

## Eigendom in de virtuele dimensie

Het traditionele begrip “eigendom” wordt ingekaderd door de relatie tussen de mens en een zaak. Met andere woorden: “wie is eigenaar waarvan”? Daarbij wordt deze eigendom veelal geregistreerd door bijvoorbeeld een bank of de overheid. Deze bank of overheid heeft daarvoor een centrale administratie nodig om alle gegevens vast te leggen.

Het gevolg hiervan is dat ieder individu moet vertrouwen op de bank of de overheid. En, het mag niet onvermeld blijven, ieder individu dient de dienstverleners te betalen voor deze geleverde diensten.

De financiële crisis van 2008, en andere malversaties in de financiële sector, heeft echter geleid tot een afname van vertrouwen in de financiële tussenpersonen. Veel mensen zoeken een alternatief voor de van oudsher bekende deelname aan sociale en financiële instituties. De crypto Cultuur, die bij velen bekend is geworden door de Bitcoin, biedt een verstorend alternatief voor de traditionele manieren van communicatie en handel (Edward D. Baker, *Trustless Property Systems and Anarchy: How Trustless Transfer Technology will shape the Future of Property Exchange*, 45 *Sw. L. Review* 351 (2015-2016)).

Cryptografie is een manier om vertrouwen te structureren. Het is een methode waarbij geheimhouding wordt geregeld. Het leger gebruikte dit om gegevens te beveiligen. Deze cryptografie kan echter breder worden ingezet, namelijk om online transacties te beveiligen. Dit heeft tot gevolg dat het tempo en de efficiency van eigendomsverschuivingen aanzienlijk kan toenemen.<sup>1</sup> Hoe werkt dit systeem dan?

Stelt u zich voor dat iedereen een set van twee sleutels heeft. Een van de sleutels is openbaar; iedere persoon op de wereld heeft zo’n sleutel. De andere sleutel is privé. De sleutels zijn weliswaar wiskundig aan elkaar gelieerd, maar het is niet mogelijk om de openbare sleutel te gebruiken om de privé sleutel te achterhalen. Met de openbare sleutel kan men berichten versturen, Bitcoins versturen. De openbare sleutel is de toegang tot uw brievenbus. Iedereen kan hiermee iets in uw brievenbus gooien. Maar alleen de eigenaar van de brievenbus heeft de tweede sleutel, de privé sleutel om de brievenbus te openen en de inhoud ervan te bekijken (Edward D. Baker, *Trustless Property Systems and Anarchy: How Trustless Transfer Technology will shape the Future of Property Exchange*, 45 *Sw. L. Review* 351 (2015-2016) p. 354). Cryptografie is daarbij het beveiligingsmechanisme van de transacties.

Maar daarmee zijn we er nog niet. Voorkomen moet worden dat hetzelfde goed meerdere malen wordt verkocht en geleverd. Stel, ik heb een stuk grond en wil dat in eigendom overdragen aan B. In de off-line wereld wordt een dergelijke transactie geregistreerd in het kadaster. Dit om te voorkomen dat ik het stuk grond, nadat ik het heb verkocht en geleverd aan B, nogmaals verkoop en lever aan C. Ook online bestaat een register. Een TPL (Trusted Public Ledger) is een openbare lijst, die de keten van eigendom beschrijft aangaande een zaak of een goed met waarde. Iedere zaak op een TPL is daarbij uniek, en is de zaak overgedragen, dan is deze alleen toegankelijk voor de nieuwe eigenaar. Is een transactie eenmaal cryptografisch beveiligd, dan wordt deze transactie gepubliceerd op een algemeen grootboek (“the Blockchain”).

Ter verduidelijking: het traditionele PayPal werkt als een Trusted Third Party (tussenpersoon), die een transactie begeleidt en afsluit. TPL daarentegen gebruikt geen tussenpersoon. Het maakt het mogelijk dat gebruikers digitale eigendom veilig en

---

<sup>1</sup>

anoniem over het netwerk kunnen uitwisselen. TPL's gebruiken daarbij een systeem van cryptografische bewijzen om een transactie te beveiligen.

Nu staat of valt elk eigendomssysteem uiteraard met de kwestie van nakoming. Als een transactie is afgewikkeld, moeten beide partijen hun kant van de overeenkomst nakomen. TPL's maken transacties tussen twee personen mogelijk door software programma's die elementen van het traditionele overeenkomstenrecht vertalen in "trustless transactions" over het netwerk. We spreken dan van "Smart Contracts" (Deze term en uitvinding zijn afkomstig van Nick Szabo, zie: Jay Cassano, What are Smart Contracts? Bitcoin's Killer App, FAST COMPANY, <http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app>, laatst geraadpleegd 2 november 2016). Deze "smart contracts" maken niets mogelijk dat voorheen onmogelijk was. Het enige wat ze doen is dat ze je toestaan gewone problemen op te lossen op een manier die minder vertrouwen vergt dan voorheen. Menselijke oordelen zijn uit het systeem gefilterd; het geheel is geautomatiseerd. Met andere woorden, "smart contracts" voeren automatisch de contractuele voorwaarden uit via het "als-dan" principe. Nakoming werkt aldus automatisch. Als een voorgeprogrammeerde voorwaarde wordt geactiveerd, voert het "smart contract" de corresponderende contractuele voorwaarde uit.

Volgens Fairfield (Joshua Fairfield, Smart Contracts, Bitcoins, and Consumer Protection, *71 Wash. & Lee L. Review Online* at. 35 (2014)). bestaat momenteel een discrepantie tussen on-line contracteren en off-line contracteren. Online kunnen consumenten namelijk niet onderhandelen. Een consument kan alleen klikken op de button "Ik accepteer", het bedrijf dat het goed aanbiedt dicteert de voorwaarden. Off-line contractenrecht daarentegen staat in de sleutel van partij autonomie en onderhandelingsvrijheid. Smart contracts kunnen hier een oplossing bieden, waardoor consumenten ook on-line onderhandelingsruimte hebben.

*Anka Ernes*