HC 7A, 15-10-18, Automatische contracten en blockchain I

'Do ut des' betekent ik geef opdat gij geeft. Vroeger offerden de Latijnen een witte os aan Jupiter, opdat Jupiter hen beschermde. Daar komt deze uitspraak vandaan. Tegenwoordig kun je dit vertalen naar: boer A verkoopt aan handelaar B een koe, opdat B aan A 1.000 euro betaalt. Dit wordt ook wel de wederkerige overeenkomst genoemd.

De wederkerige overeenkomst
De totstandkoming van een wederkerige overeenkomst kan worden geformaliseerd. Denk bijvoorbeeld aan het in een systeem invoeren dat er koeien worden besteld als er minder dan 20 koeien worden geteld door de boer. Daarnaast kan de uitvoering van de overeenkomst ook worden geformaliseerd. Denk hierbij bijvoorbeeld aan het gebruik van een QR-code bij het doen van een betaling. Het is daarbij wel van belang of het objectief meetbaar is. Als er bijvoorbeeld de opdracht wordt gegeven om een portret te maken en het portret is gelukt, wordt er 5.000 euro uitbetaald. Dit is een subjectieve bepaling; wanneer is het portret gelukt? Bij zulke inspanningsverbintenissen is het lastig om een computer te laten bepalen of er is voldaan aan de verbintenis.

Geautomatiseerde totstandkoming
Problemen die spelen bij geautomatiseerde totstandkoming van wederkerige overeenkomsten zijn:
- De koppeling van de wil aan de verklaring (oneigenlijke dwaling).
- Het moment van totstandkoming.
- Vertrouwensdiensten.

Automatische contracten
Automatische contracten komen mogelijk maar niet noodzakelijk geautomatiseerd tot stand. Het gaat erom dat de nakoming van de verbintenissen is geautomatiseerd, zoals de betaling (iDeal), het geven van toestemming (licenties), kanscontracten en informatieproducten.

Geautomatiseerde nakoming
Het automatiseren en programmeren van bepaalde verbintenissen is zeker mogelijk. Zoals eerder genoemd is het hierbij erg van belang of de verbintenis objectief bepaalbaar is. Daarnaast is een tweede vraag of het vervolgens wel uit kan (is het voordelig?). Bij een grote hoeveelheid aan transacties en in geval van complexe berekeningen kan het zeer waarschijnlijk uit. Hierbij is de belangrijkste regel 'gigo' (garbage in, garbage out). Dit wil zeggen dat als je verkeerde informatie invult in het systeem, het systeem ook onjuiste antwoorden geeft. Het automatiseren van de uitvoering van contracten is slechts interessant bij massabestellingen en niet bij een eenmalige transactie.

Vertrouwen
Beide partijen moeten vertrouwen hebben in het systeem. De importeur en vaste producent hebben een raamovereenkomst (Interchange Agreement), deze partijen vertrouwen elkaar. In zo'n geval hebben partijen ook meer vertrouwen in het systeem.

Smart contracting
Geautomatiseerde bestelling en betaling bij levering is smart in een EDI-omgeving. Als partijen elkaar niet goed kennen werkt de afhandeling suboptimaal. Kan dat niet smarter?

Blockchain

De blockchain zou de oplossing kunnen bieden voor problemen als gebrek aan vertrouwen. Aspecten van de blockchain zijn:

- Gedistribueerde administratie. De administratie ligt niet op een centrale plek (zoals het geval is bij banken), maar bij alle deelnemers aan de blockchain.
- Integer en onveranderbaar. De blockchain is niet kraakbaar.
- Gevoed van buitenaf.
- Kan open of besloten zijn. Bij open blockchain kan iedereen er toegang tot krijgen. Bij een gesloten blockchain moet je toestemming krijgen om erbij te kunnen (je dient jezelf te identificeren en mogelijk te voldoen aan andere eisen).
- Cryptocurrency.
- Bitcoin.
- Ethereum.

De functies van blockchain zijn:

1. Betaling.
2. Registratie.
3. Smart contracting. Dit gaat over alle transacties die je via blockchain kan doen. Hiervoor werd deze term al gebruikt voor automatisch contracteren. Wij hanteren de term ‘smart contracting’ om automatisch contracteren via blockchain aan te duiden.

Cryptocurrency en betaling

Cryptocurrency heeft niet alleen de functie van het kloppend maken van de administratie, maar heeft ook een waarde. Het feit dat het op een blockchain is, maakt het ook nog:

- Transparant. Alle transacties zijn openbaar.
- Onveranderbaar.
- Integer. Het systeem zou het opmerken als twee keer dezelfde bitcoin wordt gebruikt voor een transactie (= double spending).

Het gebruik van de blockchain gebeurt normaal gesproken centraal, maar het kan ook gedistribueerd (zonder centrale aansturing). Bij de bitcoin beschikt iedereen over het register, terwijl in het gecentraliseerde gebruik de bank alleen het register heeft. De wallets van deelnemers zijn beveiligd, maar als dit niet genoeg is, dan is er ook beveiliging tegen double spending. Problemen die zich voordoen bij de beveiliging van wallets zijn:

- Wachtwoord vergeten.
- Wachtwoord aan een derde gegeven.
- Wachtwoord is achterhaald door een derde door phishing of hacking.
- Bitcoins weggegooid. Dit kan bijvoorbeeld doordat de pc waarop de wallet staat kapot gaat.

De transacties worden gecontroleerd door nodes (=deelnemers). Het verkrijgen van cryptocurrency kan door:

- Mijnen. Miners krijgen bitcoins. Een minor berekent de juiste oplossing voor een transactie, hiervoor ontvangt hij een beloning in bitcoin.
- Kopen of ruilen.

Kan cryptocurrency worden aangemerkt als geld?

- Het heeft geen fysieke vorm, maar dat is niet noodzakelijk.
- Betaalmiddelen hoeven ook niet per se van de overheid afkomstig te zijn. Men kan ook een geldmiddel contractueel afspreken.
- Het is in ieder geval geen giraal geld, want giraal geld is een vordering op een bank. Cryptocurrency staat op zichzelf en is geen vordering.
- Het is ook geen elektronisch geld, want dat is een vordering op de uitgever.

Er dient verder onderscheid te worden gemaakt tussen betaling met cryptocurrency en betaling voor cryptocurrency. Betaling met cryptocurrency houdt in dat je iets koopt en betaalt met cryptocurrency. Betaling voor cryptocurrency wil zeggen dat je je 'gewone' geld inlevert in ruil voor cryptocurrency.

HC 7B, 18-10-18, Automatische contracten en blockchain II

Smart contracting
Smart contracting gaat via blockchain met een automatisch contract. Een van de platforms waarbij je smart contracts kan opzetten is het Ethereum. De beloftes van Ethereum (waar adverteren ze mee) zijn vooral crowdfunding-projecten of crowdsale-projecten. Iedereen kan anoniem gebruik maken van decentrale netwerken waarbij geen tussenpersoon nodig is, om via de blockchain met behulp van cryptocurrency op een geautomatiseerde wijze contracten in de lucht te krijgen en te houden.

Als aan de door het systeem waarneembare criteria is voldaan, dan kan het systeem de nakoming in behandeling nemen, waarvoor geen tussenpersoon nodig is. Dit voldoet aan de eis dat er sprake moet zijn van objectief beoordeelbare criteria. Onder een smart contract uitkomen is wel een stuk lastiger, omdat het programma vooral kijkt of er aan de criteria voldaan is voor smart contracting. Wil je eruit komen dan zou je het hele programma moeten opbreken en een nieuwe maken.

Problemen die je tegenkomt in de praktijk bij smart contracts zijn:
- Koppeling van feitelijke handelingen in de wereld aan smart contract. Denk hierbij bijvoorbeeld aan als de koper van een koelkast deze niet betaalt, dat de koelkast zichzelf uitschakelt (technoregulering).
- Probleem menselijke beoordeling.
- Nu toekomstige betaling alvast vastleggen. Smart contracting kan zorgen voor een probleem met betrekking tot de liquiditeit.

DAO was een crowdfunding project waarbij iets van 100 miljoen euro werd opgehaald. Door een fout in het systeem konden de ontwikkelaars het geld steeds ongemerkt naar zichzelf toetrekken. Er konden twee dingen worden gedaan:
- Het systeem laten doordenderen, of
- het programma helemaal afbouwen door het toebrengen van een fork (als het systeem niet doet wat partijen willen). Hiermee wordt de wil van partijen weggepoetst die ten grondslag ligt aan het smart contract.

Je kunt je aanmelden bij een blockchain onder een pseudoniem. De vraag is of dit ook volledig anoniem is. Je pseudoniem zou namelijk te herleiden kunnen zijn naar jou. Daarnaast is het soms geen goed idee dat consumenten onder een pseudoniem zich kunnen aanmelden. Denk hierbij aan mensen met een gokverslaving.

Do ut des revisited
Wederkerigheid is geen formeel automatisme. Als contracten worden geprogrammeerd, dan wordt van alles overgelaten aan het programma en missen er allerlei menselijke instrumenten. Voorbeelden van deze menselijke instrumenten zijn:
- Een regel geldt niet als deze in strijd is met de redelijkheid en billijkheid.
- Dwaling en bedrog. Denk hierbij aan het hiervoor genoemde voorbeeld van DAO.
- Een programma kan een overeenkomst niet kwalificeren.
- Een programma kan geen rekening houden met onvoorziene omstandigheden.
- Bescherming van de zwakkere partij.

- Het programma ziet niet of de inhoud van de overeenkomst wenselijk is of niet (ongeoorloofde oorzaak).

Voorwaarden van het succesvol kunnen bouwen van smart contracting

- Geschikte verbintenissen (objectief bepaalbaar).
- Economische haalbaarheid (voldoende interessant om het IT-systeem het werk te laten doen).
- Toegevoegde waarde boven centrale database (gedistribueerde administratie).
- Vertrouwen in programmatuur en externe informatie (oracles). Bij onjuiste (externe) informatie komt er een onveranderbare uitkomst uit het systeem.
- Inzet van fondsen. Het probleem van de liquiditeit moet er niet zijn.
- Dwangbuis moet ook geen bezwaar zijn.
- Indien noodzakelijk: identificatie deelnemers. Hiermee kan geen openbare blockchain worden gevormd.
- Gejuridiseerd platform waarbij is voldaan aan de informatieplichten.