The Hague **Security Delta**

Notitie Risico-Analyse in Onzekerheid

Blockchain (Kansen en Bedreigingen)

HSD
The Hague **Security Delta**

info@thehaguesecuritydelta.com | thehaguesecuritydelta.com | @HSD_NL

Inhoudsopgave

1. Risicoanalyses om de dynamiek voor te blijven

De wereld verandert snel. Dat er sprake is van een ‘technologische tsunami’ wordt breed erkend. Desondanks worden we niet zelden overvallen door rap opkomende technologieën die, naast nieuwe kansen, ook nieuwe bedreigingen inhouden die soms veel verder gaan dan wat we op grond van onze ervaringen uit het verleden konden verwachten. Dit moet en kan beter. Niemand kan de precieze aard en timing van de grote veranderingen en de daaruit voortvloeiende nieuwe risico’s voorspellen, maar goede analyses stellen ons wel in staat om de range aan mogelijkheden te verkennen en ons zo actief voor te bereiden op wat komen gaat.

Deze notitie is bedoeld om voor een concrete casus – de snelle vooruitgang in Distributed Ledger Technology (DLT) (de generieke naam van block chain-achtige technieken) - te schetsen hoe een scenariogedreven risicoanalyse ons in staat stelt om (1) de kansen die nieuwe technologie biedt in kaart te brengen om (2) de nieuwe of verschuivende risico’s en dreigingen die hierbij opdoemen te karakteriseren, teneinde (3) de oplossingsrichtingen te verkennen om deze risico’s en dreigingen tegen te gaan of te beheersen. Het is daarbij van belang te beseffen dat deze nieuwe risico’s en dreigingen opkomen in een dynamische systeemcontext. Nieuwe patronen van verknoping en fragmentatie, van samenwerking en conflict, van winnaars en verliezers ontstaan: op mondiale schaal (geopolitieke orde), diep in onze samenleving (het maatschappelijk weefsel) en op alle tussenniveaus (in de rol van Europa versus de lidstaten bijvoorbeeld). Er is sprake van complexe(re) verbindingen omdat interne en externe veiligheid in elkaar overvloeien. In het veiligheids¬ecosysteem worden andere en meer verschillende spelers van belang. Er ontstaan daarbij nieuwe risico’s en dreigingen die onmogelijk goed vallen te snappen en aan te grijpen vanuit de bestaande structuren, omdat deze de ordening uit het verleden weerspiegelen.

Deze notitie kan worden gezien als een vertrekpunt voor een proces waarin de snelle technologische ontwikkelingen op het gebied van DLT (en andere gebieden[1]) met een veiligheidsbril op worden bezien. Zo dient de notitie als input voor een HSD-Café in november 2017, waar verschillende organisaties samenkomen om, aan de hand van kansen en bedreigingen van AI en Blockchain, risico-analyse toe te passen. Op deze wijze wil HSD Office de partners in HSD en alle overige belanghebbenden informeren over de mogelijke veiligheidsimplicaties van de snelle ontwikkelingen op, bijvoorbeeld, het gebied van DLT, om vervolgens in scenariogedreven risicoanalyses gezamenlijk te bepalen welke innovatieve veiligheids¬oplossingen nodig zijn. Deze notitie en het bijbehorend proces bieden tevens houvast voor de agendering en de toekomstige ontwikkeling, rol en positionering van HSD.

[1] Tegelijk met deze notitie over DLT verschijnt een soortgelijke notitie over Artificial Intelligence.

2. Eerste Kennismaking

Blockchain als mogelijke *game changer*

> "In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation. The technology could prove to have the capacity to deliver a new kind of trust to a wide range of services. As we have seen open data revolutionise the citizen's relationship with the state, so may the visibility in these technologies reform our financial markets, supply chains, consumer and business-to-business services, and publicly-held registers." [2]

De digitale valuta Bitcoin is de oorsprong van een nieuwe aanpak voor het bijhouden van financiële transacties. De onderliggende technologie registreert elke valutatransactie in identieke kopieën van een digitaal grootboek (*ledger*) dat wordt gedeeld door de gebruikers van de valuta. Financiële instellingen, toezichthouders, centrale banken en overheden onderzoeken nu de mogelijkheden om deze benadering te gebruiken voor het stroomlijnen van een groot aantal verschillende diensten. Maar de mogelijke toepassingen gaan veel verder dan de financiële wereld, en kunnen de hele economie en de samenleving radicaal veranderen. Het zal de wijze waarop mensen en organisaties afspraken maken en de manier waarop we allerlei materiële en niet-materiële zaken van waarde - aandelen, obligaties, geld, vastgoed, diamanten, de inhoud van een zeecontainer, titels, identiteit, wie deed wat en wanneer, stemmen enz. - vastleggen op zijn kop zetten. Vertrouwen wordt niet langer gegarandeerd door gekende tussenpartijen (*trusted third parties*), maar door slimme computercode en genetwerkte consensus.

Mogelijk dat veel van de toepassingen van deze *distributed ledger technology* (DLT) – veelal bekend als *block chain*[3] - pas op middellange termijn ontstaan vanwege allerlei vormen van weerstand vanuit bestaande structuren en omdat de benodigde aanpassingsprocessen van de overheid en de particuliere sector omvangrijk en langdurig zijn. Maar de implicaties zijn groot en ook in een overgangsperiode van belang. Beleidsmakers moeten daarom reeds nu inzicht ontwikkelen in wat deze technologie en haar toepassingen inhouden; om vervolgens te bezien hoe de kansen te benutten en de eventuele negatieve gevolgen te bestrijden.

Belangrijke kenmerken van gedistribueerde grootboeken (distributed ledgers):
Gedistribueerde database. Alle partijen in een DLT-toepassing hebben toegang tot de volledige database - d.w.z. het grootboek met zijn volledige transactiegeschiedenis - vastgelegd in identieke kopieën die verspreid zijn opgeslagen.
Rechtstreekse communicatie. Communicatie tussen transactiepartners is rechtstreeks in plaats van via een vaste tussenpersoon of centraal knooppunt. Elke partij kan de gegevens van zijn transactiepartners direct verifiëren.
Gedetailleerde toegangscontrole. DLT maakt het mogelijk precies vast te leggen wie wat wanneer kan doen met de database.
Transparantie en permanentie. Zodra een transactie is ingevoerd in de database en alle kopieën zijn bijgewerkt, kan de transactie niet worden gewijzigd of verwijderd. Wijzigingen zijn publiekelijk zichtbaar.
Macht bij de gebruikers. Gebruikers hebben controle over al hun informatie en transacties. Het beheer van de database is gezamenlijk.
Algoritmische logica. Softwarealgoritmen kunnen automatisch - snel en goedkoop - transacties triggeren

[2] Uit Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser, 2016.
[3] Block chain is een specifieke invulling van DLT. Voor deze analyse is het onderscheid maar beperkt relevant, en worden de twee begrippen veelal door elkaar gebruikt.

Vertrouwen als basis voor een succesvolle maatschappij

In zijn boek *Trust: The Social Virtues and the Creation of Prosperity* (1995), stelt Francis Fukuyama dat het vermogen om ander mensen te vertrouwen en op die basis met ze samen te werken (hij noemt dat 'sociaal kapitaal') de grondslag is voor economisch succes. Fukuyama schetst hoe in de loop van de geschiedenis 'intermediaire sociale organisaties' - gilden, vakbonden, vrijwilligersorganisaties – ontstonden, die als ruggengraat van een maatschappelijk weefsel van vertrouwen de ontwikkeling van moderne kapitalistische structuren mogelijk maakten. Hij merkt op dat een samenleving dit over lange tijd opgebouwde sociaal kapitaal in snel tempo kan spenderen. Vertrouwen moet dan steeds meer door zware legalistische constructies en controlemechanismen worden afgedwongen.

Dit eroderen van vertrouwen zien we om ons heen zien gebeuren, op allerlei niveaus. We zien een toename van geopolitieke rivaliteit. De samenwerking van landen binnen Europa en tussen Europa en de VS staat onder druk. In veel samenlevingen zien we de opkomst van protestpartijen, naast een groeiend leger van niet-stemmers die alle vertrouwen in 'de politiek' hebben verloren. Het jaarlijkse Edelman *Trust Barameter*-rapport, gebaseerd op een online enquête van 33.000+ respondenten in 28 landen, schildert een vrij somber beeld. De titel van het document, *An Implosion of Trust*, onderstreept dat.[4] Het vertrouwen in traditionele instellingen - overheden, bedrijven, NGO's en media - is in 2016, in een opgaande economie, gedaald tot een niveau vergelijkbaar met dat tijdens de financiële crisis van 2008/2009. 85% van de respondenten meent dat bovengenoemde instellingen hun belangen niet goed in het oog houden. In driekwart van de 28 onderzochte landen heeft de meerderheid geen vertrouwen in hun overheid.

Tegelijk zien we, als tegenbeweging, een steeds sterker verknoopte netwerkwereld ontstaan. Allerlei verbanden en samenwerkingsvormen worden 'van onderaf' gecreëerd, vaak gebruikmakend van sociale media. In het Internet der Dingen communiceren alledaagse objecten met personen en met andere objecten, en kunnen op grond hiervan autonome beslissingen nemen. Ook hier speelt vertrouwen in de gezonde beslissingen van anderen een grote rol; vertrouwen van mensen in autonome systemen, van autonome systemen in mensen en van het ene systeem in het andere. DLT kan dit vertrouwen expliciet maken.

Vertrouwen digitaal organiseren

DLT past in deze netwerkwereld die van nature gedistribueerd is. Personen en organisaties kunnen met behulp van DLT hun reputatie transparant maken en loskoppelen van het oordeel van specifieke partijen - met hun belangen en voorkeuren, menselijke of systeemfouten, ongelukken, hacking, besluiteloosheid en corruptie. Dit alles kan worden vervangen door vertrouwen in een gedeeld mechanisme dat toegankelijker, transparanter en veiliger is. DLT levert praktische oplossingen, maar heeft (daarmee) tevens de potentie om in meer fundamentele zin 'vertrouwen' als belangrijk fundament onder een goed functionerende samenleving te schragen. Zover zijn we echter nog lang niet. Er is nog helemaal geen sprake van een stabiel 'gedeeld mechanisme'. En de kennis van en het begrip over de betekenis en werking van DLT, zowel bij het grote publiek als bij veel van de partijen die er professioneel door geraakt zullen worden, is nog beperkt.

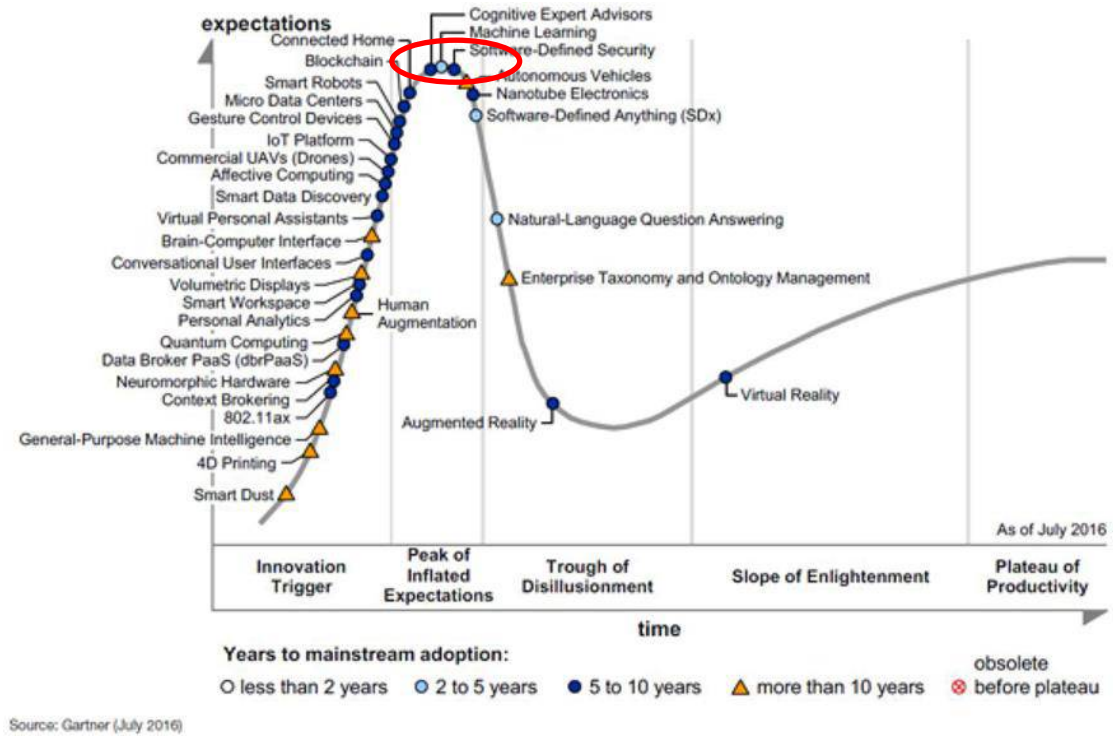
Dat neemt niet weg dat DLT wel degelijk grote potentie heeft. In deze notitie interpreteren we het begrip DLT in ruime zin. Het gaat niet alleen om de technologie om gedistribueerde digitale grootboeken bij te houden; maar ook om de systemen en tools voor identiteitsbeheer, authenticatie en autorisatie noodzakelijk voor regulering van de toegang tot de grootboeken; de eventuele toezichtstructuren; en de 'smart contract'-toepassingen (computeralgoritmes) om transacties automatisch uitvoerbaar te maken.

4 https://www.edelman.com/trust2017/

3. Technologische Stand van Zaken

Hype of hoop?

DLT is nog in een vroeg stadium van ontwikkeling. De technologie werd in 2008 uitgevonden specifiek om de digitale munt Bitcoin te creëren. In Gartners *hype cycle* staat blockchain hoog op wat de 'piek van opgezwollen verwachtingen' wordt genoemd, met het gevaar om spoedig terug te vallen in de 'vallei van desillusie'.



Figuur 1: Blockchain in de Gartner *hype cycle* 2016[5]

De hoge verwachtingen zien we terug in de markt, in een veelheid aan DLT-pilotprojecten. Tegelijk is het te vroeg om van een doorslaande succes te spreken. Niet alleen de algemene ervaring met nieuwe, (potentieel) disruptieve technologie belichaamd in de Gartner hype cycle noopt tot voorzichtigheid. Ook de praktijk is weerbarstig. Het bekendste toepassingsgebied van block chain betreft digitale valuta's zoals Bitcoin. Deze kennen wereldwijd inmiddels een aardige marktkapitalisatie (tientallen miljarden dollars, afhankelijk van sterk fluctuerende wisselkoersen, zie https://coinmarketcap.com/). Tegelijk zien we dat ze vooral gebruikt worden voor criminele transacties en speculatie.

In maart 2015 lanceerde de *Global Agenda Council on the Future of Software & Society* de *Technological Tipping Points Survey*. In deze enquête werd ruim 800 leidinggevenden en deskundigen uit de ICT-sector gevraagd naar hun mening over 21 omslagpunten – het moment waarop een specifieke technologische verschuiving grootschalig zichtbaar zou worden in de maatschappij. De respondenten konden bijvoorbeeld aangeven 'dat is al gebeurd', '20+ jaar' of 'nooit'. Twee omslagpunten hadden betrekking op DLT:
De eerste keer dat een regering belasting heft met behulp van blockchain technologie; en

5 http://www.gartner.com/newsroom/id/3412017

10% van het wereldwijde bruto binnenlands product wordt opgeslagen op block chain technologie. 73,1% van de respondenten gaf aan dat het eerste vóór 2025 het geval zou zijn; 57,9% vond dat voor het tweede. De verwachting, kortom, is dat DLT *mainstream* gaat worden, maar dat daar nog wel enkele jaren overheen zal gaan.

Figuur 2: Een goed denkbaar adoptiepad[6]

Werking en terminologie

Merk op dat de terminologie in dit nieuwe veld aan verandering onderhevig is en er nog nauwelijks algemeen aanvaarde definities bestaan. De Engelse termen worden veelal ook in het Nederlands gebruikt.

Een **distributed ledger** (gedistribueerd grootboek) is een type database die verspreid is over meerdere sites, landen of instellingen en gebruikt wordt om activa (zaken van waarde, zoals geld of vastgoed) en transacties (overdracht van eigendom) daarin te registreren. Wijzigingen in de database worden in enkele minuten of uren verwerkt in alle kopieën. Deze database kan openbaar (**public**) of in meer of mindere mate besloten (**private**) zijn. Een distributed ledger vereist een expliciete organisatie van vertrouwen in de - soms benoemde en afgebakende, soms onbekende en onbegrensde - reeks van partijen die het grootboek beheren en valideren. Dit is anders dan voor een traditioneel enkelvoudig grootboek, waarin dat vertrouwen intrinsiek is belegd bij de specifieke organisatie die het grootboek bezit en beheert.

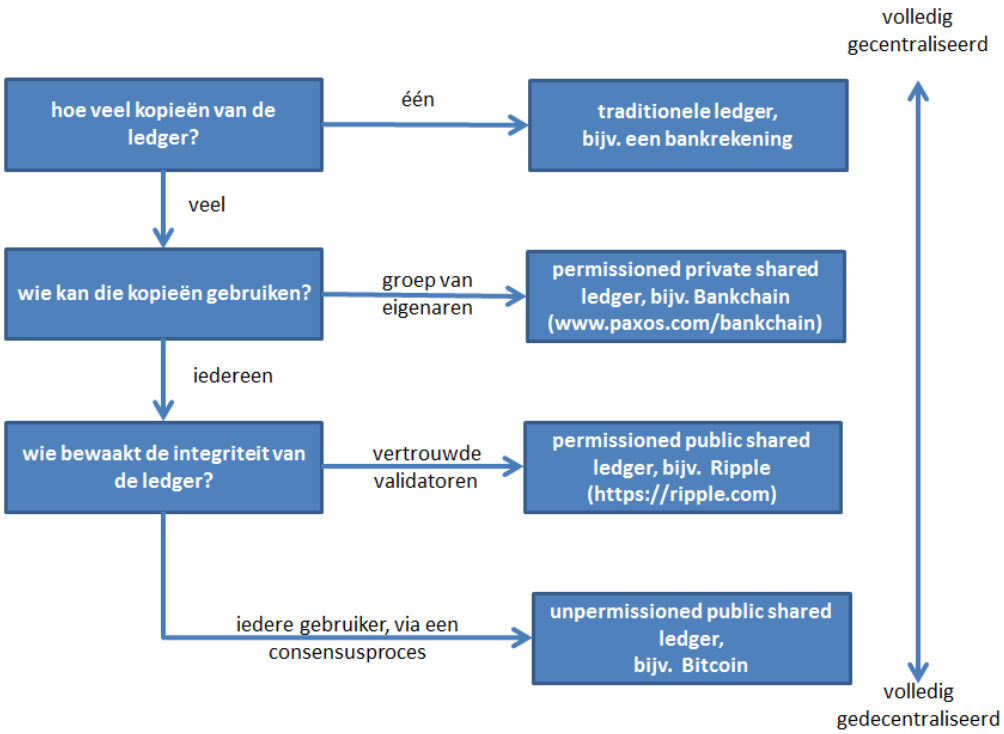
Er zijn veel vormen van distributed ledgers, waarbij zowel de structuur van de database als het proces van toevoegen en goedkeuren van transacties varieert. Een **block chain** (of blockchain) is een van die vormen. De echte nieuwigheid is dat de database regels over een aan de database toe te voegen transactie kan vaststellen (de zogeheten **business logic**), gekoppeld aan de transactie zelf. Dit in tegenstelling tot conventionele databases, waarbij regels voor de gehele database gelden

[6] Accenture, Blockchain Technology: Preparing for Change, 2015.

of gekoppeld zijn aan een applicatie die op de database werkt, maar niet per transactie kunnen worden ingesteld.

Het **valideren** van toe te voegen transacties door gebruikers met de juiste permissies staat bekend onder de algemene term **consensus.** Geen enkele partij kan voorkomen dat een transactie wordt toegevoegd aan het grootboek als het consensusproces daartoe besluit (bijvoorbeeld als er een quorum wordt bereikt). Als het consensusproces voor iedereen openstaat, is er sprake van een **unpermissioned (of permissionless) ledger**. Deze heeft tot doel iedereen in staat te stellen gegevens te leveren aan het grootboek en een eigen identieke kopie te hebben. Een unpermissioned ledger kan ook de vorm hebben van een overal geldend document dat niet kan worden bewerkt, bijvoorbeeld een testament of een eigendomsbewijs.
In een unpermissioned ledger neemt het consensusproces tijd in beslag.[7] Gedurende een bepaalde periode - zeg een tot twee uur - zijn transacties niet volledig geverifieerd. Na deze periode wordt er van uitgegaan dat de transacties voldoende 'diep' zijn ingedaald in de gedistribueerde database om als vaststaand te kunnen worden beschouwd.

Als deelnemers in het consensusproces zijn voorgeselecteerd, spreken we over een **permissioned ledger.** De gemeenschappelijkheid kan dan veel eenvoudiger worden gehandhaafd dan voor unpermissioned ledgers. Het wereldwijde financiële transactiesysteem Ripple, bijvoorbeeld, gebruikt een lijst van *Unique Node Validators* van maximaal 200 bekende, onbekende of gedeeltelijk bekende partijen waarvan men kan aannemen dat de kans dat ze samenspannen om de zaak te bedriegen zeer klein is. Permissioned ledgers zijn zeer goed verifieerbaar omdat het consensusproces een digitale handtekening creëert die door alle partijen kan worden gezien.



Figuur 3: Verschillende typen distributed ledger

[7] Deze vertraging is een belangrijk obstakel voor het gebruik van Bitcoin-achtige systemen voor snelle transacties, zoals financiële handel.

Een van de eerste beslissingen bij het opzetten van een distributed ledger betreft de netwerkarchitectuur van het systeem. Gebruikers bereiken consensus over hun grootboek, de lijst van geverifieerde transacties, via communicatie en communicatie is nodig om nieuwe transacties te schrijven en goed te keuren. Deze communicatie vindt plaats tussen nodes (knooppunten), die elk een kopie van het grootboek bevatten en de andere knooppunten informeren over nieuwe informatie: nieuw ingediende of nieuw geverifieerde transacties. Private ledger operators kunnen bepalen wie een node mag voeren en hoe deze nodes verbonden zijn. Een node met meer verbindingen zal sneller informatie ontvangen. Evenzo moeten nodes een minimum aantal verbindingen handhaven om als actief te worden beschouwd. Een node die de overdracht van informatie beperkt of verkeerde informatie verstuurt, moet kunnen worden herkend en uitgesloten om de integriteit van het systeem te handhaven.

Nauw verbonden met DLT is het vraagstuk van identiteitsmanagement. In essentie is vertrouwen een risicobeoordeling tussen twee of meer partijen. In cyberspace is vertrouwen gebaseerd op twee belangrijke eisen: bewijs me dat je bent wie je zegt dat je bent (authenticatie); en bewijst me dat je de machtiging hebt die nodig is om te doen wat je vraagt (autorisatie). In ruil daarvoor zal ik je aantonen dat ik betrouwbaar ben door op een veilige, efficiënte en betrouwbare manier diensten of producten aan je te leveren. Authenticatie en **identificatie** zijn onderling verbonden, maar zijn niet hetzelfde. Authenticatie vereist niet dat ik je identiteit ken, maar vereist dat je me een merkteken geeft dat onlosmakelijk verbonden is met je identiteit, bijvoorbeeld een nummer van een creditcard of bankpas, of een vingerafdruk gekoppeld aan een biometrisch paspoort. Omgekeerd, als ik mijn merkteken aan iemand verstrek, wil ik zeker weten dat ik dat aan de juiste persoon of organisatie doe. Het is net zo belangrijk dat organisaties hun gebruikers kunnen authentiseren als omgekeerd.
De digitale omgeving biedt de mogelijkheid voor het creëren van krachtige en robuuste systemen en tools voor authenticatie, autorisatie en identiteitsbeheer, terwijl tegelijk de privacy wordt beschermd. Een voorbeeld van een dergelijk systeem is de *public key infrastructure* (PKI). Een andere voorbeeld is het *Register of Legal Organizations* (ROLO), een internationale norm voor authenticatie van organisaties - in tegenstelling tot individuen - die wordt ontwikkeld. In ROLO leggen organisaties vast wat elke medewerker kan en mag in interactie met andere organisaties. Zo wordt de veiligheid en de betrouwbaarheid van organisaties en/in productieketens gewaarborgd. Bij Airbus en de ontwikkeling van de JSF wordt al zo gewerkt. Zo kan achteraf precies worden uitgezocht wie wanneer welk schroefje van welke leverancier heeft aangedraaid.

Een volgende stap is digitaal vast te leggen wat partijen met elkaar afspreken. In een **smart contract** (slim contract) zijn de voorwaarden en bepalingen die te maken hebben met waarde- en eigendomsoverdracht in computertaal in plaats van in juridische taal opgenomen. Slimme contracten kunnen automatisch worden uitgevoerd door geschikte distributed ledger-systemen. Een slim contract kent lage kosten voor afsluiting, controle en handhaving. Daarmee wordt het economisch haalbaar om ook voor transacties met relatief lage waarde contracten te sluiten. Risico's zijn gelegen in het vertrouwen dat men stelt in (de opsteller van) de contractcode en in het computersysteem dat het contract uitvoert. In dit stadium zijn de risico's en voordelen nog grotendeels theoretisch omdat de technologie nog in de kinderschoenen staat.

Bitcoin is een online equivalent van contant geld. Maar cash transacties worden niet standaard vastgelegd en er is een probleem met vervalsingen. Bij Bitcoin zorgt het grootboek van transacties - een unpermissioned distributed ledger - voor hun authenticiteit. Net als voor cash moeten Bitcoins in een (virtuele) portemonnee worden opgeslagen. Als deze niet goed in de gaten gehouden wordt, kunnen ook Bitcoins worden gestolen. Een fundamenteel verschil tussen conventionele valuta's en

Bitcoins is dat de eerste uitgegeven worden door centrale banken, en de laatste door de wereldwijde samenwerking die Bitcoin is.

Ontwikkelagenda

Op diverse gebieden is verdere ontwikkeling noodzakelijk voordat het volledige potentieel van DLT en verwante technologieën gerealiseerd kan worden. Stuk voor stuk lijkt dat goed te doen; de grootste uitdaging is de onderlinge afhankelijkheid. Dit houdt in dat diverse ontwikkelingen samen moeten komen voordat grootschalige uitrol van DLT-toepassingen mogelijk is.

Technologie

Het oplossen van uitdagingen zoals transactiesnelheid, het verificatieproces en datalimieten zijn van cruciaal belang om DLT breed toepasbaar te maken. Zo vereist het bijhouden van een volledige transactiegeschiedenis veel geheugen en het consensusproces soms veel rekenkracht. Een specifiek voorbeeld van dit laatste is het 'minen' van Bitcoins. De mijnwerkers van het Bitcoin-netwerk rekenen 450 duizend biljoen oplossingen per seconde door om transacties te valideren en daarmee nieuwe Bitcoins te verdienen. Het benodigde computervermogen slurpt energie.

Interoperabiliteit

Om de kracht van DLT te maximaliseren, moeten grootboeken onderling interoperabel zijn, onder meer door gestandaardiseerde of tenminste compatibele vormen van authenticatie. Dit vereist afspraken over interoperabiliteit van gegevens, van beleid en van de effectieve uitvoering van internationale normen.

Operationele toepassingen

Er zijn allerlei praktische vragen op te lossen. Hoe worden de activa overgedragen tussen traditionele grootboeken en distributed ledgers? Is een slim contract in staat om alle gebeurtenissen en functies die zich gedurende de levenscyclus van een activa voortdoen te verwerken? Wat gebeurt er als nieuwe parameters contracten potentieel beïnvloeden? Hoe kunnen steeds grotere grootboeken kosteneffectief worden opgeslagen?
Een andere uitdaging is een gebruik van smartphones, als het de facto vertrouwde gebruiksapparaat voor een groot deel van de wereldbevolking, als middel om veilige geauthentiseerde interacties te plegen. Hier zijn al voorzieningen voor beschikbaar. De nieuwste smartphones bevatten belangrijke beveiligingsfuncties, zoals een Trusted Platform Module, die digitale certificaten en cryptografische sleutels beveiligt; en een Trusted Execution Environment en Trusted User Interface, gewapend tegen malware.

Beheer en regulering

Beheer (governance) omvat de regels die zijn vastgesteld door de eigenaars van en deelnemers aan een digitaal grootboek om hun privébelangen beschermen; aangevuld met wet- en regelgeving vastgesteld door een of meerdere onafhankelijke autoriteiten om de bredere belangen van de maatschappij, nationaal en/of internationaal, te beschermen. In het algemeen zal de overheid dit bredere kader creëren en een toezichthoudende partij benoemen, alleen of in samenwerking met andere overheden.
Er zijn derhalve twee sets van regels die de werking van DLT-toepassingen inkaderen: de klassieke regels vastgesteld door de wet- en regelgever; en de technische regels die de werking van de in software gecodeerde algoritmen bepalen. Er moet minstens zoveel aandacht zijn voor goede technische regels en de naleving ervan als voor het wettelijke kader. De uitdaging is evenwicht te vinden tussen de belangen van de deelnemers aan het systeem, de bredere belangen van de samenleving en de weerbaarheid van het systeem tegen systeemrisico's of criminele activiteiten;

terwijl tegelijkertijd een te strak regelgevend kader dat innovatie remt vermeden moet worden. De interactie tussen de wettelijke en technische kaders biedt ook nieuwe mogelijkheden. Technische regels kunnen worden gebruikt om de naleving van wettelijke regels te waarborgen, en daarmee de kosten van naleving verminderen. Het bepalen van het optimale evenwicht tussen beheer en regulering, en tussen wettelijke en technische regels, vereist ongebruikelijke vaardigheden, waaronder de samenwerking tussen advocaten, wiskundigen en computerdeskundigen om veel van de belangrijkste problemen op te lossen.

In dit krachtenspel zijn er nog veel onbeantwoorde vragen die ontwikkelingen kunnen remmen. Wanneer zullen regelgevende instanties een toelichting geven over acceptable & best practices voor het gebruik van gedistribueerde grootboeken? Hoe behandelen de autoriteiten geautomatiseerde contracten en digitale activa die worden overgedragen via DLT? Zal de wetgever traditionele en DLT-transacties anders behandelen? Hoe kan het wettelijk kader accommoderen voor zowel slimme als traditionele contracten? Hoe zal DLT eisen voor financiële rapportage beïnvloeden; voldoet bijvoorbeeld een transactiegeschiedenis van een gedistribueerd grootboek voor verantwoordingsdoeleinden? Kan eigendom van financiële activa met zekerheid en finaliteit worden overgedragen? Moeten tegenpartijen identificeerbaar zijn en gekoppeld zijn aan een rechtspersoon? (Wanneer) komt er een einde aan de onzekerheid over de wettelijke status van cryptovaluta als Bitcoin?

Controle, beveiliging en privacy

Ondanks dat er diverse effectieve oplossingen bestaan, zijn er nog steeds problemen met betrekking tot cybersecurity die moeten worden aangepakt voordat het grote publiek hun persoonlijke gegevens zal vrijgeven in DLT-toepassingen.

Integratie en transitie

DLT-toepassingen vereisen significante veranderingen aan of vervanging van bestaande systemen. Naast de technische uitdaging, kunnen ook de hoge investeringskosten in de aanloop naar wijdverbreide toepassing van DLT een belangrijke drempel vormen. Tenslotte, minstens zo belangrijk, is er het benodigde culturele aanpassingsproces. DLT betekent een verschuiving naar een gedecentraliseerde werkwijze dat adaptatie van leveranciers en gebruikers vereist. Voor organisaties en overheden betekent dit dat een zorgvuldig transitiepad moet worden ontwikkeld. Dat kan niet in isolatie. DLT-toepassingen functioneren altijd in een netwerk, dus samenwerking is onontkoombaar.

Acceptatie

Accpetatie als basisvoorwaarde voor grootschalige uitrol is geen vanzelfsprekendheid. Een eerste moeilijkheid is de sterke associatie van de technologie met Bitcoin. Bitcoin heeft voor veel burgers, overheden en beleidsmakers de associatie met criminele transacties en het dark web. Tegelijk zijn digitale valuta's zoals Bitcoin van belang voor centrale banken en ministeries van financiën over de hele wereld die ze met grote belangstelling bestuderen vanwege hun efficiëntie en de transparantie van transacties. De associatie met een duistere parallelwereld moet echter verdwijnen wil de technologie echt postvatten.

Een tweede communicatieprobleem is de verwarrende reeks termen. De term 'distributed', bijvoorbeeld, kan leiden tot de misvatting dat, omdat er iets wordt verdeeld, er dus geen algemene controleautoriteit of eigenaar is. Dit kan wel of niet het geval zijn: er is een breed spectrum van distributed ledger-modellen, met verschillende graden van centralisatie en verschillende soorten toegangscontrole, die passen bij de verschillende zakelijke behoeften (zie Figuur 3). De kernboodschap is dat door de technologie volledig te begrijpen, de overheid en de particuliere sector

dát ontwerp kunnen kiezen dat het beste past bij een bepaald doel, waarbij veiligheid en (centrale) controle in balans kan worden gebracht met het gemak, de lage kosten en de transparantie van DLT.

De noodzaak van experimenteren

Concept Development & Experimentation (CD&E) is onontkoombaar. Men moet vertrouwd raken met de technologie: hoe werkt het, wat kunnen we ermee en welke valkuilen en beperkingen zijn er? Omdat DLT een generieke technologie is, niet specifiek ontwikkeld voor een bepaald toepassingsgebied, moet er gekeken worden of dit beperkingen oplevert en hoe een specifieke invulling aan de technologie kan worden gegeven.

CD&E begin vaak met een proof of concept - experimenten om te bewijzen dat de technologie werkt. Al snel moeten ook de gebruikers worden betrokken: dekt het een (eventueel latente) behoefte, werkt het in de praktijk? Juist vanwege het gemeenschappelijke karakter van de technologie wordt het al snel complex. Bij elke oplossing moet rekening worden gehouden met aspecten als prestaties, schaalbaarheid, wet- en regelgeving, privacybescherming en vertrouwelijkheid. Samenwerking tussen partners is extreem belangrijk.

De ervaring leert dat laboratoriumsituaties of zelfs ‘live’ pilotprojecten wel in staat stelt de meer voor de hand liggende veiligheidsproblemen in nieuwe ICT-toepassingen te ontdekken en te corrigeren, maar dat de noodzakelijke inkadering juist de ‘unknown unknowns’ buitensluit. Veel veiligheidslekken treden pas op tijdens daadwerkelijk gebruik en niet in experimenten, hoe uitgebreid ook. Wel is het goed mogelijk dat experimenteren de (mentale) flexibiliteit verhoogt om sneller fouten te her- én erkennen, en naar een oplossingsmodus om te schakelen.

De overheid moet overwegen hoe regelgeving kan bijdragen aan een omgeving waarin nieuwe operationele DLT-toepassingen goed kunnen worden onderzocht teneinde overheden en bedrijven in staat te stellen om te experimenteren, zowel in gecontroleerde omgevingen als in de feitelijke praktijk, waarbij niet kan worden gewacht op 'perfecte' oplossingen.

4. Implicaties voor de Samenleving

Bestaande toepassingen beter en goedkoper regelen

Grootboeken zijn sinds de oudheid gebruikt om zaken van waarde en het bezit daarvan vast te leggen. Dit gebeurde in de oudheid op kleitabletten, later op papier en sinds enkele decennia in computersystemen. Deze laatste stap was niet veel anders dan de overgang van papier naar bytes. De echte innovatie gaat nu pas plaatsvinden, waarbij algoritmen het mogelijk maken om distributed ledgers te creëren met eigenschappen en mogelijkheden die veel verder gaan dan wat traditionele grootboeken konden bieden. Ze kunnen overheden helpen om belastingen te verzamelen, afdrachten te regelen, paspoorten uit te geven, vluchtelingen te identificeren8 en in algemene zin de integriteit van overheidsdiensten te waarborgen. In de gezondheidszorg kunnen patiëntendossiers veilig en beter worden bijgehouden en gedeeld. Het Internet der Dingen zal mede geschraagd worden door DLT, ingezet voor het waarborgen van de integriteit van de tussen objecten, organisaties en personen uit te wisselen data. Feitelijk is er geen sector waar DLT niet kan worden ingezet.

Diverse overheden zijn reeds begonnen DLT toe te passen. De Estse regering experimenteert al een aantal jaren met een vorm van DLT, bekend als de Keyless Signature Infrastructure (KSI). KSI stelt burgers in staat om de integriteit van hun dossiers in overheidsdatabases te verifiëren. Het (b)lijkt ook voor insiders onmogelijk om illegale handelingen in dergelijke overheidsdiensten uit te voeren. Dit vermogen om de burgers te verzekeren dat hun gegevens veilig en accuraat blijven, heeft Estland geholpen om allerlei digitale diensten te starten, zoals een e-Business Register en een e-Tax. Deze verminderen de administratieve lasten voor staat en burger.

Ook het bedrijfsleven ziet de grote mogelijkheden. DLT biedt aanzienlijke operationele kostenvoordelen. Niet alleen is de toepassing van nature kosteneffectief, ook duplicatie en inefficiënties in controle en coördinatie kunnen worden vermeden. De mogelijkheid om informatie over vrijwel alle activa te digitaliseren en veilig te bewaren, van rijstzakken via diamanten9 tot intellectuele eigendom, stelt organisaties in staat hun eigendom te verifiëren en de status ervan veel goedkoper te volgen.

Block chain zet vaart achter containertransport in de Rotterdamse haven[10]
Van de 40 dagen dat containers onderweg zijn van Midden-China naar Midden-Europa staan ze ongeveer 16 dagen stil. De papierwinkel voor registratie en controle speelt hierbij een rol, maar het komt vooral doordat partijen niet real-time informatie delen. Als een schip een half uur eerder of later de haven binnenkomt, kan de vrachtwagenchauffeur zijn eigen proces dus niet aanpassen. Bij een transport zijn zeker 20 tot 25 partijen betrokken: verzender, douane, havenautoriteiten, stuwadoor, vracht- en wegvervoerder, ontvanger, bank etc. Die partijen doen niet alleen zaken met Rotterdam, maar ook met andere havens. Daarom wil men toe naar een open omgeving. Havens delen al informatie via het Port Community System, maar met block chain kan de efficiency worden verbeterd en de kosten omlaag gebracht. Naast juridische en IT-kwesties is vooral de schaalbaarheid een uitdaging. Het validatieproces van block chains houdt in dat de meerderheid van de betrokkenen die transactie goedkeuren. Dit kunnen dat op termijn wel duizenden partijen

[8] Accenture werkt samen met Microsoft aan de ontwikkeling van een digitaal netwerk voor de identificatie van vluchtelingen en anderen die geen officiële identiteitspapieren hebben, gebaseerd op blockchaintechnologie; https://tweakers.net/nieuws/126127/accenture-maakt-netwerk-met-blockchain-voor-identificatie-van-vluchtelingen.html
[9] Het bedrijf Everledger levert een grootboek dat de identiteit van diamanten verzekert, van het mijnen via het slijpen tot het verkopen en verzekeren. Zo kan fraude worden verminderd en voorkomen dat bloeddiamanten op de markt komen.
[10] https://time.tno.nl/nl/artikelen/blockchain-zet-extra-vaart-achter-containertransport-in-rotterdamse-haven/

zijn. Er moeten dus manieren worden gevonden om heel frequent afspraken met elkaar te borgen. Block chain levert iedereen voordeel op: partijen helpen elkaar om het proces te verbeteren. Dit in tegenstelling tot bijvoorbeeld e-commercebedrijven en sociale netwerksites die veel data naar zich toetrekken, zichzelf eigenaar van die data maken en daardoor nog winstgevender worden.

Nieuwe toepassingen dankzij grotere inclusiviteit

DLT-toepassingen, en specifiek de meer open en gedecentraliseerde vormen hiervan, bevorderen een gelijk speelveld. Transacties worden overal op dezelfde manier en op dezelfde tijd goedgekeurd, ongeacht waar ze in de wereld werden uitgegeven. Besturing vindt plaats door een consensusproces dat alle deelnemers even verantwoordelijk en gelijkwaardig maakt.

DLT biedt grote kansen voor de 2,5 miljard mensen wereldwijd die momenteel geen toegang hebben tot het financiële systeem. Zij hebben geen controleerbare financiële historie, en kunnen geen lening krijgen of contract afsluiten om een bedrijf te starten. Met een identiteit en reputatie op basis van DLT zijn geen gecentraliseerde diensten nodig om deze functies te verzorgen. Een donor in Nederland kan, op basis van een goede financiële reputatie vastgelegd in een publieke ledger, simpel een kleine bedrijfslening geven aan een persoon in Burkina Faso die hij nog nooit eerder heeft ontmoet. Een ander praktisch voorbeeld is dat DLT relatief simpel landeigendom kan vastleggen in landen zonder goed kadaster. In Bangladesh wordt landeigendom nog grotendeels vastgelegd met papieren versies van akten en kaarten. Vele daarvan zijn zo oud dat ze nauwelijks nog leesbaar zijn. Het kan na de aankoop van land jaren duren voordat iemand het eigendomsbewijs krijgt. De meeste rechtszaken in Bangladesh gaan over conflicten over land. Mensen verlaten mensen bij overstromingen hun land niet omdat ze bang zijn het na terugkomst niet meer te kunnen claimen. Een relatief simpel en goedkoop DLT-systeem zou dat kunnen voorkomen.

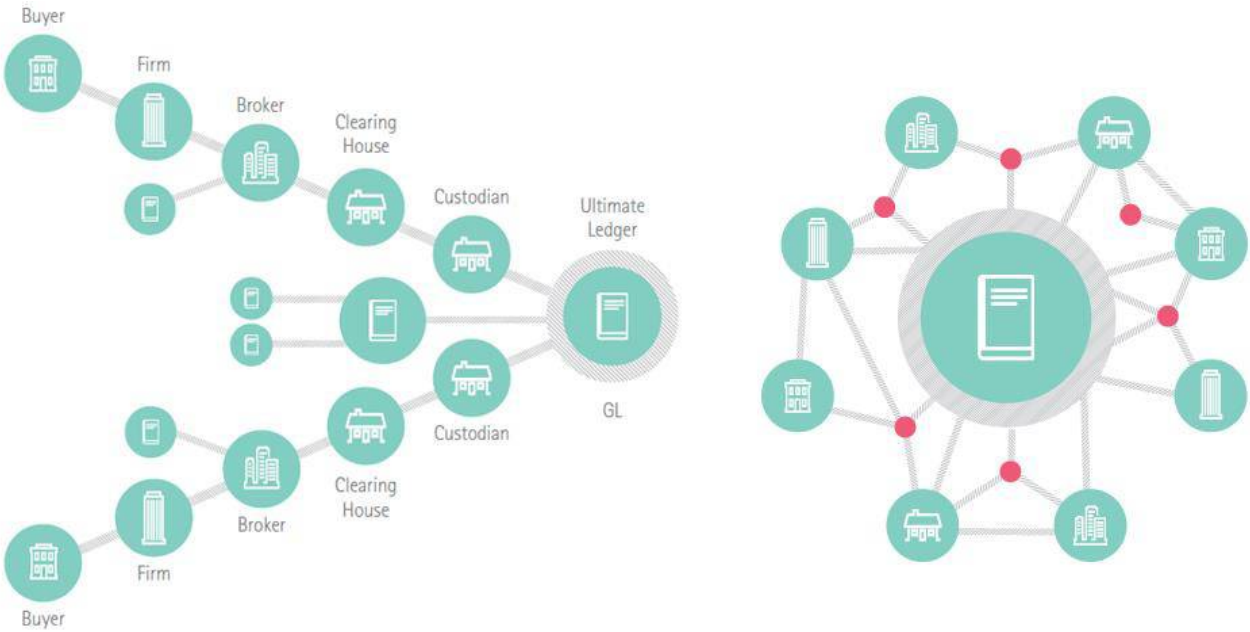
Het is te verwachten dat, naarmate de technologie vertrouwder wordt en goedkoop op de particuliere markt beschikbaar komt, veel meer (materiële en niet-materiële) zaken die waarde vertegenwoordigen in de vorm van digitale ledgers worden vastgelegd.

Verdwijnen van tussenlagen

DLT is een platformtechnologie. Ver(der)gaande toepassing ervan draagt bij aan de transformationele kracht van platformtechnologieën in het algemeen. Kort gezegd maken dergelijke technologieën allerlei tussenlagen overbodig door leveranciers en kopers of gebruikers van een product of dienst direct met elkaar te verbinden, een proces dat ‘disintermediatie’ wordt genoemd. DLT maakt veel financiële tussenpersonen overbodig, zoals banken, notarissen en accountants – althans in hun huidige vorm. Maar ook tussenhandelaren in de energiesector of gezondheidszorg bijvoorbeeld, en zelfs ‘nieuwe economie’-bedrijven als Uber en AirBnB zullen worden geraakt. De meeste toeleveringsketens kunnen veel efficiënter ingericht worden.

Ethereum (https://www.ethereum.org/) is een gedistribueerd platform op basis van block chain dat ‘slimme contract’-functionaliteit biedt. Deze technologie maakt efficiënte en veilige transacties mogelijk zonder gecentraliseerde bemiddeling. Zodra de condities zijn overeengekomen en beide activa - bijvoorbeeld een product en de betaling ervan - klaarstaan, worden zij voorzien van een uniek merkteken en uitgewisseld. Een contract dat traditioneel een bedrijf veel geld voor juristen, tussenpersonen etc. zou hebben gekost, kan nu bijvoorbeeld worden vastgelegd in minder dan 100 regels smart contract (pseudo) code. Voorlopig zijn advocaten, accountants en toezichthouders nog nodig (naast programmeurs) om slimme contracten te ontwikkelen en te faciliteren. Maar het is zeker dat dit proces verder zal worden geautomatiseerd, tussenpersonen zullen verdwijnen en de kosten van contractueel vastgelegd vertrouwen sterk zal afnemen.

Een vergaand gebruik van DLT-toepassingen leidt tot het verdwijnen van veel bestaande banen en het ontstaan van nieuwe banen (maar wellicht minder), en zo tot een andere verdeling van welvaart - met alle maatschappelijke gevolgen (en onrust) van dien. Sociale ontwrichting ligt hierbij op de loer. Dergelijke transformatieprocessen kunnen zeer wel de politieke en maatschappelijke stabiliteit ondergraven, zelfs als DTL tegelijkertijd op macroniveau tot een grotere welvaart en eventueel tot een rechtvaardiger verdeling ervan en een efficiëntere en transparantere overheid (zie hieronder) kan leiden.



Figuur 4: Kapitaalmarkten in 2017 en in 2025[11]

De positie van bestaande instituties staat op de tocht

Door de decentraliserende werking van DLT komt de overheid, althans in zijn huidige functioneren, onder druk te staan. Veel van de overheids*functies* blijven relevant, zoals het innen van belastingen (inclusief het verminderen van belastingfraude), het uitgeven van paspoorten, het beschermen van kritische infrastructuur tegen cyberaanvallen, het organiseren van verkiezingen, het uitvoeren van programma's voor sociale zekerheid en het garanderen van de veiligheid van de burger. Tegelijk is het de vraag of de huidige *organisatie* in grote, gecentraliseerde en bureaucratische overheidsdiensten nog de beste vorm is om deze deze functies uit te voeren. Vanuit DLT-perspectief is het antwoord duidelijk: nee, dergelijke overheidsfuncties kunnen effectiever, goedkoper, klantvriendelijker en controleerbaarder worden georganiseerd in een meer decentrale en open vorm.

Maar ook veel bedrijven die nu een schatkamer aan big data over de voorkeuren en gedragingen van consumenten bezitten - de grote 'winnaars' van de afgelopen jaren zoals Google/Alphabet, Facebook, AirBnB, Amazon - kunnen hard worden geraakt als DLT hun data-monopolies aantast. In hun boek *Blockchain Revolution. How the Technology Behind Bitcoin Is Changing Money, Business, And The World* (2016), beschrijven Don en Alex Tapscott hoe individuen weer zelf controle krijgen over hun virtuele persoonlijkheid – een persoonlijkheid die nu in stukjes en beetjes is opgeslagen in allerlei databases van overheden en bedrijven, in de profielen op Facebook en LinkedIn etc.

[11] Accenture, Blockchain Technology: Preparing for Change, 2015.

"Blockchain can enable every person to have a unique and verifiable reputation-based identity that allows them to participate equally in the economy. The implications of this equality are profound." Idealisten zien in DLT een instrument voor een eerlijkere verdeling van welvaart, voor een transparantere en beter aanspreekbare overheid en voor een revitalisering van de democratie: "officials could be elected with a smart contract that specifies what they will do when elected, and that they won't get paid unless they do what the electorate demanded rather than what their funders demanded."

Het concept van 'waarde' verschuift

In een wereld waar kennis, informatie, netwerken en toegang de belangrijkste waarden vertegenwoordigen, kan de grootste conceptuele impact van een wijdverbreide toepassing van DLT liggen in de wijze waarop het concept van (economische) waarde en rijkdom in het algemeen wordt gemeten - en beleefd. Rijkdom kan in de toekomst worden gebaseerd op het potentieel om middelen te *activeren*, in plaats van op het eigendom van die middelen. DTL is hierbij een cruciale technologie die in staat stelt om snel en in detail te zien welke middelen beschikbaar zijn en wat hun toestand is en om eigenaar / beheerder en (tijdelijk) gebruiker te matchen. Of dit een positieve ontwikkeling is of niet, hangt af van hoe hij door de overheid, het bedrijfsleven en de maatschappij in zijn geheel wordt gemanaged.

Game Changer?

De disruptieve werking van DLT reikt in potentie veel verder dan de bedrijfssectoren en diensten die zij rechtstreeks kan innoveren. De meeste economische en sociale interacties in onze maatschappij zijn gebaseerd op vertrouwen. DLT biedt een krachtige vorm om dit vertrouwen digitaal te codificeren. De bedenkers van de technologie hadden daarbij een extreme mate van transparantie en inclusiviteit voor ogen. In de praktijk kan DLT ook allerlei meer gesloten en exclusieve vormen aannemen, hetgeen deze transparantie deels ondermijnt. Het lijkt erop dat naarmate DLT-applicaties meer gesloten zullen zijn, de disruptieve werking ook beperkter is, omdat ze dan eerder een kosteneffectieve vervanging voor bestaande toepassingen vormen dan echt anders georganiseerde alternatieven.

DLT, in welke vorm dan ook, biedt grote mogelijkheden niet alleen voor het codificeren van vertrouwen, maar tevens voor de vergaande automatisering van 'vertrouwde' interacties. Een validatieproces waarbij de deelnemende gebruikers geen personen of instanties zijn, maar 'dingen'. Objecten in het Internet der Dingen die onderling bestellingen en betalingen verrichten bijvoorbeeld. Met name in het faciliteren van dergelijk autonoom gedrag ligt de grootste disruptieve kracht van DLT. Waarbij tevens de vraag opdoemt wat een van de grote voordelen van DLT, transparantie, nog waard is.

5. *So What* voor de veiligheid

Blockchain intrinsiek veilig?

Betekent de transparantie en controle die blockchain / DLT zijn gebruikers biedt, in combinatie met de robuustheid verbonden aan de decentrale opzet, dat DLT-toepassingen intrinsiek veel veiliger zijn dan de systemen die ze vervangen? In theorie en tot op zekere hoogte in de praktijk is dat inderdaad het geval. Er zullen minder *single points of failure* zijn. Bepaalde vormen van fraude zijn veel moeilijker te plegen.

Tegelijk blijven andere vormen van manipulatie bestaan en dienen zich ook nieuwe vormen aan. Toepassingen voor het vastleggen en overdragen van waarde en eigendom vormen vaak een keten. DLT in enge zin richt zich vooral op het verbeteren en efficiënter maken van wat vaak al het veiligste deel van de keten is, namelijk het deel dat nu door banken, verzekeringsmaatschappijen, kadasters e.d. wordt afgedekt: professionele partijen met redelijk tot goed beveiligde (zij het niet fail safe) systemen. Het gaat echter veel vaker fout aan de 'randen' van dergelijke systemen, bij onoplettende gebruikers of in de interfaces tussen de verschillende systemen. DLT kan ook daar wellicht iets betekenen, bijvoorbeeld omdat het aantal 'randen' vermindert en de overblijvende 'randen' transparanter zijn. Maar of dat echt helpt is niet op voorhand evident.

Hieronder gaan we nader in op de consequenties voor veiligheid van DLT. We kijken eerst naar de technologie zelf en de toepassingen waarin de technologie een belangrijke rol speelt; en vervolgens naar de mogelijke veiligheidsimpact van een wijdverbreide gebruik van DLT-toepassingen als maatschappelijke *game changer*.

Publieke versus private vormen van blockchain

Als we de veiligheid van de technologie op zich beschouwen, is het onderscheid tussen de publieke vorm van DLT-toepassingen en de verschillende gradaties van (meer) private vormen van belang.

Bitcoin is bij uitstek een publieke vorm van DLT. Omdat iedereen volkomen anoniem Bitcoin-transacties kan lezen en schrijven, is Bitcoin momenteel vooral verbonden met handel op de zwarte markt. Het neemt dan de rol over van cash, dat ook anoniem van eigenaar kan wisselen; maar dan in een veel hanteerbaardere vorm.[12] Maar ook als Bitcoin vooral voor legitieme doeleinden gebruikt zou worden, leidt het systeem tot onverwachte veiligheidsuitdagingen. Omdat het consensusprotocol van Bitcoin - het 'minen' - veel computerkracht en daarmee energie verbruikt, werken de meeste Bitcoin-miners in landen met goedkope elektriciteit. Dit leidt tot netwerkcentralisatie en biedt grotere gelegenheid aan gebruikers om door geheime samenwerking (wat in het jargon '*collusion*' heet) consensus te bereiken over voor hun winstgevende, maar voor het systeem als geheel ongewenste, transacties.

Dergelijke problemen hebben geleid tot een toenemende interesse in vormen van block chain waarin het aantal gebruikers en hun rechten in meer of mindere mate zijn ingeperkt, en sprake kan zijn van één of een klein aantal toezichthoudende partijen. Private distributed ledgers bieden controle over wie het grootboek van geverifieerde transacties kan lezen, wie transacties kan indienen en wie deze kan verifiëren. De toekomst voor DLT ligt eerder hier dan in de radicaal publieke toepassingen die de oorsprong van de technologie vormen.

[12] Zodra virtuele digitale geldstromen tussen niet of nauwelijks te traceren partijen leiden tot fysieke stromen (drugs, wapens, smokkelwaar, illegale migranten etc.), ontstaan er direct weer aangrijpingspunten voor misdaadbestrijding.

Er is een breed spectrum aan opties tussen volledig gedecentraliseerde unpermissioned ledgers en volledig geautoriseerde permissioned ledgers. Vanuit het perspectief van veiligheid bieden (goed ontworpen) unpermissioned ledgers een geweldige veerkracht en robuustheid die permissioned ledgers, of andere toepassingen met gecentraliseerde functies, missen. Permissioned ledgers hebben weer meer mogelijkheden om vertrouwen centraal te borgen. Er zijn tussenvormen die het beste van twee werelden trachten te verenigen.[13] Gegeven het spectrum aan oplossingen is het belangrijk om de specifieke toepassings- en veiligheidseisen te analyseren alvorens te beslissen welk type grootboek te gebruiken.

Neem bijvoorbeeld een overheidssysteem voor het beheren en uitbetalen van uitkeringen. Zo'n systeem moet ten alle tijde beschikbaar zijn. De grootste bedreiging zou waarschijnlijk komen van opportunistische cybercriminelen die zich richten op individuele gebruikers. Prioriteiten in de beveiliging zouden dan zijn:

1. Het systeem moet zo ontworpen zijn dat het minimale kennis en inspanning van individuele gebruikers vereist, d.w.z. dat er slechts een klein aantal keuzes en configuraties moet zijn, met duidelijke feedback over de gevolgen;
2. Als randapparaten zoals smartphones worden gebruikt, zorg ervoor dat de sleutels die een gebruiker identificeren veilig worden benaderd en niet toegankelijk zijn voor andere toepassingen;
3. Het digitale grootboek zelf moet worden gedistribueerd over een uitgebreid netwerk van servers om goed tegen netwerkonderbrekingen te zijn opgewassen;
4. De authorisatiedienst voor uitbetaling dient gecentraliseerd te worden op specifieke hardware met zeer goede fysieke en digitale beveiliging.

Een heel ander voorbeeld is een systeem dat door overheden en/of NGO's kan worden gebruikt voor het verdelen van noodhulp. Belangrijk is de integriteit van transacties te waarborgen om te voorkomen dat fondsen worden afgetapt voor andere doeleinden; en de beschikbaarheid van het systeem te garanderen tijdens rampen en noodsituaties. Dreigingen kunnen afkomstig zijn uit natiestaten die geopolitiek voordeel zouden kunnen krijgen van het verstoren van transacties of van oneerlijke partijen binnen de hulpbehoevende staten. Daarom:

1. Het systeem moet draaien op een klein, goed beveiligd specifiek netwerk van servers die officiële kopieën van het grootboek bevatten met offline back-ups;
2. Klanten worden aangemoedigd hun eigen netwerken van grootboeken op te zetten, met advies over een veilig ontwerp dat regelmatige updates of correcties van de servers in het basisnetwerk mogelijk maakt;
3. Het moet kunnen en gebruikers moeten er rekening mee houden dat het systeem offline wordt genomen als er een ernstige netwerkaanval wordt vermoed.

DLT biedt een grote mate van flexibiliteit om heel verschillende gebruikseisen te accommoderen. Tegelijk legt dit ook nadruk op het ontwerpproces waarin de juiste keuzes moeten worden gemaakt.

[13] Een dilemma blijft het volgende. De behoefte aan een DLT-toepassing veronderstelt een mate van wantrouwen, of in ieder geval de erkenning dat de belangen van verschillende gebruikers niet per se overeenstemmen. Ontwikkelaars van publieke block chain-systemen vragen individuele gebruikers om in te stemmen met voorgestelde wijzigingen in het systeem, om er zo voor te zorgen dat wijzigingen alleen worden aangenomen als ze in het belang van het systeem als geheel zijn. De operators van een private block chain kunnen er daarentegen voor kiezen om veranderingen unilateraal te implementeren, ook al zijn sommige gebruikers het er niet mee eens. Hoe hiermee om te gaan is een belangrijk vraagstuk in de verdere ontwikkeling van DLT.

Blockchain-principes en (on)veiligheid

Laten we de belangrijkste kenmerken van blockchain / DLT (zie textbox in *Eerste Kennismaking*) langslopen om te bezien wat ze betekenen voor de veiligheid van DLT-systemen.

Gedistribueerde database

Bestaande methoden van data management, zeker van persoonsgegevens, betreffen vaak grote, oudere IT-systemen die binnen een enkele instelling draaien en zo *single points of failure* vormen. Bovendien zijn aan deze systemen een aantal netwerksystemen toegevoegd om te communiceren met gebruikers en tussen instanties om verschillende grootboeken die eenzelfde transactie moeten weerspiegelen te synchroniseren. Deze interfaces zijn aangrijpingspunten voor criminele acties en voegen complexiteit toe die beveiliging bemoeilijkt. Het geheel is kwetsbaar voor cyberaanvallen. In tegenstelling hiermee is DLT inherent moeilijk te verstoren, omdat er in plaats van een enkele database meerdere gedeelde kopieën van dezelfde database bestaan. De methoden waarmee informatie wordt beveiligd en bijgewerkt zorgen ervoor dat deelnemers er zeker van kunnen zijn dat alle kopieën van de grootboek op een bepaald moment elkaar overeenkomen. Een cyberaanval, bijvoorbeeld, moet alle kopieën tegelijkertijd aanvallen om succesvol te zijn. Daarmee zijn gedistribueerde grootboeken niet immuun voor criminaliteit, omdat in principe iedereen die een manier vindt om een kopie rechtmatig te wijzigen, alle kopieën van de grootboek verandert (zie verder).

Rechtstreekse communicatie

Omdat elke partij simpel en direct de gegevens van zijn transactiepartners kan verifiëren wordt het tegenpartijrisico sterk verminderd. Frauduleuze tussenpersonen zijn uitgespeeld. Keerzijde is dat achter een transactiepartner een criminele organisatie schuil kan gaan. Elke gebruiker of account van een DLT-toepassing heeft een uniek ‘adres’ om zich te identificeren. Transacties vinden plaats tussen deze unieke adressen. In bepaalde toepassingen kunnen gebruikers ervoor kiezen om anoniem te blijven achter dit adres of hun eigenlijke identiteit te delen met anderen. Dit wordt ‘pseudonimity’ genoemd: eenduidige, maar eventueel gemaskeerde identiteit.

Communicatie tussen nodes is essentieel voor het consensusproces en voor het actueel houden van de gedistribueerde kopieën van het grootboek. Een node die de overdracht van informatie beperkt of verkeerde informatie verstuurt moet kunnen worden herkend en uitgesloten om de integriteit van het systeem te handhaven. De operators van een private ledger voor, bijvoorbeeld, grondstoffenhandel kunnen de meest centrale posities in het netwerk toewijzen aan gevestigde handelspartners; en van nieuwe nodes vereisen dat ze verbinding houden met een van de centrale nodes als beveiligingsmaatregel om ervoor te zorgen dat ze zich gedragen zoals verwacht. Een belangrijke (veiligheids)vraag is hoe om te gaan met nodes die niet of nauwelijks actief zijn.

DDoS-aanvallen vanuit het systeem zelf (in het geval van gecorrumpeerde nodes) vormen een mogelijk probleem. Door grootscheeps ‘spam’-transacties te genereren kan het gehele netwerk worden stilgelegd.

Gedetailleerde toegangscontrole

DLT maakt het mogelijk precies vast te leggen welke gebruiker(sgroep) wat wanneer kan doen. De veiligheid van het systeem is hierbij gebaat. De meeste authorisatiesystemen zijn gebaseerd op cryptografisch gegenereerde sleutels die recht geven tot handelingen in het grootboek. Als een hacker, dief of tegenstander zo’n sleutel in handen krijgt, kan hij ‘legitiem’ handelingen uitvoeren in

de database. Merk op dat dit een persoonlijke beveiligingsfout betreft en geen systeemfout.[14] Het gedistribueerde karakter van DLT vormt hier een nadeel: decryptiepogingen of reproductie van sleutels die op de computer van een hacker plaatsvinden kunnen worden uitgevoerd zonder dat iemand anders het merkt. In meer private DLT-oplossingen kunnen additionele identificatie- en/of autorisatie-eisen worden gesteld om veiliger met verloren of gestolen sleutels om te kunnen gaan.

Transparantie en permanentie

De transparantie die DLT introduceert betekent dat diverse vormen van fraude moeilijker worden of verdwijnen. Omdat een eenmaal toegevoegd transactie niet meer kan worden gewijzigd of verwijderd, is het achteraf met de boeken knoeien niet meer mogelijk. Het betekent echter ook dat als een frauduleuze transactie in de boeken terecht is gekomen, dit niet meer achteraf kan worden gecorrigeerd.

In unpermissioned ledgers duurt het enige tijd voordat transacties volledig zijn geverifieerd. Deze vertraging is een kwetsbaarheid van het systeem, omdat een transactie die aanvankelijk lijkt te zijn geverifieerd, later deze status kan verliezen.

DLT-toepassingen kunnen bovendien aanleiding geven tot privacy-issues. In een unpermissioned ledger kunnen alle partijen de gehele geschiedenis van transacties volgen, ook wanneer ze geen partij waren in de transactie. Het 'recht om te worden vergeten', waarbij informatie uit een grootboek verwijderd moet worden, is niet simpel te implementeren in een gedistribueerde omgeving. Daarnaast zijn er uitdaging verbonden aan slimme contracten die toegang hebben tot de gegevens om transacties te verwerken en zo de bron van lekken kunnen vormen.

Macht bij de gebruikers

Zeker wanneer sprake is van een beperkt aantal bekende gebruikers met het recht om transacties goed te keuren, kunnen deze samenspannen om het systeem te manipuleren. Ook kan het systeem worden ‘gegijzeld’ door criminelen om zo valse transacties goed te keuren: een zogenaamde *consensus hijack*. In een unpermissioned ledger staat dit bekend onder de naam ‘51% attack’.[15]

Algoritmische logica / smart contracts

Het is bekend dat traditionele datamanagementsystemen vaak een flink percentage niet eenduidige, verouderde of onnauwkeurige gegevens bevatten, veelal veroorzaakt door menselijk fouten bij invoer en reproductie. Naast allerlei andere problemen, bemoeilijkt dit het proces van verificatie - met allerlei veiligheidsproblemen van dien. Voor DLT-systemen geldt dat de kwaliteit van de data veel beter gegarandeerd kan worden. Gebruikers kunnen vertrouwen dat transacties exact worden uitgevoerd zoals het (overeengekomen) protocol voorschrijft. Door het gebruik van softwarealgoritmen kan worden afgedwongen dat de data, naast tijdig en algemeen beschikbaar, compleet, consistent en accuraat is. De keerzijde is dat dergelijke algoritmen vatbaar zijn voor programmeerfouten. Dit geldt ook voor slimme contracten. Net als bij elke software geldt hoe complexer het contract, hoe gevoeliger voor programmeerfouten.[16]

Cruciaal is - niets nieuws - dat in het ontwerp van dergelijke toepassingen van het begin af aan ‘veiligheid’ een centrale ontwerpparameter is en ook in de implementatie en het feitelijk gebruik goed geregeld wordt. De werking van DLT-systemen is veel transparanter dan van conventionele gesloten

14 Het ‘systeem’ in bredere zin kan strenge beleidslijnen en procedures voor het beheer van sleutels afdwingen. De beveiliging van gedistribueerde grootboeken wordt zo een belangrijke taak en onderdeel van de maatschappelijke uitdaging om de digitale kritische infrastructuur te beschermen.
15 http://www.pfhub.com/bitcoin-loose-half-value-facing-coordinated-51-attack-1688/
16 Inderdaad blijkt een groot aantal sjablooncontracten beschikbaar op het web significante kwetsbaarheden te bevatten. Zie http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/

systemen. Goede voorbeelden kunnen simpel worden overgenomen en bewezen 'best practices' worden toegepast. Dit neemt niet weg dat het bouwen en onderhouden van DLT-systemen mensenwerk is. Fundamentele fouten in het ontwerp kunnen er in extremo toe leiden dat één corrupte transactie het hele grootboek besmet en zo de instorting van het hele systeem kan veroorzaken. Het simpel kunnen overnemen van publieke oplossingen kan tot wijd verspreide problemen leiden als die oplossingen toch veiligheidslekken blijken te bevatten.

Naarmate DLT bredere toepassing vindt zullen er onverwachte veiligheidsuitdagingen opdoemen - zoals dat ook bij de Bitcoin block chain is gebeurd. Net als bij andere producten- en dienstenontwikkeling loont het om een goed doordachte veiligheidsarchitectuur te ontwerpen die niet alleen bekende veiligheidsproblemen adresseert, maar ook flexibel genoeg is om in te spelen op nieuwe problemen terwijl het product al op de markt is en lastig meer fundamenteel kan worden aangepast.
We moeten ons daarbij niet beperken tot de block chain variant van DLT. Andere implementatievormen zijn wellicht beter en veiliger. Een voorbeeld is IOTA[17]. Dit alternatief voor block chain-implementatie is maakt het (relatief dure en onveilige) concept van een groep van toegewijde validators (de 'miners' in Bitcoin) overbodig. Verder is, als voorbeeld, de Bitcoin-ledger weliswaar gedistribueerd, maar wel in zijn geheel in de cloud opgeslagen - met de risico's vandien. IOTA stapt ook van dit principe af en staat partionering toe, met opslag niet per se in de cloud maar op (eventueel specifiek beveiligde) 'eigen' servers. Zeker in dit jonge vak- en toepassingsgebied staat de techniek niet stil.

Bundeling én distributie van beveiligingskennis

Zoals voor veel ICT-systemen geldt ook voor DLT-toepassingen dat individuele gebruikers en veel organisaties niet in staat zijn om alle veiligheidsaspecten te overzien; laat staan afdoende maatregelen te nemen en alle ontwikkelingen bij te houden. Er ontstaan centrale punten waar beveiligingskennis gebundeld wordt om op basis van deze kennis beveiligingsproducten en -diensten te leveren. Idealiter ontstaat een markt van dergelijke kenniscentra (in een mix van bedrijven en publieke instanties) die elkaar scherp houden en aanvullen. Het gevaar bestaat echter dat schaalvoordelen het nieuwe toetreders zeer lastig maken, waarmee de diversiteit van deze markt onder druk komt; een dergelijke tendens is inderdaad zichtbaar in (segmenten van) de cyber security markt. Een actief overheidsbeleid om diversiteit van de markt te waarborgen is dan gewenst, zoals dat onder meer in het Verenigd Koninkrijk gebeurt.[18]

Bredere gevolgen voor maatschappelijke veiligheid

Uitgaande van een - zeker niet vaststaand, maar wel goed voorstelbaar - scenario waarin DLT-toepassingen een grote vlucht nemen voor het vastleggen van steeds meer verschillende zaken die waarde vertegenwoordigen. Wat kan dit in algemene zin betekenen voor de aard van de grote veiligheidsuitdagingen waarmee onze samenleving te maken heeft?

Aan de ene kant biedt DLT (en de met DLT samenhangende processen en structuren) de mogelijkheid om een ongekende verfijning aan te brengen in veiligheid en privacy. Onder invloed van de digitalisering en federatieve samenwerking komen de disciplines van business continuïteit, crisismanagement, cybersecurity en anti-fraude samen. Mits goed ontworpen, kunnen DLT-systemen (in brede zin) de samenkomende eisen vanuit deze disciplines accommoderen door de

17 https://blog.iota.org/automating-machine-transactions-and-building-trust-in-the-4th-industrial-revolution-d3219a157396
18 Zie onder meer "UK intelligence agencies turn to start-ups on cyber security", https://www.ft.com/content/6cdfa82e-77bd-11e7-a3e8-60495fe6ca71

brede waaier aan verschillende oplossingen te benutten en die per toepassingsgebied, per activa, maar eventueel ook per gebruiker en per transactie toe te spitsen.

Aan de andere kant kan grootschalige toepassing van DLT het fundamentele weefsel van onze maatschappij ingrijpend beïnvloeden en zo, als we niet uitkijken, bijdragen aan sociale ontwrichting en daarmee aan destabilisatie van onze samenleving. De onderliggende filosofie van gedistribueerde consensus, open source, transparantie en gemeenschappelijkheid vormt een bedreiging voor iedere gecentraliseerde, hiërarchische structuur. Dit is op zichzelf goed nieuws omdat hiermee de nadelen van hiërarchieën kunnen verdwijnen: duplicatie, extra kosten, de potentie voor machtsmisbruik en risico's van wanbeheer. Maar hiërarchieën hebben ook voordelen. Ze bieden duidelijkheid wie waarover gaat en hoe invloed kan worden uitgeoefend. Duidelijke regels geven bovendien maatschappelijke en politieke stabiliteit. Het ondergraven van de hiërarchische structuren waarop onze huidige maatschappij is gebouwd knaagt aan deze stabiliteit.

Overheden vormen zo'n gecentraliseerde, hiërarchische structuur. Zo is in de huidige verhoudingen de controle over geld, en daardoor over de economie, een taak van de overheid. Alternatieve valutasystemen zoals Bitcoin, uitgevonden en beheerd buiten overheidscontrole, vormen een bedreiging voor die taak – en knagen daarmee aan de legitimiteit van de overheid en aan het sociale contract tussen burger en overheid.[19]

Natiestaten - met hun cruciale rol in het garanderen van veiligheid voor burgers en bedrijven - worden al uitgedaagd door globalisering en fluïde grenzen. Een breed gebruik van DLT zou nog een extra dimensie aan deze uitdaging toevoegen. Natiestaten en hun uitvoeringsorganen houden ook in de toekomst grote waarde; maar moeten zich wel - wellicht drastisch - omvormen. Een belangrijk voorbeeld is de representatieve democratie. Een kerntaak van een democratische overheid is te zorgen voor een juiste (her)verdeling van hulpbronnen onder burgers, organisaties en bedrijven. Dit gaat verder dan de verdeling van financiële middelen en omvat ook immateriële activa zoals veiligheid, democratie, toegang tot de rechtsstaat; en economische voorwaarden, zoals de bevordering van vrije markten, een lage en stabiele inflatie, de bescherming van eigendomsrechten en het garanderen dat contracten worden nagekomen.

In het 'sociale contract' tussen burger en overheid is bepaald hoe de regels voor een 'juiste' (her)verdeling worden vastgesteld - door middel van parlementaire vertegenwoordiging bijvoorbeeld. In de historische ontwikkeling van het democratisch model is het overheidsapparaat dat de (her)verdeling uitvoert steeds groter en centraler geworden, en daarmee ver verwijderd geraakt van de burgers. Omgekeerd is de complexiteit van onze samenleving deels ook weer het resultaat van deze centralisatietendens.

Toepassing van DLT biedt overheden de gelegenheid om hun (her)verdelingstaken efficiënter, effectiever en klantvriendelijker uit te voeren. Maar het biedt ook de mogelijkheid om de democratische mechanismen die bepalen wat een juiste (her)verdeling is te vernieuwen én om er voor te zorgen dat de voordelen van deze (her)verdeling daadwerkelijk terecht komen bij degenen die daar het meest recht op en baat bij hebben. Een belangrijke voorwaarde is dat de betreffende overheden mee kunnen gaan in de daartoe vereiste decentralisatie- en transparantieslag die toepassing van DLT vereist. Voorwaar geen sinecure!

19 Merk op dat sommige van de oorspronkelijke ontwikkelaars en aanhangers van Bitcoin sterk anti-overheid zijn; en Bitcoin als een instrument zien om de invloed van de overheid sterk terug te dringen.

6. Risicoanalyse in Onzekerheid

Hoe moeten we de (veiligheids)risico's inschatten van een opkomende technologie waarvan we de reikwijdte, de timing en het mogelijke disruptieve karakter nog niet goed kunnen doorgronden? En dan hebben we het nog niet eens over de *wisselwerking* met diverse andere grote trends waarvoor in meer of mindere mate hetzelfde geldt. Traditionele risicoanalyses, veelal gebaseerd op een technische 'maakheids'-gedachte en werkend binnen een afgebakend domein, kunnen slecht omgaan met onzekerheden en complexe verbanden. Een alternatieve manier van risicoanalyse stelt 'scenario's' en 'discussie' centraal. Vertrekpunt is de vraag wat een gewenst of vereist niveau van veiligheid is, of in meer kwantitatieve termen het acceptabel risico. Dit is geen uitkomst van een berekening maar onderwerp van debat en, uiteindelijk, een politiek-maatschappelijke keuze. In dit debat moeten de effecten die kunnen optreden en de (maatschappelijke) impact en kosten van verschillende maatregelen worden afgewogen. Nut en noodzaak van, in ons geval, DLT-toepassingen moet worden afgezet tegen mogelijke effecten van grootschalige invoering van DLT op veiligheid en de impact van maatregelen om ongewenste effecten te mitigeren. Dergelijke afwegingen kunnen worden gemaakt door bedrijven voor de ontwikkeling van producten en diensten en door overheden om kaders en regels te stellen.

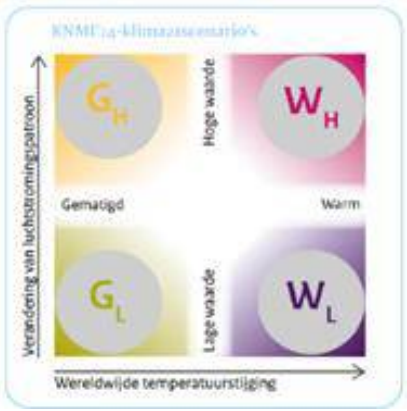
De impact van DLT op de samenleving kan niet nauwkeurig op voorhand worden voorspeld. Wel kunnen de diverse mogelijke effecten in kaart worden gebracht als ondersteuning voor besluitvorming en als basis om te identificeren wat de kritieke processen en effectieve oplossingsrichtingen zijn. Hiervoor bestaan verschillende technieken. Twee mogelijke technieken zijn:

1. Adaptieve planning: uitwerken van verschillende hoekpunten die samen het speelveld omvatten.
2. Probabilistische risicoanalyse: uitwerken van kansverwachtingen rekening houdend met onzekerheden

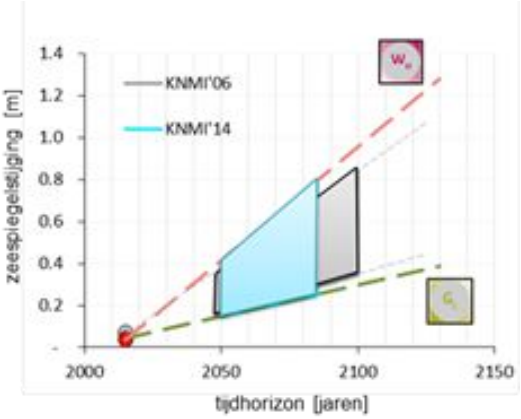
Adaptieve planning

Door het werken met verschillende scenario's (verhaallijnen) kan men het speelveld van mogelijke ontwikkelingen in kaart brengen. De scenario's schetsen bijvoorbeeld wat de effecten zijn van het mainstream worden van DLT-toepassingen op een aantal momenten in de toekomst, ingekaderd door een aantal randvoorwaarden. Door verschillende aannames voor deze randvoorwaarden te hanteren en op een aantal hoekpunten in scenario's te beschrijven, worden de bandbreedtes van mogelijke effecten zichtbaar gemaakt. Er wordt geen uitspraak gedaan over de waarschijnlijkheid van ieder van de scenario's.
Op basis van deze scenario's kunnen de effecten in kaart worden gebracht). De bandbreedte en methodiek geven vervolgens handvatten om de potentie van diensten, producten en of beleid inzichtelijk te maken. Hierbij kan ook gebruik worden gemaakt van de 'reële opties'-aanpak om de kosten in te schatten van het zich voorbereiden op meerdere mogelijke toekomsten.[20] Per scenario kan in kaart worden gebracht wat het effect (de baten) zijn van deze maatregelen. Door de scenario's onderling te vergelijken blijkt of deze maatregelen in alle gevallen werken of slechts voor een enkel scenario.

20 'Reële opties' (real options) hebben een vergelijkbare functie als financiële opties, maar dan voor 'fysieke' investeringen. In onzekere tijden heeft het soms de voorkeur om risico's te spreiden en onomkeerbare keuzes zolang mogelijk te vermijden. Dit kan door een bredere portefeuille van verschillende opties te ontwikkelen, om vervolgens op basis van nieuw beschikbare informatie de meest geëigende optie(s) te lichten (en de overige te laten verlopen). Reële opties-theorie gebruikt de logica achter financiële opties, waarbij methoden bedacht om financiële opties (zowel 'put' als 'call') te waarderen als voorbeeld dienen om reële opties van een prijskaartje te voorzien.



Deltascenario's gebruikt in het Deltaprogramma



Effecten van klimaateffecten uit deltascenario's van 2006 en 2014 op de zeespiegelrijzing als functie van de tijd

Figuur 5: Voorbeeld van deltascenario's voor waterveiligheid[21]

Figuur 5 visualiseert, als voorbeeld, hoe een dergelijke scenariogedreven analyse wordt gedaan voor de bescherming van Nederland tegen wateroverlast.[22] Uit de klimaatmodellen van het KNMI worden twee sleutel-variabelen gelicht: de wereldwijde temperatuurstijging en de luchtstomingspatronen. Dit zijn de twee assen in het figuur links. De klimaatmodellen geven een range aan waarbinnen deze variabelen kunnen veranderen; de vier scenario's in het figuur links – Gematigd/Laag, Gematigd/Hoog, Warm/Laag en Warm/Hoog – vormen de hoekpunten van deze range. Welk scenario werkelijkheid wordt bepaalt de zeespiegelrijzing voor de komende eeuw. Dit, op zijn beurt, is bepalend voor de mate waarin we bijvoorbeeld onze dijken moeten verzwaren. Vanuit de statistische modellen zijn alle scenario's denkbaar. Het is dan een politieke en maatschappelijke keuze waar we vanuit gaan in onze maatregelen tegen zeespiegelrijzing; waarbij duidelijk zal zijn dat minder risico lopen meer geld kost. De scenariogedreven analyse doen geen uitspraak over deze keuze, maar is wel van cruciaal belang om (1) de problematiek goed in kaart te brengen; en (2) de discussie over mogelijke maatregelen en hun kosten en baten te objectiveren.

Op vergelijkbare wijze kunnen we sleutelvariabelen definiëren voor de ontwikkelingen op het gebied van DLT. De TU Delft heeft in een brainstorm als voorbeeld de volgende assen benoemd:

1. De economie: het aantal toepassingen in verschillende sectoren dat DLT gebruikt en de mate waarin deze sectoren geïntegreerd zijn. Extremen: toepassing in een beperkt aantal gescheiden sectoren vs. brede en verstrengelde toepassing door de hele economie.
2. Evolutie of revolutie: de mate waarin (en evt. snelheid waarmee) DLT leidt tot een vervanging van bestaande systemen of tot nieuwe toepassingen. Extremen: langzame vervanging omdat 'oude' systemen nog lang waarde blijven vertegenwoordigen vs. een kettingreactie omdat achterblijven geen optie is.
3. Democratisering: de mate waarin de decentralisatie is vormgegeven en diensten en produkten 'as a service' worden aangeboden via DLT. Extremen: van (vooral) gesloten

21 https://www.helpdeskwater.nl/onderwerpen/applicaties-modellen/applicaties-per/watermanagement/watermanagement/nationaal-water/kopie-werkt/uitvoer/
22 https://www.tudelft.nl/en/tpm/about-the-faculty/departments/multi-actor-systems/research/projects/adaptive-delta-management/

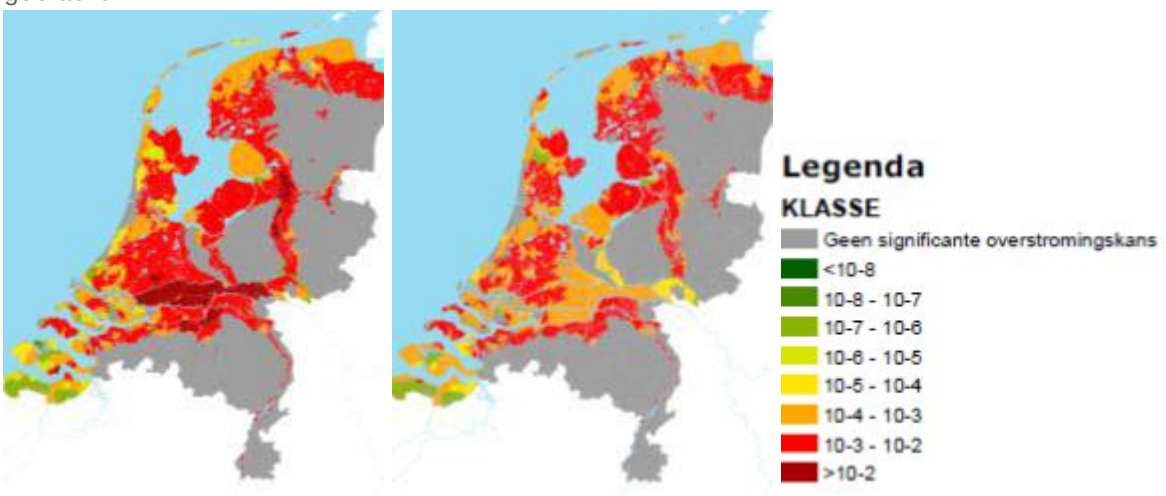
systemen met een monopoliserende werking tot (vooral) open systemen verkrijgbaar voor allerlei deeltoepassingen.

4. Gelijkheid: De mate waarin DLT leidt tot diverse gelijkwaardige ‘peer to peer’ toepassingen of dat er enkele grote spelers het netwerk domineren. Extremen: van ‘winners take all’-markt tot een levendige open markt met heel veel aanbieders.

Voor de combinatie van de extremen op deze assen kunnen duidelijk te onderscheiden scenario’s worden ontwikkeld die gezamenlijk het speelveld van mogelijkheden opspannen; om daarmee de discussie te voeden over robuuste maatregelen en oplossingen.

Probabilistische risicoanalyse

Een andere manier om risico-onzekerheid proberen te vangen is probabilistische risicoanalyse. Hierbij wordt getracht om de effecten van ontwikkelingen te kwantificeren rekening houdend met onzekerheden. Gebruik kan worden gemaakt van dezelfde scenario’s als bij adaptieve planning. Echter nu houden we rekening met ‘n’ (een al dan niet groot aantal) verschillende scenario’s met telkens net andere effecten. Door de risico’s in al deze scenario’s statistisch te benaderen kan ‘het’ risico worden vertaald in termen van verwachtingswaardes en bandbreedtes voor bijvoorbeeld euro’s per jaar of slachtoffers per jaar maar ook andere parameters als toegenomen werkloosheid per jaar etc. Op een vergelijkbare manier kunnen ook effecten van *maatregelen* in kaart worden gebracht.



Figuur 6: Plaatsgebonden overstromingskans voor (links) en na (rechts) versterken waterkeringen

Om de (bandbreedte van) effecten in kaart te brengen kunnen modellen gebruikt worden om de gevolgen te kwantificeren. Hierbij is het van belang om de parameters te benoemen waarin deze effecten worden beschreven. Voor de hand liggende parameters zijn kosten, werkloosheid, vertrouwens- en welvaartsindices voor de bevolking en de impactcriteria zoals gebruikt in de Nationale Risicobeoordeling.[23]

[23] Binnen de rijksbrede strategie Nationale Veiligheid wordt jaarlijks een Nationale Risicobeoordeling (NRB) opgesteld, waarin een aantal veiligheidsthema’s wordt geanalyseerd in de vorm van scenario’s die langs een vaste meetlat worden gelegd: de NRB-methodiek. De resultaten hebben tot doel beleidsmakers inzicht te geven in de relatieve waarschijnlijkheid en impact van de verschillende scenario’s. Dit inzicht is van belang om capaciteiten te benoemen, beleid te formuleren en prioriteiten te stellen met als doel Nederland zo goed mogelijk voor te bereiden op verschillende soorten rampen en dreigingen. Zie https://www.nctv.nl/binaries/nat.risicobeoordeling-6-definitief_tcm31-32706.pdf

De waarschijnlijkheid en onzekerheid kan in kaart gebracht worden met behulp van statistische en big data-modellen, en wellicht ook door gebruik te maken van gamingtechnieken. Gezien de aard van de technologie is de vraag of al deze informatie daadwerkelijk gemodelleerd kan worden, of dat hier te veel tijd (en geld) mee gemoeid is. Een alternatieve of aanvullende manier is door expertkennis te ontsluiten om zo de benodigde informatie rondom de scenario's in te schatten.

Hulpmiddelen op meerdere niveaus

Bovenstaande methoden kunnen bijdragen aan een debat of afweging over te maken keuzes over maatregelen of wat we onder een acceptabel veiligheids-/risiconiveau verstaan. De methoden schrijven deze afweging niet voor maar zijn een hulpmiddel. De methoden kunnen worden uitgewerkt op een hoog abstractieniveau, maar ook op groot detailniveau. Naarmate het detailniveau toeneemt is het, om de werklast binnen perken te houden, wel van belang om een goed beeld te hebben van de relevante én significante parameters die in meer detail worden uitgewerkt.

Al ons ervaring met risicoanalyses leert ons één ding: in de complexe werkelijkheid ontstaan altijd onverwachte risicovolle situaties die niet uit de modellen vooraf kwamen. Juist het denken in en werken met scenario's geeft de mentale flexibiliteit om hierdoor niet in een kramp te schieten. Bovendien legt deze constatering nadruk op het *proces* van risicoanalyse: niet een eenmalige exercitie, maar een continue herijking op basis van steeds nieuwe gegevens en inzichten uit de theorie en uit de praktijk.

7. Ter Afsluiting

In deze paper hebben we de volgende lijn van redeneren gevolgd.

De **toepassingsmogelijkheden** van block chain reiken veel verder dan bitcoin en andere cryptovaluta; het is zelfs zo dat bitcoin een associatie met illegaliteit en speculatie meebrengt die feitelijk tegengesteld is aan de essentiële eigenschappen van de technologie. Digital Ledger Technology (DLT), de generieke naam van block chain-achtige technieken, kan een rol spelen in alle sectoren waarin waarde en bezit en de overdracht daarvan aan de orde is.

Voordat DLT-toepassingen mainstream kunnen gaan worden moet er nog veel gebeuren. De **uitdagingen** zijn deels technisch, maar liggen vooral op vlak van organisatie, regelgeving en beheer, transitie vanuit de huidige situatie en acceptatie van de technologie. Stuk voor stuk goed te doen, maar niet per se eenvoudig in samenhang op te lossen. Pilotprojecten zijn nodig - en ook reeds volop in ontwikkeling en uitvoering - zodat praktische, juridische en beleidsimplicaties kunnen worden onderzocht.

Vertrouwen is een cruciale pijler onder de inrichting van onze economie en samenleving. In de huidige praktijk zijn vaak vertrouwde tussenpersonen - zoals banken of notarissen, maar ook allerlei overheidsdiensten - nodig om transacties tussen partijen te garanderen. DLT is een simpel, goedkoop en transparant alternatief om vertrouwen vast te leggen, maar dan rechtstreeks tussen de transactiepartijen - personen, instanties en ‘dingen’ (als in het ‘Internet der Dingen’) - en met hele gedetailleerde regels wie wat wanneer mag doen. DLT bedreigt daarmee gevestigde belangen en ondergraaft de huidige best practices van, bijvoorbeeld, waardeoverdracht, financieel toezicht, privacy en eigendom van data. De positie van veel instanties die nu als tussenpersoon en beheerder optreden, waaronder de overheid in zijn huidige centraal georganiseerde vorm, staat op het spel. Alleen daarom al heeft DLT **‘game changing’ potentie** op het niveau van de samenleving als geheel.

DLT als technologie kan systemen voor het vastleggen van waarde en bezit in de kern (het grootboek van transacties) **intrinsiek veiliger** maken. Vormen van fraude zullen dan moeilijker worden of verdwijnen. Ook zullen er minder single points of failure zijn. Tegelijk blijven allerlei **veiligheidsissues ‘aan de randen’** van dergelijke toepassingen bestaan en ontstaan er zelfs nieuwe. Zo is het beheer van digitale sleutels die toegang geven tot het digitale grootboek is een belangrijk veiligheidsuitdaging. In bredere zin is identiteitsmanagement een cruciaal onderwerp, met in theorie en in de praktijk veel mogelijkheden voor manipulatie. Speciale aandacht vergen bepaalde block chain-toepassingen waarin één gecorrumpeerde transactie het hele systeem kan ondermijnen. Verder betekent de automatisering van transactieprocessen, in het bijzonder in het geval van smart contracts, dat menselijke programmeerfouten en bewust ingebouwde achterdeurtjes het veilige gebruik kunnen ondermijnen. Vanwege het open karakter van DLT-toepassingen zullen dergelijke loopholes minder makkelijk verstopt blijven. Tegelijk creëert het een laagdrempeligheid, onder meer vanwege de ruime mogelijkheden van hergebruik, die de snelle verspreiding van applicaties met (al dan niet moedwillige) veiligheidslekken juist bevordert.

DLT als potentiële game changer kan de wijze waarop onze samenleving functioneert drastisch veranderen. Grootschalige toepassing zou een **forse verschuiving van macht** van centrale instanties naar decentrale partijen, vaak individuen, betekenen; een ontwikkeling die ook door andere technologische toepassingen wordt gevoed. Als de (centraal georganiseerde) overheid zich niet drastisch anders gaat inrichten en opstellen, staat haar macht en de geloofwaardigheid op het

spel. De opkomst van autonoom opererende systemen is een andere bredere ontwikkeling die door DLT-toepassingen zal worden versterkt. DLT stelt in staat om **allerlei transacties zonder menselijke betrokkenheid** te plegen. Hoewel de transacties op zich transparant horen te zijn, is het de vraag hoezeer de (niet-menselijke) redeneringen die tot de transacties leiden dat ook zijn. Het risico dat dergelijke autonome processen uit de hand lopen is niet denkbeeldig. In dit brede perspectief kan **politieke en maatschappelijke instabiliteit** een gevolg zijn, met alle veiligheidsconsequenties van dien.

Onze analyse ondersteunt en illustreert de behoefte aan **brede(re), veelal scenariogedreven risicoanalyses** in het licht van (technologische) ontwikkelingen met een potentieel - maar vooraf niet goed in te schatten - game changing karakter. De onzekerheid over de daadwerkelijke impact van de betreffende ontwikkeling / technologie, de timing ervan en (vooral) de wisselwerking met allerlei andere ontwikkelingen die elkaar kunnen versterken of juist dempen maken dergelijke brede analyses noodzakelijk.

Colofon

Notitie Risico-Analyse in Onzekerheid - Blockchain (Kansen en Bedreigingen)

Een publicatie in opdracht van

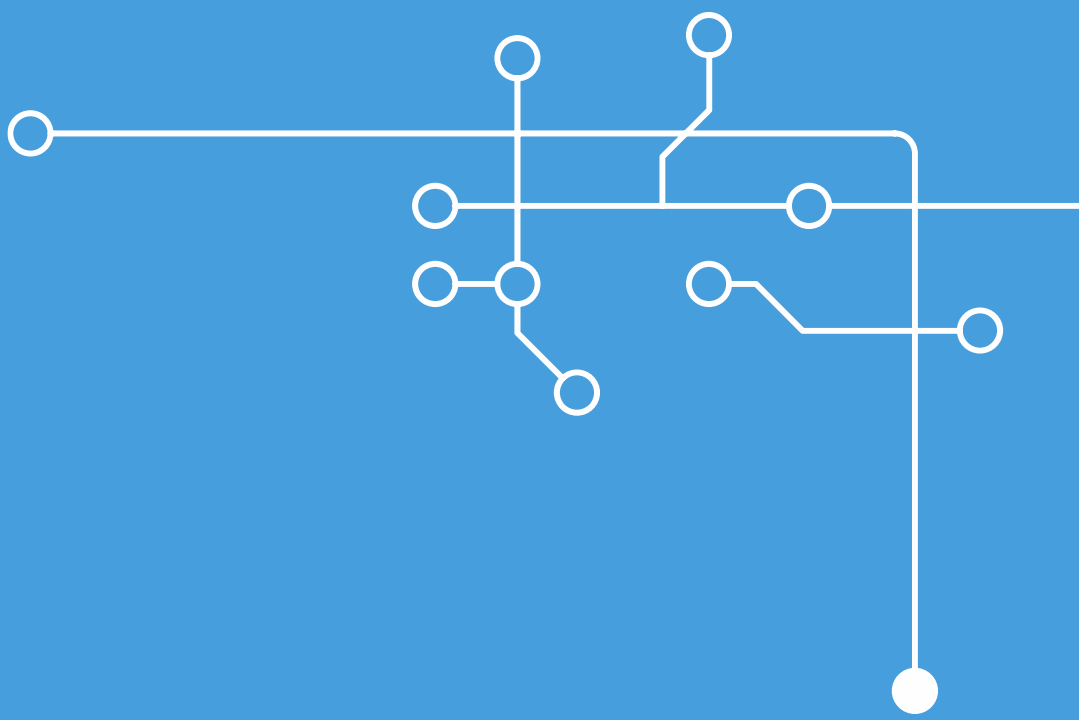
The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595AN Den Haag
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Auteur

Frank Bekkers.

Met dank voor de uitgebreide bijdrage van Bas Kolen en collega's van de TU Delft die de basis heeft gevormd voor het hoofdstuk *Risicoanalyse in Onzekerheid*.

Dank ook aan de inbreng van de volgende gesprekspartners: Zeki Erkin van EWI TU Delft, Bas Kolen van de TU Delft, Ronald Prins van Fox-IT en René Pluis van Cisco Systems.



The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN The Hague, The Netherlands
+31(0)70 204 51 80

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL