

DIGITALISERING VAN CONTANT GELD

BACHELORSRIPTIE INFORMATIEKUNDE

Auteur: Marijn van der Zaag, student 0615242, marijn@vdsaag.nl

Begeleider: Prof. dr. Bart Jacobs

Datum: 20-7-2012

Radboud Universiteit Nijmegen



Inhoud

1	Probleemstelling.....	3
1.1	Hoofd- en deelvragen	3
1.1.1	Deelvraag 1: Voor welke transactiesituaties is nog geen bruikbare ICT beschikbaar?	3
1.1.2	Deelvraag 2: Welke nieuwe ICT zou een contantloze samenleving mogelijk maken?	3
2	Verantwoording.....	3
3	Theoretisch kader.....	4
3.1	Security.....	4
3.2	Privacy.....	5
3.3	Belangen van de banken	6
3.4	Belangen van Ondernemers	6
3.4.1	Concrete redenen van ondernemers voor uitsluitend gebruik van contant geld.....	7
3.5	Belangen van Particulieren	7
3.5.1	Concrete redenen van particulieren voor het gebruik van contant geld	8
3.6	Belangen van de maatschappij	8
4	Methode	8
4.1	Deelvraag 1.1.1	8
4.2	Deelvraag 1.1.2.....	9
5	Resultaten	9
5.1	Deelvraag 1: Voor welke transactiesituaties is nog geen bruikbare ICT beschikbaar?	9
5.1.1	Kosten van elektronische betaling voor de ondernemer	9
5.1.2	Het regelen van een pinapparaat.....	10
5.1.3	Technische problemen.....	10
5.1.4	Zwart geld.....	11
5.1.5	Particulieren die met andermans geld betalen	11
5.1.6	Mensen zonder bankrekening	11
5.1.7	Buitenlanders zonder Nederlandse bankrekening.....	12

5.1.8	Ontbrekende kennis of vaardigheden	12
5.1.9	Contant geld voor budget management	13
5.1.10	Tijdelijke kas met contant geld.....	13
5.1.11	Persoonlijke spaarpot thuis.....	14
5.1.12	Retourbetalingen.....	14
5.1.13	Plaatselijke betalingen tussen particulieren.....	14
5.1.14	Ontraceerbaarheid (anonimiteit)	15
5.1.15	Gebruik van contant geld uit gewoonte.....	15
5.1.16	Zwaaien met flappen en rinkelen met munten.....	15
5.1.17	Gebrek aan vertrouwen in de technologie.....	15
5.2	Deelvraag 2: Welke nieuwe ICT zou een contantloze samenleving mogelijk maken?.....	16
5.2.1	Uitbreiding van bestaande ICT voor nieuwe elektronische betaalmogelijkheden.....	16
5.2.2	Een gedecentraliseerd systeem als cashvervanger	20
6	Conclusie en discussie	24
6.1	Vervolgonderzoek	25
7	Literatuur	26

1 Probleemstelling

Geld is in de Nederlandse samenleving en daarbuiten niet meer per se iets fysieks. Geld kan worden gezien als informatie (namelijk een beschikbaar tegoed, zoals de nummertjes op een bankrekening) en geldstromen dus als communicatie. Omdat de ICT hard is ontwikkeld in de afgelopen decennia, ligt het voor de hand dat contant geld in de toekomst niet meer nodig is. Het aantal contante betalingen en het aantal opnamen van contant geld zijn dan ook al jaren aan het dalen en het aantal elektronische transacties stijgt tegelijk. [1] Er zijn tegenwoordig veel supermarkten met kassa's die geen contant geld meer accepteren. Vanuit oogpunt van efficiëntie is dit een logische ontwikkeling, omdat contant geld onder andere fysiek transport, geldautomaten, tellen en wisselen vereist. Dit roept de vraag op of we in de toekomst nog altijd contant geld willen blijven gebruiken naast de elektronische betaalmiddelen. Waarom gebruiken we tegenwoordig nog contant geld? Voor sommige situaties is contant geld nog echt het enige bruikbare betaalmiddel, maar er spelen ook de onderwerpen privacy en security. Aan welke eisen waaraan contant geld voldoet, voldoen de algemeen gebruikte elektronische betaalmiddelen nog niet? Zou dit 'gat' met ICT-innovatie gevuld kunnen worden of is het te verwachten dat het wenselijk is om contant geld altijd te behouden? In dit onderzoek worden mogelijkheden gezocht om alle geldtransacties elektronisch te doen.

1.1 Hoofd- en deelvragen

HOOFDVRAAG: (HOE) KAN ICT ERVOOR ZORGEN DAT CONTANT GELD OVERBODIG IS?

1.1.1 Deelvraag 1: Voor welke transactiesituaties is nog geen bruikbare ICT beschikbaar?

Dit wordt een analyse van de in het theoretisch kader beschreven redenen waarom nog contant geld wordt gebruikt. Zijn de problemen tijdelijk van aard, bijvoorbeeld omdat ouderen nog moeten wennen aan elektronisch betalen, of is er echt nog technische innovatie nodig voordat overgestapt zou kunnen worden naar een contantloze samenleving? 'Bruikbaarheid' gaat over functionaliteit, maar ook randvoorwaarden als robuustheid.

1.1.2 Deelvraag 2: Welke nieuwe ICT zou een contantloze samenleving mogelijk maken?

Voor de situaties die gevonden zijn in de eerste deelvraag: welke innovaties zijn gewenst? Kan technologie overal een oplossing bieden, of blijven er altijd redenen bestaan om contant geld te gebruiken?

2 Verantwoording

Zoals al gezegd in de probleemstelling, is contant geld in de huidige maatschappij in theorie meestal niet meer per se nodig en wordt het ook steeds minder gebruikt. Er worden elk jaar weer stapjes

genomen om ICT meer in te zetten ten koste van contante betalingen. Nederlanders hebben eigenlijk sowieso al een probleem als ze geen bankrekening hebben en de kortste weg tussen twee bankrekeningen is digitale communicatie. Het gebruik van contant geld kan men daarom zien als een omweg met allerlei logistieke, materiële en arbeidsintensieve consequenties. Toch zijn er nog belangrijke redenen om contant geld te gebruiken in dit tijdperk. In dit onderzoek wordt gezocht naar ICT die deze redenen zou kunnen wegnemen, ten bate van gemak en efficiëntie van het betalingsverkeer. Tegelijk wordt ook gekeken naar de nadelen die deze voorgestelde innovaties hebben, zodat een beeld kan worden gevormd over de vraag of we in de toekomst nog contant geld willen blijven gebruiken. Dit geeft een zorgvuldig afgewogen doel aan waar ontwikkelaars en andere betrokken partijen zich het beste op kunnen richten, en een voorstel voor mogelijke manieren om het te bereiken.

3 Theoretisch kader

De scope wordt gesteld op transacties en opgeslagen geld in Nederland, omdat de onderzoeker de cultuur en staat van technische ontwikkeling hier kent. In andere delen van de wereld moet wellicht rekening gehouden worden met andere omstandigheden en waarden. De belanghebbenden zijn **banken** (inclusief alle werknemers zoals kantoorpersoneel), **ondernemers** (inclusief kassapersoneel), **particulieren** (mensen die geld uitgeven of ontvangen) en (voor zover niet onder de vorige groepen te scharen) **de maatschappij** als geheel. Er wordt van uitgegaan dat de overheid volledig in dienst staat van de maatschappij, en dat de overheid dus geen aparte belangenpartij is. De belangen van deze groepen op het gebied van het verschil tussen contante en elektronische betalingen worden hieronder uiteengezet, maar eerst een algemeen overzicht over de verschillen tussen de twee op het gebied van veiligheid en privacy.

3.1 Security

In Nederland is een bepaalde hoeveelheid geld in omloop om ons economisch systeem mogelijk te maken. Door een natuurlijk egoïsme zullen er altijd mensen zijn die hun persoonlijke deel op oneerlijke wijze proberen te vermeerderen, door middel van zelf geld 'bijmaken' of door geld ergens vandaan te stelen. Deze menselijke neiging maakt het onderwerp security heel erg belangrijk.

Met contant geld is beveiliging relatief overzichtelijk. Er zijn namelijk twee dingen voor nodig, allebei fysiek van aard. De eerste is het voorkomen van vervalsing door gebruik van moeilijk te kopiëren echtheidskenmerken (voorkomen van ongeautoriseerd geld maken) en de tweede is het beschermen van de locatie van het geld, bijvoorbeeld door kluisen en beheerde portemonnees (voorkomen van stelen). Bij elektronische tegoeden gaat het voorkomen van die problemen heel anders. Abstract gezien worden ook daarbij echtheidskenmerken en beveiligde 'locaties' (informatiedragers en op een ander niveau bankrekeningen) gebruikt, maar het valt onder een heel ander vakgebied, namelijk cryptografie. Omdat de meeste mensen weinig van cryptografie snappen, hebben mensen op de beveiliging van hun contant geld veel meer invloed en ook meer verantwoordelijkheid. Schade door elektronische geldfraude wordt daarom tot nu toe door banken vergoed, al hebben ze zich daartoe niet officieel verplicht in de gebruiksvoorwaarden.

De Nederlandse Vereniging van Banken brengt fraudecijfers op een optimistische manier naar voren [2], maar uit die cijfers blijkt wel dat er in 2011 (€92 mln) met veel meer geld is gefraudeerd dan in

2010 (€57 mln). Verreweg de meeste schade en ook de grootste verergering zit hem in skimming (€40 mln in 2011) en fraude met internetbankieren (€35 mln in 2011). Blijkbaar is elektronisch geldverkeer voor de grote dieven interessanter dan contant geld.

Naast het voorkomen van toegang van ongeautoriseerden (dieven), valt ook beschikbaarheid onder security, volgens de *CIA Triad* 'confidentiality, integrity, availability'. Een transactie met contant is altijd beschikbaar zolang er contant geld aanwezig is; men overhandigt dan gewoon het geld. Benodigd wisselgeld moet dan echter ook vaak beschikbaar zijn. Contant geld zelf is beschikbaar bij onder andere banken, geldautomaten en de eigen spaarpot. Uiteraard moet het wel bewust zelf meegenomen worden. Als het in de portemonnee of kassa zit, is het beschikbaar. Elektronische betalingen hebben het voordeel dat het volledige tegoed op een bank in principe bij relevante plekken als betaalautomaten en ATM's beschikbaar is met een pinpas en bijbehorende code. Het digitale en centrale karakter in combinatie met de beveiliging maakt een flexibele beschikbaarheid mogelijk, maar men is daarbij wel afhankelijk van automaten en de benodigde digitale communicatie. Vanuit particulieren onderling gezien is de beschikbaarheid juist weer niet zo goed, omdat voor een elektronische overschrijving een internetverbinding nodig is. Qua beschikbaarheid zijn contant geld en bankrekeningen met de bijbehorende transactiemogelijkheden zo verschillend, dat het volledig van de gebruikers en situatie afhangt welke van de twee de voorkeur heeft.

Ook *onweerlegbaarheid* speelt nog een rol. Dit is de waarborg dat een transactie niet kan worden ontkend. Contant geld biedt die waarborg zelf niet, dus daarvoor kunnen bonnetjes en handtekeningen worden gebruikt. Bij bankoverschrijvingen zorgt de bank, de centrale vertrouwde partij, voor onweerlegbaarheid. Decentrale digitale geldsystemen moeten ook een onweerlegbaarheid ingebouwd hebben, omdat anders geen veilige betaling op afstand mogelijk is, bijvoorbeeld bij een internetbestelling.

3.2 Privacy

Het onderwerp privacy hangt samen met beveiliging, het centrale karakter van bankrekeningen en het decentrale karakter van contant geld. Voor elektronische transacties zoals die nu voornamelijk gebeuren (PIN, chipknip, creditcard) hebben banken en ondernemers informatie nodig van de betaler en ontvanger. Zo kan de ondernemer bijvoorbeeld het rekeningnummer van alle elektronisch betalende klanten en het bedrag en de datum van de transacties op pinbonnen bekijken. Bij directe overschrijvingen en gebruik van iDeal staat dit zelfs jarenlang tussen de lijst met af- en bijschrijvingen op internet. De transacties zijn gekoppeld aan een rekeningnummer en elk rekeningnummer aan een persoon. Die informatie is digitaal opgeslagen en door netwerken als het wereldwijde internet ook nog in theorie van veraf beschikbaar. Natuurlijk is het ook in het belang van banken om die transactie-informatie goed te beschermen, maar als alle transacties elektronisch zouden gebeuren, geeft dit bijvoorbeeld de overheid in principe erg veel macht. Het zou zelfs kunnen dat de overheid van de VS uit naam van internationale veiligheid privacygevoelige gegevens als deze transacties via SWIFT (Society for Worldwide Interbank Financial Telecommunication) zullen opeisen bij Nederlandse banken. Ook is algemeen bekend dat 100% veiligheid nooit gegarandeerd kan worden, dus van tijd tot tijd zullen er misschien hackers zijn die erin slagen transactiegegevens te verkrijgen, aangezien die informatie heel waardevol kan zijn.

Het is niet per se nodig dat beveiligde, opgeslagen transacties te traceren zijn naar de betaler. David Chaum stelde in 1983 voor om een beveiliging met 'blind signatures' te gebruiken om ontraceerbaarheid van onschuldigen in combinatie met veiligheid te garanderen. [3] Stefan Brands

hield zich later bezig met hetzelfde probleem en schreef daarover het boek *'Rethinking public key infrastructures and digital certificates: building in privacy'*:

"De oplossing voor het privacy-probleem ligt volgens Brands in een nieuw soort digitaal certificaat dat hij heeft ontwikkeld. Het belangrijkste kenmerk van dat certificaat is dat iedere houder zelf kan bepalen welke persoonlijke informatie hij of zij prijsgeeft op elk moment. [...] Wanneer je gaat rekeningrijden is alleen de afschrijving van het juiste bedrag van belang. Daarbij hoeft je identiteit niet bekend te zijn. Pas wanneer er sprake is van fraude, wanneer een muntje twee keer uitgegeven wordt bijvoorbeeld, zou het mogelijk moeten zijn om uit een code de identiteit van de betrokkenen te achterhalen. Met mijn methoden is dat op efficiënte en veilige wijze te realiseren. De transacties van eerlijke gebruikers blijven echter ontraceerbaar" [4]

Brands heeft verschillende patenten verkocht (o.a. aan Microsoft), maar zijn ideeën zijn niet terug te zien in het hedendaagse betalingsverkeer.

Contant geld is niet zo traceerbaar als de gangbare digitale transacties. Briefgeld heeft wel een identificatienummer, maar dat hoeft normaal gesproken helemaal niet bekeken of opgeslagen te worden en dat gebeurt dus ook alleen heel gericht voor het opsporen van criminelen. Nergens hoeft de informatie opgeslagen te worden hoe veel contant geld een bepaald persoon op een bepaald moment bezit en daarmee ook niet dat een bepaald persoon er een bepaald product mee heeft gekocht. Het bezit van dat geld is simpelweg fysiek gegeven, bijvoorbeeld doordat het in de portemonnee van de eigenaar zit. De enige manieren waarop iemand anders daar ongevraagd achter komt, zijn door te eigenaar te fouilleren, te bespioneren of een huiszoeking te doen. De geldbezitter heeft veel controle op wie inzicht heeft in zijn financiële zaken en dat geeft dus privacy.

Bij een scenario waarin alle transacties met pin, chipknip of creditcard worden gedaan, hebben banken volledige greep op alle geldstromen. De complete betalingsdata van alle klanten zijn in hun beheer en die informatie zou veel waard zijn voor bijvoorbeeld adverteerders. In theorie is ook veel meer bemoeienis van overheid (belastingdienst) en onderzoekerswerk mogelijk. Als niet kan worden uitgegaan van volledig vertrouwen in de overheid, kan men dus bang zijn voor effectieve en efficiënte onderdrukking. Omdat de veel geaccepteerde elektronische betaalmiddelen allemaal gecentraliseerde systemen zijn, is contant geld het enige algemeen geaccepteerde betaalmiddel waarmee privacy is gewaarborgd. Dat is de reden dat veel contant geld wordt gebruikt in het criminele circuit, maar kan ook een reden zijn voor brave burgers om bijvoorbeeld in een slijter of seksshop contant te betalen.

3.3 Belangen van de banken

De Nederlandse banken zijn samen verantwoordelijk voor de distributie van contant geld. Het is een taak die hun is opgedragen, maar de banken hebben er geen direct belang bij. Het zou banken veel geld besparen als deze taak niet meer nodig was, dus er is een duidelijk belang bij het verdwijnen van contanten. Er zijn dan geen automaten meer nodig voor opnemen van contant geld, geen geldtransporten, er hoeft geen geld meer te worden geteld enzovoorts. Er is wel meer elektronische infrastructuur nodig omdat het aantal elektronische betalingen toeneemt, maar voor het grootste deel is die infrastructuur (met de nodige beveiligingsmaatregelen) er toch al. Banken zijn dan ook over het algemeen voorstanders van een conversie naar contantloos [5].

3.4 Belangen van Ondernemers

Voor ondernemers is het heel erg belangrijk tevreden klanten te hebben. Zolang klanten om wat voor reden dan ook contant willen betalen, zullen de meeste ondernemers die mogelijkheid willen

blijven bieden [1] [5]. Hun eigen, directe belangen hebben vooral met betaalkosten en kassabeveiliging te maken.

Een onderzoek in 12 uiteenlopende branches concludeerde dat elk van de ondervraagde ondernemers enkele procenten tot ruim 70% zou besparen op betaalkosten kosten als alle betalingen elektronisch zouden gebeuren [6]. Dit heeft verschillende oorzaken zoals het wisselen, storten, controleren op echtheid en kopen van contant geld en de kosten van pinautomaten en contracten met de bank. De ambulante handel heeft wel wat extra aandachtspunten bij elektronische transacties, omdat een vaste dataverbinding ontbreekt, omdat elektronica gevoeliger is voor weersomstandigheden en bijvoorbeeld bij een val stuk kan gaan.

Kassabeveiliging wordt veel simpeler als er geen contant geld meer wordt gebruikt, want overvallers kunnen geen geld stelen dat niet in de winkel ligt. Dit geeft ook een veiliger gevoel bij caissier(e)s. Elektronische beveiliging is op zich ook heel ingewikkeld, maar omdat de ondernemer er weinig verantwoordelijkheid over heeft, is dat vanuit zijn gezichtspunt geen probleem. Wel moet de ondernemer erop kunnen vertrouwen dat het werkt en moeten verantwoordelijkheden en aansprakelijkheid helder zijn.

3.4.1 Concrete redenen van ondernemers voor uitsluitend gebruik van contant geld

Voor een contantloze samenleving zou het nodig zijn dat alle ondernemers elektronische betalingen accepteren. De ondernemer kan de volgende redenen hebben om geen elektronische betaalmogelijkheid te bieden:

1. Het bieden van bestaande elektronische betaalmogelijkheden kost te veel geld
2. Het kost te veel moeite of kennis om te regelen
3. Het risico op technische problemen is te groot
4. De ondernemer wil contant betaald worden om het geld zwart te houden

3.5 Belangen van Particulieren

Particulieren hebben belang bij het hebben van veel betaalmogelijkheden, privacy en natuurlijk weer veiligheid van hun geld. Als mensen altijd overal met elke gewenste methode, anoniem en veilig kunnen betalen en hun geld op de gewenste manier kunnen beheren, dan zijn waarschijnlijk al hun belangen behartigd. Concreter gaat het hier bijvoorbeeld om betaalgemak, overzicht in de eigen geldstromen (waar sommigen het contant geld in de portemonnee voor gebruiken) en beschikbaarheid over het eigen tegoed. Voor dat laatste is het belangrijk dat mensen elektronisch kunnen betalen. Ook willen mensen in staat zijn iemand anders iets van hun geld te laten kopen, bijvoorbeeld als ouders hun kind naar de bakker sturen. Daarvoor is nu nog steeds contant geld het medium. Chipknip is in principe ook geschikt, maar dat wordt niet veel geaccepteerd.

3.5.1 Concrete redenen van particulieren voor het gebruik van contant geld

Voor een contantloze samenleving zou het nodig zijn dat alle particulieren alle betalingen elektronisch doen. Mensen kunnen in de volgende situaties reden hebben om dat niet te doen en dus contant te betalen:

1. Iets kopen in opdracht, van iemand anders' geld
2. Ontbreken van een bankrekening (daklozen, toeristen, vluchtelingen)
3. De betaler heeft geen Nederlandse bankrekening (toeristen)
4. Onbegrip van elektronische betaalwijzen of angst voor techniek (ouderen)
5. Gebruik van contant geld om een budget bij te houden
6. Gebruik van een tijdelijke kas waarvoor men geen aparte bankrekening aan wil vragen (bv. de kas voor een studentengala)
7. Thuis geld sparen in een zelf beheerde spaarpot
8. De transactie betreft een retourbetaling, dus van ondernemer naar klant
9. Betalingen tussen particulieren onderling, met name als ze samen uit zijn of het geld een cadeau is
10. Ontraceerbaarheid (anonimiteit)
11. Het is aangeleerd en een gewoonte
12. Het aanzien van het bij zich hebben van (veel) contant geld
13. Geen vertrouwen in technologie.

3.6 Belangen van de maatschappij

Zoals eerder in dit hoofdstuk is behandeld, geeft de opslag van alle transactie-informatie mogelijkheden voor controle door onder andere de overheid. Er speelt een privacyprobleem, maar de mogelijkheden kunnen ook positief worden benut. Zo kunnen criminelen makkelijker gepakt worden, wordt belastingaangifte makkelijker en kunnen betalingen niet meer zwart worden gedaan. Volgens De Nederlandsche Bank zou het de maatschappij een hoop geld besparen als we alle transacties elektronisch zouden doen. Als we slechts uitgaan van de gebruikelijke elektronische betaalmethoden als PIN en creditcard, moet men echter wel veel vertrouwen hebben in banken en de overheid om dit efficiëntie-argument significant te noemen.

4 Methode

4.1 Deelvraag 1.1.1

De in het theoretisch kader genoemde redenen om contant geld te gebruiken worden geanalyseerd met behulp van literatuur en eigen (informatiekundig) inzicht. Hier wordt voornamelijk onderscheid gemaakt tussen redenen die met de tijd zullen verdwijnen door gewenning en andere ontwikkelingen, en redenen die om ICT-innovatie vragen.

4.2 Deelvraag 1.1.2

In literatuur zijn innovaties te vinden die ondernemers wensen [1] en uitgewerkte ideeën voor elektronische betalingen. [7] [8] [9] Met behulp van die literatuur en eigen inzicht worden manieren gezocht (zo veel mogelijk op functioneel niveau) om ICT in te zetten zodat contant geld niet meer nodig zal zijn. Het resultaat hiervan is een schets van mogelijke ICT-oplossingen en hun gewenste functionaliteit, en een overzicht van problemen waar ICT geen oplossing kan bieden.

5 Resultaten

5.1 Deelvraag 1: Voor welke transactiesituaties is nog geen bruikbare ICT beschikbaar?

5.1.1 Kosten van elektronische betaling voor de ondernemer

Een reden die ondernemers geven voor het niet aanbieden van elektronische betaalmogelijkheden is dat dat te veel geld kost. Onderzoek van de Stichting Bevorderen Efficiënt Betalen (BEB) heeft deze redenering weersproken:

“Wij hebben [...] kunnen constateren dat meer pinnen leidt tot lagere totale kosten op jaarbasis voor het betalingsverkeer van de ondernemer. Nog niet alle ondernemers realiseren zich dit en hebben nog het (achterhaalde) beeld dat contante betalingen voor hen financieel aantrekkelijker zijn.” [6]

Deze belangenstichting streeft ernaar, zoals de naam doet vermoeden, ondernemers en consumenten te laten overstappen van het gebruik van contant geld naar elektronische transacties. Een van hun resultaten is het Convenant Betalingsverkeer 2005, waarmee alle ondernemers 1 cent korting krijgen op elke pintransactie vanaf 1 januari 2005. Ook hebben ze subsidies geregeld voor pinpakketten voor kleine ondernemers. Mede door deze inspanningen zijn dus de kosten van pinbetalingen omlaag gegaan. In het onderzoek van Stichting BEB is ook de ambulante handel, met een gemiddeld transactiebedrag van slechts €9, meegenomen. Ook die ondernemers zouden volgens de resultaten tientallen procenten aan betalingskosten besparen door alle contante betalingen voortaan elektronisch te laten verlopen.

Als onze maatschappij overgestapt zou zijn naar een contantloze samenleving, zou de prijs echter weer omhoog kunnen gaan vanwege de afhankelijkheid van het elektronisch betaalsysteem, dat sinds januari 2012 in handen is van de commerciële partijen Visa (V-pay, alleen Europa) en MasterCard (Maestro, ook buiten Europa). Als er geen non-proprietary transactiesysteem meer is, kan het betalingsverkeer lijden onder een ‘vendor lock-in’. Om dit risico helemaal te voorkomen, moet er een onafhankelijk, open betalingssysteem beschikbaar zijn. Mogelijkheden voor zulke systemen zijn genoemd in 5.2.2. Dit punt van kosten voor de ondernemer wordt verder niet expliciet behandeld, omdat voorlopig concurrentie zal blijven bestaan tussen Visa en MasterCard.

Volgens Cash Report 2011 [5] is het overigens ook nog niet voldoende onderzocht of elektronische transacties voor de samenleving als geheel nu goedkoper zijn dan contante.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.2 Het regelen van een pinapparaat

De volgende reden die ondernemers geven voor het niet aanbieden van elektronische betaalmogelijkheden is dat dat te veel moeite of kennis kost om het te regelen. Er zijn inderdaad meerdere dingen nodig, namelijk een apparaat dat gekocht of gehuurd moet worden, een dataverbinding (vaste telefoon, vast breedband of mobiel internet) en een contract met de bank. Er moet dus ook uitgezocht worden wat voor het bedrijf de optimale keuze is tussen de beschikbare diensten en apparaten. Dit kost tijd en moeite, maar alle benodigde informatie hiervoor is op internet aanwezig. Er zijn ook verschillende totaalpakketten te verkrijgen, waardoor niet alles apart geregeld en beheerd hoeft te worden. De website www.slimmepinpakketten.nl heeft een pakkettenvergelijker die negen aanbieders heeft geselecteerd in samenwerking met de Stichting BEB.

Het regelen van pinmogelijkheden vereist dus geen specialist, maar wel wat tijd. Die benodigde tijd valt echter waarschijnlijk in het niet bij alle andere bij-activiteiten die bij het ondernemerschap komen kijken, zoals administratie, beheer van panden, bevoorrading, etcetera. Het regelen van pinmogelijkheden wordt in de toekomst wellicht nog wat makkelijker. Het betreft hier echter geen innovatie van ICT, omdat er altijd hardware, communicatie en bankcontracten geregeld zullen moeten worden om elektronisch betalingsverkeer mogelijk te maken.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.3 Technische problemen

Het volgende genoemde probleem is de kans op technische problemen. In een samenleving met slechts contant geld zijn die er weinig, hoewel het dan wel mogelijk is dat briefjes per ongeluk scheuren of de kassa klem zit. De technische problemen zijn relatief overzichtelijk en vaak door leken op te lossen. We leven echter in een samenleving waarin de meeste mensen hun inkomsten op de bankrekening gestort krijgen en contant geld daardoor meestal uit een ATM (pinautomaat om contant geld op te nemen) komt. Deze automaten kennen ook storingen, zoals voorkwam in augustus 2011 [10]. Problematischer zijn storingen van betaalautomaten waar klanten proberen af te rekenen. Dit kunnen problemen in hardware of software zijn ([11]), maar het kwetsbaarst is de dataverbinding met de bank. Een pintransactie lukt alleen als eerst bij de betreffende bankrekening is gecontroleerd of het saldo voldoende is, dus die verbinding is cruciaal. Gebruikers van smartphones weten dat het mobiele netwerk in Nederland lang niet zo robuust is als bijvoorbeeld het stroomnet. Op festivals, waar veel mensen vlak bij elkaar tegelijk proberen te pinnen, komt het vaak voor dat het netwerk daarvoor niet voldoende bandbreedte tot zijn beschikking heeft (dit heeft de onderzoeker zelf ervaren tijdens werk achter verschillende festivalkassa's). Zodra transacties mislukken, zullen ze bovendien opnieuw geprobeerd worden, wat leidt tot nog meer transactie pogingen waarvan er nog minder blijken te slagen. De zorgen van ondernemers over afhankelijkheid van pinbetalingen zijn dus zeker terecht. Dit is geen reden om de mogelijkheid überhaupt niet te bieden, maar betekent wel dat in de huidige situatie pinnen niet robuust genoeg is zonder offline of asynchrone betaalvormen als alternatieve mogelijkheid.

Een reden die ondernemers niet snel expliciet zullen noemen maar die wel relevant is in deze context, is dat alle pinpassen en pinautomaten afhankelijk zijn van dezelfde technologie, geschaard onder de wereldwijde standaard 'EMV' (Europay, MasterCard, Visa). Eventuele storingen zullen daardoor al snel grote problemen kunnen geven. Sinds 'Het Nieuwe Pinnen' gebruiken we alleen maar passen en automaten met EMV-chips.

Chipkniptransacties hebben ongeveer even veel last van technische storingen als contante betalingen (gegeven dat het contante geld moet worden opgenomen bij een ATM), omdat die transacties asynchroon gebeuren: de verbinding met de bank is dus niet direct tijdens de transactie nodig. Het is een interessante tegenstelling dat er aan de ene kant zorgen worden uitgesproken over transactiekosten en (eventuele) technische storingen, en aan de andere kant de chipknip, die op dat gebied misschien prima oplossingen biedt, op de meeste plekken niet meer geaccepteerd wordt.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.4 Zwart geld

De laatste reden die ondernemers hebben voor het behoud van contante betalingen is dat het dan zwart kan worden gebruikt, wat overigens sterk samenhangt met het anonieme karakter van contant geld. Dit is echter tegen de wet en dit specifieke belang is dus niet eentje die per se behartigd moet worden. De mogelijkheid van ontraceerbaarheid is echter wel van maatschappelijk belang. We willen niet in een dictatuur leven; iedereen is in onze samenleving onschuldig tot schuld is bewezen. De met deze reden samenhangende belangen worden dus in de volgende deelvraag behandeld, maar dit specifieke punt van zwart geld niet.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.5 Particulieren die met andermans geld betalen

Voor particulieren is een belangrijke reden om contant geld te gebruiken de situatie waarin bijvoorbeeld ouders hun kind naar een winkel sturen om iets te kopen van het geld van de ouders. Een pinpas in de huidige vorm is hiervoor niet geschikt, want de ouders zouden de controle over hun geld verliezen als ze de pas en pincode meegeven. Een chipknip is in dit geval bruikbaar (mits met chip betaald kan worden natuurlijk), maar dan is ook een saldolezer nodig voor de ouders om te zien hoe veel geld eraf is gehaald. Die bestaan, al hebben weinig mensen ze ooit gezien. Voor deze betaalsituatie bestaat dus bruikbare ICT, maar het is de moeite waard om te kijken naar andere oplossingen. Chipknip wordt door gedaalde pinkosten namelijk alleen nog maar gebruikt voor vaste catering en automaten [12]. Misschien kunnen banken een service verlenen door het uitgeven van deelpinpassen met een zeer laag en/of makkelijk instelbaar maximaal besteedbaar bedrag, een eigen pincode en een e-mail of sms ter notificatie per besteding aan de rekeninghouder. Dit zou ook de gewenste vrijheid en controle kunnen geven.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.6 Mensen zonder bankrekening

Er zijn mensen in Nederland die geen bankrekening hebben. Deze hebben natuurlijk geen pin- of chippas en kunnen daarom bijvoorbeeld bij winkels niet elektronisch betalen, behalve met een pre-paid creditcard of pre-paid chipknip, die op hun beurt ook weer niet zomaar elektronisch te kopen zijn zonder bankrekening. Nederlandse banken hebben renseigneringsplicht, wat betekent dat ze bepaalde informatie over al hun rekeninghouders moeten doorspelen aan de belastingdienst. Om hieraan te kunnen voldoen, moet iedereen die een rekening opent zich identificeren en ook het burgerservicenummer (BSN) geven. Aangezien er in Nederland mensen zijn, zoals vluchtelingen, die de vereiste Nederlandse identificatiebewijzen niet hebben, kunnen de mensen zonder bankrekening

niet worden genegeerd. Deze mensen hebben waarschijnlijk niet veel te besteden, maar moeten uiteraard wel kunnen betalen en op dit moment is dat elektronisch bijna niet te doen. In theorie is dit op te lossen met anonieme chipkaarten, ongeveer zoals de anonieme variant van de OV-chipkaart of de telefoonkaarten voor telefooncellen (maar dan oplaadbaar). Er kan zelfs gedacht worden aan gedecentraliseerde systemen als Bitcoin. Als iemand geen bankrekening heeft, betekent dat zeker niet dat diegene ook geen telefoon heeft. In Afrika is bijvoorbeeld in de meeste landen het telefoongebruik de afgelopen jaren erg hard gestegen; telefoons zijn daar gebruikelijker dan bankrekeningen [13]. Sommigen stellen dat meer mensen op aarde een telefoon hebben dan een bankrekening, al is hier geen betrouwbare bron voor gevonden. Om een elektronische betaalmethode toegankelijk te maken voor iedereen, moet echter waarschijnlijk toch iets anders worden bedacht.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.7 Buitenlanders zonder Nederlandse bankrekening

Als de consument geen Nederlandse bankrekening heeft, kan hij meestal gewoon in Nederland elektronisch betalen vanaf een buitenlandse bankrekening. Toch kan het problemen geven, bijvoorbeeld omdat mensen in de VS gewend zijn met creditcard te betalen en die in Nederland op de meeste plekken niet wordt geaccepteerd. [1] In België is het bijvoorbeeld bij pinautomaten en ATM's nog vaak onvoorspelbaar of er nu wel of niet betaald of geld opgenomen kan worden met een Nederlandse pinpas. Er wordt wel steeds meer gebruik gemaakt van dezelfde internationale standaarden en in Europa zijn hierover afspraken gemaakt. In een persbericht over een akkoord uit mei 2009 staat:

“Binnen enkele jaren kunnen alle consumenten met hun betaalpas in heel Europa zonder problemen afrekenen met pinnen.” [14]

Omdat culturen over de hele wereld ondanks de globalisatie toch nog enorm verschillend blijven, en dus vast ook op dit gebied, moet er rekening gehouden worden met mensen die in Nederland willen betalen zonder een Nederlandse bankrekening te hebben. Daarmee wordt deze situatie vergelijkbaar met de situatie van mensen die helemaal geen bankrekening hebben en dit vraagt dus om een soortgelijke oplossing. Een contantloze samenleving is op dit moment niet acceptabel voor deze groepen.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.8 Ontbrekende kennis of vaardigheden

Het komt voor dat mensen contant betalen om de reden dat ze de elektronische betaalmiddelen niet begrijpen of, breder nog, een algemene angst of afkeer tegen ICT hebben. Dit zullen vrijwel alleen ouderen zijn, want op scholen van haast alle niveaus wordt tegenwoordig geacht dat de leerlingen/studenten computers gebruiken bij hun leerwerk, daarom kan men ervan uitgaan dat de nieuwere generaties daarmee om kunnen gaan. Nederlanders groeien al jaren op met ICT, en het betalen met een pinpas is minder ingewikkeld dan het besturen van een auto of het reizen met het openbaar vervoer. Normaal ontwikkelde mensen wordt geacht dit soort dingen te kunnen en accepteren in onze samenleving en daarom is het genoemde probleem tijdelijk. Het is uiteraard ook niet op te lossen met ICT-innovatie. Contant geld zal sowieso nog voorlopig bestaan en tegen de tijd dat er eventueel een omschakeling heeft plaatsgevonden, zullen de genoemde ouderen er niet meer

zijn. Mensen die over 50 jaar geen simpele elektronische transactie kunnen uitvoeren, zullen sowieso moeilijk functioneren in de maatschappij en misschien ook niet in staat zijn zelfstandig contant te betalen.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.9 Contant geld voor budget management

Er is een groep mensen die contant geld gebruikt om een (of meerdere) budget(ten) bij te houden. Dit adviseert het Nibud [15] voor mensen die met hun pinpas snel verleid zijn onverstandige aankopen te doen of mensen die via hun bankrekening onvoldoende overzicht hebben over hun uitgaven en inkomsten. Voor het beheren van bankrekeningen zijn tegenwoordig veel mogelijkheden; zo kunnen het saldo en af- en bijschrijvingen via een smartphone worden gecontroleerd en is er software die met exports uit zo'n rekeningoverzicht alle mutaties op een gewenste manier kan rangschikken en (grafisch) weergeven, zoals AFAS Personal [16]. Maar misschien hebben juist de mensen die het meest belang hebben bij overzicht over hun financiële situatie het minst geld voor een smartphone en mobiel internetabonnement. Verder biedt een portemonnee, of bijvoorbeeld meerdere spaarpotten of envelopjes, waar een vantevoren vastgesteld bedrag per tijdseenheid in gaat mogelijkheden die een hedendaagse bankrekening niet heeft. Met stapeltjes contant geld kunnen sommige mensen zichzelf goed dwingen niet meer uit te geven dan een bepaald verstandig maximum. Dit is in theorie ook mogelijk met digitale portemonnees zoals de chipknip, maar het saldo moet dan wel op elk moment gecontroleerd kunnen worden, bovendien moet iedereen zo veel chippassen kunnen gebruiken als het aantal bij te houden budgetten om de genoemde mogelijkheden van contant geld te kunnen benutten. Deze mogelijkheid bieden banken nu niet. Daarnaast wordt het lastig als elke chippas zijn eigen pincode heeft, dus die codes zullen zelf gekozen moeten kunnen worden. Uit deze analyse blijkt dat op dit moment de beschikbare ICT onvoldoende is voor de groep mensen met de betreffende wensen. Om contant geld te vervangen zal hier dus nog iets voor bedacht moeten worden.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.10 Tijdelijke kas met contant geld

Het gebruik van een tijdelijke kas waarin contant geld wordt bewaard, lijkt op de situatie van mensen die verschillende budgetten contant bijhouden. De verschillen zijn echter dat aan een tijdelijke kas geen bankrekening is gekoppeld (misschien moet de kas na enige tijd worden verdeeld over verschillende rekeningen, zoals die van studieverenigingen na een studentengala) en dat er geld ingestopt wordt van verschillende particulieren. Dat maakt een chippas ongeschikt. Om aan dit doel elektronisch te beantwoorden is innovatie nodig. Misschien is het een goed idee een elektronische spaarpot te ontwikkelen waar met een chippas geld op te zetten en af te halen is. Er is echter een controlesysteem voor chipknippassen, waarmee banken fraude willen detecteren door te controleren of de afschrijvingen van elke chipknippas niet het totaal aan bijschrijvingen overschrijden. Als overschrijvingen tussen chipknippassen mogelijk worden zonder tussenkomst van de bank, vormt dit een probleem voor die fraudedetectie. Hierover dus meer bij het beantwoorden van de tweede deelvraag.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.11 Persoonlijke spaarpot thuis

Om verschillende redenen kunnen mensen thuis geld willen oppotten. Bijvoorbeeld om onafhankelijk van een bankrekening geld te sparen, verjaardagsgeld te verzamelen of te sparen voor een bepaalde uitgave. Het ontduiken van belastingen kan ook een reden zijn, maar dat betekent niet het zelf oppotten onmogelijk gemaakt moet worden (vergelijkbaar met zwart geld bij ondernemers). Bij een eventuele overschakeling naar een contantloze samenleving moet deze mogelijkheid open blijven en dat is niet mogelijk met de huidige technologie. Dit probleem lijkt veel op de hiervoor genoemde situatie.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.12 Retourbetalingen

Meestal zullen consumenten ondernemers betalen voor hun producten of diensten, maar het komt ook voor dat de transactie de andere kant op moet gebeuren. Soms moet een betaalfout worden hersteld of wordt een bedrag aan de consument teruggegeven als de ondernemer in gebreke blijft. Zogenaamd 'retourpinnen' wordt door ondernemers genoemd als wenselijke innovatie in [1]. Dit artikel gaat echter voorbij aan de negatieve implicaties van deze mogelijkheid op gebied van security. Voor ondernemers is een van de belangrijke voordelen van een contantloze samenleving namelijk dat ze niet meer zomaar overvallen kunnen worden door de afwezigheid van contant geld. Als retourpinnen mogelijk wordt, kunnen overvallers echter toch gewoon medewerkers weer dwingen om ter plekke geld naar hun over te maken. Een belangrijk verschil met het stelen van contant geld is wel dat zo'n overval misschien moeilijk anoniem te doen is, omdat er een rekeningnummer bekend wordt. Retourpinnen is dus misschien een wenselijke innovatie en waarschijnlijk technisch haalbaar, maar er moet nog wel goed over veiligheid worden nagedacht.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.13 Plaatselijke betalingen tussen particulieren

In uiteenlopende situaties willen particulieren, die geen pinbetalingen kunnen accepteren, onderling transacties verrichten. Dit is in theorie altijd via bankrekeningen te doen, maar er zijn genoeg concrete situaties te verzinnen waarin dit niet wenselijk is. Om zo'n transactie ter plekke elektronisch te verrichten, moet een computer of smartphone met internetverbinding gebruikt worden. Niet overal zijn computers beschikbaar en voorlopig heeft niet 100% van alle mensen in Nederland een smartphone met internet. Ook is het uit veiligheidsoverwegingen niet verstandig banktransacties op iemand anders' apparatuur te doen, bovendien is een banktransactie (in de huidige Nederlandse cultuur) vaak te onpersoonlijk voor bijvoorbeeld een verjaardagscadeau. Mocht de genoemde spaarpot uit 5.1.11 ingevoerd worden dan is dit een mogelijke oplossing, maar alleen als iedereen zo'n spaarpot thuis zou hebben. Anonieme tegoedkaarten zijn misschien ook geen gek idee. In elk geval is ook deze situatie zonder contant geld in de huidige situatie niet naar tevredenheid op te lossen.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.14 Ontraceerbaarheid (anonimiteit)

Mensen die veel belang hechten aan de anonimiteit die contant geld biedt, worden misschien al snel verdacht genoemd. Toch heeft iedereen recht op een zekere privacy, en zoals uiteengezet in het theoretisch kader schieten bankoverschrijvingen daarin tekort als de bank of overheid niet 100% te vertrouwen zijn. Daarnaast kan elke gegevensbeveiliging gekraakt worden als een hacker maar goed genoeg is en er genoeg tijd aan besteedt. Traceerbaarheid is een belangrijk verschil tussen contant geld en de algemeen geaccepteerde elektronische betaalmiddelen. Alleen contant geld biedt anonimiteit, tenzij innovatie ontraceerbare alternatieven gaat bieden.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: ja

5.1.15 Gebruik van contant geld uit gewoonte

Waarschijnlijk worden veel contante transacties gedaan zonder erover na te denken, gewoon omdat het een aangeleerde en ingesleten gewoonte is. Een duidelijk voorbeeld hiervoor is de visverkoper op de markt uit [1]. Hij heeft zijn pinapparaat weer weggedaan omdat maar weinig mensen bij hem elektronisch betaalden, terwijl mensen vis in de supermarkt toch meestal zullen pinnen. Dit is een soort cirkel die geneigd is zichzelf in stand te houden: mensen zijn gewend bij ambulante handel contant te betalen en daardoor bieden die ondernemers als reactie daarop ook vaak de mogelijkheid niet om elektronisch te betalen. Dit is echter wel te doorbreken, want tegenwoordig hebben we een landelijk dekkend netwerk voor mobiel internet en bij de meeste 'vaste' winkels heeft de ontwikkeling naar veel elektronische betalingen ook plaatsgevonden. De gewoontes van consumenten zijn wel belangrijk op korte termijn, maar de samenleving is altijd in ontwikkeling. Gewoonteverandering op lange termijn zal dus hoogstwaarschijnlijk vanzelf gebeuren.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.16 Zwaaien met flappen en rinkelen met munten

Pronken met contant geld kan aanzien geven. In het licht van dit onderzoek is dat een lastig punt. Het is maar de vraag of het echt 'cool' kan worden gevonden om bijvoorbeeld op een telefoonscherm een banksaldo te laten zien. Het laten rinkelen of ritselen van geld in een broekzak is moeilijk te vergelijken met het laten zien van nummertjes op een scherm. Een grote rol flappen is voor sommigen een goede manier om indruk te maken. Hier zijn ook talloze andere manieren voor, zoals dure elektronica, voertuigen of sieraden. De culturele rol van contant geld is het onderzoeken waard, maar past niet binnen de scope van dit onderzoek. Geen technische innovatie gaat hier uitkomst bieden, omdat het om een essentieel verschil tussen contant en digitaal geld gaat.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.1.17 Gebrek aan vertrouwen in de technologie

Deze reden van consumenten om contant te betalen kan verschillende onderliggende redenen hebben. Het kan bijvoorbeeld gaan om robuustheid, traceerbaarheid en veiligheid. Al deze punten zijn al apart behandeld, vandaar dat deze overkoepelende reden overbodig is om verder te behandelen.

Vraagt om (technische) innovatie en wordt dus in 5.2 behandeld: nee

5.2 Deelvraag 2: Welke nieuwe ICT zou een contantloze samenleving mogelijk maken?

Zoals in 5.1 duidelijk is geworden, worden er eisen gesteld aan geld en transacties waaraan pin, chipknip en creditcard niet voldoen. Dit hoofdstuk stelt bestaande systemen en uitbreidingen van bestaande systemen voor die wel aan (een deel van) deze eisen voldoen, en bij nationale invoering dus contant geld overbodig zou kunnen maken. De gevonden eisen zijn:

1. Robuustheid, storingsongevoeligheid zoals van contant geld en chipknip
2. De mogelijkheid iemand beperkte toegang te geven tot je tegoed om iets mee te kopen
3. Elektronisch betalen zonder Nederlandse bankrekening
4. Mogelijkheid (virtuele) 'potjes' te hebben om geld in te stoppen, thuis of in 'the cloud', die niet gekoppeld zijn aan een bankrekening
5. Mogelijkheid te betalen uit meerdere (virtuele) 'portemonnees' zonder gebruik van meerdere bankrekeningen of meerdere pincodes
6. Mogelijkheid voor (personeel van) bedrijven om ter plekke geld aan een klant te geven
7. Mogelijkheid voor particulieren om elkaar geld te geven
8. Ontraceerbaarheid van transacties en gespaard/opgeslagen geld

In 5.1 is geconcludeerd dat al deze eisen essentieel zijn om van een contantloze samenleving een succes te maken. Om 3 en 4 digitaal mogelijk te maken, moet de uitgevoerde innovatie *gedecentraliseerd* zijn. Alleen die aanpak maakt het mogelijk dat geen bankrekening nodig is. De enige mogelijk redelijke vervanger van contant geld is daarom zogenaamde 'cryptocurrency'. Zulke gedecentraliseerde systemen zijn bedacht en gemaakt, maar ze verkeren nog in een experimentele fase. [17] [7] [8] Kan cryptocurrency ook voldoen aan eis 1? Dit vraagt om vervolgonderzoek. In 5.2.2 wordt een begin gemaakt, vooral met de vraag of deze mogelijkheid echt aan de gevonden eisen zou kunnen voldoen en ook of het haalbaar is.

Nu dit onderzoek heeft uitgewezen dat contant geld alleen (misschien) kan worden vervangen door revolutie van het elektronisch betalen (reeds geaccepteerde systemen hebben immers te grote beperkingen), is het misschien een goed idee ons eerst te richten op mogelijke evolutie naar een contantarme samenleving. Contant geld wordt dan behouden, voor de eigenschappen dat het los van een bank of digitale communicatie (robuustheid en ontraceerbaarheid) gebruikt kan worden, en bestaande digitale systemen kunnen worden uitgebreid om ze geschikt te maken voor meer situaties. Hierop wordt ingegaan in 5.2.1.

5.2.1 Uitbreiding van bestaande ICT voor nieuwe elektronische betaalmogelijkheden

De bestaande elektronische vormen van geld waar op de meeste plekken in Nederland mee betaald kan worden, zijn gekoppeld aan een bankrekening en dus ook traceerbaar. Met uitbreidingen van die systemen kunnen eisen 1, 3, 4 en 8 dus niet worden ingewilligd. Voor de overige behoeften die door pin, chipknip en creditcard nu niet worden gedekt, zijn echter wel innovaties denkbaar die het mogelijk zouden maken, zonder meteen aan een compleet nieuw betaalsysteem te beginnen.

5.2.1.1 Een deelpas

Dit idee beantwoordt aan de eisen 2 en 5 uit 5.2, en in beperkte mate ook 7. Banken zouden de service kunnen ontwikkelen dat rekeninghouders één of enkele extra pinpassen kunnen aanvragen met speciale eigenschappen. Elke rekeninghouder heeft dan naast de hoofdpas een gewenst aantal deelpassen. Deelpassen gebruiken een eigen code, of zijn desgewenst codevrij. Voor hoofdpassen is immers een code vereist omdat het ineens toegang geeft tot het gehele tegoed, terwijl de deelpas toegang geeft tot een deel. De rekeninghouder kan dan op de website van internetbankieren op elk moment voor elke gekoppelde deelpas het beschikbare tegoed instellen. Ook zou een optie gemaakt kunnen worden om in te stellen of geld opgenomen kan worden met die pas of dat er alleen maar mee betaald kan worden. Zo houdt de rekeninghouder optimale controle over zijn geld en heeft de deelpasgebruiker overal waar gepind kan worden de mogelijkheid het beschikbaar gestelde geld te gebruiken. Deze mogelijkheden zijn erg relevant voor ouders die hun kinderen naar de supermarkt sturen voor boodschappen. Ook kunnen rekeninghouders hun deelpas(sen) voor zichzelf gebruiken om budgetten bij te houden op de manier die het Nibud voorstelt ([15]).

Deze deelpas kan eventueel ook worden gebruikt voor een soort kinderbankrekening als 'subrekening' van de ouder(s). In dat geval is een pincode overigens wel aanbevolen. De deelpas heeft ten opzichte van contant geld en een chippas de voordelen dat het tegoed op internet kan worden aangepast, de gemaakte transacties kunnen worden opgezocht en geen oplaadpunt of geldautomaat hoeft worden opgezocht. Tegelijk hoeft de 'echte' pas van de rekening dus niet te worden afgestaan. Banken hoeven voor de ontwikkeling van deze service ook geen revolutionaire nieuwe technologie te bouwen. Aangezien banken graag van contant geld af willen, zou dit dus een goede aanbeveling kunnen zijn. Banken kunnen geld vragen voor deelpassen, maar om de invoering te versnellen, kunnen ze er ook voor kiezen de service gratis beschikbaar te stellen.

5.2.1.2 Retourpinnen

Om punt 6 elektronisch mogelijk te maken, is volgens bronnen [5] en [1] de mogelijkheid van 'retourpinnen' (negatieve pintransacties) gewenst. Dit vereist wel een nieuwe vorm van autorisatie. De partij waar het geld vandaan komt, wil immers beschermd zijn tegen diefstal en dat is in het geval van retourpinnen niet de klant maar het bedrijf. Aan de kant van het pinapparaat zal dus authenticatie moeten gaan plaatsvinden. Wellicht volstaat echter een software-update van pinapparaten om dit mogelijk te maken. Ook aan de ondernemerskant zitten immers al voldoende knoppen op de apparaten (nummers, pijltjes, menu-toetsen etc.) en de benodigde infrastructuur is ook al aangesloten.

Als retourpinnen mogelijk wordt, ontstaat een nieuw veiligheidsprobleem. Er wordt namelijk een nieuw soort winkeldiefstal mogelijk, waarbij direct de bankrekening van het bedrijf wordt geplunderd. Dieven kunnen dus, door het personeel te dwingen mee te werken, meer geld stelen dan alleen wat in de kassa zit. In tegenstelling tot contante betalingen en diefstallen van contanten zijn pintransacties echter traceerbaar. Dat zal helpen in het opsporen van de dader (verdachte, in juridische zin) en daarmee deze vorm van diefstal ontmoedigen. Een dief kan dit weer omzeilen door andere rekeninghouders te gebruiken als 'money mules', maar dit maakt wel dat de diefstal een stuk meer voorbereiding eist. Ook deze money mules zijn strafbaar wegens medeplichtigheid aan criminaliteit en zij kunnen relatief makkelijk gepakt worden. Zodra deze manier van werken algemeen bekend is, zal geen weldenkende burger meer zomaar meewerken, ondanks de beloningen die fraudeurs hun beloven. Zo uitnodigend als de mogelijkheid om te graaien in een openstaande kassa is deze vorm van diefstal dus niet.

Het is te verwachten dat deze voorgestelde innovatie inderdaad een geschikte en haalbare aanvulling zal zijn op de bestaande mogelijkheden voor elektronische transacties, mits de ondernemer in staat is een maximaal retourpinbedrag per transactie of per dag in te stellen.

5.2.1.3 Chip 2 chip

In het tv-programma 'Het beste idee van Nederland' won Marc Karreman in 2005 de hoofdprijs voor zijn idee 'Chip 2 chip'. Hij heeft een apparaat bedacht waar twee gewone chipknippassen in kunnen, waarmee een bedrag zou kunnen worden overgeschreven van de ene naar de andere chippas. Dit idee zou dus een oplossing zijn voor punt 7. Karreman heeft geen prototype kunnen bouwen, maar alleen een visueel demonstratiemodel. Dat is ook niet zo vreemd, omdat het apparaat dat hij voor ogen had ook aan meer eisen moet voldoen dan hij waarschijnlijk wist. Ook de jury van het programma die de prijs uitreikte, wist waarschijnlijk niet goed hoe chipknips werken.

Chipkniptransacties zijn namelijk traceerbaar om fraude te voorkomen. Een 'Chip 2 chip'-apparaat zou deze mogelijkheid breken. Een manier om dit uit te leggen is dat eigenlijk op de chipknip geen geld staat. Het 'saldo' op de chipknip is als het ware 'opzij gelegd' bij de bank. Als een chiptransactie vanuit een chipapparaat van een winkel naar de bank wordt verstuurd, wordt het geld overgemaakt naar de rekening van de winkel. Bij het opladen van een chipknip is ook contact met de bank vereist. Als het apparaat dit (mobiele) contact zou bieden, is het voordeel van de chipknip eigenlijk al weg. Dan kan er net zo goed direct tussen rekeningen gestort worden. Als men het geld dan op de chipknip wil hebben, kan dat weer vanaf de eigen bankrekening. Dat zal ook de enige methode zijn die banken zullen toestaan, omdat ze de traceerbaarheid willen behouden. Al het (digitale) geld blijft dus van- en/of naar bankrekeningen gaan en kan niet elektronisch verschoven worden tussen twee dragers zoals chipknips. Wat in theorie nog wel zou kunnen, is dat het mogelijk wordt om de chipknip van iemand anders op te laden uit eigen rekening. Dit is echter geen mobiele oplossing, omdat men naar een oplaadpunt moet. Handiger dan contant geld is dit dus in de meeste gevallen niet.

5.2.1.4 Mobiele overschrijving

Omdat een ontraceerbare cashervanger al in 5.2.2 beschreven is, blijft voor het bieden van mogelijkheid 7 met behulp van systeemuitbreiding alleen de mobiele overschrijving over. Dit vereist dus een internetverbinding. De grote banken RaboBank, ING en ABN AMRO hebben al een tijdje een mobiele applicatie voor smartphones om overschrijvingen mee te kunnen doen. Triodos heeft dat bijvoorbeeld nog niet en ook geen mobiele site, maar internetbankieren is ook daar wel mogelijk op een telefoon. Telefoons kunnen ook als authenticatiemiddel dienen, zoals ING dat doet door TAN-codes te sms'en, maar dit is niet erg veilig. Meestal wordt gestreefd naar authenticatie via twee gescheiden kanalen, zodat men in controle blijft als één kanaal door een kwaadwillende is overgenomen. Voor het behouden van een even sterke beveiliging moet dus naast de telefoon nog steeds een authenticatieapparaatje worden gebruikt.

Mobiele overschrijvingen zijn niet in alle situaties ideaal. Zoals gezegd zijn de applicaties nog in ontwikkeling, maar ook is men afhankelijk van mobiel internet, wat lang niet iedereen heeft. Het is dus nog geen transactiemogelijkheid waarop gerekend kan worden en die door iedereen gebruikt kan worden. Ook kunnen overschrijvingen tussen verschillende banken wel een dag duren. Dat is een probleem als men elkaar niet vertrouwt (geen directe controle mogelijk) of als het geld meteen nodig is. Technische innovatie zal voorlopig verder gaan op dit gebied en het is te verwachten dat smartphonegebruik verder zal stijgen. Communicatie binnen en tussen banken is in de afgelopen

decennia sneller geworden en die trend zou kunnen doorzetten. Mobiele overschrijvingen zouden in de loop der jaren kunnen uitgroeien tot een gangbare manier van betalen. Als dit is gebeurd, is dit een oplossing voor punt 7, al blijven de nadelen op gebied van robuustheid en traceerbaarheid bestaan.

5.2.1.5 Alternatieve mogelijkheden

Pre-paid oplaadbare creditcards verdienen in dit onderzoek nog aandacht, al is het reeds gebruikte technologie. Strict genomen is deze techniek misschien onterecht onderbelicht gebleven in 5.1. Pre-paid creditcards voldoen namelijk wel aan het grootste deel van de genoemde eisen, maar ze kosten ook geld. Consumenten zitten niet te springen om betaalmethoden waar transactiekosten en/of periodieke kosten aan vast zitten, aangezien het gebruik van contant geld hun niks kost. Vandaar dat er pas in deze paragraaf aandacht aan wordt besteed. In Nederland zijn verschillende versies van MasterCard en Visa te verkrijgen [18]. Particulieren kunnen geld tussen de kaarten overmaken o.a. via sms [19], dus internet is niet altijd nodig. Omdat voor pre-paid creditcards vele methoden worden aangeboden voor opladen en transacties, mag deze optie als redelijk robuust worden gezien, al zijn er misschien meerdere verschillende kaarten nodig om in elke denkbare situatie te kunnen betalen. Er is geen bankrekening nodig en iedereen mag zo veel kaarten aanvragen als hij wil. Betalen met pre-paid creditcards is zeer toegankelijk, want bijvoorbeeld Maestro wordt wereldwijd geaccepteerd en voor transacties tussen kaarten kan een telefoon die kan sms'en volstaan. Ook is het goed denkbaar dat retourbetalingen kunnen plaatsvinden als ondernemers geld overschrijven naar de pre-paid creditcard van een klant. Deze kaarten voldoen dus aan bijna alle gevonden eisen. De ontraceerbaarheid is echter wel discutabel. Pre-paid creditcards kunnen ontraceerbare betalingen mogelijk maken als ze worden opgeladen met contant geld. Als echter hiervoor contant geld nodig is, betekent dat dus dat de kaarten geen volwaardige vervanger van contant geld zijn. Het ziet ernaar uit dat ontraceerbaarheid niet gewaarborgd kan worden met andere oplaadmethoden, omdat de andere methoden redelijk tot goed gemonitord worden. Er is per definitie digitale communicatie nodig voor creditcardtransacties, in tegenstelling tot contante transacties, en dat betekent dus automatisch dat die informatie beschikbaar is. Er worden ook significante kosten gerekend per kaartanschaf, per maand (voor Exacard bijvoorbeeld €3,50), per jaar, per betaling, per opname uit een geldautomaat en/of per keer opladen. Gebruik van meerdere kaarten wordt dus prijzig, terwijl men contant geld zomaar zonder bijkomende kosten kan verdelen. Het is alleen aannemelijk dat mensen massaal aan de pre-paid creditcards zouden willen gaan als de kosten hiervoor door de regering en banken collectief worden verdeeld, zoals dat nu ook gebeurt met contant geld. Mocht dat gebeuren, dan is het nog steeds onwaarschijnlijk dat pre-paid creditcards ontraceerbaar kunnen worden gebruikt, om dezelfde redenen als waarom pin, chipknip en bankoverschrijvingen traceerbaar zijn. Met pre-paid creditcards zoals die nu worden geaccepteerd kunnen we dus in theorie ver komen, maar een echte contantgeldvervanger zal het niet voor iedereen zijn. Overigens lijken de meeste mobiele betaaltechnieken (Google Wallet en betaaldiensten van telefoonproviders) veel op creditcards: als ze niet gekoppeld zijn aan een bankrekening, dan wel aan een andere vertrouwde derde partij, die daarmee kosten maakt die doorberekend moeten worden.

Het door onderzoekers beschreven *RO-cash* [8] is een enigszins vergelijkbaar systeem, met name omdat ook bij deze techniek wordt uitgegaan van een centrale, controlerende, vertrouwde derde partij die de kaarten met door hun gekozen beveiliging uitbrengt. Kaarten met de voorgestelde techniek zijn voor zover op internet te vinden niet in omloop en het is dan ook moeilijk te achterhalen of een eventuele implementatie het ook mogelijk zou maken dat particulieren onderling offline betalingen verrichten. Het artikel noemt slechts betalingen van consument naar winkel. Wel

zeggen de onderzoekers dat het systeem ontraceerbaarheid biedt door 'partially blind signatures'. Het systeem lijkt misschien nog het meest op een ontraceerbare vorm van de chipknip en dat kan het voor veel mensen interessant maken. Het houdt echter ook in dat een bankrekening nodig is en daardoor voldoet ook RO-cash niet aan alle gestelde eisen. Ook het systeem zonder naam dat Eslami en Talebi hebben bedacht [7] vereist bankrekeningen en heeft het niet over betalingen tussen particulieren.

5.2.2 Een gedecentraliseerd systeem als cashvervanger

De mogelijkheid om contant geld volledig te vervangen wordt hier enigszins uitgediept. Kan een gedecentraliseerd geldsysteem aan alle eisen voldoen zonder nieuwe problemen te introduceren? Kan contant geld echt worden vervangen door een elektronisch alternatief? Het ontwerpen van een gedecentraliseerde cashvervanger heeft minstens een grote uitdaging: hoe wordt voorkomen dat een digitale portemonnee wordt gebackupt en later opnieuw gebruikt, als er geen bank is die dit controleert? Het is zeer de vraag of dit offline en ontraceerbaar mogelijk is.

De brede invoering van een gedecentraliseerd elektronisch betalingssysteem zou revolutionair zijn. Het gaat hier namelijk niet alleen om nieuwe techniek om een oud doel te bereiken, maar eigenlijk vooral om een nieuwe, decentrale valuta en daarmee een eigen economie, onafhankelijk van banken. Dit onderwerp is niet direct de insteek van dit onderzoek, maar het is wel onvermijdelijk als het gaat om ontraceerbaar elektronisch betalen. Het is namelijk niet mogelijk ontraceerbare euro's te maken, om de reden dat alleen de Europese Centrale Bank in samenwerking met centrale banken van de eurolanden euro's mag uitgeven. Gedecentraliseerde systemen gaan in tegen alle huidige gevestigde financiële systemen. Op ontraceerbare valuta hebben overheden geen vat. Dat is prettig voor brave burgers die prijs stellen op hun privacy en niet willen dat al hun aankopen jarenlang in te zien zijn, met de kans dat hun rekening geblokkeerd wordt als ze onterecht beschuldigd worden van terrorisme. Het is ook perfect voor criminelen en belastingontduikers, die natuurlijk niet gepakt willen worden. Rechtbanken verbieden wel eens dingen die zowel illegaal als legaal gebruikt kunnen worden, zoals de torrentsite The Pirate Bay. Ook hierbij zijn er brave mensen die het volkomen legaal gebruiken en gebruikers die inbreuk maken op copyrights. De laatste groep is relatief zo groot, dat de rechters uiteindelijk besloten dat The Pirate Bay niet meer toegankelijk mocht zijn. [20] Het is mogelijk dat een soortgelijke afweging wordt gemaakt bij cryptocurrency, omdat het waardevol gereedschap is voor kwaadwillenden. Tegelijk is het te verdedigen dat iedereen het recht heeft een ander te betalen op een manier naar eigen wens. Als iemand daarvoor cryptocurrency gebruikt, is dat helemaal geen bewijs dat diegene het geld gestolen heeft of de belasting ontduikt. Deze eventuele problemen met de overheid spelen nog niet nu cryptocurrency nauwelijks gebruikt wordt, maar kunnen wel het grootste vraagstuk opleveren als het echt populair wordt. Overigens is de controle die de overheid heeft op een gecentraliseerde valuta ook belangrijk voor de stabiliteit van de valuta. Om bijvoorbeeld 'bank runs' (die economische crises veroorzaken of versterken) te voorkomen, staan overheden garant voor bedragen op bankrekeningen. Dit zorgt voor stabiliteit van de valuta en bij een gedecentraliseerd systeem zal niemand voor die stabiliteit verantwoordelijk zijn. Op Quora.com heeft de econoom Adam Cohen naast dit argument nog andere bezwaren tegen Bitcoin (en cryptocurrency in het algemeen) uiteengezet [21]. Over de juridische en economische vraagstukken wordt hier niet verder uitgeweid; dat is stof voor vervolgonderzoek.

Een Google-zoekactie op 'cryptocurrency' levert voornamelijk resultaten over Bitcoin op, dus op dit systeem wordt eerst geconcentreerd. Bitcoin heeft al tienduizenden gebruikers [22].

5.2.2.1 Hoe werkt Bitcoin?

Bitcoin bestaat uit een peer-to-peernetwerk waarin transacties worden verwerkt in de 'blockchain', waarin alle transacties zijn opgeslagen die ooit zijn gedaan. Ongeveer elke 10 minuten wordt door de computers in het bitcoinnetwerk samen een block uitgerekend, een set van transacties die in die tijd is gedaan. Het door het netwerk controleren van transacties en het continu bouwen van de blockchain is waar de beveiliging van het systeem op is gebaseerd. Als iemand een transactie doet, gebruikt diegene zijn private key voor de digitale handtekening, waarmee wordt bewezen dat de transactie is gedaan door de eigenaar van de bitcoins. Iedereen kan dat narekenen met de bijbehorende public key, zonder dat daaruit zomaar de private key berekend kan worden (asymmetrische cryptografie). Verder is bij een transactie natuurlijk een bedrag vereist (dat kan bijvoorbeeld 1,55 BTC zijn) en de public key van de ontvanger, wat fungeert als 'rekeningnummer'. Deze informatie vormt de basis van een transactie die het netwerk in gestuurd wordt. Er wordt gebruikgemaakt van hashes om te zorgen dat de private key niet uit de transactie kan worden gehaald. Een samenvatting van een transactie van de Bitcoin wiki (en.bitcoin.it):

Suppose Alice wants to send a bitcoin to Bob.

- *Bob sends his public key to Alice.*
- *Alice adds Bob's public key along with the amount she wants to transfer to a message: a 'transaction' message.*
- *Alice signs the transaction with her secret private key.*
- *Alice broadcasts the transaction out over the bitcoin network for all to see.*

Strikt genomen heeft een 'bitcoinportemonnee' geen saldo dat ergens is opgeslagen; er bestaan alleen maar transacties in de 'cloud'. Het bezit van een portemonnee (eigenlijk alleen een private key) betekent niks meer dan het bewijs dat bepaalde transacties naar jou zijn gedaan. De transacties worden alleen opgenomen in de blockchain door gebruikers die het hebben geaccepteerd (door met de publieke sleutel te controleren of de juiste privésleutel is gebruikt). Om te zorgen dat pogingen tot double-spending niet leiden tot succesvolle transacties, is het peer-to-peernetwerk essentieel. Als een transactie eenmaal in een blockchain staat, wat tot tien minuten kan duren, wordt het erg lastig de transactie nog ongedaan te maken. En omdat elke wijziging van een block vereist dat alle volgende blocks opnieuw worden uitgerekend, is het enkele blocks later niet meer te doen om de transactiegeschiedenis te wijzigen, tenzij de aanvalleur meer dan 50% van de totale rekenkracht van het bitcoinnetwerk in z'n macht heeft. Consensus in het netwerk over de transactiegeschiedenis is de basis van de beveiliging van het systeem.

Transacties kunnen offline worden 'gemaakt', tijdelijk opgeslagen op een medium naar keuze als een stukje tekst en later naar het netwerk geupload. Na uploaden kan de transactie nog worden afgekeurd, bijvoorbeeld doordat in de tussentijd de bitcoins een tweede keer zijn besteed. De ontvangende partij kan er dus niet zomaar van uitgaan dat hij het geld echt ontvangt, zolang de transactie niet online is. Dit is een groot verschil met het offline digitale betaalsysteem dat we al kennen; de chipknip. De chipknip is offline al beveiligd tegen double-spending, want het saldo wordt bijgehouden in de chip en het is niet makkelijk dat zonder betaling op te waarden. Daarnaast staat de bank garant voor de transactie. Bij fraude heeft de bank, dus niet de ondernemer, een probleem met de fraudeur. Dat probleem is te overzien, omdat de bank macht heeft over rekeningen, inclusief die van de fraudeur. Door het centraal geregelde karakter kan de ondernemer gerust het chipapparaat de hele dag offline houden.

5.2.2.2 Voldoet Bitcoin als vervanger van contant geld?

Aan de hand van het lijstje uit 5.2 wordt hier beredeneerd of Bitcoin beantwoordt aan alle eisen waaraan gangbare elektronische betalingen niet voldoen:

1. Robuustheid, storingsongevoeligheid zoals van contant geld en chipknip

Zoals in de vorige paragraaf is geconcludeerd, is voor een veilige transactie (waarbij de betalende partij niet zomaar vertrouwd wordt) een internetverbinding nodig. Als snelheid belangrijk is, zoals in winkels, betekent dit dat een bitcoinbetaling nauwelijks robuuster is dan een pinbetaling. Wat wel in het voordeel van Bitcoin spreekt, is dat het open source is en de gewenste software en gegevensdrager dan ook heel vrij te kiezen is, naar gelang wat de situatie wenst. Elektronica die uitvalt, kan ter plekke vervangen worden door ander elektronica die het nog doet. De internetverbinding is hedendaags echter een vereiste en zeker een mobiele verbinding is in Nederland nog best wel storingsgevoelig.

Er is echter een mogelijke oplossing gevonden in de vorm van de Bitcoincard [23]. Deze 'Mycelium Smartcard' op creditcardformaat maakt het mogelijk dat gebruikers hun 'eigen', vrije radionetwerk hebben om zonder internetverbinding bitcointransacties te doen én te verifiëren. [24] Dit netwerk bestaat uit draadloze ad-hocverbindingen (direct) tussen de smartcards. Het is denkbaar dat dit in combinatie met internetverbindingen een zeer robuust betaalnetwerk kan vormen, mits er voldoende smartcards in de omgeving verspreid zijn. Dit laatste is natuurlijk een cruciale vereiste. De smartcards zouden tot 300 meter ver verbindingen kunnen leggen, dus er zijn er veel nodig voordat deze technologie een echte doorbraak kan leveren. Ze zijn echter voor meer toepassingen geschikt dan alleen bitcointransacties, zoals het sturen van berichtjes, dus het is niet onmogelijk dat deze apparaatjes populair genoeg worden om een goed betaalnetwerk mee op te zetten. Het is voorlopig slechts toekomstmuziek, maar het biedt mogelijkheden.

2. De mogelijkheid iemand beperkte toegang te geven tot je tegoed om iets mee te kopen

Er kan even een bitcoinportemonnee worden aangemaakt voor dit doel. Er bestaat bijvoorbeeld de site www.instawallet.org. Bij het openen van de site geeft het direct nieuwe codes die men kan gebruiken als portemonnee. Naar de portemonnee kan een transactie worden gemaakt en de private en public key kunnen aan iemand gegeven worden om de coins te gebruiken. Als gebruikers eenmaal snappen hoe dit uitgevoerd kan worden, zijn het slechts enkele simpele stapjes.

3. Elektronisch betalen zonder Nederlandse bankrekening

Cryptocurrency als Bitcoin werkt volkomen los van bankrekeningen.

4. Mogelijkheid (virtuele) 'potjes' te hebben om geld in te stoppen, thuis of in 'the cloud', die niet gekoppeld zijn aan een bankrekening

Dit is geen probleem; men kan zo veel portemonnees gebruiken als gewenst.

5. Mogelijkheid te betalen uit meerdere (virtuele) 'portemonnees' zonder gebruik van meerdere bankrekeningen of meerdere pincodes

Hierbij worden dus bijvoorbeeld de portemonnees uit 4 gebruikt om uit te betalen. Elke portemonnee heeft wel z'n eigen private key. Omdat de techniek die precies voor de transacties wordt gebruikt niet door een bedrijf of overheid wordt opgelegd, zijn er wel verschillende mogelijkheden voor de eindgebruiker wat betreft de manier van authenticatie en autorisatie. Zo

zouden de private keys door software beheerd kunnen worden, beveiligd met een 'master'-wachtwoord. Bitcoin laat helemaal over aan de gebruiker hoe die z'n private keys bewaart.

6. Mogelijkheid voor (personeel van) bedrijven om ter plekke geld aan een klant te geven

Dit kan uiteraard, maar om overvallen te voorkomen, moet wel rekening gehouden worden met het feit dat de private key volledige toegang geeft tot de digitale kas. Ondernemers hebben niet automatisch de bescherming van traceerbaarheid die bankoverschrijvingen en dus ook retourpinnen bieden. Als de private key goed beschermd wordt, zodat overvallers niet gewoon geld kunnen pakken zoals dat kan met een contantkassa, is een geslaagde overval alleen mogelijk door het personeel onder bedreiging te dwingen een transactie te maken. Dit risico is onvermijdelijk aanwezig zolang bedrijven in staat willen zijn hun klanten ter plekke geld te geven. Met cryptocurrency is wel de opsporing moeilijker dan met gecentraliseerd geld, dus daarom is wellicht retourpinnen een beter systeem voor deze toepassing.

7. Mogelijkheid voor particulieren om elkaar geld te geven

Gebruikers van dezelfde cryptocurrency kunnen elkaar geld geven, ongeacht locatie. Dit kan door een transactie of door het weggeven van een hele portemonnee door de private key te geven. Als mensen elkaar vertrouwen, kan een transactie ook goed offline, zie hiervoor 1.

8. Ontraceerbaarheid van transacties en gespaard/opgeslagen geld

Ook bij een gedecentraliseerd systeem moet controle plaatsvinden, bijvoorbeeld tegen double-spending. Bitcoin gebruikt hier een peer-to-peernetwerk voor, dat transacties controleert tot consensus 'ontstaat'. Het hele netwerk bij elkaar 'kent' alle transacties die gedaan zijn. [25] Omdat er geen centrale, algemeen vertrouwde partij is in een gedecentraliseerd systeem, is er bij Bitcoin voor gekozen dat alle transacties publiek moeten zijn. Strict genomen zijn dus alle transacties door iedereen te traceren, alleen geeft dit op zich niet zo veel informatie. Zo hoeft men zich niet te legitimeren bij het 'maken' van een portemonnee, portemonnees kunnen gedeeld worden en iemand zal vaak meer dan één portemonnee gebruiken. Bron [26] gaat in op de privacycontrole die bij Bitcoin speelt. De schrijvers hebben gevonden dat anonimiteit met bitcointransacties moeilijk te waarborgen is en verwachten dat Bitcoin minder anonimiteit biedt dan veel gebruikers denken. Als men de koppeling tussen een persoon en een publieke sleutel of bitcoinadres kent, kunnen makkelijk transacties boven water gehaald worden op sites als blockexplorer.com. Maar dan is nog niet bekend naar wie of wat het geld ging, bovendien is het erg makkelijk om weer een nieuwe portemonnee te gaan gebruiken.

Ontraceerbaar is Bitcoin in elk geval niet en of men er anoniem gebruik van kan maken, hangt vooral af van de moeite die erin gestoken wordt door anderen om gegevens te achterhalen. Geen centrale autoriteit is in het bezit van alle persoonlijke informatie; dat is dan weer in het voordeel van anonimiteit.

Of Bitcoin voldoende anonimiteit biedt, is dus discutabel. Maar als het gaat om het vervangen van contant geld, is het online karakter van het transactiesysteem nog het grootste probleem. Met contant geld kunnen mensen simpelweg overal betalen en de ontvangende partij weet meteen zeker of het geld ontvangen is. Dat is met Bitcoin niet zo, dus is dit geen waardige vervanger.

5.2.2.3 Kan een gedecentraliseerd geldsysteem contant geld vervangen?

Zijn er systemen bedacht die het nadeel van Bitcoin niet hebben? Is het mogelijk een veilig offline alternatief te gebruiken, waarbij het tegoed dus daadwerkelijk op een drager naar keuze is opgeslagen, in plaats van op een controlerend netwerk? Waarschijnlijk niet.

Ripple is een ander gedecentraliseerd betaalsysteem [27]. Het werkt heel anders dan Bitcoin en geeft ook andere nadelen. Het deelt het nadeel dat het systeem niet volledig offline te gebruiken is. Over andere gedecentraliseerde geldsystemen is onvoldoende informatie te vinden op internet. Een uitvoerige zoektocht in databases van wetenschappelijke literatuur leverde geen artikelen op over gedecentraliseerde geldsystemen die offline en ontraceerbaar te gebruiken zijn. De zoekacties 'decentralised untraceable offline' en 'decentralized untraceable offline' (zoekopties: AND, all fields) gaven op ScienceDirect bijvoorbeeld geen enkel resultaat. Er wordt aangenomen dat ook een gedecentraliseerd geldsysteem niet in staat zal zijn contant geld volledig te vervangen.

6 Conclusie en discussie

Met uitbreidingen van de algemeen geaccepteerde elektronische betaalmethoden (pin, bankoverschrijving, chipknip en creditcard) kan worden voorzien in een deel van de behoeften waar nu nog alleen contant geld voor geschikt is. De 'deelpas' (5.2.1.1) maakt het mogelijk een deel van een bankrekeningtegoed beschikbaar te stellen aan iemand anders die er dan mee kan betalen. Het maakt ook mogelijk meerdere 'budgetten' of 'virtuele portemonnees' bij te houden met slechts één bankrekening. 'Retourpinnen' (5.2.1.2) zou het mogelijk maken dat een ondernemer ter plekke geld stort op de rekening van een klant die bij de kassa staat. Mobiele overschrijvingen met behulp van smartphones (5.2.1.4) maken mogelijk dat particulieren op een willekeurige plek elektronisch geld uitwisselen. Deze innovaties zijn echter allemaal afhankelijk van bankrekeningen en dat geeft beperkingen die ervoor zorgen dat contant geld hiermee niet helemaal vervangen kan worden. Contant geld is namelijk storingsongevoelig, vereist geen bankrekening, kan naar eigen wens verdeeld worden (slechts beperkt door de grootte van de beschikbare biljetten en munten) en is praktisch ontraceerbaar. Gebruik van pre-paid creditcards kan wel robuuster zijn en vereist geen bankrekening, maar biedt nog steeds weinig vertrouwen op gebied van ontraceerbaarheid en kost relatief veel geld voor de consument. Gevonden voorstellen voor alternatieve betaalsystemen vereisen een bankrekening.

De mogelijkheid om toch elektronisch geld te gebruiken aan alle eisen van contant geld voldoet, kan men zoeken in gedecentraliseerde cryptocurrency. De technieken hiervoor worden al gebruikt, maar zijn nog experimenteel. De crux is echter dat als er geen bank is als centrale autoriteit, er voor voldoende beveiliging een netwerk van gebruikers nodig is zoals bij Bitcoin. Dit geeft weer een nadeel op gebied van robuustheid, om nog niet te spreken van de revolutionaire eigenschappen van een nieuwe decentrale valuta. De eigenschappen 'volledig offline te gebruiken' en 'volledige onafhankelijkheid van banken' lijken onverenigbaar met voldoende veiligheid voor e-cash totdat een werkbare implementatie eventueel ooit het tegendeel bewijst.

Daarmee is geconcludeerd dat contant geld voorlopig nodig blijft. Een contantloze samenleving zou acceptabel kunnen zijn met twee breed geaccepteerde betalingsvormen: eentje waarbij een bankrekening vereist is maar geen internetverbinding en eentje waarbij wel een internetverbinding

vereist is maar geen bankrekening. Minstens een van de twee moet dan ook ontraceerbaar te gebruiken zijn.

6.1 Vervolgonderzoek

Voor elke in 5.2.1 voorgestelde innovatie kan worden onderzocht wat een goede implementatie van het idee zou zijn. Hoe kunnen banken de diensten 'deelpas', 'retourpinnen' en mobiele overschrijving het beste leveren?

Het meeste onderzoek is nog te doen in cryptocurrency. Er zijn al werkende systemen, maar hoe zouden die echt gebruiksvriendelijk en overal toepasbaar worden? En wat zijn de implicaties als cryptocurrency veel populairder wordt? Zouden overheden een stokje willen steken voor gedecentraliseerde valuta, of zouden ze misschien eisen stellen aan de gebruikte systemen? Wat zijn de implicaties van een nieuwe, wereldwijde valuta die door miljarden mensen geadopteerd zou kunnen worden?

Ook kan men zich afvragen hoe belangrijk mensen het vinden dat geld aan te raken is. Willen mensen graag rinkelen en ritselen met munten en bankbiljetten in hun zak, of erin zwemmen zoals Dagobert Duck? Het is niet echt praktisch om met de hand geld te tellen als het ook automatisch in een computer kan gebeuren, maar misschien vinden sommigen het tellen van fysiek geld wel heel leuk. Ook dit soort menselijke sentimenten spelen mee bij de vraag of we ons contant geld willen vervangen.

7 Literatuur

- [1] L. Heuts, A. van Schijndel en Regioplan, „Naar een contantloze detailhandel,” Hoofdbedrijfschap Detailhandel & Detailhandel Nederland, Den Haag, 2011.
- [2] Nederlandse Vereniging van Banken, „Betalingverkeer veilig ondanks toename fraude,” 26 03 2012. [Online]. Available: <http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/betalingsverkeer-veilig-ondanks-toename-fraude.html>. [Geopend 03 06 2012].
- [3] D. Chaum, „Blind signatures for untraceable payments,” *Crypto*, pp. 199-203, 1982.
- [4] G. Harberink, „Privacy is een wassen neus,” *Cursor/5*, vol. 42, 7 Oktober 1999.
- [5] G. C. Solutions, „Cash Report 2011,” Utrecht, April 2011.
- [6] EIM (Panteia), „De praktijk van het betalingsverkeer,” Zoetermeer, 8 maart 2011.
- [7] Z. Eslami en M. Talebi, „A new untraceable off-line electronic cash system,” *Electronic Commerce Research and Applications*, nr. 10, pp. 59-66, 2010.
- [8] W.-S. Juang, „RO-cash : An efficient and practical recoverable pre-paid offline e-cash scheme using bilinear parings,” *The Journal of Systems and Software*, nr. 83, pp. 638-645, 2010.
- [9] D. Lekkas en D. Spinellis, „Implementing regular cash with blind fixed-value electronic coins,” *Computer Standards & Interfaces*, vol. 29, pp. 277-288, 2007.
- [10] ING, „Reactie ING op storing geldautomaten,” 12 08 2011. [Online]. Available: http://www.ing.nl/nieuws/nieuws_en_persberichten/2010/08/reactie_ing_op_storing_geldautomaten.aspx. [Geopend 13 04 2012].
- [11] R. Schoemaker, „Webwereld; Storing bij 500 pinautomaten - update,” 16 11 2011. [Online]. Available: <http://webwereld.nl/nieuws/108579/storing-bij-500-pinautomaten---update.html>. [Geopend 13 04 2012].
- [12] Currence, „Currence,” [Online]. Available: www.currence.nl. [Geopend 6 2012].
- [13] Auteur niet vermeld, „Not just talk,” *The Economist*, 27 01 2011.
- [14] Nederlandse Vereniging van Banken, „Banken en detailhandel gaan voor Europees betalingsverkeer,” 27 05 2009. [Online]. Available: <http://www.nvb.nl/home-nederlands/pers/persberichten/europees-betalingsverkeer.html>. [Geopend 14 04 2012].
- [15] Nibud, „Verleidingen - Nibud voor scholieren,” 2012. [Online]. Available: <http://www.nibud.nl/scholieren/uitgaven/verleidingen.html>. [Geopend 15 04 2012].
- [16] AFAS, „AFAS Personal,” 2011. [Online]. Available: <http://www.afaspersonal.nl/>. [Geopend 15 04 2012].

- [17] Bitcoin ATM, „Bitcoin ATM,” Bitcoin ATM, 2012. [Online]. Available: <http://www.bitcoinatm.com/>. [Geopend 10 06 2012].
- [18] Onbekend, „Prepaid Creditcard.nl,” [Online]. Available: <http://www.pre-paid-creditcard.nl>. [Geopend 17 07 2012].
- [19] UniRush, LLC, „How do I transfer money using my mobile phone?,” UniRush, [Online]. Available: <http://www.rushcard.com/faq/question.aspx?id=152>. [Geopend 18 07 2012].
- [20] J. Schellevis, „Ook andere providers moeten The Pirate Bay blokkeren,” Tweakers.net, 10 05 2012. [Online]. Available: <http://tweakers.net/nieuws/81883/ook-andere-providers-moeten-the-pirate-bay-blokkeren.html>. [Geopend 17 07 2012].
- [21] A. Cohen en andere auteurs, „Bitcoin: Is the cryptocurrency Bitcoin a good idea?,” 2011. [Online]. Available: <http://www.quora.com/Bitcoin/Is-the-cryptocurrency-Bitcoin-a-good-idea>. [Geopend 22 6 2012].
- [22] Various, „Current Network Status - Bitcoin wiki,” [Online]. Available: https://en.bitcoin.it/wiki/Current_Network_Status. [Geopend 25 06 2012].
- [23] Bitcoincard team, „Bitcoincard | This will change everything,” [Online]. Available: <http://bitcoincard.org/>. [Geopend 18 07 2012].
- [24] K. Dotson, „SiliconANGLE » Bitcoincard Puts Cryptocurrency In Your Wallet With A Mycelium Smartcard,” Silicon Angle, 08 06 2012. [Online]. Available: <http://siliconangle.com/blog/2012/06/08/bitcoincard-puts-cryptocurrency-in-your-wallet-with-a-mycelium-smartcard/>. [Geopend 18 07 2012].
- [25] ?, „Bitcoin Block Explorer,” [Online]. Available: <http://blockexplorer.com/>. [Geopend 23 06 2012].
- [26] F. Reid en M. Harrigan, „An analysis of Anonymity in the Bitcoin System,” Ithaca, NY, 2011.
- [27] Ripple, „Ripplepay.com,” [Online]. Available: <https://ripplepay.com/>. [Geopend 20 07 2012].
- [28] H.-C. Yu, K.-H. Hsi en P.-J. Kuo, „Electronic payment systems: an analysis and comparison of types,” *Technology In Society*, vol. 24, pp. 331-347, 2002.