Schuldposities in handelsrelaties met Perspectives: bitcoin, no blockchain!

|  |  |  |
| --- | --- | --- |
| Joop Ringelberg | 18-03-18 | Versie: 1 |

# Introductie

Als mensen uitsluitend ruilhandel zouden bedrijven, was geld niet nodig. Maar de bakker krijgt ook klanten die wel brood willen maar de bakker niet iets gelijkwaardigs kunnen teruggeven. Daar is geld voor nodig. En geld is ook nodig om krediet te verschaffen. Krediet is in essentie een vorm van vooruit betalen (meer hierover in een ander stuk).

# Arie, Bea en Chris

Arie bakt een Appeltaart. Bea heeft een boek en Chris een CD. Bea is dol op appeltaart en neemt die van Arie over. Maar ze rekenen niet af in geld: in plaats daarvan leggen ze hun transactie vast in een Zaak waarin vastligt dat Arie de taart leverde en Bea 7 euro schuldig is aan Arie.

Chris wil graag Bea’s boek en zij gaan op dezelfde manier een transactie aan, ook ter waarde van 7 euro. Bea heeft nu zowel een schuld aan Arie, als een schuldbekentenis van Chris. Die heffen elkaar op.

Arie, tenslotte, neemt Chris’ cd over voor 7 euro. Nu heeft iedereen zowel een geregistreerde schuld als een gelijkwaardige schuldbekentenis en daarmee is alles vereffend.

Arie, Bea en Chris deden geen ruilhandel, want in geen enkele transactie gingen gelijkwaardige goederen over en weer. Toch zijn geen euro’s gebruikt: in plaats daarvan voerden ze een nauwkeurige registratie van schuldposities – en dat is natuurlijk precies wat geld óók is.

# Bedrog

Arie zou goed garen spinnen als hij tegenover Chris kon doen alsof hij zijn taart voor 14 euro aan Bea had geleverd, want dan kon hij nog een tweede cd van Chris overnemen. Chris zou dan nog 7 euro overhebben nadat hij Bea’s boek had gekocht. Maar daar zou hij niets meer mee kunnen, want Arie noch Bea hebben op dat moment nog schulden[[1]](#footnote-1).

Omgekeerd, Bea zou graag anderen willen doen geloven dat ze Aries taart voor minder dan 7 euro had gekocht, want dan hield ze na verkoop van haar boek nog geld over voor andere dingen.

Elke speler heeft dus baat bij twee vormen van bedrog:

1. de prijs van aankopen lager voorstellen;
2. de prijs van verkopen hoger voorstellen.

Merk op dat als Arie later ten onrechte tegen anderen zegt dat hij de taart voor meer dan 7 euro heeft verkocht, Bea (de koopster) daar niet rechtstreeks door benadeeld wordt. Op dezelfde manier is Chris niet direct benadeeld, want hij heeft immers een bona fide transactie met Arie afgesloten (hij levert twee cd’s voor 14 euro).

Maar het is een probleem van het systeem. Er zou teveel geld in omloop zijn. Bij een kleine hoeveelheid is dat misschien niet zo erg. Maar stel dat dit bedrog bij elke transactie plaatsvond, dan was op elk moment de hoeveelheid geregistreerde schuldbekentenissen (geld) even groot als de totale transactiegeschiedenis! Dat zou gevolgen hebben, b.v. inflatie, of – terecht – verlies van vertrouwen in het systeem. En dus verlies van het systeem, want geld = vertrouwen.

# Onweerlegbaarheid

Alle spelers hebben er dus baat bij om de integriteit van het systeem te handhaven. En dat vereist onweerlegbaarheid van transacties. Als Arie niet kàn voordoen alsof hij zijn taart duurder heeft verkocht, is er niets aan de hand.

De enige die kan weten dat Arie bedriegt, is Bea. Zij weet immers precies voor hoeveel ze de taart heeft gekocht!

In Perspectives zouden we de systeemintegriteit waarborgen door Bea te betrekken in de transactie tussen Arie en Chris. Dat zouden we rechtvaardigen door het feit dat Arie de schuldbekentenis van Bea *gebruikt* om de CD van Chris aan te schaffen. De transactiezaak tussen Arie en Chris heeft dan de volgende rollen:

* Arie: koper van een CD ter waarde van 7 euro
* Chris: verkoper van een CD ter waarde van 7 euro
* Verkoop van taart aan Bea: een verkooptransactie met een schuldenaar ter waarde van 7 euro
* het verhandelde Goed: de CD.

Op het moment dat Arie en Chris de zaak opzetten, *moet* Arie Bea erbij betrekken. Want zonder schuldenaren met een gezamenlijke schuld aan Arie gelijk aan de prijs van het verhandelde goed, gaat Chris niet akkoord.

Maar zodra Arie Bea erbij betrekt, stuurt Bea’s computer de gegevens over de transactie tussen haar en Arie naar Chris. En Bea stuurt natuurlijk de werkelijke prijs (zij heeft er geen belang bij om de prijs hoger voor te stellen). Dus als Arie beweert dat hij meer heeft ontvangen, loopt hij direct tegen de lamp bij Chris!

Onweerlegbaarheid is verankerd in het systeem.

# Wat is de administratieve last?

In het echte leven ontvangen de meesten van ons maandelijks een inkomen en geven dat in de loop van de maand erop uit. Ieders actuele rekeningstand is de uitkomst van de optelling van historische inkomsten en uitgaven. Maar dat gaat terug tot het moment van oprichten van de rekening. Dat zou betekenen dat, om een transactie aan te gaan, de koper de transactiegeschiedenis van zijn gehele voorafgaande leven moet delen met de verkoper!

Dat gaat niet werken.

Stel nu dat de verkoper erop vertrouwt dat

* de vorige transactie van de koper bona fide is verlopen;
* de vorige transactiepartner (van de koper) de rekeningstand van de koper heeft gecontroleerd (en goed heeft bevonden, want anders was hij de transactie niet aangegaan).

Dus, concreet: de koper biedt een transactie Zaak aan met de volgende rollen:

* de vorige transactie (van de koper, een transactie met precies dezelfde soorten rollen en eigenschappen, maar andere actoren)
* de koper (hijzelf dus)
* de verkoper
* het goed, met de prijs

Bovendien heeft deze transactie de volgende externe eigenschappen:

* de rekeningstand van de koper na de transactie (en dat is de rekeningstand van de vorige transactie *minus* de prijs van het goed)
* de rekeningstand van de verkoper na de transactie (en dat is zijn rekeningstand *plus* de prijs van het goed).

Tenslotte, de verkoper wordt betrokken bij deze vorige transactie.

Dit is in essentie dezelfde opzet als bij het voorbeeld van Arie, Bea en Chris. De koper kan niet liegen over zijn rekeningstand, want zijn vorige transactiepartner bevestigt die naar de verkoper. Het cruciale verschil met dat voorbeeld is dat we hier de *rekeningstanden* van de transactiepartners doorgeven.

Nu volgt een recursief denkproces:

1. de verkoper kan controleren dat de aan hem voorgestelde transactie bona fide is;
2. de verkoper krijgt de garantie van de vorige verkoper dat de rekeningstand van de koper klopt;
3. dus de verkoper kan aan de vòlgende transactiepartner van de koper garanderen dat diens rekeningstand klopt!

Dit geldt voor elke transactie, tot het beginpunt, toen de rekening van de koper opgericht werd met een stand van 0.

De administratieve last blijft dus beperkt tot inzicht in en betrokkenheid bij de *vorige transactie* van je voorgenomen transactiepartner. Vanwege die betrokkenheid wordt je door die vorige transactiepartner onafhankelijk geïnformeerd over de rekeningstand van je voorgenomen transactiepartner. Een recursieve redenering laat zien dat je je dan kunt baseren op die rekeningstand.

ContextBuilders

oprichter

rekeninghouder

Systeem van Arie

gebruiker

Rekening Arie = 0

Vorige partner

Vorige transactie

Rekening Bea = -7

Appeltaart

Verkoper

koper

Prijs = 7

Vorige partner

Vorige transactie

Rekening Bea = 0

Boek

Verkoper

Koper

Prijs = 7

gebruiker

Systeem van Bea

gebruiker

Systeem van Chris

Rekening Arie = 7

Rekening Chis= -7

Vorige partner

Vorige transactie

Rekening Chris = 0

CD

Verkoper

Koper

Prijs = 7

Rekening Arie = 0

# Kun je dezelfde rekeningstand tweemaal gebruiken?

Er is nog een denkbare vorm van bedrog.

Arie heeft zijn taart verkocht aan Bea. Hij heeft zijn resulterende rekeningstand gebruikt in een transactie met Chris, wiens cd hij kocht. Maar nu wil hij bij Dirk een diner betalen en hij komt op het idee dat hij de transactie met Chris gaat verzwijgen (want dan ziet Dirk een hogere rekeningstand!). Dus, hij probeert met Dirk een zaak aan te gaan voor het diner waarbij de transactie met Bea de rol van de vorige transactie speelt.

Maar Bea, die daar natuurlijk bij betrokken wordt, zal dat afwijzen: immers, haar transactie met Arie *speelt al een keer de rol van vorige transactie*, namelijk die tussen Arie en Chris. Deze vorm van bedrog is dus ook onmogelijk.

Dit is het equivalent van dezelfde bitcoin tweemaal proberen uit te geven. De blockchain verhindert dat. Bij Perpectives verhindert de vorige transactiepartner dat.

1. In het algemeen zijn er natuurlijk meer spelers in de wereld en dan zou Chris daar zijn tegoed kunnen besteden. Het probleem zou niet anders zijn, maar moeilijker en later aan het licht komen. [↑](#footnote-ref-1)