DOOR JACOB BOERSMA

Blockchain als bouwsteen voor de verzekeringswereld

Blockchaintechnologie kan de verzekeringswereld ingrijpend veranderen. De mogelijke impact wordt soms zelfs vergeleken met de komst van internet. Steeds meer organisaties verdiepen zich dan ook in de mogelijkheden van de blockchain om transacties efficiënter, goedkoper en betrouwbaarder te maken. Maar hoe werkt deze technologie nou eigenlijk?

J. Boersma MSc is senior manager bij Deloitte Risk Advisory en leidt het blockchainteam in Nederland.

BITCOIN

Blockchain is in 2009 voor het eerst in de praktijk gebracht als de technologie achter bitcoin. De bitcoin blockchain is vergelijkbaar met een digitaal grootboek dat wordt bijgehouden door een gedistribueerd netwerk van computers. Er is daarbij geen centrale partij die de verbinding verzorgt tussen de verschillende deelnemers of die bepaalt wie welke gegevens te zien krijgt. Het is een zogenaamd 'peer-to-peer' netwerk, zonder tussenpersonen. Dit is een wezenlijk verschil met centraal ingerichte systemen van bijvoorbeeld banken, waarbij er één partij is die alle informatie heeft en bepalend is voor het goedkeuren van transacties. Zo'n partij vormt daarmee een aanvalspunt voor hackers bijvoorbeeld bij een Denial of Service aanval. Een gedistribueerd blockchain netwerk is robuuster en kent niet zo een 'single point of failure'.

Gecentraliseerd (traditioneel) Gedistribueerd (blockcain)

Om ervoor te zorgen dat er geen centrale database nodig is, heeft iedere computer in het netwerk een identieke kopie met alle informatie over alle eerder gedane transacties. Dit is de daadwerkelijke *blockchain* in een blockchainnetwerk. Alle deelnemers in het netwerk controleren alle transacties die worden ingestuurd en als deze correct zijn (in lijn met de geschiedenis zoals die in de blockchain staat), worden ze toegevoegd aan een nieuw 'block' die door cryptografie als een 'chain' (ketting) aan het vorige block wordt gekoppeld. Hiervoor wordt gebruik gemaakt van een zogenaamde hash functie, die een unieke digitale vingerafdruk berekent van het blok met transacties.

Opgeslagen transacties kunnen daardoor niet meer worden gewist of veranderd zonder de ketting te breken (iets wat zichtbaar is voor alle deelnemers). Elke transactie is daarnaast zelf ook digitaal ondertekend met een unieke sleutel van de verzender. Op het moment dat een nieuw blok wordt berekend en toegevoegd aan ieders kopie van de blockchain, krijgt het een tijdcode mee, een zogenaamde time stamp. Daarmee is achteraf altijd te achterhalen wanneer een bepaalde transactie heeft plaatsgevonden.

SMART CONTRACTS

In een blockchainnetwerk, waarbij alle deelnemers iedere transactie contoleren voordat deze het gedeelde kasboek wordt toegevoegd, kunnen we ook andere controles gaan toevoegen en daarmee voorwaarden in een betaling programmeren. Deze conditionele betalingen worden ook wel 'smart contracts' genoemd, omdat het zelfuitvoerende afspraken zijn waarbij de software automatisch bepaalde voor gedefinieerde acties uitvoert. De term is echter wat verwarrend omdat het hier om computercode gaat en niet om juridische contracten.

Een voorbeeld: een betaling wordt geprogrammeerd met de voorwaarde dat deze alleen doorgaat als 99 andere mensen ook eenzelfde betaling uitvoeren binnen bepaalde tijd. Hiermee kun je dus een crowdfundingactie opzetten. Of een transactie gaat pas door als een container met een bepaald serienummer in de haven van Rotterdam is aangekomen en gescand, wat dan automatisch de overdracht van het geld in gang zet en mogelijk overdracht van andere gegevens zoals douanepapieren en certificaten.

Het blockchainnetwerk Ethereum (na bitcoin de grootste actieve blockchain) is speciaal gebouwd om zeer complexe smart contracts te kunnen uitvoeren. Het is zelfs mogelijk om complete bedrijfsprocessen te modelleren als software die autonoom wordt uitgevoerd op dit gedistribueerde netwerk.

VERZEKERING ALS SMART CONTRACT

Een verzekeringsproduct kan ook worden gemodelleerd als een conditionele transactie en daarmee worden opgenomen als smart contract op de blockchain. Bijvoorbeeld: een smart contract wordt geprogrammeerd met de voorwaarden dat er maandelijks premie betaald moet worden aan het bijbehorende blockchainadres en dat een bepaald bedrag aan de verzekeringsnemer overgemaakt moet worden als er meer dan X millimeter regen valt in een bepaald gebied. Door een koppeling aan een *oracle*, een externe bron, in dit geval het KNMI, gaat het smart contract in werking op het moment dat de regenval gerapporteerd wordt, mits alle premiebetalingen zijn gedaan. Dit gebeurt geheel automatisch, volgens de afgesproken voorwaarden en volstrekt transparant en betrouwbaar voor de verzekeringsnemer.

Andere voorbeelden zijn reisverzekeringen die automatisch uitbetalen op het moment van vertraging of uitval van een vlucht (met de website van de luchtvaartmaatschappij als externe bron), of overlijdensrisicoverzekeringen die automatisch uitbetalen aan persoon X als persoon Y overlijdt (met het bevolkingsregister als onafhankelijke bron).

De keuze voor een goed oracle is hierbij wel van belang. Niet alleen moet deze bron digitaal zijn (zodat het blockchainnetwerk deze kan raadplegen), maar moet ook betrouwbaar zijn, aangezien de uitvoering automatisch plaatsvindt en het manipuleren van een oracle daarmee interessant kan zijn voor hackers. Voor extra betrouwbaarheid zou een smart contract zo geprogrammeerd kunnen worden dat het de informatie uit meerdere bronnen combineert, of bijvoorbeeld meerdere partijen te laten stemmen, waarbij de meerderheid beslist.

MEER DAN (VIRTUEEL) GELD

Veel van de toepassingen van blockchaintechnologie hebben betrekking op geldtransacties, en dan met name die van virtuele valuta, die enkel bestaan op de blockchain zelf, zoals bitcoin, ether (de valuta van Ethereum), litecoin en nog vele andere.

Het is echter mogelijk om ook andere zaken op een blockchain te registreren, zolang deze maar uniek digitaal kunnen worden gerepresenteerd. Zo zijn er al toepassingen om bijvoorbeeld het eigendom van vastgoed op te slaan op een blockchain (in feite een gedecentraliseerd Kadaster), of bijvoorbeeld eigendom van kunstwerken en diamanten. Dat laatste kan doordat iedere geslepen diamant uniek is en er daardoor een unieke 'vingerafdruk' van te meten is die weer digitaal kan worden gemaakt en in de blockchain kan worden opgenomen.

Ook identiteitskenmerken kunnen op deze manier digitaal op de blockchain worden gezet en door de eigenaar ervan betrouwbaar door worden gestuurd naar andere partijen. Zo kun je met een identiteitssysteem op de blockchain bijvoorbeeld bewijzen dat je boven de 18 bent of dat je toegang hebt tot bepaalde patiëntendossiers, zonder dat je andere aspecten van je identiteit (zoals naam, adres of geboortedatum) hoeft te onthullen.

PUBLIEK VERSUS BESLOTEN

Door het delen van de informatie met alle partijen in het netwerk geeft een blockchain een onafhankelijk en betrouwbaar beeld van de historie en de huidige stand van zaken. Door het decentrale karakter is er geen centrale server die gehackt kan worden of een centrale partij die gegevens zou kunnen manipuleren of achterhouden.

Voor sommige bedrijven en overheden is het idee van een open blockchainnetwerk, waar iedereen aan kan deelnemen en waarbij iedereen alle transacties kan zien, echter niet wenselijk. Zij willen vertrouwelijke gegevens uit kunnen wisselen binnen een besloten groep. Hiervoor maken ze steeds vaker gebruik van besloten blockchainplatformen, zogenaamde *private blockchains*. Hierbij is er wel weer een centrale partij (of groep van partijen) die bepaalt wie er toegang krijgt tot de blockchain. Maar eenmaal binnen werkt het net zoals in de publieke blokchainnetwerken, met alle voordelen van dien voor betrouwbare informatie-uitwisseling. Het bekendste platform voor private blockchains is Hyperledger.

VOOR- EN NADELEN

De voordelen van een blockchainnetwerk worden uit bovenstaande wel duidelijk: voor allerhande vormen van waardeoverdracht en vertrouwensdiensten maakt het tussenpersonen overbodig en verhoogt betrouwbaarheid en controleerbaarheid. De techniek staat echter nog in de kinderschoenen en er is nog een aantal uitdagingen die overwonnen moeten worden voordat echt grootschalig gebruik mogelijk wordt.

Een van de belangrijkste barrières is de wet- en regelgeving. De cryptomunten die op de blockchain gebruikt worden als betaalmiddel worden door de meeste landen niet erkend als geld en vallen daardoor niet onder dezelfde wetgeving. Dit maakt het bijvoorbeeld lastig voor blockchainbedrijven om zich te laten registreren als betaalinstelling of om te bepalen wat de belastingregels zijn die ervoor gelden. Ook de koersschommelingen van cryptovaluta maakt dat het voor veel bedrijven niet aantrekkelijk is om zich direct met deze virtuele munten te laten betalen. Het is wachten op de eerste 'virtuele euro's' of andere door banken of overheden uitgegeven cryptocurrencies. Sommige overheden experimenteren er al wel mee; zo kunnen bedrijven in Zwitserland bijvoorbeeld hun belasting al in bitcoin betalen.

Ook op andere gebieden dan betalingsverkeer kan de wetgeving een uitdaging zijn. Zo dwingen de nieuwe privacyregels van de AVG een bedrijf om persoonsgegevens van een klant te verwijderen op diens verzoek. Maar wat als die persoonsgegevens op een blockchain staan die geen eigendom is van één partij en die juist gebouwd is om onwijzigbaar te zijn? Een verzekeraar die verzekeringsproducten op de blockchain wil zetten zal er dus goed voor moeten waken dat er alleen onversleutelde, pseudonieme gegevens op die blockchain worden gezet en geen voor derden herleidbare klantdata. ■