NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Verkenning Blockchain Beheersing

Audit en control in het ecosysteem

Kennisgroep Keteninformatiemanagement

Oktober 2021

Postadres: Postbus 7984, 1008 AD Amsterdam

Bezoekadres: Antonio Vivaldistraat 2, 1083 HP Amsterdam

Telefoon: 020-3010380

E-mail: norea@norea.nl

www.norea.nl

Inhoud

Inhoud 3

Voorwoord 4

Management samenvatting 5

Deel 1 7

1 Inleiding 8

2 Blockchain in kort bestek 12

3 Externe organisatie en platformeconomie 20

Deel 2 24

4 Audit en control in het ecosysteem 25

5 Blockchain beheersing 32

6 Auditvoorbeelden ter illustratie 40

7 Afsluiting 46

Bijlagen 48

Selectie literatuur 49

Kennisgroep Keteninformatiemanagement 50

Kennisgroep leden 51

Voorwoord

De introductie van wat nu blockchain technologie genoemd wordt is slechts tien jaar geleden. Gedurende deze periode heeft de oorspronkelijke belofte zich ontwikkeld van een betalingsplatform voor cryptovaluta naar iets dat groter, innovatief en disruptief is. Diverse twijfels zijn weggenomen en blockchain is stevig verankerd in het strategisch denken van organisaties in sectoren en toepassingsgebieden. Organisaties zijn nu meer dan ooit betrokken bij blockchain ontwikkelingen en laten dit steeds meer zien door concrete implementaties als onderdeel van hun normale bedrijfsvoering. Blockchain wordt steeds meer gezien als een integraal onderdeel van organisatorische innovatie.

Bij netwerkorganisaties zal het vraagstuk van audit en control een grotere rol gaan spelen. Voor IT- en financial auditors vormen samenwerking in ecosystemen en digitalisering een betrekkelijk nieuw onderwerp. In de klassieke accountancy en bedrijfseconomie is alle aandacht immers gericht op de interne beheersing van een organisatie. Zodra organisaties gebruik gaan maken van blockchain technologie in hun bedrijfsprocessen, heeft dit direct effect op de interne beheersing en verantwoording bij die organisaties. Blockchain technologie kent op zichzelf geen fundamentele verschillen met andere technologieën, maar leidt wel tot serieuze consequenties op specifieke risicogebieden anders dan IT. Deze trend dwingt tot de doorontwikkeling van audit en andere assurance producten in de richting van netwerkauditing. Het is de vraag of auditors zich voldoende bewust zijn van de risico's naarmate de integratie met netwerkpartners intensiever wordt en de innovatie in technologie toeneemt.

De NOREA Kennisgroep Keteninformatiemanagement heeft in 2019 een thematische werkgroep opgericht. Deze werkgroep richt zich vanuit het perspectief van integrale auditing op het verkennen van de inzichten over het verstrekken van assurance bij informatiesystemen, waarbij gebruik wordt gemaakt van blockchain. De doelstelling is het in stappen ontwikkelen van een Blockchain Control Framework, dat in de beroepspraktijk gebruikt kan worden bij het beheersmatig goed inrichten en het verstrekken van assurance door auditors in situaties waarin blockchain van toepassing is. Deze verkenning geeft een tussenrapportage met een beeld van de stand van zaken in de eerste fase van ontwikkeling.

Management samenvatting

De NOREA Kennisgroep Keteninformatiemanagement is in 2019 gestart met het analyseren van de beheersingsaspecten van blockchain toepassingen. Dit zal resulteren in een Blockchain Control Framework, dat is gebaseerd op generieke kaders en onderzochte blockchain cases. Als tussenresultaat is in deze publicatie de blockchain technologie nader toegelicht en zijn de implicaties ervan voor interne beheersing en (IT) auditing uitgewerkt. De belangrijkste observaties van de Kennisgroep in deze zoektocht zijn:

1. Iedere nieuwe generatie technologie kan leiden tot een nieuwe generatie beheersings-maatregelen en/of auditbenaderingen. Ook al is er geen causaal verband dat de interne beheersing en auditaanpak direct moet mee veranderen, bij blockchain zal dit wel deels nodig zijn. Niet alle risico's zijn met het huidig beheersingsinstrumentarium toereikend af te dekken. Een blockchain netwerk is in feite een gedistribueerd grootboek cq. informatiesysteem met gestructureerde gegevensuitwisseling tussen en door samenwerkingspartners in een ecosysteem, dat gepaard gaat met een diversiteit aan belangen en risicogebieden. De IT-auditor wordt voor het verstrekken van zekerheid over de betrouwbare opzet en werking van een complete blockchain toepassing eigenlijk een ecosysteem auditor.

2. Bij blockchain toepassingen in ecosystemen zijn de interne organisatie en beheersingsmaatregelen belangrijker dan de technologie op zichzelf. Blockchain technologie kent op zichzelf geen fundamentele verschillen met bekende technologieën zoals PKI, hashing, online berichtenverkeer en interconnectiviteit, maar leidt wel tot serieuze consequenties op specifieke risicogebieden, zoals ecosysteem governance, data(kwaliteits)management, informatiebeveiliging, financiering en verrekening. Blockchain vereist een multidisciplinaire sturing op en beheersing van risicogebieden en een gedegen organisatorische inrichting van (informatieverwerkende en IT-) beheer(s)processen.

3. De IT-omgeving van een organisatie die een blockchain toepassing implementeert, transformeert rond de koppelvlakken in een ecosysteem op zichzelf. Hierbij is haar eigen interne IT-beheersing en informatiebeleid afhankelijk van het bredere ecosysteem en de individuele deelnemers. De verschuiving van informatiesysteem onder eigen beheer naar een gedistribueerd grootboek betekent derhalve ook een gedeeltelijke verschuiving naar een gedistribueerde beheersomgeving. Een IT-audit van een blockchain toepassing zou gebaat zijn bij een brede benadering en ons inziens een netwerkaudit. Nadeel is dat er een enkele of gezamenlijk optredende opdrachtgever voor een dergelijke netwerkaudit nodig is.

4. Financiële en IT-auditors dienen zich goed bewust te zijn van de veranderingen in risico's naarmate de externe integratie in ecosystemen en technologische innovatie sterk toenemen. Hierbij wordt het relevant om een "control"-benadering uit te breiden met een "trust"-benadering, ook bij besloten blockchain netwerken. Daarbij zal bovendien meer aandacht voor soft controls wenselijk zijn, aangezien organisaties en

belanghebbenden bewust zijn geworden dat regels en “harde” maatregelen alleen niet voldoende zijn voor complexe beheersingsvraagstukken, en dat “zachtere” elementen zoals cultuur, leiderschap, waarden, normen en gedrag cruciaal zijn. Soft controls zijn niet alleen van belang voor de sturing, maar ook voor het toezicht en de verantwoording. Natuurlijk zullen toezichthouders vooralsnog minimaal de harde beheersingsmaatregelen van een blockchain getoetst willen zien.

5. Blockchain zou de rol van een centrale Trusted Third Party, zoals een bank, overbodig kunnen maken. In een aantal blockchain implementaties, bijvoorbeeld bij cryptocurrencies, is dit mogelijk gebleken. Bij vele andere zakelijke blockchain-toepassingen zien wij toch weer een centrale coördinerende organisatie ontstaan. Deze draagt zorg voor de gezamenlijke beleidsvorming, sturing van het totstandkomingsproject, aansluiten van systemen van deelnemers, operationele zaken, financiële verrekening, e.d.

6. Naarmate blockchain technologie volwassener wordt, zal de belangrijkste uitdaging op weg naar grootschalige adoptie liggen op het gebied van governance, stakeholder management, kosten/batenverhouding en - inmiddels ook - energieverbruik/duurzaamheid. Daarbij zal het dominante ketenprobleem dat blockchain oplost en de doorzettingsmacht van de initiërende partij leidend zijn.

7. Blockchains zijn van nature al gauw internationaal van aard, waardoor de wet- en regelgeving uit verschillende landen van toepassing is. Het voldoen aan fiscale- en privacywetgeving, het beschermen van bedrijfsgevoelige gegevens en intellectuele eigendomsrechten, het naleven van bewaartermijnen e.d. bleken aanvankelijk showstoppers voor grootschalige uitrol. Intussen zijn hiervoor inherent compliant oplossingen voor blockchain ontwikkeld.

8. Standaard blockchain protocollen, beheersings- en normenkaders krijgen een steeds belangrijkere rol. Technische innovaties kennen veelal niet gelijk één of enkele wereldwijde standaarden, maar vanuit beheersingsoogpunt kunnen ze het implementeren en het auditen van blockchain toepassingen vergemakkelijken. Een reeds grondig getest standaardprotocol betekent bijvoorbeeld dat niet alle technische maatregelen en IT General Controls in iedere audit opnieuw hoeven te worden getoetst, maar dat de nadruk wordt gelegd op zaken als smart contracts, data-integriteit, autorisaties, e.d. Als één blockchain-brede netwerkaudit niet haalbaar is, heeft het de sterke voorkeur om zoveel mogelijk hetzelfde kader te hanteren. Totdat blockchain verder is uitgekristalliseerd en een standaardkader is uitgewerkt zullen principle-based auditing en professionele oordeelsvorming van belang blijven.

De Kennisgroep zal het NOREA Blockchain Control Framework verder ontwikkelen, deze in een aantal praktijksituaties evalueren en begin 2022 publiceren. Mocht u daaraan een bijdrage willen leveren neem dan gerust contact met ons op.

Deel 1

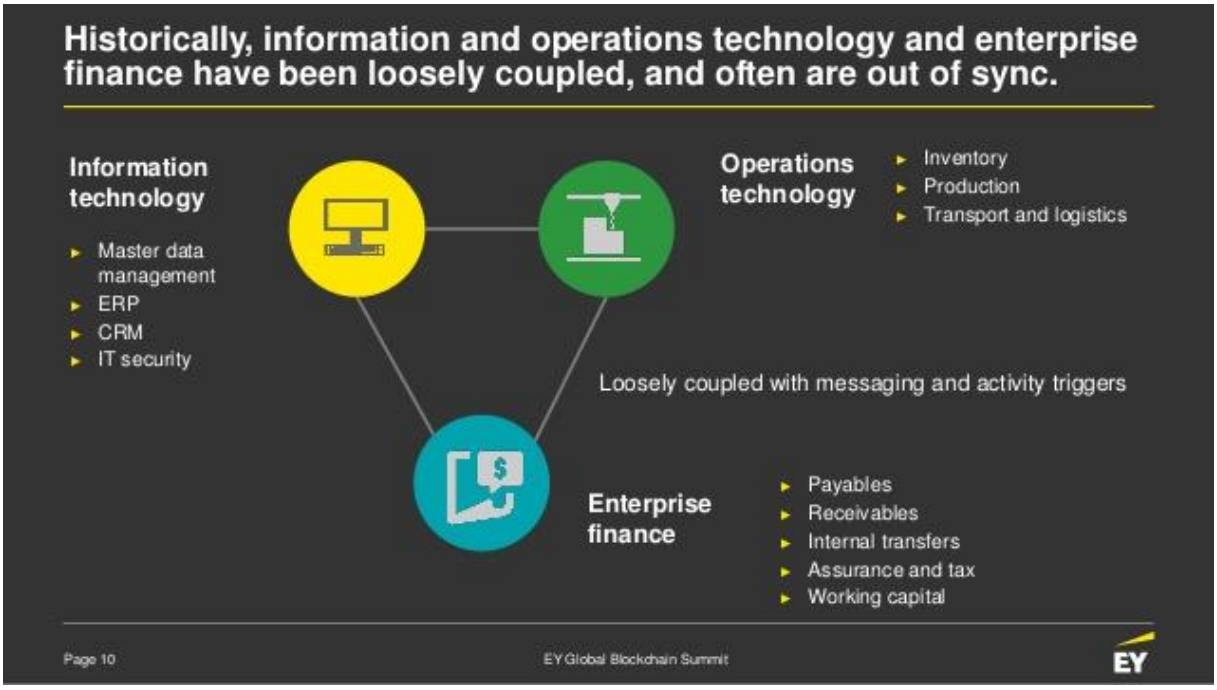
1 Inleiding

Blockchain (distributed ledger technology) is een veelbesproken onderwerp in de wereld van technologie, audit en control. De opkomst van blockchain technologie verliep parallel met de virtuele handel van de Bitcoin op de beurs en wordt daarmee vaak vereenzelvigd. De voordelen van de toepassing achter de virtuele muntenhandel van de Bitcoin en andere crypto-currencies zijn echter niet onopgemerkt gebleven. Blockchain heeft de potentie om een “game changer” te zijn. Dat heeft onder andere te maken met het wegvallen van de noodzaak van trusted third parties. Bovendien kan blockchain voor veel doeleinden worden gebruikt binnen de private- en publieke sector zoals financiële transacties, onroerend goed, goederen, muziek en andere waardevolle assets. Wanneer een organisatie voor haar bedrijfsprocessen gebruikmaakt van blockchain technologie heeft dat direct effect op de informatiehuishouding en interne beheersing van de organisatie. De blockchain is namelijk in feite een chronologische database waarin gegevens worden opgeslagen. Dit betekent dat transacties die eenmaal zijn opgeslagen niet meer kunnen worden aangepast. Adequate preventieve interne beheersingsmaatregelen zijn dan van cruciaal belang.

Er wordt vaak verondersteld dat blockchain een passende oplossing is voor menig maatschappelijk vraagstuk, terwijl traditioneel sprake is van totstandkoming van (monetaire) transacties met tussenkomst van (onafhankelijke) partijen, die een aanzienlijk deel van de transactiekosten veroorzaken. Blockchain kent ook criticasters die de voordelen en nadelen anders beoordelen. Zo zou blockchain in theorie tot gewenste voordelen kunnen leiden, maar wordt de praktische invulling daarvan volgens hen onderschat. Veelgenoemde tegenargumenten op basis van de huidige literatuur zijn bijvoorbeeld:

- de complexiteit van blockchain technologie;
- de twijfel rondom de internationale wet- en regelgeving met het waarborgen van privacy (AVG) zodra persoonsgegevens worden opgenomen in de blockchain;
- het toenemende energieverbruik door additionele transacties in de informatieketen (duurzaamheid);
- het gebrek aan benodigde uniforme infrastructuur en consensus over algoritmen (‘’slimme contracten’’);
- de verwerking van transacties in blockchain duurt lang (seconden);
- de grenzen van opslagtermijnen en opslagcapaciteit komen in zicht doordat data niet verwijderd wordt;
- vraagstukken op het gebied van cybersecurity en privacy.

De toepassing van blockchain kan gepaard gaan met een herontwerp van bedrijfsprocessen en een significante daling van de transactiekosten, omdat tussenpersonen binnen een netwerk worden vervangen door een gedistribueerd grootboeksysteem waarin vastlegging van overeengekomen transacties plaatsvindt. De betrouwbaarheid (integriteit) van deze vastlegging vormt het primaire voordeel binnen het netwerk van samenwerkende partijen.



Bron: EY Global Blockchain Summit 2021

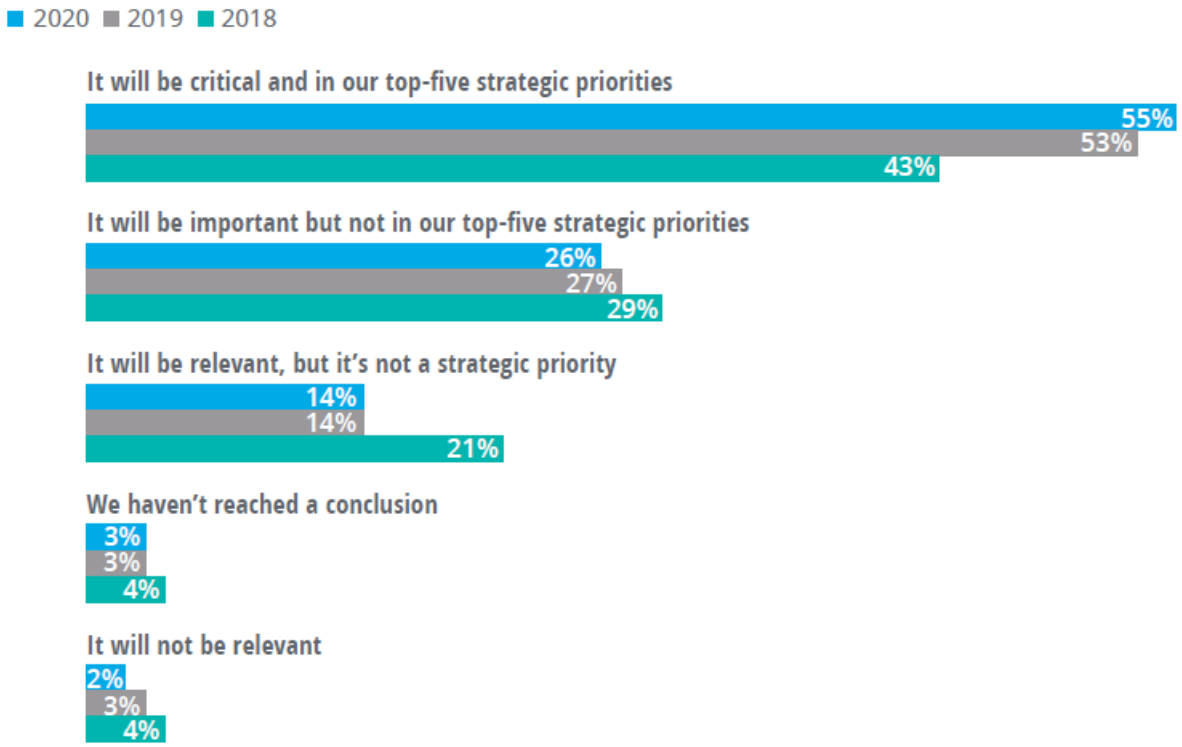
Technologische innovatie, voortschrijdende digitalisering en toename in externe samenwerking hebben vergaande consequenties voor de bedrijfsvoering van organisaties. Deze transformatie in organisatie en technologie gaat allerminst aan de financiële functie voorbij. In de digitale wereld willen de stakeholders zekerheid over de financiële situatie en de informatiehuishouding. De vraag is echter of de accountant voldoende digitaal onderlegd is om in de nabije toekomst zich een oordeel te vormen over de financiële situatie en de interne beheersing van de organisatie. Het vooraf programmeerbare en onweerlegbare karakter van blockchain maakt het mogelijk om de wereld van accountancy en accounting te innoveren. Blockchain zal naar verwachting processen en systemen efficiënter en transparanter maken met minder bureaucratie en control- en verantwoordingssystemen.

While blockchain was once classified as a technology experiment, it now represents a true agent of change that is affecting the entire organization.

Bron: Deloitte's Global Blockchain Survey 2020

De invoering van blockchain werkt disruptief en doorbreekt de status quo. Het opent nieuwe markten en doorbreekt de posities van tussenpersonen. Idealiter zijn er bijna geen menselijke handelingen meer nodig voor de verwerking van transacties en is de planning- en control cyclus met al zijn rapportages en formats anders en wellicht gedeeltelijk overbodig. De vraag hierbij is of het object van de controle gaat veranderen, of dat slechts de wijze van controleren anders wordt, of een combinatie van beiden. In de bestudeerde literatuur worden hier geen specifieke uitspraken over gedaan.

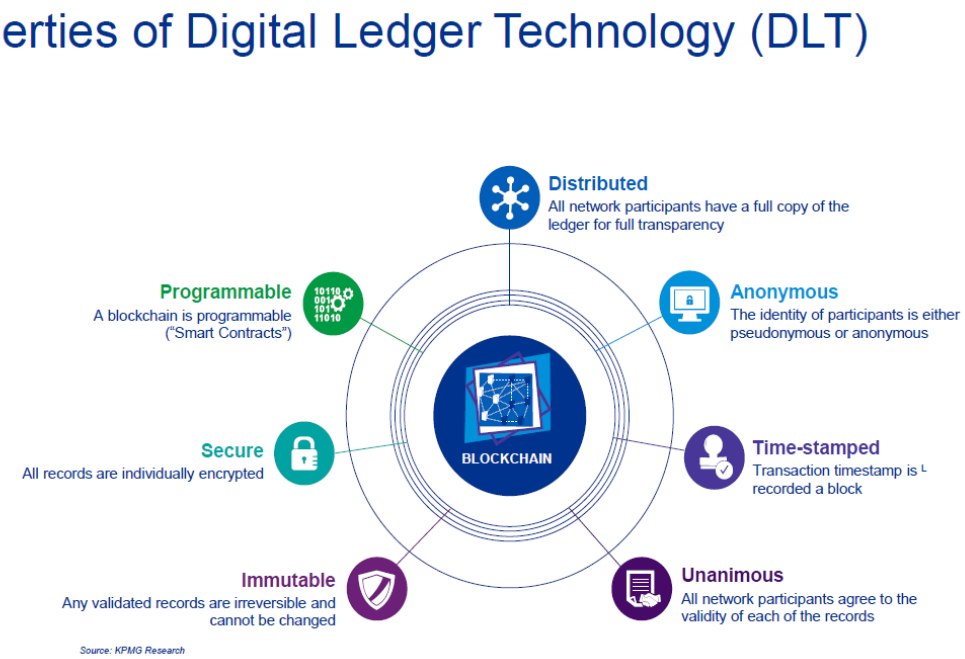
Het Blockchain Control Framework, onderwerp van deze verkenning door de Kennisgroep Keteninformatiemanagement, beoogt met de kennis van bedrijfsprocessen en technische randvoorwaarden van blockchain systemen een antwoord te geven op de vraag welke beheersmaatregelen vanuit het perspectief van auditing noodzakelijk zijn om met een redelijke mate van zekerheid assurance te kunnen verstrekken. Hierbij zullen ook observaties worden betrokken van de voortgang van blockchain projecten en welke risicogebieden hierin worden ervaren met betrekking tot processen en informatiesystemen. Dit zal inzicht verschaffen in de af te dekken risico's en derhalve in de benodigde beheersmaatregelen om een blockchain toepassing succesvol te benutten.



Bron: Deloitte's Global Blockchain Survey, 2020.

2 Blockchain in kort bestek

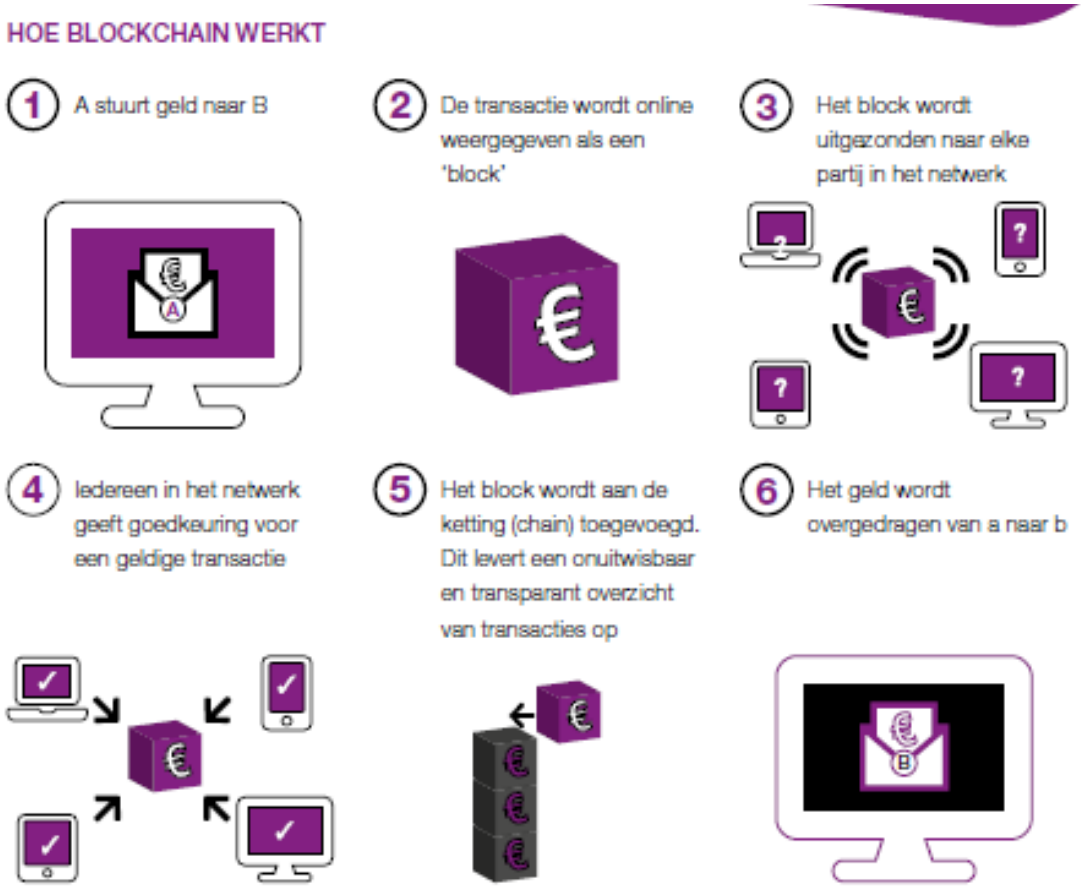
Kort gezegd is een blockchain een keten van data-elementen, ook wel blokken genoemd, in volgorde van totstandkoming. De blockchain is een gedistribueerde database die permanente, transparante en integere opslag van data beoogt te waarborgen. De datastructuur is te vergelijken met een grootboek, waarbij minimaal twee partijen betrokken zijn bij de vastlegging van gegevens binnen een geautoriseerd ''peer-to-peer'' netwerk. De blockchain kenmerkt zich in de basis als een open en decentraal netwerk waarin gegevensmutaties door de betrokken partijen integraal worden bijgehouden zonder tussenkomst van derden. Het garanderen van onderling vertrouwen vormt de essentie van de blockchaintechnologie.



Bron: KPMG Research, 2021

Een blockchain is het beste te vergelijken met een spreadsheet die ergens in de cloud staat. Het bestand wordt met meerdere mensen gedeeld die er in kunnen werken en tegelijkertijd ook wijzigingen van anderen kunnen zien. Men werkt dus altijd in de laatste, up-to-date versie. De blockchain is vergelijkbaar; het is een gedeeld register van transacties dat door iedereen kan worden ingezien. Het register van transacties is georganiseerd in een chronologische keten van blokken. Nieuwe transacties worden vrijwel real-time opgenomen in een nieuw blok en worden daarmee onomkeerbaar. Het valideren van de transacties gebeurt niet op één centrale plek, maar op een netwerk van computers. Iedere transactie wordt door het netwerk gecontroleerd. Als bij een transactie iets niet klopt, dan keurt het netwerk de transactie af en wordt deze niet opgenomen in een blok. De "frauduleuze" transactie gaat dan niet door.

Dit betekent ook dat een blockchain netwerk niet centraal wordt beheerd, maar dat alle deelnemers een gezamenlijke verantwoordelijkheid dragen. Er bestaat dus geen centrale autoriteit, waar dit in een normale database wel het geval is. Het is een gedistribueerd netwerk waar alle deelnemers van het netwerk het eigendom gelijk verdelen, de distributed general ledger.



Bron: Onguard Fintech Barometer, 2018

Blockchain als technologie is te waardevol om door organisaties te worden genegeerd. De voordelen van blockchain zijn grofweg te categoriseren naar drie domeinen die aansluiten op de definitie van de blockchain: permanentie, transparantie en integriteit.

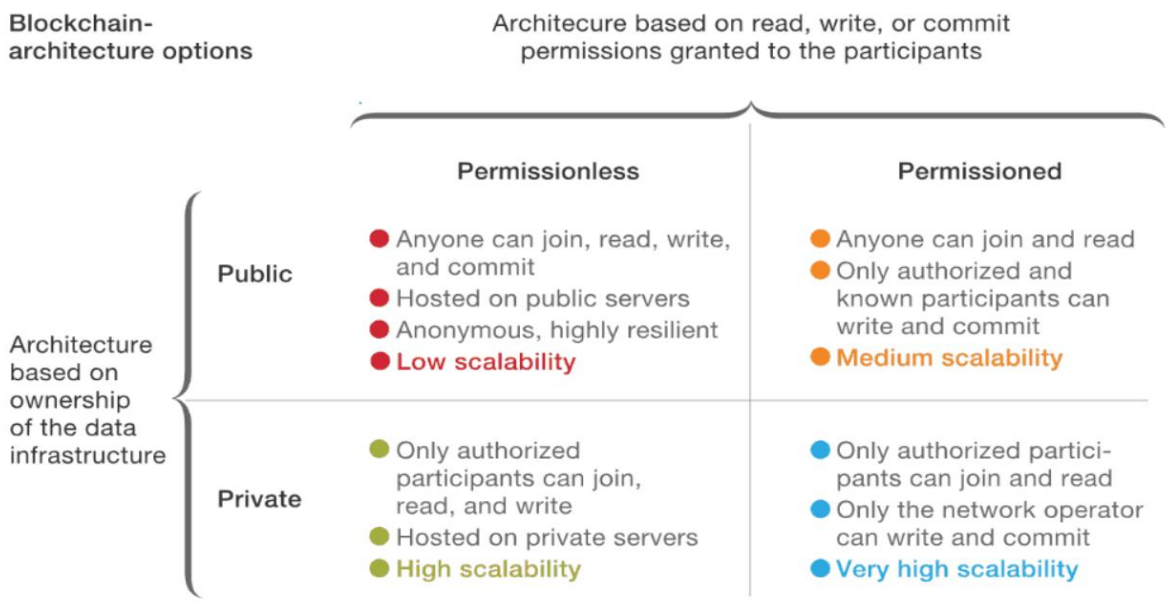
Blockchain heeft de potentie om diverse processen te transformeren. Dat heeft onder andere te maken met het wegvallen van de noodzaak van tussenkomst van derde partijen en tussenpersonen. Bij transacties in de huidige businessmodellen is er sprake van 'dure' derde partijen die benodigd zijn om de transactie te valideren. Deze derde partijen vallen met de toepassing van blockchain technologie weg. De onveranderlijkheid van blockchain zou de betrouwbaarheid van gegevens en tegenpartijen met verminderde kans op fraude vergroten, waardoor het vertrouwen toeneemt. Twee zakelijke partijen die transacties uitvoeren, hoeven niet meer hun eigen gegevens van de transactie bij te houden en gebruiken in plaats daarvan de blockchain als enige bron van waarheid. Blockchain biedt derhalve kansen voor procesefficiëntie en draagt ook zorg voor betere beveiliging. Vertrouwen speelt een belangrijke rol.

Public en private netwerken

Blockchain kan worden toegepast in twee type omgevingen: public en private. De keuze voor een type omgeving is afhankelijk van de casus en aard van processen. De public blockchain kenmerkt zich door een open netwerk dat voor eenieder toegankelijk is. Het publiek, zijnde de betrokken partijen, hoeft daarvoor niet te voldoen aan voorwaardelijke mechanismen om toegang te verkrijgen tot de transactieketen. Integendeel, de public blockchain staat juist open voor zoveel mogelijk toetreders. Dit heeft een positieve invloed op de te waarborgen betrouwbaarheid van de data in de blockchain. Een bekende toepassing die gebruikmaakt van de public blockchain technologie is de Bitcoin.

Een private blockchain is uitsluitend beperkt tot daartoe bevoegde partijen die veelal een schakel vormen binnen het proces waaruit de transacties voortvloeien. Doordat er restricties zijn gelegd op het aantal toetreders tot de private blockchain worden de security risico's eveneens verlaagd. Daarnaast verlopen het besluitvormings- en transactieproces binnen de blockchain hierdoor inherent efficiënter ten opzichte van een public blockchain. Het realiseren van een snellere transactieverwerking vormt een relevant argument in het voordeel van het hanteren van een private blockchain.

Doordat binnen een private blockchain restricties worden gedefinieerd op basis waarvan de blockchain uitgaat dat sprake is van geautoriseerde toegang tot de opgeslagen informatie, suggereert dit het bestaan van een centrale autoriteit en/of centraal punt die naleving van de gemaakte afspraken nagaat. Hoewel de onafhankelijkheid van een centrale autoriteit typerend is voor het gebruik van de blockchain in het algemeen, lijkt de private blockchain per definitie niet te ontkomen aan dit fenomeen. Als zodanig kan dit eveneens als relatief nadeel, in ieder geval ten opzichte van public blockchain, worden beschouwd. Dit kan worden gerelativeerd door de eveneens noodzakelijke aanwezigheid van een autoriteit in andere decentrale datagedreven omgevingen.

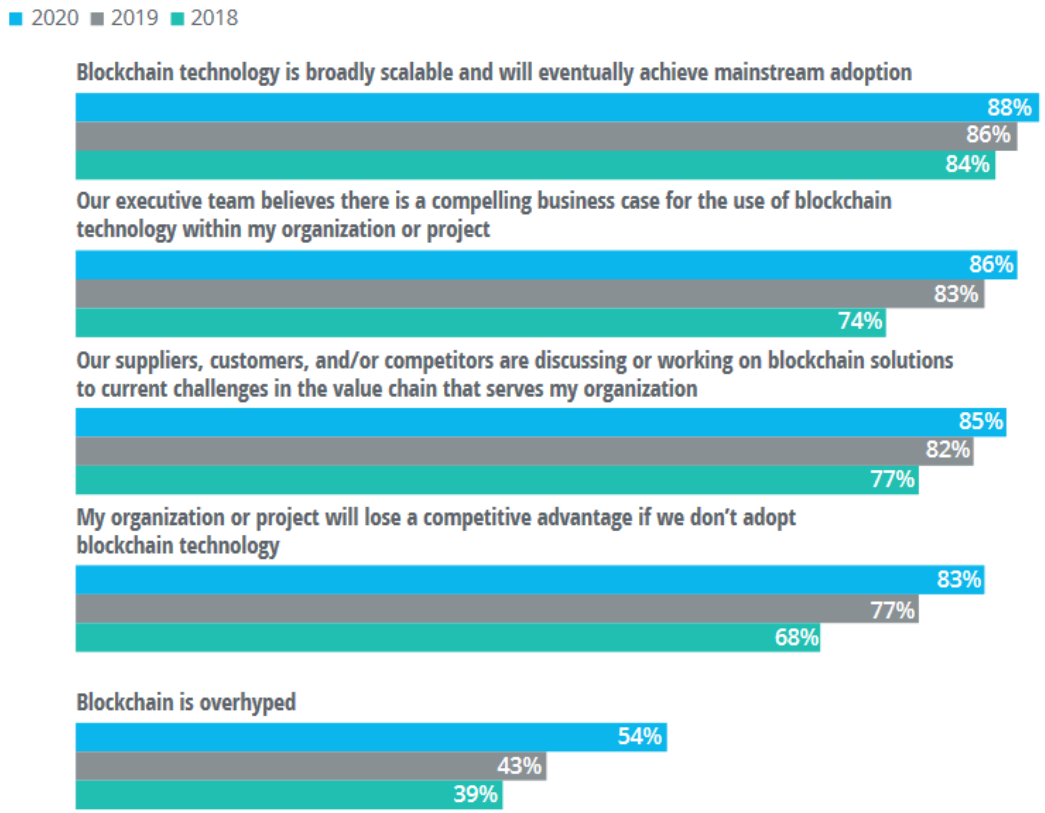


Bron: McKinsey & Company

Het onderscheid tussen 'public' en 'private' aan de ene kant en 'permissioned' en 'permissionless', wel of niet beperkt toegankelijk, aan de andere kant, dient slechts als startpunt voor het ontwerp van de gedistribueerde grootboeken. Het is van belang voor de inrichting van de bedrijfsprocessen en voor de interne beheersing van organisaties om rekening te houden met de classificatie van de blockchain die een organisatie gebruikt. Afhankelijk van het op te lossen vraagstuk zal de organisatie een keuze moeten maken. Een hybride versie is ook mogelijk, namelijk een combinatie van één of meer gedistribueerde grootboeken.

Relevant voor de beroepsuitoefening van accountants, controllers en IT-auditors is de private blockchain. Deze vertegenwoordigt ten opzichte van de public blockchain meer maatwerk en is meer toegespitst op de organisaties waarin deze wordt toegepast en op de processen waarin de blockchain een vertrouwensfunctie dient te vervullen met betrekking tot opgeslagen informatie. Een primair verschil met de public blockchain is de benodigde autorisatie om toegang te krijgen tot de private blockchain. Er bestaat dus een bestuurlijke hiërarchie. Dit houdt per definitie in, dat authenticatiemechanismen moeten worden gedefinieerd om toegang tot de vastgelegde transacties in de private blockchain te normeren.

Bij transacties in de huidige businessmodellen is sprake van derde partijen die benodigd zijn om een transactie te valideren. Deze derde partijen vallen met de introductie van blockchain technologie weg. De onveranderlijkheid van blockchain zou de betrouwbaarheid van gegevens en tegenpartijen vergroten, waardoor het vertrouwen toeneemt. Twee zakelijke partijen die transacties uitvoeren, hoeven niet meer hun eigen gegevens van de transactie bij te houden en zouden in plaats daarvan de blockchain gebruiken als enige bron van waarheid. Blockchain biedt derhalve voordelen voor procesefficiëntie en draagt ook zorg voor betere beveiliging. Het vertrouwen komt vanuit het systeem in plaats vanuit de tussenpersoon.

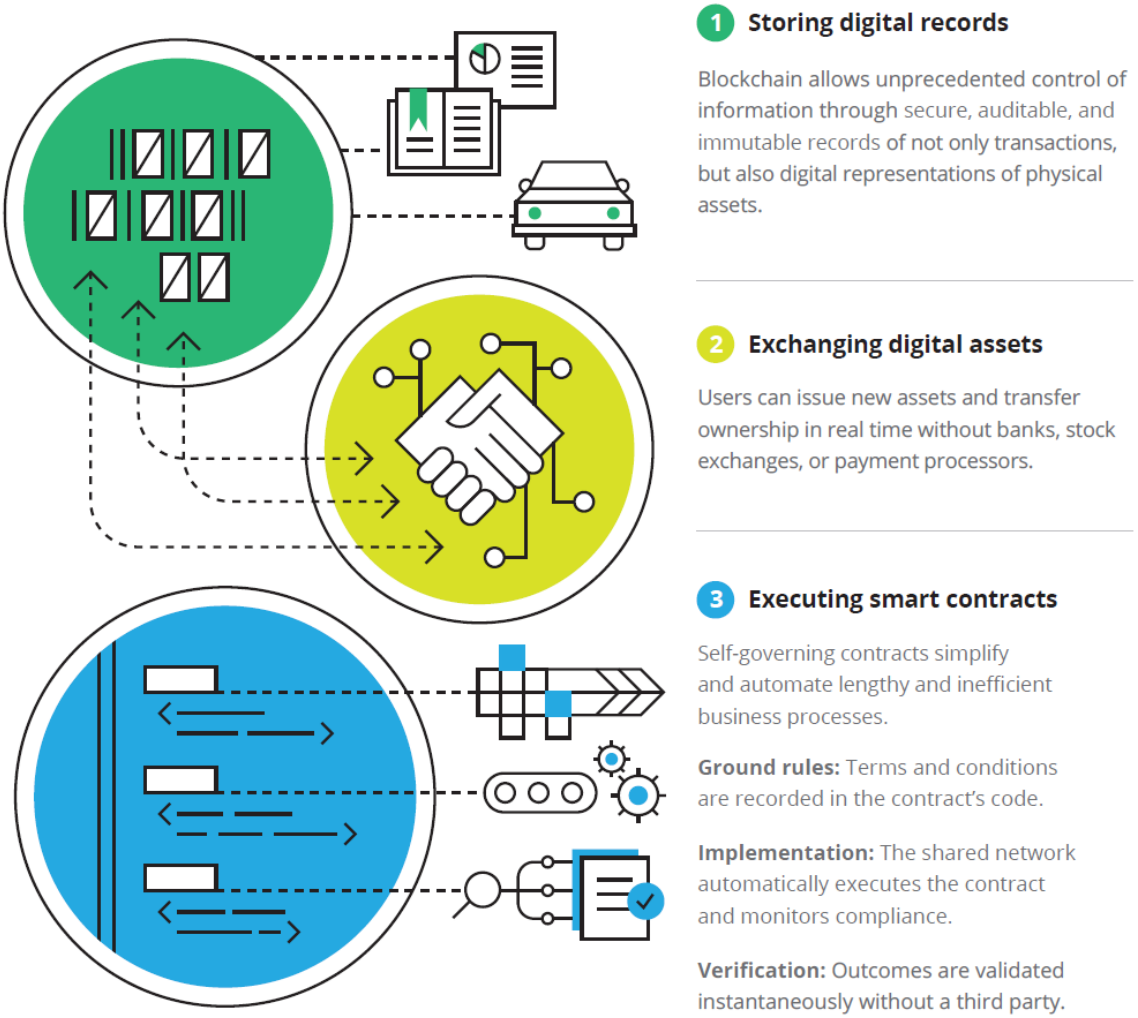


Bron: Deloitte 2020 Global Blockchain Survey

Three levels of Blockchain

Naarmate de behoefte aan draagbare, beheersbare digitale identiteiten groeit, kunnen organisaties blockchain technologie op hoofdlijnen toepassen voor de volgende drie doeleinden die ook wel de 'three levels of Blockchain' worden genoemd:

1. Opslaan van digitale transacties en digitale representatie van fysieke activa
2. Uitwisseling van digitale gegevens en geleverd met gebruiksrecht
3. Geautomatiseerd transactieprotocol (script) dat de voorwaarden van een contract uitvoert



In bovenstaand overzicht worden drie niveaus van toepassing van blockchain genoemd. Niet alleen verschillen deze van functionaliteit, ook de impact op de accountantscontrole en de benodigde IT-audit neemt sterk toe. Op het eerste niveau komen nieuwe techniek en werkwijzen die aandacht behoeven. Op het derde niveau kan zelfs de hele aanpak van de accountants-controle door bijv. frauderisico tot heroverweging leiden. Dit zal het geval zijn wanneer vastgoed- en andere grote financiële transacties onomkeerbaar met smart contracts afgewikkeld gaan worden. In de volgende tabel wordt als voorbeeld een inschatting gegeven van de impact op de accountantscontrole en IT-audit.

Inschatting impact Blockchain op verschillende niveaus					
Blockchain niveau			**Impact op IT-audit**		**Impact op financial audit**
1	Opslaan van digitale transacties en digitale representatie van fysieke activa		Beperkt, IT-auditor moet zich nieuwe techniek toe-eigenen		Beperkt, accountant moet zich bewust zijn van nieuwe risico's
2	Uitwisseling van digitale gegevens en geleverd met gebruiksrecht		Stevig, de impact van de uitwisseling en de gebruikte technische voorzieningen moet worden beoordeeld		Gemiddeld, de accountant moet de risico's kennen en vertrouwen op de door de IT-auditor beoordeelde voorzieningen en beheersmaatregelen
3	Geautomatiseerd transactieprotocol (script) dat de voorwaarden van een contract uitvoert		Hoog, IT-auditor moet volledig nieuwe audit uitvoeren op basis van risico analyse		Hoog tot zeer hoog. Naast impact op de auditaanpak, moet de accountant de risico's op fraude beoordelen t.o.v. het bedrijfsprofiel en de -typologie.

Bron: ICTU, Ruud Mollema, 2021

Smart contracts worden gebruikt om proceshandelingen te automatiseren aan de hand van voorgeprogrammeerde condities. De condities betreffen de voorwaarden, oftewel de business rules set, waaraan moet worden voldaan voordat de transacties tussen partijen worden voltooid. Deze smart contracts zijn niet per definitie gebaseerd op blockchain-technologie, maar de ontwikkelingen rondom de blockchain leiden wel tot toenemende interesse in smart contracts gezien de onderscheidende attributen van de blockchain technologie. Zij kunnen worden geprogrammeerd op de blockchain waardoor deze contractuele transacties binnen de blockchain worden geautomatiseerd. Hierdoor zijn permanentie, transparantie en integriteit gewaarborgd.

Wel dient hierbij rekening te worden gehouden dat op blockchain gebaseerde smart contracts zichtbaar zijn voor alle deelnemers in de blockchain. Deze smart contracts zijn kwetsbaar indien deze niet goed gecodeerd zijn. Dit kan leiden tot de situatie dat software bugs dus ook merkbaar en zichtbaar zijn, terwijl hiervoor niet altijd meteen een oplossing beschikbaar is. Er kunnen dus security holes in de codering van smart contracts zitten, waardoor mogelijke security breaches kunnen ontstaan. Ook hier kan vertrouwen een belangrijke rol spelen.

Het proces waarin smart contracts met name van toegevoegde waarde zijn betreft de waardeoverdracht. In de praktijk kan sprake zijn van meerdere te doorlopen processtappen voordat een waardeoverdracht kan worden gefinaliseerd tussen bijvoorbeeld twee partijen. Hierbij zal veelal eveneens sprake zijn van een te verrichten (tegen-)prestatie door de betrokken partijen. Door de benodigde processtappen en prestaties te programmeren kan een derde, onafhankelijke partij onnodig worden gemaakt. Het vervolgens elimineren van deze derde partij door smart contracts zou als een waardevolle toevoeging aan de blockchain kunnen worden beschouwd, met name als het gaat om het afdwingen van een vertrouwensrelatie tussen partijen die met elkaar transacties uitwisselen.

Het consensus protocol vormt de basis van de blockchain technologie en gaat uit van minimale voorwaarden om de werking van blockchaintechnologie te garanderen. In feite zijn deze voorwaarden te beschouwen als preventieve, voorgeprogrammeerde maatregelen. Doordat deze minimale voorwaarden, praktisch en technisch gezien, niet altijd kunnen worden gegarandeerd, brengen deze per definitie risico's met zich mee welke in ogenschouw moeten worden genomen bij gebruik en risicobeheersing van de blockchain.

Een goed systeem van interne beheersing biedt veel voordelen voor een organisatie. Zo geeft het vertrouwen aan het management en de medewerkers dat de doeleinden worden behaald. Het geeft aan hoe de organisatie functioneert en het helpt verrassingen te voorkomen. Zodra een organisatie gebruik maakt van de blockchain technologie voor haar bedrijfsprocessen, heeft dat direct effect op de interne beheersing van de organisatie.

3 Externe organisatie en platformeconomie

Platformeconomie en samenwerking

In de huidige platformeconomie maken organisaties in bedrijfsleven en publieke sector deel uit van een ecosysteem. Het succes van deze ecosystemen en netwerkorganisaties wordt mede bepaald door het vermogen tot samenwerking met netwerkpartners zoals afnemers, toeleveranciers, kennisinstellingen en personen. Netwerkpartijen hanteren veelal intensieve gegevensuitwisseling, maken hierbij gebruik van digitale systemen en functioneren in allianties. Zij zijn met elkaar verbonden via informatieketens en hebben met elkaar verenigbare doelen. Door samenwerking en door communicatie in ketens en netwerken is het geheel hierdoor meer dan de som der delen.

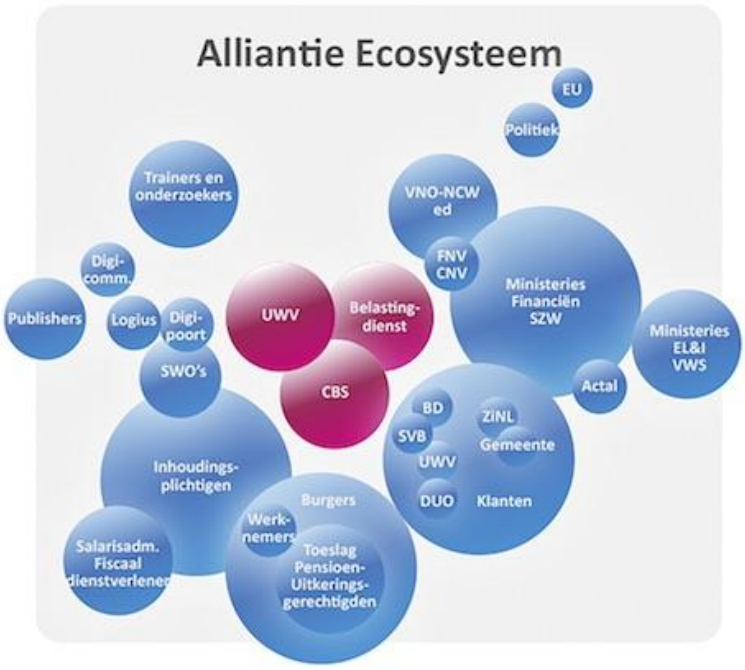
Een dergelijke extended enterprise is een uitgestrekt weefsel van relaties, waarbij alle niveaus en functiegebieden zijn betrokken en waarin de interne en externe grenzen vervagen. Deze nieuwe vorm van organisatiestructuur, externe organisatie en integratie, is niet simpelweg een schepping van procesgerichte organisaties die hun bedrijfsprocessen horizontaal hebben gemaakt om zodoende kosten te besparen en sneller te kunnen reageren. Het heeft voornamelijk te maken met een fundamentele heroverweging van de aard en het functioneren van organisaties en van de relaties tussen organisaties en personen.

> Blockchains will do for networks of enterprises and business ecosystems what ERP did for the single company.

Processen en systemen, die specifiek ontworpen zijn om traditionele grenzen van een organisatie te overschrijden, zullen een groeiend onderdeel van de digitale economie en informatiesamenleving uitmaken. De ontwikkeling naar crossovers, veelal via dataplatforms, is gericht op integratie van processen en systemen op organisatie-overstijgend niveau.

Digitale connectie tussen ketenpartners

Organisaties maken deel uit van een netwerk met andere organisaties. Om mee te kunnen in de snelle technologische ontwikkeling en in de innovatie van producten en diensten zijn vaak competenties nodig die men niet zelf in huis heeft of waarvoor de benodigde (financiële) middelen ontbreken. En steeds meer vindt de concurrentie plaats op het niveau van samengestelde producten en diensten. Afnemers vragen om een geïntegreerd pakket van zakelijke of publieke dienstverlening dat niet door één organisatie te leveren is. In onze huidige economie krijgt concurrentie het karakter van een strijd tussen clusters van ondernemingen.



Bron: Loonaangifteketen 2018

Maatschappelijke uitvoeringsketens, zoals bijvoorbeeld zorg, sociaal domein, politie en justitie, worden steeds belangrijker door voortschrijdende specialisatie, toenemende afhankelijkheden, hogere maatschappelijke eisen en toenemende interactie en samenwerking. Daarnaast ontstaan betere ketenprestaties en privacybevordering door de stroomlijning van informatie-uitwisseling.

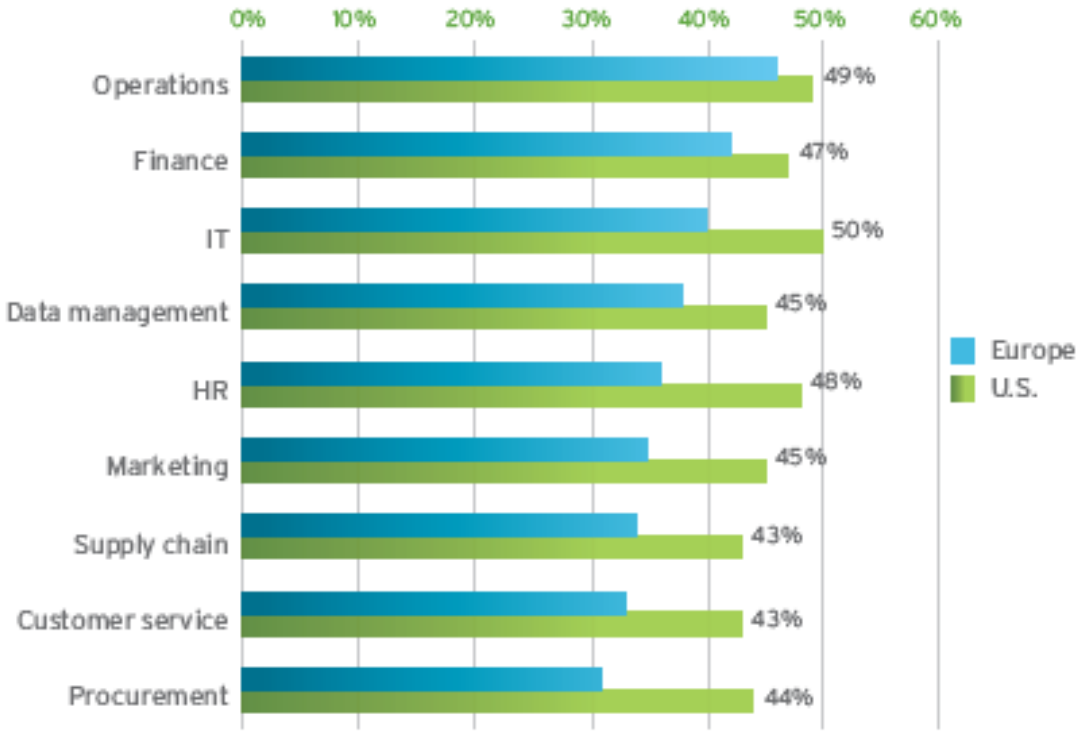
Met de toenemende populariteit van dergelijke allianties ontstaat ook een nieuw terrein van besturing: besturen over de grenzen van de organisatie heen. Met als meest wezenlijke verschillen met de traditionele ondernemingsbesturing het ontbreken van volledige controle en van een centrale autoriteit die de doorslag kan geven bij besluitvorming. Besturing vindt plaats in gezamenlijkheid; netwerkpartners met mogelijk verschillende belangen moeten gezamenlijk beslissingen nemen.

Digitalisering maakt in toenemende mate virtuele integratie van bedrijfsprocessen tussen organisaties onderling mogelijk. Dit geldt in het bijzonder voor organisaties die actief zijn in online consumentenmarkten en die gebruikmaken van moderne digitale markten en -platformen. Vele vormen van publieke dienstverlening door de overheid lenen zich eveneens voor afwikkeling via online webportalen of andere digitale mechanismen. Bij dit proces van digitalisering van informatieproducten en dienstverlening worden de mogelijkheden van digitale connectie beschouwd als een belangrijke drijfveer voor meer klantgerichtheid en efficiëntie.

De infrastructuurbenadering, waarbij gedacht wordt aan het opzetten van voorzieningen voor gezamenlijk gebruik, wordt meer relevant naarmate organisaties IT-afhankelijker worden zoals het geval is bij blockchain. Zodra binnen een ecosysteem een overkoepelend informatiebeleid wordt vastgesteld, dan zal zich dat moeten richten naar de ontwikkeling in de deelnemende organisaties. Het beleid dat daar wordt gevoerd zal in het ecosysteem moeten doorwerken. In

dit geval is een benadering vanuit een digitale informatie-infrastructuur een goed uitgangspunt ter ondersteuning van het “informeren en communiceren” binnen een ecosysteem en met de omgeving. Er is dan sprake van een transformatie naar een ecosysteem met behulp van informatietechnologie, met name door de schaalgrootte van de processen die met IT worden ondersteund.

De bedrijfseconomische gevolgen hiervan zijn in het bijzonder de aanzienlijke investeringen die hiermee gepaard gaan en tegelijkertijd de noodzaak om kapitaalvernietiging zoveel mogelijk te voorkomen.



Bron: Cognizant; Effecten van blockchain op belangrijke bedrijfsprocessen; 2018.

Interconnectie en interoperabiliteit

Interoperabiliteit op basis van standaardisering is een noodzaak voor goede dienstverlening en bedrijfsvoering van de overheid en de efficiencywinst van bedrijven. Formele informatiesystemen met gestructureerde applicaties en data zullen bijvoorbeeld snel worden aangevuld of vervangen door informele informatiesystemen met ongestructureerde data. Collaboratiesystemen, mobiele toepassingen, sociale media en de cloud vormen krachtige instrumenten waarmee informatie een onmiddellijk effect krijgt. De koppeling van ERP systemen van leveranciers en klanten voor het plaatsen van orders, het verzenden van facturen en rekeningen en het bijhouden van de stand van zaken, bespaart organisaties een aanzienlijke hoeveelheid geld in vergelijking met methoden in het verleden. Toch is dit nog maar het prille begin van digitaal zakendoen die de stofwisseling van bedrijfsleven en overheden doet

veranderen, en waardoor de relaties tussen ondernemingen, overheden en samenleving structureel zullen veranderen.

Een stap daarnaast is interoperabiliteit, waarbij tevens steeds meer private blockchain implementaties van de grond komen. Met behulp van interoperabiliteit integreren private en publieke blockchain netwerken en ontwikkelen zich in alliantie-ecosystemen en commerciële platformen. Hierdoor wordt grotere efficiëncy in de ketens en netwerken gerealiseerd, met integratie van bedrijfsvoering en processen met het bijbehorende integrale informatiebeleid en datamanagement.

Vooral in het geval van nieuwe technologie en ecosystemen zullen audit en control een grotere rol gaan spelen, maar ook een ander karakter krijgen. Digitalisering betekent niet alleen dat de communicatie in de keten verandert, maar vooral ook dat meer informatie beschikbaar komt (big data), dat informatie sneller verwerkt kan worden (fast-close) en dat sneller betere analyses gemaakt kunnen worden (business intelligence). Vanuit de heterogeniteit van belangen en achtergronden (network governance en collusion) ontstaat behoefte aan een systematische benadering van het besluitvormingsproces, mede met het oog op doorlooptijd, kosten en beoogde consensusvorming. Alleen langs een soms moeizame weg kan interoperabiliteit tot stand komen.

Bron: Deloitte's 5 Blockchain Trends for 2020, march 2020

Deel 2

4 Audit en control in het ecosysteem

Control en integrale auditing

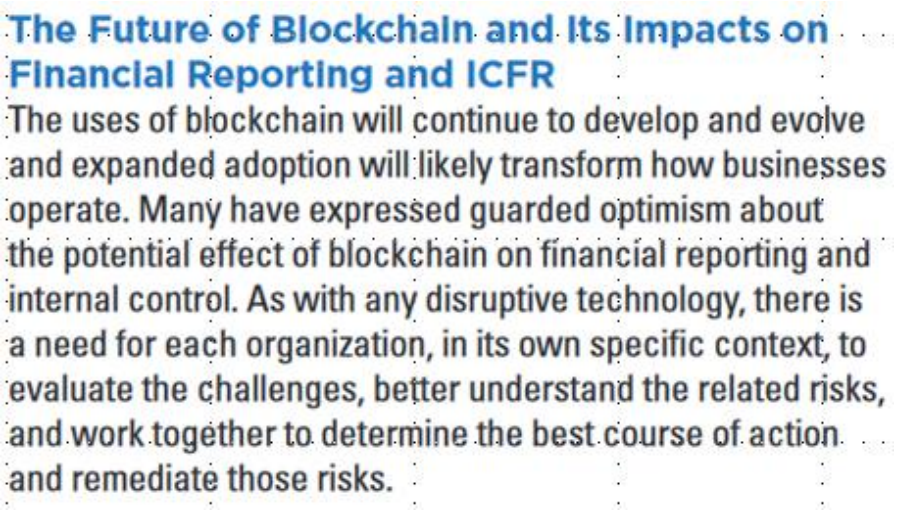
Technologische innovatie en de voortschrijdende digitalisering hebben vergaande consequenties voor de bedrijfsvoering van organisaties. In dit verband zijn drie stadia van technologische ontwikkeling, prominente technologische innovaties te onderscheiden, ieder met eigen consequenties voor het werkveld van de financiële functie: *digitalisering* (waaronder robotisering), *dataficering* (data analytics en big data) en *transformatie* (meer in het bijzonder blockchain). De stadia digitalisering en dataficering omvatten in feite beschikbare technologische innovaties, maar dit geldt niet voor het stadium transformatie en meer in het bijzonder blockchain. In ieder geval niet wat de toepassing betreft in het werkveld van accounting, control en auditing.

Vooral bij nieuwe technologie zoals blockchain en nieuwe organisatievormen zoals ecosystemen zullen audit en control niet alleen een grotere rol spelen, maar ook een ander karakter krijgen. Door een audit in het gehele netwerk of ecosysteem uit te voeren is het mogelijk dat de auditor de partners terugkoppeling geeft over de kwaliteit en risicobeheersing. Daarnaast kan de auditor de netwerkpartners adviseren over maatregelen die getroffen kunnen worden om strategische doelstellingen en risicogebieden af te dekken. Door invulling van zowel de attestfunctie als de adviesfunctie draagt de IT-auditor bij aan het verbeteren van de beheersing van het netwerk en het verschaffen van zekerheden.

Een netwerkaudit beziet het totale ecosysteem en kijkt dus over organisatiegrenzen heen. Dit zorgt tegelijkertijd voor de toegevoegde waarde van een netwerkaudit, aangezien belangrijke risico's veelal op de grensvlakken van organisaties liggen. Vaak wordt een netwerk niet als geheel maar per afzonderlijke schakel (deelnemende partner) bestuurd en beheerst. Voor zover het netwerk wél als geheel wordt bestuurd, ontbreekt meestal de beheersing via onafhankelijke toetsen tijdens en na afloop van het netwerkproces.

Een netwerkaudit is moeilijk uitvoerbaar omdat elke zelfstandige partner eigen toetsingsnormen heeft. Bovendien hangt de belangstelling voor audits af van hoe tegen een audit wordt aangekeken. Een netwerkaudit is hierdoor nog steeds een onbekend en onbemind fenomeen; netwerken zouden te ingewikkeld zijn om te auditen. Hierbij neemt de kans namelijk toe op specifieke auditproblemen, zoals: de scope van de audit is te groot en moeilijk af te bakenen, het aantal betrokkenen is te groot, de bestuurlijke verhoudingen zijn niet helder gedefinieerd en de belangen van de betrokkenen zijn verstrengeld.

Een efficiënt blockchain netwerk is gebaat bij digitalisering van de gegevensuitwisseling tegen zo laag mogelijke kosten, bezien over het gehele ecosysteem en dus zonder suboptimalisering. De realisatie van blockchain netwerken, het zijn in feite interorganisationele communicatie-stelsels en dataplatforms geworden, heeft vaak ingrijpende gevolgen. De dynamieken in allianties en nieuwe technologie zoals blockchain leiden tot forse potentiële groeigebieden voor de uitwisseling van allerlei data en de uitbreiding met andere transactiestromen. En dit alles in combinatie met privacy en security compliance.



Bron: COSO Blockchain and Internal control, july 2020

Voor een betrouwbare blockchain zullen verschillende aspecten binnen de administratieve organisatie geregeld moeten worden. Een adequate IT-omgeving voor de aangesloten organisaties in de blockchain is cruciaal. Thema's zoals cyber security, data protectie, cloud architectuur, risicomanagement en IT governance worden alleen maar belangrijker. Te denken valt ook aan procedures voor de distributie en het veilig opslaan van cryptografische sleutels, waarmee toegang tot de blockchain gekregen kan worden. Daarnaast moet ook zekerheid bestaan dat geen ongewenste nodes worden aangesloten op de blockchain. Om deze risico's te beheersen dienen duidelijke afspraken in de vorm van smart contracts met de deelnemers gemaakt te worden (certificering), zodat de IT-omgeving per deelnemer veilig is en dat verplichtingen duidelijk zijn bij eventuele incidenten. Hierbij kan ook de daartoe bevoegde centrale autoriteit nodig zijn die daarop toeziet.

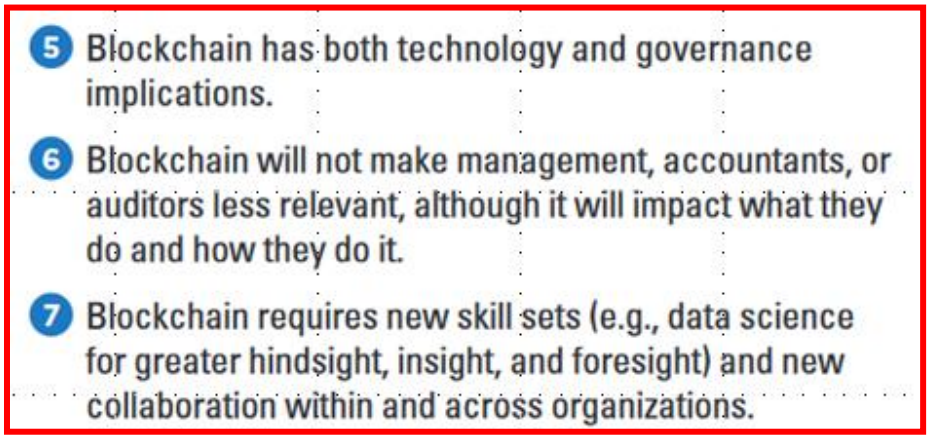
From	To
Double entry bookkeeping	Triple entry bookkeeping
Centralised organisations with central databases	Value chain IT with shared ledgers
Manual transaction entry	Cryptographically secured transactions
Sample testing	Entire population testing
Individual departments recording goods, debtors, creditors, bank accounts	Smart contracts managing flow of goods and money
Audit trail to be documented by auditee	Immutable audit trail outside organisation
Physical assets	Tokenised assets
Once a quarter / year reporting	Continuous reporting possible
Financial audit with IT component	IT audit with financial audit component

Bron: KPMG, 2018

Niet de interne organisatie en inrichting, maar de context wordt hierdoor meer bepalend voor de zekerheden die gezocht worden. Professional judgement en principle based auditing vormen hierbij eerder een solide uitgangspunt dan de gangbare, meer operationele normenkaders en procedures. Integrale auditing in netwerken maakt een betere verschaffing van zekerheden en een betere samenwerking binnen netwerken mogelijk. Bovendien wordt de informatie-voorziening over het functioneren van het netwerk als geheel versterkt. Dit heeft geleid tot de noodzaak tot een herindeling en doorontwikkeling van integrale auditing.

Blockchain assurance

Blockchain gaat de administratieve organisatie niet vervangen, maar leidt tot andere accenten in de beheersing van (IT)- risico's en de vastlegging en inrichting van de administratieve en operationele processen. Blockchain zal leiden tot een andere wijze van kijken naar de beheersing van risico's en de vastlegging en inrichting van processen. De noodzaak voor een goede administratieve organisatie en interne controle (AO/IB) blijft bestaan, waarbij het zwaartepunt zal gaan verschuiven van handmatige controles naar nog meer geautomatiseerde en functioneel geïntegreerde controles. Uitwisseling van gegevens is volledig geïntegreerd in de informatie-systemen en is daardoor niet meer op zichzelf zichtbaar.



Bron: COSO Blockchain and Internal control, july 2020

Het is de vraag of de accountant zich voldoende bewust is van de veranderingen in risico's naarmate de samenwerking binnen het ecosysteem (externalisatie en integratie) intensiever wordt en de innovatie in technologie toeneemt. Internet is de basis geworden van nieuwe verdienmodellen, nieuwe processen en nieuwe manieren voor het distribueren van kennis. Uiteindelijk leiden deze ontwikkelingen tot nagenoeg volledig gedigitaliseerde organisaties waarin de processen, informatiesystemen en procedures digitaal zijn geregeld, wellicht zelfs met ingebouwde beheersmaatregelen.

Professor De Man (VU Amsterdam) heeft vanuit het perspectief van alliantiebesturing in het bedrijfsleven onderzoek gedaan. Hij geeft twee benaderingen van besturing weer: control en trust. De controlbenadering definieert kaders en doet dit vooral via formele regels en procedures. Er wordt vanuit gegaan dat mensen uit eigenbelang handelen en dat samenwerkingspartners niet alleen overlappende doelstellingen hebben, maar tegelijkertijd ook een conflicterend belang. Vanuit een controlbenadering wordt vooral gezocht naar waarde-creatie door het delen van kosten en risico's, het scheppen van marktmacht en het optimaliseren van processen door samenwerking. In termen van besturingstechnieken vertaalt de control-benadering zich in een sterke nadruk op strategie, structuren en systemen. In de trust-benadering staat de motivatie om samen te werken centraal. De vraag hierbij is hoe in een alliantie van de onderlinge verschillen gebruik kan worden gemaakt om waarde te creëren en hoe mensen kunnen worden gemotiveerd zoveel mogelijk bij te dragen. De aanname achter de trustbenadering is dat niet zozeer sprake is van mogelijk conflicterende doelen, maar dat door samenwerking juist complementaire doelen kunnen worden bereikt. Binnen een trustbenadering zijn andere besturingstechnieken relevant dan binnen een controlbenadering. Meer dan op systemen ligt de nadruk op gezamenlijke normen en waarden en de opbouw van vertrouwen tussen partners.

Afgezien van de discussie of de ene benadering beter is dan de andere, geldt dat in sommige omstandigheden meer controle-elementen van belang zijn, terwijl in andere situaties de elementen van de trustbenadering meer aandacht verdienen. Nadat de strategische keuze is gemaakt voor een control- of een trustbenadering of een combinatie, kan een gedetailleerd operationeel besturingsmodel en auditmodel worden ontworpen.

Impact op jaarrekeningcontrole en interne beheersing

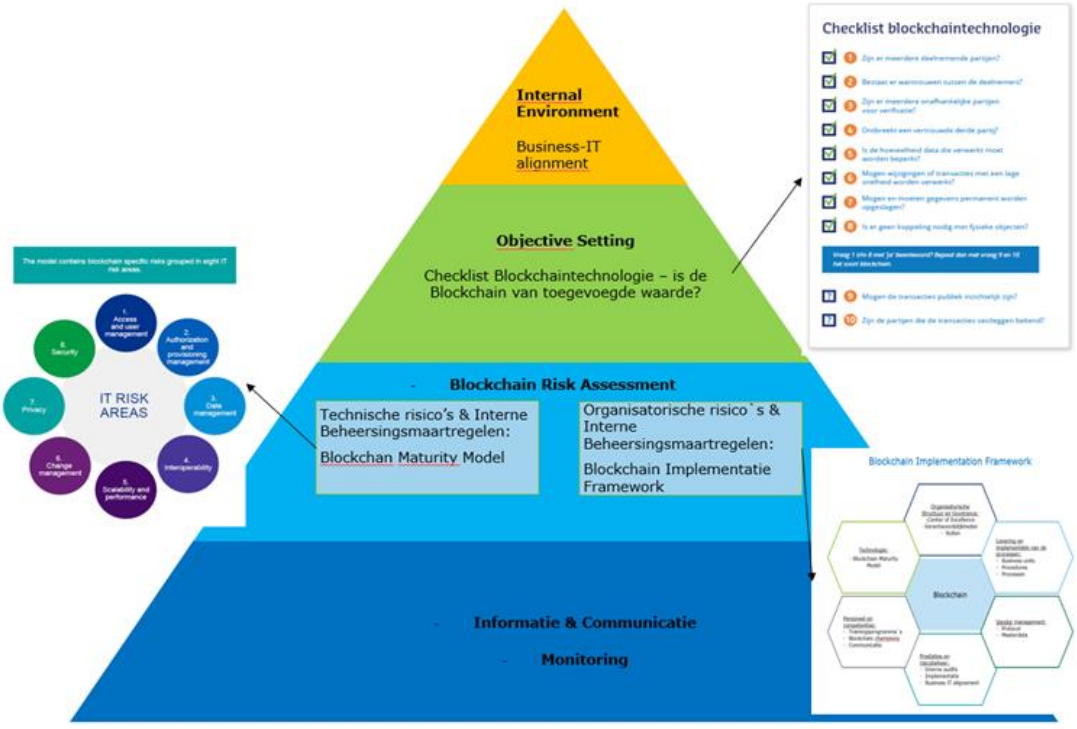
Zodra organisaties gebruikmaken van blockchain technologie in hun bedrijfsprocessen, heeft dit direct effect op de interne beheersing bij die organisaties. Het beheersen van de risico's in een netwerk is een gezamenlijke verantwoordelijkheid van de partners. De verwachting is dat de impact van nieuwe technologie zoals blockchain vernieuwend zal zijn op de jaarrekening-controle en interne beheersing van organisaties. Als organisaties blockchain toepassen in hun veelal externe bedrijfsprocessen, dan zal dit aanzienlijke gevolgen hebben voor de controleren-de en goedkeurende functie, en dus voor IT- en financial auditors. Deze technologische transformatie gaat dus allerminst aan de financiële functie voorbij. De kwaliteitsbewuste IT-auditor en accountant zien ook dat de digitale trends diverse risico's, maar ook kansen met zich meebrengen. Voor financiële managers zijn netwerken van organisaties een betrekkelijk nieuw interessegebied. In de klassieke accountancy en bedrijfseconomie is alle aandacht gericht op de interne beheersing van een organisatie, als middelpunt van de omgeving.

Interne beheersing omvat de systematische maatregelen die door een organisatie zijn ingesteld om:

- haar activiteiten op een ordentelijke en efficiënte manier uit te voeren;
- activa en middelen te beschermen;

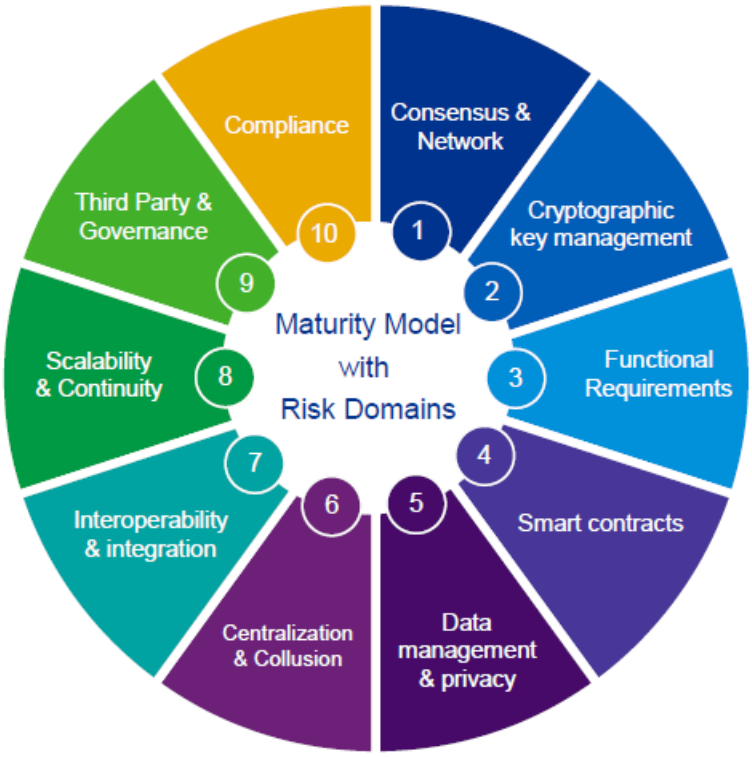
- fouten, fraude en diefstal te ontmoedigen en op te sporen;
- te zorgen voor de juistheid en volledigheid van de boekhoudgegevens;
- betrouwbare en tijdige financiële en managementinformatie te produceren;
- te zorgen voor de naleving van haar beleid en plannen.

De betrouwbaarheid van een blockchain zou idealiter vooraf moeten worden gegarandeerd. Dit kan alleen door de juiste inrichting van de organisatie met betrekking tot de interne beheersing van het bedrijfsproces c.q. de blockchain. Het onderstaande referentiekader als voorbeeld geeft inzicht in de diverse aspecten waar een organisatie rekening mee dient te houden bij het toepassen van blockchain technologie om de betrouwbaarheid van de interne beheersing binnen de bedrijfsprocessen te kunnen waarborgen. Een dergelijk referentiekader mag echter niet worden geïnterpreteerd als compliance-instrument, maar als een model om richting te geven aan de inrichting van de interne beheersing zodra een organisatie gebruik maakt of gaat maken van blockchain technologie binnen haar bedrijfsprocessen. Het algemene beheersingsmodel '*COSO II* of *Enterprise Risk Management Framework* (ERMF), in combinatie met *COBIT 2019*, kan als basis gebruikt worden om de interne beheersing in kaart te brengen en te verbeteren.



Bron: Deloitte 2019; VU referaat Smolders/Van Dijke.

Door de aard van blockchain technologie brengt het implementeren ook nieuwe (specifieke) risico's met zich mee, die niet van toepassing zijn bij traditionele gecentraliseerde systemen. De vraag is dan of de nieuwe blockchain implementatie in control is wanneer het in productie wordt gebracht. KPMG heeft een model ontwikkeld dat helpt om grip te krijgen op de specifieke technische risico's die van toepassing zijn bij de implementatie van blockchain technologie, genaamd het Blockchain Maturity Model.



Bron: KPMG Maturity Model, Compact, 2018

Het KPMG Blockchain Maturity Model geeft een opsomming van een aantal relevante IT risico's onderverdeeld naar verschillende domeinen. De risico's zijn geïdentificeerd op basis van hetgeen voornamelijk in de onderzochte literatuur naar voren is gekomen en zien ook met name toe op het gedistribueerd universeel grootboek. De risico's rondom data management richten zich met name op de kwaliteitscriteria van de data in de blockchain: integriteit, beschikbaarheid en vertrouwelijkheid. Zoals benoemd als onderdeel van interoperabiliteit zal informatie vanuit een organisatie lokaal over moeten gaan naar een gedistribueerd netwerk draaiend op het internet. In geval van (persoons-)gevoelige informatie en de daaraan gerelateerde privacy wetgeving zullen derhalve adequate beheersmaatregelen moeten worden getroffen om ongeautoriseerd toegang en gebruik van deze gegevens te voorkomen. De blockchain steunt bovendien op het consensus protocol mechanisme, waardoor data integer opgeslagen blijft in de blockchain en tevens continu beschikbaar is voor belanghebbenden.

Het doel van het model is om blockchain zo goed mogelijk te implementeren en ook de risico's / interne beheersing in kaart te brengen. Dit om significante kostenbesparingen en efficiency te

kunnen behalen. Het model brengt niet alleen de specifieke risicogebieden en bijbehorende interne beheersingsmaatregelen in kaart, maar het helpt de organisatie ook begrip te krijgen van de volwassenheid na implementatie. De niveaus van volwassenheid worden per risicogebied in kaart gebracht. Deze indeling helpt organisaties om inzicht te krijgen in de gebieden die extra aandacht behoeven. Teneinde de volwassenheid van de blockchain rondom de risicogebieden aan te duiden, wordt bij het Blockchain Maturity Model van KPMG gebruik gemaakt van vijf volwassenheidsniveaus, namelijk:

Level 1: Initial	de Blockchain is onvoorspelbaar, slecht controleerbaar en reactief
Level 2: *Managed*	de Blockchain is vormgegeven voor projecten en is veelal reactief
Level 3: *Defined*	de Blockchain is vormgegeven voor de organisatie in zijn geheel en is pro-actief
Level 4: *Quantitatively managed*	de Blockchain is in control en er wordt goed gemonitord
Level 5: *Optimizing*	de Blockchain is in control, er wordt gemonitord en er vindt verbetering plaats

Afhankelijk op welk niveau organisaties zich bevinden, kunnen de inhoud en intensiteit van risicogebieden verschillend zijn en daarmee ook de beheersmaatregelen. Bijvoorbeeld, de transparante permanente vastlegging van (persoons-)gegevens in de blockchain, waar meerdere partijen inzicht in hebben, heeft nu reeds (AVG) compliance-risico's in het licht van nieuwe wet- en regelgeving op een later moment. Dit betreft één van de voornaamste discussies als het gaat om implementatierisico's met betrekking tot de blockchain.

> Despite the widely recognized benefits of speed and transparency, blockchain technology is still maturing, and there is no generally accepted global regulatory framework in place. This obligates all parties within a blockchain to agree on mutually accepted terms while complying with local laws and regulations.

Bron: Deloitte's Global Blockchain Survey 2020.

5 Blockchain beheersing

Een blockchain netwerk is in feite een gedistribueerd informatiesysteem voor partners in een ecosysteem, dat gepaard gaat met diversiteit in context, belangen en risicogebieden. De IT-auditor wordt hierdoor voor assurance provisioning een ecosysteem auditor.

Inleiding

Bij de diverse referentieprojecten en expertgesprekken is naar voren gekomen dat blockchain implementaties een zeer groot aantal risicogebieden kennen, die relevant zijn voor zowel de interne besturing en beheersing als voor de assurance provisioning door accountants, controllers en IT-auditors. Blockchain pretendeert fraudebestendig te zijn, maar de praktijk heeft inmiddels anders aangetoond. Er zijn diverse gevallen bekend, met name in Azië, waarbij op basis van vervalsingen van digitale eigendomscertificaten grootschalige fraude heeft plaatsgevonden. Dit betekent in feite dat intellectual property rights sterk in waarde kunnen verminderen.

Blockchain technologie kent op zichzelf geen fundamentele verschillen met andere technologieën, maar leidt wel tot serieuze consequenties op andere risicogebieden, zoals network governance en collusion. Naar voren is gekomen dat organisatie en inrichting veelal een grotere rol spelen dan de technologie op zichzelf. Wellicht dat bij de noodzakelijke versterking van de interne beheersing de toepassing van modellen zoals COSO en COBIT nieuwe inzichten kan leveren in het kader van assurance provisioning.

De traditionele audits van informatiesystemen en IT blijven heel waardevol, maar bij blockchain komt assurance vooral te liggen op die risicogebieden die een meer bestuurlijk en interactief karakter hebben, bijvoorbeeld governance, bestuurlijke organisatie, financiering en onderlinge verrekening. Het decentrale karakter van open blockchain netwerken baart hierbij natuurlijk zorgen, doordat er geen hiërarchie bestaat.

Architectuur van Blockchain Control Framework (BCF)

Het is belangrijk om bij het opstellen van de architectuur van het Blockchain Control Framework (BCF) de contouren te bepalen van de audit objecten die relevant zijn voor assurance provisioning bij blockchain netwerken. Bij het BCF wordt uitgegaan van de volgende vier Audit Domeinen (hoofddomeinen), die hierna nader worden beschreven en uitgewerkt:

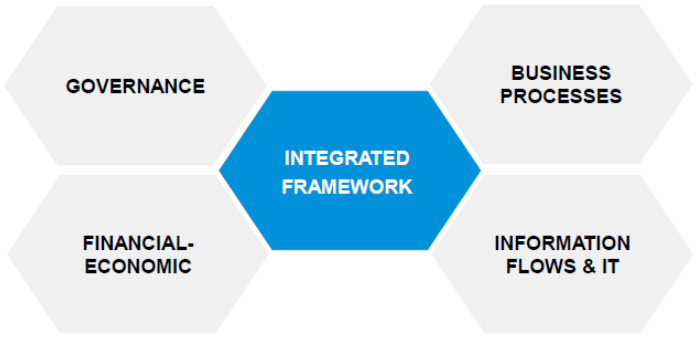
- Governance
- Financieel domein
- Processen domein
- Informatiestromen en IT

Context gebonden factoren

De toepassing van het BCF vereist een multidisciplinaire benadering. Bij de audit dient namelijk rekening te worden gehouden met factoren die traditioneel niet tot het vakgebied van de IT-of financial auditor behoren. De benadering van de IT-auditor wordt minder eenzijdig door een ecosysteem benadering. De IT-auditor stopt niet bij de grenzen van de IT omgeving van de organisatie. Het gaat verder tot de beheersing van het grotere netwerk, consortium en de individuele deelnemers met wie transacties worden uitgevoerd. Het wordt dus een vereiste voor de beroepsgroep dat IT- en financial auditors zichzelf moeten toerusten met de vereiste kennis en vaardigheden voor het auditen van het ecosysteem, en daarbij grensoverschrijdende risicogebieden met controls kunnen vaststellen.

Er zijn drie typen van context gebonden factoren, waarvan de inhoud en intensiteit bepaald worden door de specifieke situatie:

- Welke selectie van risicogebieden met welke controls is toepasbaar en relevant in de specifieke situatie?
- In welke ontwikkelingsfase bevindt zich het specifieke blockchain netwerk? Hierbij wordt het gebruikelijke onderscheid gemaakt in: planning, ontwerp, bouw en beheer.
- Wat is de mate van politieke, bestuurlijke of strategische intensiteit, die een rol speelt bij het verschaffen van zekerheden in een specifieke situatie?



Audit domein	Control doelstelling	Risico ID	Risico-Gebied	Beheers-maatregel	Korte omschrijving
Governance Domein					
Financieel domein					
Processen domein					
IV-IT domein					

Figuur: BCF modelontwikkeling in uitvoering

Audit domeinen en risicogebieden

Bij de uitwerking van de Audit domeinen worden de volgende (multi-disciplinaire) risico-gebieden onderscheiden:

Audit domeinen	Risicogebieden
Governance	• Strategische doelstellingen • Governance & Management • Wetgeving en regelgeving • Bestuurlijke organisatie
Financieel domein	• Financiering investeringen • Verrekening netwerkpartners • Kosten-baten analyse
Processen domein	• Bedrijfsprocessen • Sociaal-organisatorische processen • Marketing & Communicatie
IV & IT domein	• Data Management & Data Architecture • Data Privacy & Security • Interconnectivity • Cryptographic key management • Smart contracts • Centralisation & Collusion • Interoperability & Integration • Scalability & Continuity • Platform standardisation & Migration

Risicogebieden met korte omschrijving

GOVERNANCE	
Strategische doelstellingen	Welke aanleidingen en doelstellingen spelen een rol. Doelstellingen kunnen zowel politiek als strategisch van aard zijn. Naast inzicht in betrokken netwerkpartners dient een belangenanalyse opgesteld te zijn, omdat sprake is van macht en autonomie.
Governance & Management	Structuur en opzet van organisatie en inrichting van zowel bestuurlijk-strategische aansturing als tactisch-operationeel beheer. Noodzaak tot oprichting van bestuursorgaan (governance bij private blockchain netwerk) met autoriteit, mandaat en slagkracht.
Compliance, Wetgeving en regelgeving	Regulering geschiedt door middel van wet- en regelgeving, maar ook door beleidsformulering, standaardisatie en architectuur. De transparante vastlegging van (persoons)gegevens in de blockchain waar meerdere partijen inzicht in hebben kan enorme compliance risico's met zich meebrengen. Dit betreft een van de voornaamste discussies als het gaat om implementatierisico's met betrekking tot de blockchain.
Bestuurlijke organisatie	Structuur met partijen en actoren, rolpatronen, machts- en bestuursverhoudingen en eventuele nieuwe positioneringen als gevolg van nieuwe netwerkpartners en distributiekanalen. Conflictpotentieel kan ontstaan door positieverschuivingen in het netwerk. Resultaten van belangenanalyse dient zichtbaar te zijn in de opzet van organisatie.
FINANCIEEL DOMEIN	
Financiering investeringen	Welke keuze voor financieringsmodel van blockchain netwerk: exogene financiering vanuit begroting, endogene financiering vanuit gebruikersorganisatie of financiering door derden. Budget voor invoeringsproces is omvangrijk en wordt veelal onderschat.
Verrekening netwerkpartners	Welke keuze voor verrekeningsmodel. Dient vooraf opgesteld te worden en consensus bereikt. Verrekening gaat samen met opzetten van tariefstelsel en kortingsstaffels voor specifieke situaties.
Kosten-baten analyse	Kosten-baten analyse is nagenoeg altijd wenselijk, maar ontbreekt veelal als gevolg van complexiteit. Kosten en baten veranderen gaandeweg de ontwikkeling van het blockchain netwerk.
PROCESSEN DOMEIN	
Bedrijfsprocessen	Herontwerp van processen dient vanaf het allereerste begin plaats te vinden in samenhang met veranderingen in organisatiestructuur en in ontwikkeling van blockchain netwerk met diverse toepassingen. Wijzigingen in blockchain processen stellen hogere eisen aan

	kennismanagement. Toepassing van data mining en process redesign, koppeling met ERP systemen.
Sociaal-organisatorische processen	Hebben betrekking op de samenhang tussen enerzijds de invoering van de blockchain netwerk als informatie-infrastructuur en anderzijds de effecten op organisatie en mensen. Per definitie sprake van diverse partijen met verschillende culturen, achtergronden en belangen. Vereist derhalve een formele overlegstructuur. Vereist een incrementeel proces van communicatie. Partners deelname, marketing en voorlichting zijn continu noodzakelijk voor het verkrijgen van consensus en draagvlak.
Marketing & Communicatie	Professioneel proces van ontwikkeling en invoering verhoogt de kans op een succesvolle implementatie en vermindert conflict- en weerstandspotentieel. Marketing en communicatie zijn van levensbelang. Instrumenten zijn onder meer workshops, voortgangsrapportages en tussentijdse reviews.
IV & IT DOMEIN	
Data Management & Privacy	Ieder transactievoorstel wordt als definitief beschouwd. Onjuist, niet volledig of zelfs niet goedgekeurde transacties kunnen resulteren in ongewenste gevolgen zoals inbreuk op data integriteit of privacy voorwaarden doordat persoonlijke gegevens toegankelijk zijn gemaakt. Gevoelige persoonlijke gegevens kunnen niet direct in de blockchain worden opgenomen, maar wel in een parallelle blockchain op een andere locatie. Deze informatie kan desgewenst verwijderd worden. Hoewel de blockchain uitgaat van een werkende consensus protocol is er altijd nog een risico aanwezig dat de actoren rondom integriteit en consensusmechanismen niet werken, bijvoorbeeld als gevolg van ontoereikende beveiligingsmaatregelen op het niveau van de back-end (programmatuur). Omvat tevens maatregelen op het gebied van toegangsbeveiliging en functiescheiding.
Interconnectivity & Interoperability	Met de komst van blockchain kan interoperabiliteit tussen verschillende technologische generaties een uitdaging vormen. Interoperabiliteit vormt voornamelijk een risico binnen implementatietrajecten omtrent de blockchain. Het gerelateerd risico vloeit voort uit een gebrek aan aansluitingen tussen de (moderne) blockchain en de legacy IT systemen binnen een organisatie. De risico's worden zwaarwegender op het moment dat de organisatie een interface dient te realiseren vanuit een lokaal netwerk naar een blockchainnetwerk functionerend op het internet.
Cryptographic key management	Blockchains gebruiken cryptografische functies zoals hashing algoritmen en public key cryptografie om zodoende de integriteit en beveiliging van systemen te garanderen. Onzorgvuldig cryptografisch key management kan leiden tot niet goedgekeurde toegang tot systemen.
Smart contracts	Smart contracts zijn afspraken tussen blockchain deelnemers die zijn vastgelegd in het gedistribueerde grootboek. Het smart contract wordt

	als script automatisch uitgevoerd zodra voldaan is aan de overeengekomen voorwaarden. Indien smart contracts niet correct zijn overeengekomen en vastgelegd, kan dit leiden tot ongewenste gevolgen.
Centralisation & Collusion	Een blockchain bestaat uit onafhankelijke blokken en nodes, die zelfstandig functioneren. De nodes behoren tot een enkele organisatie of een consortium van organisaties. Concurrenten kunnen geblokkeerd worden voor het uitvoeren van transacties of kunnen uitgesloten worden van bepaalde functionaliteiten.
Scalability & Continuity	Het consensus model vereist coördinatie en communicatie tussen de nodes die veelal ruimtelijk van elkaar gescheiden zijn. Zij zijn tevens onderdeel van de interne IT omgeving van de eigen organisatie. Dit kan leiden tot een gebrek aan schaalbaarheid en zelfs een bedreiging vormen voor het blockchain netwerk en de betreffende processen. De prestatie bij een hoger volume aan transacties en het mogelijk opschalen van de blockchain daarbij vormt een risico op het gebied van continuïteit, met name als het gaat om kritische systemen.
Platform standardisation & Migration	Standaarden zijn afspraken die zijn vastgelegd in specificatiedocumenten en dragen bij aan interoperabiliteit en leveranciersonafhankelijkheid. Standaardisatie werkt grensoverschrijdend. De belangrijkste voordelen worden niet zozeer gerealiseerd door de optimalisatie van IT componenten op zichzelf, maar juist door de distribueerbaarheid en integratie van de verschillende IT functies. Dit geldt met name bij interconnectie.

GOVERNANCE CONSIDERATIONS

The governance considerations of a platform can make or break the success of not only your organization's implementation but the continuity of the entire platform. An exemplary case is the IBM and Maersk supply chain platform TradeLens. In 2018, the companies announced a joint venture to unify the shipping industry on a common blockchain platform. The platform was developed within a governance model that put major decision-making power in the hands of the founders, allowing them to retain the intellectual property of the shared platform and forcing other logistical companies to invest significantly in blockchain platform software. This resulted in a reluctant reception and very limited onboarding of other participants, limiting the transaction volume via this platform. As a consequence, the tipping point for success couldn't be reached. After restructuring the governance model, other companies, such as CSX, PIL and CEVA, decided to join.

The correct governance model for your platform is not a one-size-fits-all and depends on several factors. These factors include, but are not limited to:

- *strategy and mission-criticality*
- *policy/decision-making and risk sharing*
- *participant roles, responsibilities and representation*
- *node management*
- *type and variety of international regulatory jurisdictions*
- *desired permission level of features*
- *cost of ownership, incl. financing and cost charging*
- *supervisory bodies and assurance*

Bron: KPMG 2019 Steven vd Weerd, Matthijsse 1998.

Soft controls: vertrouwen en transparantie

Trust is generally not considered a control mechanism,
but is considered a substitute for control.

Het is essentieel dat tijdens de ontwikkeling en uitbreiding van blockchain netwerken aandacht wordt besteed aan het opbouwen van vertrouwen, geloofwaardigheid en reputatie. Een hoog niveau van vertrouwen binnen het ecosysteem is belangrijk om diverse redenen. Eén reden is bijvoorbeeld dat het gedrag van de gebruikers beïnvloed kan worden door het gedrag van de consortium partners. Zodra een consortium partner gaat handelen op een incompetente of

frauduleuze wijze, zullen gebruikers en partners in het ecosysteem hierdoor negatief beïnvloed worden.

De meeste blockchain netwerken streven naar een uitbreiding in partners en gebruikers. Zodra het aantal en diversiteit aan partners toenemen, zal het niveau veranderen van risico's die invloed uitoefenen op de reputatie en vertrouwen. Dit zal versterkt worden door het internationale karakter van expansie. Bijvoorbeeld, afhankelijk van verschillen in juridische systemen en beschermingen in andere landen, zal de effectiviteit van juridische beheers-maatregelen verschillend zijn. Culturele verschillen kunnen eveneens het niveau van risico en vertrouwen beïnvloeden doordat sociale normen, business culturen en risk appetites aanzienlijk kunnen verschillen van wat gebruikelijk is in de Europese Unie.

Hoewel vertrouwen niet een beheersingsmechanisme is, wordt vertrouwen wel gezien als een vervanging voor beheersing en kunnen risico's gemitigeerd worden door een hoge mate van onderling vertrouwen tussen de consortium partners. De aanbeveling is daarom om expliciet aandacht te besteden aan de ontwikkeling van vertrouwensrelaties tijdens het proces van opbouw en uitbreiding. Dit kan bijvoorbeeld gebeuren door fysieke kontakten tussen bestaande en nieuwe partners in het ecosysteem om gezamenlijk vraagstukken te behandelen. Doordat transparantie gezien wordt als middel om vertrouwen op te bouwen, dienen deze bijeenkomsten gehouden te worden in een sfeer van openheid die transparantie aanmoedigt.

6 Auditvoorbeelden ter illustratie

Diverse blockchain implementaties laten zien dat iedere blockchain omgeving een eigen set van beheersdoelstellingen, een eigen set van risicogebieden en een eigen set van controls heeft. Iedere vorm van blockchain beheersing is hierdoor context gebonden.

Hoewel de ontwikkelingen en de praktijkervaringen op het gebied van blockchain erg snel gaan, is het in dit stadium nog niet mogelijk om een éénsluidend en algemeen geldend Blockchain Control Framework op te stellen. Iedere keer is er sprake van maatwerk. Wel kan een goede indicatie worden gegeven van de verschillende regelmatig voorkomende perspectieven, zoals samenwerking en governance binnen het ecosysteem, smart contracts, data management, internationale wet- en regelgeving, privacy en security.

De ontwikkeling van het Blockchain Control Framework is een groeimodel. Onderstaande auditvoorbeelden uit de praktijk dienen als illustratie en dienen niet gelezen te worden als volledig uitgewerkte audit cases. Ieder project is afgebakend tot een bepaalde fase in het ontwikkelingsproces dan wel tot een selectie van risicogebieden. Langs deze weg betreft het dus niet een volledige weergave van de situatie, maar het geeft wel een beeld van blockchain audit en control. De vijf voorbeelden dienen hier als illustratie van professionele audit en control, ten behoeve van kennisdeling met bronvermelding.

Referentie project	
1	Diem Payment System
2	Rabobank We.Trade
3	MaaS
4	Company X
5	Havenbedrijf Rotterdam

Voorbeeld 1: Diem Payment System

Dit voorbeeld is ontleend aan een onderzoek dat is uitgevoerd door KPMG bij het initiatief van Libra (sinds kort Diem), een consortium van innovatieve organisaties zoals Facebook, Spotify, Uber en Vodafone. De doelstelling van de blockchain is een wereldwijd netwerk, gebaseerd op blockchain, voor financiële transacties.

Risks	Controls
Centralization & Collusion	
Dynamic node participation might result in the risk of network exclusion of participants	Contractually enforce that the organization will host validator nodes of the network it operates on. At least one node should be owned when transacting on a blockchain
	Monitor network activities to determine which Public Key addresses (i.e. other parties transacting on that blockchain) own validator nodes. If a participant's consensus power increases, proper escalation measures should be designed and enforced.
Network participants might achieve majority control of blockchain network. This might violate the integrity of the network	The organization must contractually enforce that they will host validator nodes for each blockchain system it uses.
	Blockchain participants contractually agree on the distribution of consensus power to prevent one party from achieving majority control.
	Monitor network activities to determine which Public Key addresses (i.e. other parties transacting on that blockchain) own validator nodes. If a participant's consensus power increases, proper escalation measures should be designed and enforced.
	In case of permissionless networks, monitor the network to ensure that centralization of the Validator power is identified appropriately.
Data Management & Privacy	
The inherent nature of blockchains might result in GDPR (e.g. "right to be forgotten") breaches	Establish data definitions and implement gatekeeper controls that ensure confidential and sensitive information is not stored on the blockchain network.
Data might be input incorrectly or incompletely.	The parties responsible for onboarding real-life object representations onto the blockchain ('Oracles') are subject to an ISAE3000 / SOC2 audit and is provided to the organisation that relies on such data.

Bron: KPMG; Steven vd Weerd; Compact, 2019/4

Voorbeeld 2: Rabobank

Rabobank is deelnemer in We.Trade, een digitaal handelsplatform voor internationale ondernemers dat gebruikmaakt van blockchain-technologie. We.Trade is transparant en ongevoelig voor fraude, waardoor het geschikt is om handel te drijven met buitenlandse partijen waarmee nog geen vertrouwensband is opgebouwd. Het werkgebied van dit ecosysteem betreft internationaal betalingsverkeer. Bij dit ecosysteem is met name onderzoek uitgevoerd naar het belang van vertrouwen bij de deelnemers in het ecosysteem en de mogelijke risicogebieden, die invloed kunnen uitoefenen op het niveau van vertrouwen.

Risk area	Risks impacting trust
1. Consensus and network	Risk associated with a blockchain not functioning as expected: - consensus algorithm not fit for purpose - cryptographic algorithms not fit for purpose - malicious behaviour by publishing nodes
2. Cryptographic key management	Risk associated with a blockchain not functioning as expected: - users losing assets - users and operators losing control
3. Functional requirements	Risks associated with innovation: - solution not aligned with business goals and practices - solution not accepted by users
4. Smart contracts	Risk associated with a blockchain not functioning as expected: - errors in smart contracts leading to loss of assets for users
5. Data management and privacy	Risks associated with regulatory and privacy risk: - risk of violating current or future privacy regulation and laws - reputational risk for participants Risk associated with a blockchain not functioning as expected - data put into the system may be false
6. Centralization and collusion	Risk associated with a blockchain not functioning as expected: - consensus algorithm manipulated - malicious behaviour by publishing nodes
7. Interoperability and integration	Risk associated with a blockchain not functioning as expected: - risk of interacting systems generating incorrect results
8. Scalability and continuity	Risk associated with a blockchain not functioning as expected: - design of blockchain constrains proper functioning - IT used by blockchain system not fit for purpose
9. Third party governance	Risk associated with the blockchain not functioning as expected: - risk of the system being disrupted or controlled by an attacker - risk of faults in code or operating practices
10. Compliance	Risks associated with regulatory and privacy risk: - risk of not being compliant with current or new regulation - data in the system may support criminal or illegal behaviour

Bron: VU Amsterdam, referaat Urwin van Lopik, Rabobank, 2020

Voorbeeld 3: MaaS

Mobility as a Service: the offer of multimodal, demand-driven mobility services, with customised travel options being offered to customers via a digital platform (e.g. mobile app) with real-time information, including payment and finalisation of transactions.

Naast het ontsluiten van verschillende nationale multimodale vervoersdiensten is deze pilot complex omdat de MaaS-app ook alle functionaliteiten moet bieden voor grensoverschrijdend vervoer. Het gaat hierbij om een aanbod op basis van persoonlijke voorkeuren, het kunnen plannen, boeken, toegang krijgen tot het vervoersmiddel en het betalen. Daarnaast moet de reiziger ondersteund worden tijdens de reis en moet de reis onderweg aangepast kunnen worden bij incidenten of vertragingen. Daarbij mag het voor deze MaaS-reizigers niet uitmaken of ze van of naar België en Duitsland reizen. Dat betekent aan de achterkant meerdere 'koppelingen' van verschillende tarief- en ticketingsystemen.

	Geldig voor alle 7 stappen				
D11	**Alg**	Gebruiker van de kaart is niet de gebruiker/eigenaar (ongeautoriseerd gebruik)	Conf / Int / Irre	TA / FA	Gebruik maken van NFC, QR, foto of vingerafdruk
D11	**Alg**	Gebruiker is niet de geregistreerde gebruiker (ongeautoriseerd gebruik)	Conf / Int	TA / FA	Gebruik maken van Multi Factor Autorisatie
D11	**Alg**	Complexe wachtwoorden worden niet afgedwongen	Conf / Int	TA	Gebruik maken van complexe wachtwoorden of apps daarvoor
D11	**Alg**	Directe (data) wijzigingen worden in databases bij partijen uitgevoerd	Conf / Int / Ava	TA	Formaliseren proces – geen directe data wijzigingen zonder aanvraag, goedkeuring, nacontrole en periodieke controle (sectorale afspraak
D11	**Alg**	Alle vervoerders hebben toegang tot de ingevulde/privé gegevens van de gebruiker	Conf / Int / Ava	TA	Zie sectie datamanagement
D11	**Alg**	Gebruikers moeten bij elke vervoerder en clearing partijen apart inloggen voor terug vragen onterechte kosten/verrekening (alleen MaaS diensten)	Conf / Int / Ava	TA / FA	Goede koppeling en onderlinge transparantie onder de vervoerders
D4	**Alg**	Incorrecte gebruik van keys (voor beveiliging van datauitwisseling)	Conf / Int / Ava	TA	Automatiseren key rotatie Automatiseren beveiligde key verspreiding Strikte policy gebaseerde controls om misbruik of hergebruik van keys te voorkomen
D4	**Alg**	Geen gebruik van privé, symmetric of hash keys			
D4	**Alg**	Hergebruik van keys			
D4	**Alg**	Geen rotatie van keys			
D4	**Alg**	Slechte bewaarplek van keys (server/database)			
D4	**Alg**	Inadequate bescherming van de keys			
D4	**Alg**	Keys zijn niet (goed) vernietigd			
D11	**Alg**	Beperkte (tot geen) audit logging – 5 jaar of 7 jaar als bewaartijd?			
D11	**Alg**	Beperkte (tot geen) weerstand (resilience) Niet beschikbaar wanneer echt nodig			
D1	**Alg**	Netwerk(en) en technische architectuur zijn onveilig	alle		Beveiliging van netwerkdiensten: Beveiligingsmechanismen,

Bron: Ministerie Infrastructuur en Waterstaat / ICTU, interne notitie, 2020

Voorbeeld 4: Company X Expert interviews

Company X leverde een case study voor dit onderzoek. Het case study project is genoemd IDA met een app die momenteel “Datakeeper’” heet. Een serie van expert interviews is met name ingegaan op de thema’s consortium vorming en data integriteit. De evaluatie door experts van Company X is met name gericht op de technische blockchain aspecten. Een belangrijke waarneming is dat het belangrijker is om de pre-condities goed te organiseren en dat de blockchain zorgvuldig is ingericht vanuit het perspectief van data integriteit.

Control objective: Data is valid, accurate and added correctly			
Risks	**Controls**	**Preventive/ detective**	**Manual/ comp/ automated**
1. Invalid or inaccurate data	Procedures are in place such that requirements for specific transactions are verified and confirmed by checks and guidelines before transactional data is added to a block	Preventive	Manual
	Nodes are identifiable and circumventable to maintain the integrity of the data on the consortium blockchain	Preventive	Automated
	Periodically check if all the data or all transactions in the consortium blockchain network are the same at all nodes	Detective	Computer-dependent
	All transactions are automatically logged and create identifier-hash mappings for each of these log entries, so the hash can always be checked automatically (hash validation control)	Detective	Automated

Bron: Tilburg University, referaat Jarno van Lint, BDO, 2021

Voorbeeld 5: Havenbedrijf Rotterdam

De Rotterdamse haven vormt een belangrijk overzees verbindingskanaal met een geschatte goederenoverslag van ongeveer 469 miljoen ton (2018). Daarmee staat het op het moment bekend als de grootste haven van Europa. Vele ondernemingen zijn gevestigd aan de Rotterdamse haven die het proces van containeroverslag beheren. Uitgangspunt voor dit onderzoek is om een analyse te maken van de voordelen van de blockchain en de inherente karakteristieken van een logistiek havenproces. Daarbij is hoofdzakelijk aandacht gegeven aan de relevante voordelen die de blockchain biedt ten aanzien van meest voorkomende inefficiënte processtappen in een transactieketen. Om dit proces zo efficiënt mogelijk te kunnen inrichten zijn beheersmaatregelen nodig, opdat de betrokken stakeholders kunnen steunen op in de informatievoorziening zoals tot stand gekomen in de blockchain. Dit onderzoek is ook ingegaan op de benodigde randvoorwaarden om relevante (IT) risico's tot een acceptabel niveau te brengen.

III. IT risico als gevolg van discontinuïteit van blockchainsystemen	Het creëren van uitwijkmogelijkheden in geval discontinuïteit van de blockchain ontstaat. De uitwijkmogelijkheid ziet erop toe dat transacties kunnen worden voortgezet binnen een vergelijkbare omgeving en tegelijkertijd continue tijdige en volledige back ups worden gemaakt van de additionele data (opdat deze bij continuïteit van de primaire omgeving weer kunnen worden terug geplaatst).
IV. IT risico als gevolg van ongeautoriseerde pogingen/toegang tot de data in de blockchain (functionerend via open source software). Dit risico resulteert in inbreuk van de vertrouwelijkheid en integriteit van data, zowel op applicatie als databaseniveau.	Inregelen van autorisaties afgestemd op de functie/rol van functionarissen op het niveau van de organisatie in combinatie met werkende authenticatiemechanismen. Autorisatiecontroles dienen eveneens op het niveau van de database te worden ingeregeld inclusief adequate functiescheidingen. Versleuteling van opgeslagen data in de blockchain vindt plaats aan de hand van (de meest) recente encryptie technieken inclusief adequate (en separate) opslag van de te hanteren van "keys" in de database. Het creëren van een extra beveiligingslaag (authenticatie) alvorens toegang kan worden verkregen tot de blockchain in de vorm van een authenticatieserver (bijvoorbeeld RADIUS). Single Sign On zou in dit geval niet van toepassing mogen zijn. Doordat de beheersmaatregelen aanvangen op het niveau van de organisatie, is het voorts een optie om een ISAE (II) af te dwingen met werkende autorisatiecontroles alvorens toegang kan wor-den verkregen tot het gedistribueerd netwerk. Tot slot dienen er specifieke maatregelen te worden getroffen over welke data wel of niet in de blockchain kan worden opgeslagen, dit kan middels preventieve (privacy)controls applicatief worden afgedwongen om de vertrouwelijkheid van de data te waarborgen.
V. IT (security) risico als gevolg blootstelling van de blockchain aan online omgevingen (internet)	Communicatieverkeer tussen lokale systemen en het gedistribueerd netwerk dient middels VPN en/of andere erkende (datacommunicatie)protocollen plaats te vinden.
VI. IT risico als gevolg van ongeautoriseerde interfaces (hetzij niet werkende interfaces) tussen lokale systemen en het gedistribueerd netwerk	Inregelen van effectieve interfacecontrols op het niveau van de organisatie. Ook hier dienen de benodigde controles onderdeel uit te maken van ISEA (II) specifiek afgestemd op de aansluiting met de blockchain, alvorens toegang kan worden verkregen tot het gedistribueerd netwerk. Om te voorkomen dat de blockchain niet gesynchroniseerd raakt met besmette data en/of virussen etc. via deze interfaces, dienen er firewalls te worden ingesteld die het inkomend verkeer screenen en afwijzen indien nodig.

Bron: VU Amsterdam, referaat Adil Ibn Lkassem, KPMG, 2019

7 Afsluiting

Paradigma's verschuiven. De beroepsgroepen voor accounting, control en auditing dienen op middellange termijn rekening te houden met zowel innovatie in technologie zoals blockchain, als met alliantievorming in ecosystemen. Zij dienen hun professionele procedures, kennis en vaardigheden hierop aan te passen. Een blockchain netwerk is in feite een gedistribueerd informatiesysteem met gestructureerde gegevensuitwisseling door partners in een ecosysteem, dat gepaard gaat met een diversiteit in belangen en risicogebieden. De IT-auditor wordt hierdoor voor vraagstukken op het gebied van beheersing en voor assurance provisioning een ecosysteem auditor.

Als de snelle ontwikkelingen in blockchain zich continueren, zal de impact in de nabije toekomst aanzienlijk zijn. Blockchain wordt gezien als een significante technologische innovatie en wordt zelfs aangemerkt als disruptief. De vele voordelen van blockchain zijn grofweg te categoriseren naar drie domeinen die aansluiten op de definitie van de blockchain: permanentie, transparantie en integriteit.

Iedere nieuwe generatie technologie kan leiden tot een nieuwe generatie beheersmaatregelen en auditbenaderingen. Blockchain leidt tot een andere wijze van kijken naar de beheersing van risico's en de inrichting van processen. Blockchain technologie kent op zichzelf geen fundamentele verschillen met bekende technologieën, maar leidt wel tot serieuze consequenties op specifieke risicogebieden. Traditionele interne systemen voor accounting, control en auditing dienen gemoderniseerd te worden.

De toepassing van blockchain technologie binnen private en public netwerken leidt tot serieuze gevolgen op het gebied van onder meer strategiebepaling en besluitvorming, alliantievorming, bestuurlijke context, cybersecurity, datamanagement, privacy, en internationale wet- en regelgeving. De traditionele audits blijven weliswaar heel waardevol, maar blockchain assurance moet dus ook liggen op die risicogebieden die een meer bestuurlijk en organisatorisch karakter hebben. Risicobeheersing en het verstrekken van blockchain assurance krijgt hierdoor een multi-disciplinair karakter.

In de context van blockchain toepassingen binnen ecosystemen is geconcludeerd dat de interne beheersmaatregelen uiteindelijk belangrijker zijn dan de technologie op zichzelf. Indien organisaties "in control" willen blijven over hun blockchain/IT omgeving, dan is hun eigen interne beheersing niet meer voldoende. Organisaties dienen er rekening mee te houden dat de beheersing van audit objecten zich uitstrekt tot het gehele werkgebied van het blockchain netwerk, dus inclusief raakvlakken met de interne beheersing van alle deelnemende organisaties in het alliantie ecosysteem. De IT control omgeving van een organisatie die blockchain implementeert, transformeert in een ecosysteem op zichzelf, waarbij haar eigen IT interne beheersing en informatiebeleid afhankelijk zijn of in ieder geval medebepaald worden door het bredere ecosysteem en de individuele deelnemers. De verschuiving naar een gedistribueerd grootboek betekent dus ook een verschuiving naar een gedistribueerde beheersomgeving.

Recentelijk is een interessant rapport uitgebracht door de Accredited Standards Committee, afdeling Financial Industry Standards. Dit rapport beschrijft een Blockchain risk management framework. Hoewel het IT gedreven framework primair gericht is voor toepassing op blockchain systemen voor het betalingsverkeer in de financiële sector, biedt het zeker aanknopingspunten voor andere toepassingen en voor andere sectoren. Er worden in dit model vanuit een IT systeembenadering vijf risicogebieden onderscheiden, die uitgewerkt worden aan de hand van interviews. De oordeelsvorming vindt plaats aan de hand van de combinatie van kwalitatieve en normatieve resultaten uit interviews. De inhoud van dit rapport bevat geen gedetailleerde audit plannen of gedetailleerde controls, maar biedt wel handvatten bij het opstellen van een audit plan. Het rapport typeert zichzelf als informatief en niet als normatief.

Blockchain technologie dwingt tot versterking van de interne beheersing en integrale auditing. IT- en financial auditors moeten zich goed bewust zijn van de veranderingen in risico's naarmate de externe integratie in ecosystemen intensiever wordt en de innovatie in technologie toeneemt. Hierbij wordt het onderscheid relevant tussen een control-benadering en een trust-benadering, ook bij besloten blockchain netwerken. Naar verwachting zal bovendien meer aandacht noodzakelijk zijn voor soft controls. Naarmate blockchain technologie meer volwassen wordt, zal de belangrijkste uitdaging op weg naar grootschalige adoptie liggen op het gebied van governance en stakeholder management.

De Kennisgroep zal het NOREA Blockchain Control Framewerk verder ontwikkelen, deze in een aantal praktijksituaties evalueren en begin 2022 publiceren. Mocht u daaraan een bijdrage willen leveren neem dan gerust contact met ons op.

Bijlagen

Selectie literatuur

Accredited Standards Committee X9, Financial Industry Standards; Blockchain risk management framework; july 2021.

Bouwman, R.; IT audit for permissioned and private blockchains; A study into IT risks and controls; referaat Vrije Universiteit; 2020.

Cognizant; Blockchain in Europe: Closing the strategy gap; London; january 2018.

COSO; Blockchain and internal control: the COSO perspective; COSO Committee of Sponsoring Organizations of the Treadway Commission, July 2020; https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf

Deloitte's 2020 Global Blockchain Survey; https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html

Duuren, N.de en Pous V.de; Multidisciplinaire aspecten van blockchain; Uitgeverij de Lex; 2019.

EY Global Blockchain Summit 2021; https://pub.ey.com/public/2021/2101/2101-3679331/blockchain-summit-2021/index.html

Fintech; Managing the risks of blockchain; Hyperlink www.bankingtech.com; March 2018.

Hofman, A.; Wat is de impact van blockchain op administratieve organisatie en interne controle?; in: FM.NL; serie blogs AO/IC; 27 september 2019.

Ibn Lkassem, A.; Blockchain in de Rotterdamse haven: een innovatieve ontwikkeling voor IT auditing; referaat Vrije Universiteit; 2019.

ISACA; Blockchain preparation audit program; 2019.

KPMG Advisory; Blockchain maturity model; Amstelveen; 2018 (https://www.compact.nl/)

Lint, J. van; A research on the development of a consortium blockchain assurance control framework; referaat Tilburg University; 2021.

Lopik, U. van; Blockchain risk area's and trust; referaat Vrije Universiteit; 2020

Man, A.P. de & others; How to survive the organizational revolution; a guide to agile contemporary operating models, platforms and ecosystems; BIS Publishers; 2019.

Matthijsse, RPHM; Informatiemanagement en control in een ketenomgeving; intreerede Fontys University of Applied Sciences; 2016.

Matthijsse, RPHM; Blockchaintechnologie dwingt tot versterking interne beheersing en integrale auditing; in: IT Auditor, 3-2020.

NBA Stuurgroep Publiek Belang; Van bankzitter naar sterspeler: de impact van technologie op de accountantscontrole; Amsterdam; juni 2019.

PWC Global Blockchain Survey 2020; https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html

Smolders, D. en Dijke, R.J. van; Blockchain: game changer voor de interne beheersing van organisaties; referaat Vrije Universiteit; 2019.

Weerd, S.; How will blockchain impact an information risk management approach; https://www.compact.nl/ ; 2019/4.

Kennisgroep Keteninformatiemanagement

Keteninformatiemanagement is een thema met maatschappelijke relevantie en impact. De Kennisgroep "Keteninformatiemanagement en Controls" van de NOREA draagt bij aan de vaktechnische profilering en ondersteuning van de beroepsgroep door totstandbrenging van relevante kennisontwikkeling, kennisdeling en producten. De Kennisgroep Keteninformatie-management heeft tot doel het ontwikkelen van een raamwerk voor het uitvoeren van ketenaudits, waarmee auditors over een toolkit beschikken om op een efficiënte en effectieve wijze de klantvragen te kunnen bedienen.

De centrale opdracht van de Kennisgroep is geformuleerd als: Hoe kan optimalisatie van (geïntegreerd) informatie- en procesmanagement in een ketenomgeving, met behoud van de eigen identiteit, een positieve bijdrage leveren aan het creëren van waarde in een keten en aan het in control zijn binnen de keten?

De toename van digitalisering leidt tot virtuele integratie van de bedrijfsprocessen tussen organisaties onderling en met hun belangrijkste stakeholders, met behoud van de eigen juridische identiteit. Vooral bij de partners in het ecosysteem, zowel bij maatschappelijke ketens als bij financiële en logistieke ketens, zal het vraagstuk van IT governance met de bijbehorende controls een grote rol gaan spelen.

De kennisgroep richt zich vanuit het perspectief Management Control en IT Auditing op het ontwikkelen van kennis op meerdere aan elkaar gerelateerde gebieden: de samenhang tussen het verkrijgen en gebruiken van informatie voor besturing en verantwoording in het ecosysteem, de inrichting van informatiesystemen binnen organisaties en binnen het ecosysteem, de betrouwbaarheid van informatie voortkomend uit de inrichting van het proces van informatievoorziening en de mogelijkheden van digitalisering.

De relevantie voor de beroepspraktijk ligt daarmee vooral in het onderzoeken hoe betrouwbare en tijdige informatie voor het besturen en beheersen van organisaties gericht op het creëren van waarde in het ecosysteem met organisaties kan worden opgeleverd. Daarmee wordt het onderwerp "informatie" in brede zin als centraal thema gepositioneerd.

Kernpunt hierbij is dat informatievoorziening en gegevensuitwisseling veelal met behulp van IT-oplossingen worden gerealiseerd, dat dit vaak op een inefficiënte en ineffectieve wijze georganiseerd is en dat afstemming van vraag naar en aanbod van informatie zowel binnen organisaties als in het ecosysteem een cruciale activiteit is, die in veel gevallen onvoldoende aandacht krijgt. Een belangrijk vraagstuk daarbij is de inrichting van informatiestromen met in het achterhoofd de transitie van outputverantwoording naar (geïntegreerd) procesmanagement over meerdere organisaties heen.

Kennisgroep leden

Voorzitter	dr. René Matthijsse RE	Retired
Kernteam	drs. Christel Maas	NOREA
Kernteam	drs. ing. Ronald Koorn RE CISA	KPMG
Kernteam	drs. Marc Welters RE RA (linking-pin bestuur)	EY
Kernteam	Ruud Mollema RE RA	ICTU
Kernteam	drs. Lucas Vousten RE RA	Joanknecht
Teamlid	drs. Michel Bosch RE EMITA	Min van Binnenlandse Zaken
Teamlid	Adri de Bruijn RE RA	PWC
Teamlid	Patrick Chu MSc RE	EY
Teamlid	Ruurd Smildiger RE	Min van Financiën
Teamlid	drs. Reza Torabkhani RE	Universiteit van Amsterdam
Teamlid	Michel Bernsen MSc RE	EY
Teamlid	drs. Youetta de Jager	ICTU
Teamlid	ir. Anske Jongsma RE CISA	Achmea
Teamlid	Wijnand Luitjes MSc RE	Mollie
Teamlid	Steven van der Weerd MSc	KPMG
Teamlid	drs. Ype van Wijk RE RA	Cobalus