BLOCKCHAINS

16/06/2018

Blockchain is een complexe technlogie die het mogelijk maakt gegevens op een veilige manier op te slaan en uit te wisselen. Er worden meerdere reeds bekende technologien gecombineerd : opslaan van gegevens in de vorm van algoritmes, peer-to-peer technologie, hashage techiek, cryptographie (met een privé of publieke sleutel/paswoord).

Het doel is om een soort automatisme te creeren, waarbij geen bemiddelaar meer nodig is, die zorgt voor vertrouwen in de transactie. In de code monétaire et financier art L223-12 wordt een wettelijke beschrijving gegeven van de blockchain : un dispositif d'enregistrement électronique partagé permettant l'authentification - een gedeelde electronische registratie die authentificatie mogelijk maakt (artikel betreffende minibons, verplichte leningen voor kleine bedrijven)

Het officiele gebruik van blockchain zal waarschijnlijk uitgebreid worden in het kader van het overdragen van effecten (voorgestelde wijziging van art L211-3 c.mon.fin.)

Maar de blockchain is veel meer dan deze legale beschrijving : het is een register waarin gegevens en feiten chronologisch worden ingeschreven zonder gewijzigd te kunnen worden (documenten, transacties, activa). Dit register wordt gepresenteerd in de vorm van een algoritme en kan vergeleken worden met een gedecentraliseerd grootboek waarvan de verschillende pagina's zichtbaar zijn op alle computers van het netwerk (les mineurs). Het controlemechanisme verzekert dat de bitcoin die overgemaakt wordt aantoonbaar in het bezit is van de persoon die de handeling heeft verricht en dat die bitcoin afkomstig is van een eerder geverifieerde regel uit het grootboek. De controleurs krijgen voor het controleren een paar bitcoins.

Een persoon die een transactie wil uitvoeren, verbindt zich op een platvorm met een blockchain netwerk. Hij/Zij schrijft onderaan de blockchain een regel, waaraan niemand anders iets toe kan voegen of iets aan kan wijzigen. Om de operatie te beveiligen en te authetificeren, hebben alle partijen van het netwerk een persoonlijke code en een publieke code (soort emailadres waarop men gecontacteerd kan worden). Nadat de pagina toegevoegd is, wordt hij beveiligd met een algoritme en geverifieerd door alle gebruikers (bv door een wiskundeprobleem op te lossen, waarvoor degene die het probleem als eerste oplost een token krijgt (crypto-économie). Als 51% van de computers van het netwerk aangeven dat de pagina authentiek is, wordt de pagina verbonden met de blockchain, waardoor zij niet meer vervalst en veranderd kan worden.

Een blockchain kan publiek of privé zijn.

Een publieke blockchain (van de overheid) werkt middels de peer-to-peer techniek : het netwerk is voor ieder open en leesbaar, en iedere deelnemer gebruikt een pseudoniem. De veiligheid van de transacties die via het netwerk worden uitgevoerd wordt gegarandeerd door het systeem zelf en niet door een derde vertrouwenspersoon.

Bij een privé blockchain worden de regels van te voren vastgesteld. De beheerder verifieert en kan op ieder moment het protocol wijzigen. Deze privé blockchains worden vooral door banken gebruikt om deze technologie te testen. Er bestaan ook hybride blockchains (consortium). In dat geval wordt het aantal deelnemers beperkt en hebben bepaalde deelnemers een vetorecht. Deze privé en hybride blockchains behoren tot de DLT (distributes ledger technology).

De blockchain kan gebruikt worden voor :

- Overdracht van gedematerialiseerde valuta dmv tokens (crypto-valuta Bitcoin of Ethers) ; doordat veel deelnemers vertrouwen in deze gedematerialiseerde valuta hebben, wordt de waarde steeds hoger : het wordt hierdoor mogelijk buiten financiele instellingen en banken om valuta over te dragen of uit te wisselen.
- Overdracht van activa dmv financiele tokens ; bv crowdfunding, DAO (decentralised autonomous organization), organisme met token-aandeelhouders die vetorecht kunnen hebben en rente over de winst krijgen. Deze technologie zou gebruikt kunnen worden voor de CO2 markt, energiecertificaten en compensation banks
- Bewaren van gegevens : een beveiligd register waarmee gegevens veilig overgedragen kunnen worden bv door de bank : KYC know your customer, de verzekeringsmaatschappijen en herverzekering, medische dossiers, technische dossiers
- Registratie via een blockchain zorgt voor een tijdstempel (time stamping), die niet aangevochten kan worden. Hierdoor kunnen conflicten tussen schuldeisers, kopers en verkopers makkelijker opgelost worden.
- Kadaster of certificering kan middels blockchain gerealiseerd worden,
- Kan gebruikt worden in geval van effectisering, electronisch stemmen, registers van gegevens zoals patienten dossiers, identiteitspapieren, burgerinformatie en diploma's
- In het geval van een smart-contract kan er een automatische handeling geprogrameerd worden, bijvoorbeeld uitbetaling van een vergoeding door een verzekeraar in geval van noodweer of vertraging van treinen/ vliegtuigen

In onze dagelijkse economie kan de blockchain nuttig zijn voor het verbeteren van de betrouwbaarheid van de systemen, de snelheid van transacties en de bescherming van gegevens.

Binnen de overheid worden eveneens veel systemen onderhouden waarin data worden bijgewerkt en overgedragen. Met blockchain kunnen systemen opnieuw worden ontworpen om beter te voorzien in de behoeften van burgers, bedrijven en overheden.

Waar nodig kunnen gegevens privé blijven en alleen op aangeven van de eigenaar worden overhandigd ter verificatie of leesbaar worden gemaakt voor gebruik.

Blockchain is een recente technologie die nog nauwelijks juridisch ombouwd is. Het is nog niet duidelijk in welke juridische categorie deze handelingen ingedeeld moeten worden en hoe eventuele risiko's juridisch ondervangen kunnen worden.

De juridische categorie bepaalt welke regeling toegepast moet worden. Tokens kunnen bijvoorbeeld gekwalificeerd worden als financieel instrument, financieel contract, goederen of niet-officiele valuta, betalingsdienst.

Op dit moment werkt deze technologie nog niet optimaal :

- De blockchain kan gehackt worden
- Er kan fraude gepleegd worden. : omdat 51 % van de computers de handeling moeten authentificeren, kan de concentratie van deze computers in handen van Chinese multinationals ervoor zorgen dat deze grens bereikt wordt door authentificatie door één bedrijf.
- Deze technologie werkt nog te traag en kost teveel energie om op grote schaal toegepast te kunnen worden (vooral de authentificatie dmv oplossen van wiskundige problemen)
- Kan gebruikt worden voor illegale operaties (losgeld opgeeist door computerhacker)
- Het pseudonimaat kan witwassen of financieren van terrorisme faciliteren
- De derde vertrouwenspersoon / intermediair lijkt onmisbaar in geval van protocol vaststellen van smart contracts en privé en hybride blockchains
- Er kan geen procedure meer gerespecteerd worden : aanmaning, betekening, motiveringsverplichting, opzegtermijn
- De risikobeheersing zal ondervangen moeten worden in geval van een technologisch probleem of hacker, wie is er verantwoordelijk voor de verliezen ? hoe kan een clausule van overmacht worden ingebouwd ?
- Als zich een probleem voordoet van de authentificatie door de 51 % deelnemers, die zich in de hele wereld bevinden, rijst de vraag welke rechtbank competent is en welk recht toegepast moet worden.

Bronnen :

- *Recueil Dalloz 2 november 2017, artikel van Mustapha Mekki*
- *watisblockchain.nl*