duur niet op tegen de waarde van de zo gevonden bitcoin. (De eerste bitcoins waren relatief snel te berekenen en maar het wordt steeds moeilijker)

Het bitcoin systeem kent individuele digitale 'munten' die gerepresenteerd worden door een heel groot getal. De getallen die als bitcoin gelden zijn getallen die door een hash functie SHA-256 (afgekort tot H) afgebeeld worden op een getal dat begint met een voorgeschreven aantal nullen. (NB normale getallen beginnen nooit met een nul, maar we kunnen denken aan getallen achter de komma). Het kost heel veel computertijd om zo'n getal te vinden. Dit proces noemt men *mining* en daar dankt het getal dan ook zijn waarde aan: de hoeveelheid computertijd maakt het getal zeldzaam of en dus de bitcoins schaars. Het contoleren of een getal A een bitcoin voorstelt kost relatief weinig tijd, men rekent dan H(A) uit. Maar het vinden van een A die voor een gegeven B voldoet aan H(A)=B is dus koste dus extreem veel computertijd. Dit wordt een *proof-of-work* genoemd. De 'verse' bitcoins krijgen naast het unieke getal ook de public key van de miner (ontdekker) mee, dus een bitcoin kan men representeren als een paar: [bitcoin-getal, P_{miner}]. Om hem veilig op te bergen kan de ontdekker dit getal versleutelen met zijn secret key en later weer terug transformeren met zijn public key.

Om een bitcoin B te *transporteren* van speler X naar speler Y gaat men als volgt te werk: er wordt een nieuwe versie van de bitcoin gemaakt waar de *historie* in zit opgeslagen. Voor verse bitcoins geldt dus B=[bitcoin-getal, P_{miner}]. Een bitcoin met representatie B wordt na overdracht van X naar Y wordt bitcoin B' en die heeft representatie: [B, P_Y, S_X ((H(B), P_Y)]. Dus we zien hier de oude bitcoin B, de publieke sleutel van de nieuwe eigenaar en de handtekening van de oude eigenaar, namelijk de versleuteling van het voorgaande met de secret key van de oude eigenaar. En als Y de bitcoin weer overdraagt aan W is de nieuwe bitcoin B": B"= [B',P_W,

[24] Satoshi Nakamoto, "Bitcoin: a peer to peer electronic cash system", www.bitcoin.org

$S_Y(B',P_W)]= [[B, P_Y, S_X (H(B), P_Y)],P_W,S_Y([B, P_Y, S_X (H(B), P_Y)],P_W)]$.



In de bitcoin is dus zijn historie te lezen, en steeds is te zien dat de oude eigenaar de nieuwe eigenaar benoemt doordat de oude eigenaar met zijn secret key de hash van de nieuwe eigenaar en de oude bitcoin versleutelt. Dus vervalsen is niet mogelijk want de vorige eigenaar zegt met zijn secret key wie de volgende eigenaar is. Om de privacy van de spelers verder te vergroten kan een speler bij elke transactie een nieuw paar keys (P en S) kiezen. Hij hoeft alleen per bitcoin de secret key S te onthouden want als hij zijn bitcoin wil uitgeven dan moet hij signeren met S. Een bitcoin eigenaar heeft een 'wallet' met daarin een lijst van zijn bitcoins met de bijbehorende S en voor de zekerheid P.

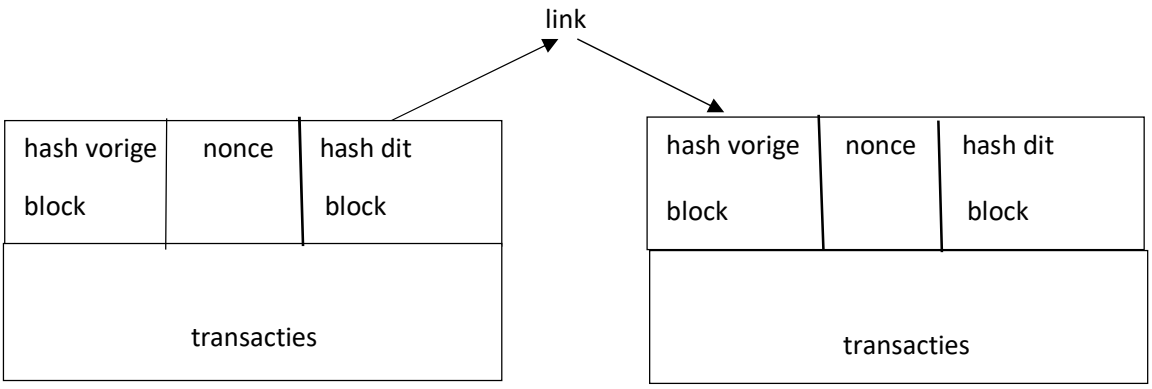
Wat niet gegarandeerd is, is dat een eigenaar van een bitcoin hem niet *meerdere* keren uitgeeft (overdraagt aan een ander). In het monetair systeem zoals hiervoor beschreven is daar een eenvoudige oplossing voor: de infrastructuur geeft bij elke transactie de bitcoin een nieuwe nummer versleuteld met de secret key van met monetair systeem en hij houdt van elke bitcoin in omloop het actuele transactienummer bij. Dit versleutelde transactienummer wordt dan onderdeel van de bitcoin. Zo kan de infrastructuur controleren dat een bitcoin niet voor de tweede maal wordt aangeboden door dezelfde eigenaar.

Maar het 'echte' bitcoin systeem wil geen centrale infrastructuur, ook al doet die nog zo weinig. En daarom is er een ander mechanisme ontwikkeld dat ook gebruik maakt van het proof-of-work principe en een zogeheten *blockchain*. Een blockchain is een openbare gedistribueerde database waarin alle bevestigde transacties van bitcoins staan. Zo'n 4000 per block, maar dat getal is niet relevant. Iedereen kan de blocks van de chain lezen maar niemand kan er iets aan

veranderen, want de blocks zijn beveiligd met een moeilijk te berekenen hash van de inhoud. Hier zit de proof-of-work in zoals we later zullen zien.

Bij elke transactie van een bitcoin krijgt deze een nieuwe representatie en wordt door de nieuwe eigenaar uitgezonden (gebroadcast) naar alle computers in het netwerk, nodes genaamd, van het bitcoin systeem (er moeten er genoeg zijn en iedereen mag mee doen). Elke node verzamelt nieuwe bitcoin representaties en *verifieert* ze op twee manieren: (1) hij checkt in de bitcoin of steeds de oude eigenaar het transport met zijn secret key heeft bevestigd en (2) hij kijkt in de actuele *blockchain* of de die daar al in voorkomt (dan wordt hij immers voor de tweede keer uitgegeven). Zodra één van deze tests negatief is wordt de transactie verwijderd. Anders komt hij de wachtrij van de node. Er is dus een publiek bekende blockchain van alle bevestigde bitcoin representaties.

De nodes zijn steeds bezig een nieuw block aan de keten toe te voegen. Om dit te doen moeten ze een proof-of-work doen. Daartoe zoeken ze een willekeurige string (nonce, een lose string, genaamd) waarmee ze de transacties in het block, dat ze aan te maken zijn, verlengen en passen daar de hash functie H op toe. Ze gaan hiermee door tot ze een getal krijgen dat begint met een voorgeschreven aan nullen. Net als bij het minen van nieuwe bitcoins! Dit proces heet daarom ook minen. Het feit dat het veel computertijd vergt om een goede hash van een block te vinden, is een garantie dat men niet kan vervalsen: als je ergens in de keten een block zou willen veranderen, dan moet je alle blocks die er na komen ook aanpassen en dit terwijl veel andere nodes bezig zijn met het toevoegen van nieuw blocks: het is praktisch onmogelijk dat proces nog in te halen. Per ca 10 minuten komt er een nieuw block vrij van één van de nodes.



De vakjes in het diagram geven niet goed de verhoudingen van de hoeveelheid dat weer: de transacties zijn veel groter dan de rest. Zij vormen de *body* van het block en de hash van de vorige, de nonce en de hash van het actuele block vormen de *header* van het block. De hash van het actuele block is dus berekend door H toe te passen op de string die men krijgt door alle

transacties achter elkaar te zetten, daar dan de hash van het voorgaande block achter te zetten en vervolgende de nonce toe te voegen. Waarbij de nonce dus gezocht moet worden zodat de hash van de hele string een voorgeschreven aantal voorloop nullen heeft, de proof-of-work. (In de praktijk zijn er wat technieken, o.a. een Merkle tree, om handiger met de hash om te gaan maar het principe is hetzelfde).

De blocks zijn dus gelinked: in een block staat de hash van het vorige aan een vorige block. Als men een block heeft kan men in principe de hele gedistribueerde database afzoeken tot men de vorige en volgende heeft. Dit kan natuurlijk handig georganiseerd worden met een tabel waarin de hashes van de blocks staan en hun adres (b.v. url).

Nodes werken altijd aan de langste keten. Zodra en een nieuw block wordt uitgezonden door een node stoppen alle anderen met hun werk en verwijderen uit hun wachtrij of block in aanbouw, de transacties die in het nieuwe block voorkomen. Het komt een enkele keer voor dat er twee verschillende nieuwe blocks tegelijk gepubliceerd worden. Dan gaat men verder met beide blocks tot er één met een nieuw block wordt uitgebreid. Dan gaat iedere node verder met de langste keten. Een ontvanger van een bitcoin moet wachten tot zijn transactie in een block is vastgelegd en liefst nog langer tot de blockchain met een aantal nieuwe blocks is uitgebreid. Dat is tijdrovend! Iemand die een bitcoin voor de tweede keer wil uitgeven en dus vals speelt, moet dat heel vlug doen nadat hij hem de eerste keer heeft uitgegeven, want de eerste transactie wordt al verwerkt in een nieuw block. Alleen als, met heel kleine kans, de tweede transactie in een ander nieuw block voorkomt dat tegelijk beschikbaar komt met het nieuwe block van de eerste transactie dan is er een probleem. Maar het betekent hooguit dat de eerste ontvanger gepasseerd wordt en de tweede het krijgt, maar niet dat de transactie uiteindelijk twee maal in de block chain terecht komt.

Bij veel betalingen heb je meer dan één bitcoin nodig net als bij betalen met chartaal geld. Er kan wissel-geld ontstaan. Dat kan allemaal eenvoudig geregeld worden.

De vraag blijft: waarom doen nodes mee aan het spel om een nieuw block voor de keten te berekenen? De incentive is een beloning die de node krijgt voor een nieuw block. Daartoe wordt van de transacties een klein bedrag (<2%) ingehouden t.b.v. de node. Zo wordt de miner beloond.

Er zijn diverse grote bezwaren aan het bitcoin systeem: (1) het rekenen met ‘munten’ waardoor je er meer per transactie nodig kan hebben en er wisselgeld ontstaat, (2) de traagheid waarmee transacties bevestigd worden waardoor het ongeschikt is voor realtime betalingen en (3) de enorme rekencapaciteit die nodig is om dit systeem op wereldschaal effectief te maken. De

energie behoefte voor dit rekenwerk is geschatte energiebehoefte van een Ierland.[25]. Voordelen zijn: (1) dat men geen centraal systeem nodig heeft, (2) dat men 'positief' geld heeft, de bitcoin vertegenwoordigt door zijn zeldzaamheid zijn eigen waarde en (3) men alle transacties bewaart en dus de hele historie op elk moment gereconstrueerd kan worden.

Het blockchain mechanisme kan ook op andere 'positief geld' systemen worden toegepast bijvoorbeeld bij effecten (aandelen en obligaties) die door een uniek nummer worden geïdentificeerd.

[25] K. O'Dwyer, D. Malone, "Bitcoin mining and its energy footprint", Irish signals and systems conference (2014)

Appendix 4: Koppeling aan het BBP en hoeveelheid basisgeld

De bedoeling is om de basisgeld bedragen op de individuele rekeningen (A, B en C) te koppelen aan het BBP. Dat wil zeggen dat die bedragen evenredig aan het nominale BBP gemaakt worden. Als het reële BBP niet verandert, stijgen en dalen de bedragen met de inflatie/deflatie. De koopkracht van het bedrag blijft gelijk. Als er ook nog productiviteitsstijging is, stijgt de koopkracht met die productiviteitsstijging. Om schokken te voorkomen, met speculatie daar omheen, moet je de rekeningbedragen frequent aanpassen. Zeg dagelijks. Dat betekent dat er dagelijks een BBP schatting beschikbaar moet zijn. Daartoe gebruiken we de som van de (reële) transacties gedurende het afgelopen jaar. Dat kan bijgehouden worden door MS, als het label *reëel* vermeld wordt bij de transacties. (zie Paragraaf 3).

Preciezer nu.
Stel, $B(t)$ is het BBP van het afgelopen jaar, aan het begin van dag t, en laat B^t de schatting ervan zijn die aan het begin van dag t gemaakt wordt.
Stel, $P_r(t)$ is de som van alle reële transacties (goederen en diensten) gedurende het afgelopen jaar, aan het begin van dag t
Het grote verschil tussen $B(t)$ en $P_r(t)$ is dat in de laatste grootheid ook alle transacties *in* voortbrengingsketens worden geteld. De fragmentatie van de voortbrenging heeft dus veel invloed. Maar als die niet al te snel wijzigt, en dat mag je verwachten, geldt dat $B(t) = \beta(t)P_r(t)$, met $\beta(t)$ een evenredigheidsconstante die maar heel langzaam met t verandert. Elke keer als er een formele schatting van het BBP beschikbaar komt, kunnen we, door ook $P_r(\cdot)$ te bepalen, een schatting krijgen van $\beta(\cdot)$. Stel, de koppeling wordt actief vanaf dag t_0. Neem aan dat de dan meest recente BBP schatting, B^-, slaat op de jaarperiode eindigend met dag $t^- - 1$ en dat we een schatting β^- hebben van de evenredigheidsconstante. Dan is de schatting aan het begin van dag t_0 van het BBP van het afgelopen jaar gelijk aan $B^0 = B^- \cdot (P_r(t_0)/P_r(t^-))$. Daarna geldt $B^t = B^{t-1} \cdot (P_r(t)/P_r(t-1))$. Tot er weer een nieuwe schatting, B^*, van het BBP komt. Neem aan die komt op dag t_N en betreft de jaarperiode eindigend met dag $t^* - 1$. Dan wordt op dag t_N de schatting gecorrigeerd met een factor $B^*/B(t^*)$. Om sprongetjes te voorkomen is aan te bevelen de correctie uit te strijken over een aantal dagen (het product van de correcties per dag moet weer gelijk zijn aan de totale correctiefactor).

Merk op dat door de koppeling van individuele rekeningen met het BBP het mogelijk wordt om bezit aan basisgeld ook uit te drukken in *pico-BBP.* Eén pico-BBP is gelijk aan $10^{-12}B^t$. Dan krijg je dus een systeem waarbij prijzen in euro's (of wat voor munt dan ook) zijn en bezit in pico's uitgedrukt wordt. De actuele schatting van het BBP, B^t, bepaalt de wisselkoers tussen pico en euro. Bij de behandeling van de wisselkoers problematiek maken we daar gebruik van.

Door de individuele rekeningen te koppelen met (de schatting van) het BBP, wordt ook gerealiseerd dat de totale hoeveelheid basisgeld in het systeem evenredig is aan (de schatting van) het BBP: $M(t) = \boldsymbol{f} \cdot B^t$. Die evenredigheid wordt niet verstoord door belasting te heffen op bezit van basisgeld, zolang het ingehouden basisgeld wordt toegevoegd aan een A-account van de overheid.

Deze evenredigheid wordt vaak verondersteld als "normaal" verband tussen BBP en geldhoeveelheid[26]. De evenredigheid kan verstoord worden door onevenredig veel financiële transacties. Het is nuttig hier ook de kwantiteitsvergelijking van Fisher bij te betrekken ($MV = PT$). In onze terminologie en beperkt tot de reële transacties is dat: $M(t) \cdot V_r = P_r(t)$, met V_r de (gemiddelde) omloopsnelheid van het basisgeld t.b.v. reële transacties in de jaarperiode eindigend met dag $t-1$. En omdat $B(t) = \beta \cdot P_r(t)$, geldt dus:
$M(t) = (B(t)/V_r \cdot \beta)$ en $\boldsymbol{f} = 1/(V_r \cdot \beta)$.

De constante $\boldsymbol{f}$ is de eerste monetaire parameter. De keus van $\boldsymbol{f}$ hangt dus samen met de fragmentatie van de voortbrenging en de omloopsnelheid van het geld. Die fragmentatie verandert natuurlijk steeds wel wat en door de toepassing van supply chain finance en vergelijkbare vormen van netwerk financiering kan de feitelijke fragmentatie ook gereduceerd worden[27]. Maar de factor β is stabiel en kan bepaald worden en het gaat dus toch vooral om de omloopsnelheid van het basisgeld. Neem aan het basisgeld wordt steeds 0,2 jaar vast gehouden, dan is $V_r = (1/0{,}2) = 5$ en als er alleen daar basisgeld voor nodig was, werkkapitaal en huishoudgeld, zou $\boldsymbol{f} = 1/(\beta \cdot 5)$ moeten volstaan.

Er is echter ook basisgeld nodig voor financiële transacties, hoewel die ook vaak om andere manieren gerealiseerd worden. Basisgeld kan nodig zijn om bij het beheer van een beleggingsportefeuille te switchen van de ene asset naar de andere. Stel je vervangt elk asset elke twee jaar en dat vraagt gemiddeld een overbrugging van 2 weken: Je verkoopt eerst en koopt twee weken later of je leent basisgeld om twee week eerder te kopen dan je verkoopt. Dan is daarvoor aan basisgeld gemiddeld ongeveer 2% van de totale waarde van de portefeuille nodig. Bij een totaal aan privé kapitaal van 6 maal het BBP (vergelijk Piketty[28]) is dat gelijk aan 12% van het BBP. Gevoegd bij de behoefte aan werkkapitaal en huishoudgeld zou dat dus leiden tot $\boldsymbol{f} = 1/(\beta \cdot 5) + 0.12$.

[26] Zie bijvoorbeeld Bezemer, "Finance and Growth; when Credit Helps and when in Hinders", INET, 2012
[27] Zie bijvoorbeeld Van der Vliet, "Concepts and Trade-Offs in Supply Chain Finance", Proefschrift TUE, 2015
[28] Thomas Piketty, "Capital in the Twenty-First Century", Harvard University Press

Dit is maar een voorbeeld om te illustreren dat zo in ieder geval een eerste referentiepunt voor $\boldsymbol{f}$ kan worden bepaald. De keus van $\boldsymbol{f}$ kan via trial-and-error worden verfijnd. Daarbij kan gebruik gemaakt worden van de mate waarin de banken gebruik maken van hun C-account. Zie hierna.

De banken kunnen basisgeld lenen via hun C-account. Ze mogen tot een bepaald bedrag negatief staan op die rekening. Die faciliteit is met name bedoeld om voldoende flexibel te zijn bij de kredietverlening ten behoeve van grote investeringen. Investeringen zijn gelijk aan besparingen ($I = S$). Maar dat wil niet zeggen dat die meteen bij elkaar komen. Stel er wordt een machine gekocht. Zolang die niet betaald is, financiert de machine leverancier. Dat zou zo kunnen blijven, dan hebben de investeringen de bijbehorende besparingen meteen gevonden. Maar in de regel gaat dat niet zo. Dan is het goed dat er een bank is die "voor kan schieten". Banken moeten gericht zijn op het verbinden van investeerders en spaarders. Het is dus belangrijk hoe lang de bank nodig heeft om de geïnvesteerde bedragen onder te brengen en hoe groot de investeringen zijn. De "gross capital formation" in de eurozone is ongeveer 20% van het BBP. Stel het duurt gemiddeld 1 jaar om dat bij spaarders onder te brengen. Dan is er totaal 0,2 $B(t)$ ruimte nodig op de B-accounts. De ruimte die je per bank beschikbaar stelt via de C-account kun je koppelen aan de door burgers en bedrijven aan de bank beschikbaar gestelde basisgeld bedragen. Dat is de monetaire parameter $\boldsymbol{g}$. Er is trial-and-error nodig om te bekijken welke factor $\boldsymbol{g}$ nodig is om de totale ruimte op de B-account gelijk te laten zijn aan wat nodig is voor de "capital formation" In bovenstaand voorbeeld $0{,}2B(t)$.

Als er meer en meer druk komt vanuit de bankwereld om de limiet op de C-account te verruimen en die ook te gebruiken voor werkkapitaal en huishoudgeld, zou dat wel eens kunnen betekenen dat de behoefte aan basisgeld daarvoor verkeerd is ingeschat.