Bijlage. Wat is een blockchain?[1]

Een gedecentraliseerde administratie

Blockchain beoogt het mogelijk te maken om een administratie te voeren, zonder afhankelijk te zijn van een centrale partij die de administratie voert. Met een blockchain wordt dus gestreefd naar *decentralisatie*. Om dit te bereiken wordt de administratie op vele computers tegelijk gevoerd. Deze computers wisselen voorgestelde mutaties[2] in de administratie onderling uit. Een zogenaamd consensus protocol moet bewerkstelligen dat alle administraties kloppen en gelijk blijven lopen, zonder enige opdracht 'van boven'. Elke computer bepaalt zelf (aan de hand van op cryptografische technieken gebaseerd bewijs) of een set (block) van voorgestelde mutaties kan worden vertrouwd (en dus zal worden toegevoegd aan de eigen replica van de administratie). Eenmaal toegevoegde gegevens blijven een rol spelen in de beveiliging van een blockchain tegen onbevoegde wijzigingen. Ze worden in beginsel dan ook niet meer verwijderd; in elk geval niet zonder consensus in het netwerk.

Soorten toepassingen

Blockchains kennen grofweg drie soorten toepassingen (die kunnen worden gecombineerd). Hieronder worden deze nader toegelicht.

1. Registers

Een blockchain kan ten eerste worden gebruikt als een *register*, dus voor het vastleggen van gegevens.

2. Tokens

Een blockchain kan ten tweede worden gebruikt om *tokens* te creëren. Tokens kunnen zeer verschillende eigenschappen hebben (bijv. wel of niet overdraagbaar, beperkte of onbeperkte oplage, deelbaar of ondeelbaar etc.) en zeer verschillende toepassingen, zoals virtuele valuta (ook wel 'native tokens' genoemd), effecten, een recht om een online dienst te gebruiken etc.

3. Smart Contracts

Een blockchain kan tot slot worden gebruikt om een *computerprogramma* (smart contract) op te bewaren en voorwaardelijk uit te voeren. Dit programma kan worden gebruikt als een soort derdenrekening. De ene partij kan hierop crypto's 'storten'. De andere partij ontvangt de crypto's zodra is voldaan aan de in het smart contract opgenomen voorwaarden. Mogelijk is hiervoor input nodig van buiten de blockchain, bijvoorbeeld de bevestiging dat een bestelde zaak is geleverd. Een zogenaamd *oracle* kan deze input leveren (en fungeert daarmee dus als een 'vertrouwde derde'). Anders dan de naam misschien suggereert is een smart contract geen vorm van (zelflerende) kunstmatige intelligentie.

Permissionless vs. permissioned blockchains

In een blockchain moeten bepaalde taken worden vervuld, zoals het rondzenden van voorgestelde mutaties, het voordragen van deze mutaties voor goedkeuring en het opslaan van goedgekeurde mutaties.

In een *permissionless* blockchain worden deze taken uitgevoerd door partijen die dit vrijwillig op zich nemen, hiervoor is geen toestemming nodig. Dit betekent dus dat iedereen die dat wil, mee kan doen aan het proces van lezen en schrijven. Omdat onbekenden op eigen initiatief kunnen meedoen, dreigt altijd het gevaar

[1] Deze uitleg is een vereenvoudigde weergave van hoe blockchains werken.

[2] Mutaties in de zin van: aan de blockchain *toe te voegen* gegevens.

van samenspanning. Om deze reden worden in *permissionless* blockchains crypto-economische prikkels ingebouwd: het verwerken van gegevens volgens het consensus protocol wordt beloond, of het schenden van het protocol wordt gestraft. Deze prikkels moeten het netwerk in staat stellen aanvallen te pareren. Dat lukt in de praktijk niet altijd.[3] Bij een 'klassieke' toepassing (centrale administratie) is er een opdrachtgever die het doel en de werking van de toepassing bepaalt en deze voor zijn rekening laat ontwikkelen en beheren. In een permissionless blockchain ontbreekt een dergelijke 'almachtige partij'. Er is een team van software ontwikkelaars dat de toepassing heeft gemaakt. Soms is niet bekend wie dat zijn. Welke partijen deze toepassing gaan downloaden en uitvoeren hebben de ontwikkelaars niet in de hand. Dat geldt ook voor uitgebrachte updates, hetgeen onder omstandigheden met zich mee kan brengen dat de toepassing splitst (doorgaat als twee toepassingen). Welke mate van decentralisatie werkelijk wordt bereikt bij moet van geval tot geval worden bezien en kan bovendien in de tijd veranderen, bijv. doordat machtsverhoudingen veranderen.

Een permissioned blockchain werkt anders. Hier is er wél een opdrachtgever. Dat kan een bepaalde organisatie zijn, maar ook een samenwerkingsverband. Deze organisatie c.q. dit samenwerkingsverband bepaalt het doel en de werking van de toepassing. De software ontwikkelaars ("core developers") zijn hier opdracht-nemer. Anders dan bij een permissionless blockchain is autorisatie nodig om een bepaalde taak uit te mogen voeren in de toepassing. Daardoor kunnen lees- en schrijfrechten ingeregeld worden. De governance is gebaseerd op afspraken tussen partijen, welke mede in de techniek worden vormgegeven.

[3] Zie bijvoorbeeld: Mike Orcutt, Once hailed as unhackable, blockchains are now getting hacked, MIT Technology Review, https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.