UHASSELT

KNOWLEDGE IN ACTION

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen

Masterthesis

Blockchaintoepassingen binnen de overheid

Martijn Vanlessen

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen, afstudeerrichting beleidsmanagement

PROMOTOR :

De heer Willem VANLAER

2018
2019

UHASSELT

KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

Faculteit Bedrijfseconomische Wetenschappen

master in de toegepaste economische wetenschappen

Masterthesis

Blockchaintoepassingen binnen de overheid

Martijn Vanlessen

Scriptie ingediend tot het behalen van de graad van master in de toegepaste economische wetenschappen, afstudeerrichting beleidsmanagement

PROMOTOR :

De heer Willem VANLAER

Literatuurstudie

1 Abstract

Blockchain technologie maakt de veilige overdracht van geld, activa en informatie via het internet mogelijk zonder tussenkomst van vertrouwde derden zoals bijvoorbeeld financiële instituties en overheden (Swan, 2015). Transacties worden gevalideerd, uitgevoerd en chronologisch geregistreerd in een onveranderlijke database, waar ze beschikbaar blijven op het internet voor *on-demand* opzoekwerk of verificatie (Swan & de Filippi, 2017). Blockchain kan mogelijks de overheid helpen bij het innen van belastingen, het leveren van sociale bijstand, het uitgeven van paspoorten, het registreren van kadasters, het verzekeren van de integriteit van de supply chain, de eerlijkheid garanderen van overheidsrecords en -diensten, etc. Vooraleer de mogelijke toepassingen geanalyseerd worden, bespreken we de belangrijkste technologische aspecten en de werking van blockchain om een beter beeld van de technologie te schetsen. Daarna worden de verschillende ontwerpen van blockchain en hun voor- en nadelen besproken. Vervolgens wordt er een framework behandeld waarmee men relatief snel inzicht kan bekomen over de bruikbaarheid van blockchain technologie bij bepaalde toepassingen. In het laatste deel van de literatuurstudie worden de mogelijke uitdagingen en implicaties voor de overheid aangehaald. Ten slotte worden enkele casestudy's besproken en geanalyseerd. Hierbij worden de mogelijke voordelen van de toepassing in kaart gebracht om door middel van benchmarking de mogelijke effecten van blockchain technologie in de Belgische context op te tekenen.

2 Inleiding

Blockchain is de technologie die aan de basis ligt van de bekende Bitcoin *cryptocurrency*. Op 31 oktober 2008 werd de *white paper* "Bitcoin - a peer-to-peer electronic cash system" door Satoshi Nakamoto gepubliceerd. Na de financiële crisis van 2008 was het vertrouwen in de financiële instituties geschaad. Nakamoto publiceerde de *white paper* als reactie op deze crisis en wou met behulp van Bitcoin de centrale autoriteit, die niet meer volledig vertrouwd werd, omzeilen. Niet veel later, namelijk op 3 januari 2009, werd het netwerk en protocol van Bitcoin gelanceerd. Zo werd Bitcoin het eerste en meest voor de hand liggende blockchain project dat de wereld liet kennismaken met deze technologie (Satoshi, 2008).

Het idee om een open, universeel toegankelijke database of grootboek te hebben, werd geboren met Bitcoin. Verder bood het Bitcoin protocol de eerste oplossing om vertrouwen te vestigen in een onveilige omgeving zonder afhankelijk te zijn van een derde partij (Ølnes, Ubacht, & Janssen, 2017). Sinds 2009 is dit digitale munt systeem uitgegroeid tot een waarde van 150 miljard dollar (met een piek van ongeveer 300 miljard in december 2017) en is nu de meest bekende applicatie van blockchain technologie (CoinMarketCap, 2019).

Inmiddels is deze technologie echter verder geëvolueerd naar een 2.0 versie. Dit is te danken aan de opkomst van *smart contracts* (Buterin, 2014). Deze *smart contracts* bestaan uit code en gegevens die zich op een specifiek adres binnen de blockchain bevinden. Hiervan wordt de uitvoering op dezelfde manier door het netwerk gevalideerd zoals bij transacties (Nugent, Upton, & Cimpoesu, 2016). De *smart contracts* bieden de mogelijkheid aan ontwikkelaars om gedecentraliseerde apps (dapps) te ontwikkelen die draaien op de blockchain. Hierdoor kende het gebruik en de ontwikkeling van blockchain een snelle expansie. De focus die eerst bij de *cryptocurrencies* lag, breidde zich uit naar applicaties ter ondersteuning van een breed spectrum aan samenwerkingsactiviteiten tussen bedrijven, organisaties en individuen. Hierdoor is de functionaliteit van blockchain sterk geëvolueerd naar een groot aantal toepassingen: bankieren, financiële markten, verzekeringen, datamanagement, stemsystemen, supply chain management, eigendomsrechten, leasecontracten, overheidsdiensten, etc. (Nugent et al., 2016).

Aangezien de technologie relatief jong is, vereist de integratie van haar toepassingen binnen bedrijven en overheden echter nog verder onderzoek. Er is nood aan experimentatie om het potentieel en mogelijke valkuilen ervan volledig in kaart te brengen. Enkele landen zoals Estland maken reeds grote inspanningen om blockchain en haar toepassingen ten volste te benutten. Het is belangrijk om na te gaan welke voordelen alsook beperkingen zij bij bepaalde toepassingen ondervonden hebben. Uit het grote scala aan toepassingen worden enkelen hiervan later nog uitgebreid besproken aan de hand van verschillende casestudy's. Deze worden als uitgangspunt gebruikt om door middel van benchmarking de potentiële effecten die deze technologie in België zou kunnen genereren te onderzoeken. Vooraleer hierop wordt toegespitst, wordt de basis van de blockchain technologie verduidelijkt om zo een kritische blik te kunnen werpen op de toepasbaarheid van deze technologie binnen de overheid. Zo worden de verschillende mogelijkheden rond het ontwerp van de blockchain toegelicht en worden de uitdagingen omtrent implementatie en bestuur besproken. Ten slotte wordt er een framework toegelicht dat een eerste evaluatie kan vormen omtrent de toepasbaarheid van blockchain voor een specifieke applicatie. Dit framework wordt

evenzeer gebruikt om de bruikbaarheid van de verschillende toepassingen van de casestudy's te beoordelen.

3 Basis van blockchain technologie

Vooraleer de mogelijke toepassingen en casestudy's kunnen worden geanalyseerd, is het belangrijk om eerst de basis van blockchain technologie uit te diepen. In deze sectie wordt er ingegaan op de werking van blockchain en waarom het gebruik van deze technologie bevorderlijk kan zijn voor zowel overheden, bedrijven als burgers. Bovendien wordt het begrip '*smart contracts*' en de rol die deze binnen de blockchain innemen, besproken. Ten slotte worden ook de kenmerken die eigen zijn aan blockchain toegelicht.

3.1 Wat is blockchain en hoe werkt het?

Blockchain technologie is de benaming die oorspronkelijk werd gegeven aan het design dat de werking van Bitcoin ondersteunt. De bedenker van Bitcoin, Satoshi Nakamoto, heeft echter nooit de term 'blockchain' gebruikt in zijn *white paper*. Bij het lezen van de *white paper* krijgt men bovendien niet de indruk dat het gaat om een revolutionaire technologie in de traditionele zin van het woord, maar eerder over een software-ontwerp gebaseerd op verschillende bestaande technologieën om zo een zuivere *peer-to-peer* versie van digitale valuta te creëren (Ammous, 2016).
Blockchain is een gedecentraliseerde database met een netwerk van *peer-to-peer* leden. Deze leden zijn in feite een groot aantal computers, die ook wel *nodes* of knooppunten worden genoemd. Het maakt gebruik van een protocol voor communicatie tussen alle *nodes* ter vorming van een netwerk zonder centrale autoriteit. Binnen de literatuur wordt de definitie van blockchain onvoldoende afgebakend. Dit komt doordat deze technologie verschillende soorten ontwerpen kent. De meeste definities omschrijven blockchain slechts in beperkte mate (Zīle & Strazdiņa, 2018). Zo definieert *Oxford Dictionaries* de blockchain technologie als 'een systeem waarin een registratie of transactie in Bitcoin of een andere *cryptocurrency* wordt bijgehouden over meerdere computers die gekoppeld zijn in een *peer-to-peer* netwerk' (Dictionaries, 2019). Veel blockchains zijn echter niet geassocieerd met een *cryptocurrency*, maar fungeren eerder als een gedeelde database. Ook *Merriam-Webster* kent een andere omschrijving van blockchain: 'Een digitale database met informatie (zoals records van financiële transacties) die gelijktijdig kunnen worden gebruikt en gedeeld binnen een groot gedecentraliseerd, openbaar toegankelijk netwerk' (Merriam-Webster, 2019). Echter hebben niet alle blockchains een publiek karakter en zijn sommigen niet volledig gedecentraliseerd. Een bredere definitie wordt door IBM gehanteerd. Vereenvoudigd stelt IBM dat 'blockchain een gedeeld en onveranderlijk grootboek is waarmee de geschiedenis van transacties kan worden vastgelegd' (Manchisi, 2018). Toch kan blockchain op een betere en meer volledige manier worden omschreven aan de hand van kernelementen die eigen zijn aan deze technologie. Zo kan men stellen dat het een datastructuur is, bestaande uit vijf kernelementen (Porru, Pinna, Marchesi, & Tonelli, 2017). Ter verduidelijking wordt elk kernelement besproken.

1) Gegevensredundantie
2) Controle van de transactievereisten vóór validatie
3) Consensusmechanisme

4) Registratie van transacties in sequentieel geordende blokken die gecreëerd worden door een consensusalgoritme
5) Transacties op basis van *public-key* cryptografie

In eerste instantie is er sprake van gegevensredundantie, het eerste kernelement. Dit slaat op het feit dat er binnen elke *node* van het netwerk een kopie van elke transactie wordt opgeslagen. Vooraleer een transactie kan plaatsvinden, moet deze echter geverifieerd worden door de *nodes* van het netwerk. Dit is het tweede kernelement. De *nodes* controleren de nodige transactievereisten door middel van *Proof-of-Work* uit te voeren. Hierbij lossen de *nodes* moeilijke, wiskundige bewerkingen op waarvan de gevonden uitkomst echter eenvoudig te verifiëren is. De eerste *node* die erin slaagt het wiskundig probleem op te lossen, stuurt deze oplossing door naar alle andere *nodes*. Op deze manier kunnen de andere *nodes* snel de juistheid van de transactie en de oplossing verifiëren. Bovendien wordt de *node* die als eerste een oplossing voor het probleem vindt, beloont met een specifieke hoeveelheid valuta van de blockchain (bv. Bitcoin of Ether). Het verifiëren van transacties met het verkrijgen van een beloning als drijfveer wordt ook wel *mining* genoemd (Ammous, 2016).
Wanneer 51% van de verwerkingscapaciteit van het netwerk, oftewel de *nodes*, de transactie uiteindelijk goedkeurt, wordt er een consensus bereikt. Enkel door middel van dit consensusmechanisme kunnen deze transacties geregistreerd worden in sequentieel geordende blokken in de blockchain (Swan, 2015). Bovendien wordt er bij registratie nog andere relevante informatie die gelinkt is aan de transactie toegevoegd. Dit gaat bijvoorbeeld over elementen zoals een tijdstempel, het bedrag of de waarde van de transactie, aan wie het werd betaald en door wie de transactie werd uitgevoerd. Deze stappen omvatten het derde en het vierde kernelement.
Indien een *node* een ongeldige of frauduleuze transactie aan de blockchain wil toevoegen, zal deze *node* eerst de *Proof-of-Work* uitvoeren. De andere *nodes* zullen de uitkomst hiervan nagaan en de transactie afwijzen omdat deze uitkomst onjuist is. Er wordt dus geen consensus bekomen. De *node* die de ongeldige transactie wilde toevoegen, zal veel middelen en dus energie verspild hebben aan de *Proof-of-Work* die uiteindelijk toch wordt afgewezen (Puthal, Malik, Mohanty, Kougianos, & Das, 2018). Dit zorgt ervoor dat het kostelijk wordt om fraude te plegen.
Ten slotte zijn transacties op basis van *public-key* cryptografie het laatste kernelement. Deze soort cryptografie wordt ook wel asymmetrische cryptografie genoemd en wordt gebruikt voor het beveiligen van berichten, data en software. Het maakt gebruik van twee mathematisch gelinkte, maar toch ongelijke sleutels, namelijk een private en een publieke sleutel (Weise, 2001). Vereenvoudigd kan men de publieke sleutel beschouwen als een e-mailadres en de private sleutel als wachtwoord van dat emailaccount. Aangezien dit laatste kernelement een zeer belangrijk aspect van blockchain vormt, worden de functies en de werking van *public-key* cryptografie verder verduidelijkt.

3.1.1 Public-Key cryptografie en de digitale handtekening

De publieke sleutel wordt door middel van een wiskundige berekening uit de private sleutel berekend, maar omgekeerd kan de private sleutel onmogelijk uit de publieke sleutel herleid worden. De publieke sleutel mag als gevolg openlijk gedeeld worden. Deze functie van *public-key* cryptografie

zorgt ervoor dat in principe iedereen gecodeerde berichten kan sturen met behulp van deze publieke sleutel. Deze berichten kunnen echter enkel ontcijferd worden door de private sleutel in bezit van de ontvanger.

Een tweede functie van de *public-key* cryptografie is het maken en verifiëren van digitale handtekeningen. Deze vormen een cruciaal element bij het digitaliseren van overheidsdiensten. Ze worden gebruikt voor het bevestigen van zowel de authenticiteit als de integriteit van digitale informatie en is vergelijkbaar met het ondertekenen van papieren documenten (Subramanya & Yi, 2006). De authenticiteit van de digitale handtekening wordt op twee manieren bevestigd. Zo is de handtekening numeriek gegenereerd uit een samenspel tussen de private sleutel van de verzender en de inhoud van het ondertekende document. De ontvanger kan de authenticiteit van de handtekening nagaan door gebruik te maken van de publieke sleutel (wiskundig gelinkt aan de private sleutel) en de handtekening van de verzender (Zhang, Shan, & Wang, 2012). Zo kunnen de ontvangers bij verificatie van de handtekening zeker zijn dat de handtekening van de verzender afkomstig is.

Daarnaast wordt bij verificatie van de handtekening de inhoud van het gesigneerde document op dat moment vergeleken met de originele inhoud. De kleinste veranderingen zorgen ervoor dat de digitale handtekening en bijgevolg het getekende document ongeldig worden. Beide aspecten zorgen voor het principe van onweerlegbaarheid (Camenisch & Lysyanskaya, 2002). De ondergetekende kan niet weerleggen dat hij of zij dat specifieke document heeft ondertekend. Let op, hierbij wordt ervan uitgegaan dat de private sleutel steeds vertrouwelijk blijft. Indien deze sleutel door anderen gekend is, kunnen handtekeningen vervalst worden. Dit houdt dus een zeker risico in voor de gebruiker indien hij niet zorgvuldig is met zijn private sleutel.

Om bovenstaande nogmaals te verduidelijken, wordt alles op een rijtje gezet. Wanneer transacties worden aangevraagd, moeten deze eerst geverifieerd worden door het netwerk. De transactie wordt uitgezonden naar het netwerk waarna de *nodes* de nodige transactievereisten nagaan door middel van *Proof-of-Work*. Dit is het oplossen of ontcijferen van de wiskundige bewerking. Wanneer de meerderheid van de *nodes* de geldigheid van de transacties goedkeuren, worden deze toegevoegd aan de blockchain (Walport, 2015). De database wordt vervolgens op elke node geüpdatet. Zij beschikken dus over dezelfde kopieën van de database en bijgevolg dus ook over de volledige geschiedenis van transacties opgeslagen in de blockchain. Daarnaast bevat elk blok ook een *hash pointer* die verwijst naar het vorige blok. Zo kunnen de blokken aan elkaar geketend worden, vandaar de naam blockchain (Buterin, 2014). Knoeien met transacties eens ze in de blockchain zijn vastgelegd wordt hierdoor praktisch onmogelijk. Het opslaan van informatie op verschillende punten wordt ook wel *distributed ledger technology* genoemd. Dit brengt een groot voordeel met zich mee. Het zorgt ervoor dat men onafhankelijk is van een centrale actor of autoriteit en dat er geen 'single point of failure' meer kan zijn (Ølnes et al., 2017).

Volgens enthousiastelingen is blockchain 'revolutionair' in de manier waarop informatie en transacties worden opgeslagen en geverifieerd. Het element van vertrouwen speelt een grote rol binnen deze technologie. Het model is gebaseerd op een groepsconsensus, waarbij het netwerk transacties valideert en hun toevoeging aan de blockchain autoriseert, vandaar ook de naam gedecentraliseerde databank. Dit in contrast met de conventionele situatie waarin één partij een database beheert en beslist over de verantwoordelijkheden voor het creëren, lezen, bijwerken en verwijderen van gegevens (Ølnes et al., 2017). Door het elimineren van de vertrouwenspersonen bij

transacties, heeft blockchain het potentieel om veel belangrijke industrieën te ontwrichten (Sultan, Ruhi, & Lakhani, 2018).

3.2 Smart Contracts

Als een blockchain de database is, dan zijn *smart contracts* de applicaties die een groot deel van de beloftes van blockchain waarmaken. Vitalik Buterin, de oprichter van Ethereum, definieert *smart contracts* als volgt: "Een mechanisme waarbij digitale activa en twee of meer partijen betrokken zijn en waar sommige of alle partijen activa investeren en activa automatisch tussen die partijen worden herverdeeld volgens een formule op basis van bepaalde gegevens die niet bekend zijn op het moment dat het contract wordt geïnitieerd" (Buterin, 2014). Met andere woorden, een smart contract is een programma dat op de blockchain draait en waarvan de correcte uitvoering wordt afgedwongen door het consensusprotocol (Luu, Chu, Olickel, Saxena, & Hobor, 2016). Dit wil zeggen dat een *smart contract* enkel wordt uitgevoerd indien de voorwaarden van dit contract zijn gevalideerd door de meerderheid van de *nodes* van het netwerk.

Aangezien de *smart contracts* zich op de blockchain bevinden, krijgen zij een uniek adres toebedeeld. Men kan een *smart contract* activeren door er een transactie naar te sturen. Vervolgens wordt het contract na validatie onafhankelijk en automatisch uitgevoerd op elke *node* van het netwerk (Christidis & Devetsikiotis, 2016).

Indien twee gebruikers een *smart contract* ondertekenen, zal het contract een beredenering bevatten dat een uitwerking heeft op de gegevens van alle delen van de database. Dit is bijvoorbeeld handig wanneer een persoon zijn adres wijzigt bij de gemeente, omdat de verandering van het adres dan ook kan worden weergegeven op zijn paspoort, rijbewijs en andere belangrijke databases. De toepassing van *smart contracts* zou de automatisering van handmatige processen vereenvoudigen bij zowel publieke als private instituties, wat op zijn beurt de productiviteit en groei zouden verbeteren (Walport, 2015).

De uitgebreide mogelijkheden van *smart contracts* hebben als gevolg dat ze voor een groot scala aan toepassingen worden overwogen. Zo zouden deze *contracts* kunnen worden toegepast voor het naleven van de regelgeving, de traceerbaarheid van producten en servicemanagement, maar ook om de productie en verkoop van namaakproducten tegen te gaan en fraude te bestrijden in de volgende industrieën: voedsel, financiële diensten, energie, geneesmiddelen, gezondheidszorg, telecommunicatie, transport, landbouw, olie en gas, etc. (Walport, 2015)

Een blockchain, gelijkaardig aan Bitcoin, die enkel transacties ondersteunt, maakt de overdracht van digitale activa tussen twee wantrouwende partijen mogelijk. Maar een blockchain die *smart contracts* ondersteunt, neemt dit een stapje verder en zorgt ervoor dat er interacties, processen met meerdere stappen, kunnen plaatsvinden tussen beide partijen (Christidis & Devetsikiotis, 2016).

Het gebruik van *smart contracts* biedt enkele voordelen. Zo kunnen de twee partijen de geprogrammeerde code inspecteren om de verschillende mogelijke uitkomsten te identificeren vooraleer ze beslissen deel te nemen aan het contract. Daarnaast is er ook zekerheid over de uitvoering van het contract aangezien de code reeds in het netwerk is geïmplementeerd en geen van beide partijen controle heeft over zowel deze code als het netwerk. *Smart contracts* zullen ook de mogelijkheid van een geschil uit de weg kunnen ruimen indien alle mogelijke uitkomsten zijn

opgenomen in het contract. Zo kunnen beide partijen het niet oneens zijn over de uiteindelijke uitkomst van een controleerbaar proces waaraan zij zelf hebben deelgenomen. *Smart contracts* werken als autonome actoren, waarvan het gedrag volledig voorspelbaar is. Men kan er dus op vertrouwen dat zij alle redeneringen zullen voortzetten zolang die redenering maar geprogrammeerd kunnen worden in de programmeertaal van de blockchain (Christidis & Devetsikiotis, 2016).
Een eenvoudig voorbeeld waar een smart contract benut kan worden, is de overdracht van eigendom, bijvoorbeeld een huis. De koper stuurt de som geld naar een smart contract. Het contract omsluit de regels van de transactie. Deze regels kunnen niet worden gewijzigd door één van de partijen zonder dat de andere hiervan op de hoogte is (Ølnes et al., 2017). Indien de verkoper de sleutel niet overhandigt binnen een bepaalde tijdsperiode zal de som geld worden teruggestuurd naar de koper. Indien de sleutel wel overhandigd wordt, zal de betaling uitgevoerd worden en het kadaster geüpdatet worden. Op deze manier kan men fraude in verband met vastgoed vermijden. Let op, bij dit voorbeeld zal een vertrouwde tussenpersoon die de overdracht van de sleutels bevestigt nog steeds noodzakelijk zijn. Toch kan men met behulp van *smart contracts* een aantal intermediaire taken van de notaris in verband met het kopen en verkopen van vastgoed automatiseren. Echter kunnen de belangrijke notariële taken zoals het opstellen van een contract, controle op de naleving en het afdwingen van het contract niet geautomatiseerd worden met behulp van blockchain (Ølnes et al., 2017). Een andere potentiële toepassing van *smart contracts* in de publieke sector is het bepalen en beheren van de tijdstippen waarop sociale bijstand zou worden uitgeleend en de voorwaarden waaronder deze uitkering zou moeten doorgaan of stoppen (Berryhill, Bourgery, & Hanson, 2018).
Kortom, een smart contract is nuttig wanneer machines, bedrijven of personen een digitale overeenkomst willen sluiten met de zekerheid, die cryptografie biedt, dat de overeenkomst wordt nageleefd in de grootboeken, databases of accounts van alle partijen bij de overeenkomst (Walport, 2015). Veel interacties die wij hedendaags met de overheid hebben, zouden geautomatiseerd kunnen worden. In sommige gevallen zouden *smart contracts* de interventie in dienstverlening sterk reduceren of zelfs overbodig maken (Berryhill et al., 2018). Toch is er nog nood aan verder onderzoek om zowel het potentieel van *smart contracts* geheel in kaart te brengen en belangrijker nog, om mogelijke fouten te voorkomen.

3.3 Kenmerken eigen aan blockchain

Uit de vijf kernelementen, dienende om blockchain zo volledig mogelijk te omschrijven, kunnen verschillende aspecten van de technologie worden herleid tot vier functionele kenmerken (Sultan et al., 2018). Deze unieke kenmerken vormen de fundering van de technologie en worden hier beknopt besproken.

3.3.1 Onveranderlijk

Een blockchain is een permanente registratie van transacties. Wanneer gegevens worden opgenomen door middel van een gevalideerde transactie zijn deze gegevens in praktijk onveranderlijk. De onveranderbare ketting van cryptografisch ondertekende transacties zorgt voor

de onweerlegbaarheid van de opgeslagen gegevens en draagt bij tot een hogere gegevensintegriteit (Lo, Xu, Chiam, & Lu, 2017). Hoewel onveranderlijkheid een van de kernkenmerken is van blockchain, is het tegelijkertijd ook een van de grootste beperkingen voor de praktische toepassingen. Er kunnen namelijk enkel blokken van gegevens aan de blockchain worden toegevoegd. In tegenstelling tot een traditionele database is er dus geen manier om data te verwijderen of te wijzigen eens deze data is ingevoerd in de blockchain. In gevallen waar men regelmatig gegevens verwijdert of wijzigt, is het gebruik van blockchain waarschijnlijk geen goede optie (Berryhill, Bourgery, & Hanson, 2018). Beleidsmakers zouden dan de voordelen van het gebruik van blockchain moeten afwegen tegen het feit dan men de data niet kan verwijderen of wijzigen. Ze moeten zich dus de vraag stellen of de onveranderlijkheid praktisch is voor het type data dat ze gaan gebruiken (Yaga, Mell, Roby, & Scarfone, 2018).

3.3.2 Gedecentraliseerd

Blockchain is gedecentraliseerd omdat het onafhankelijk is van een centraal controlepunt. De *nodes* houden elk een kopie van de database bij waaraan zij gegevens toevoegen door middel van het consensusmechanisme (Sultan et al., 2018). Een gebrek aan één enkele centrale autoriteit maakt het systeem eerlijker en beduidend veiliger. Bovendien zou een centrale autoriteit ook de macht hebben om het systeem te manipuleren en zou het een '*single point of failure*' kunnen betekenen (Lo et al., 2017).

3.3.3 Transparantie

Aangezien alle transacties op de blockchain zijn geverifieerd en vastgelegd met een tijdstempel, kunnen gebruikers gemakkelijk de vorige transacties verifiëren en nagaan in de geschiedenis van de blockchain. Het verbetert de traceerbaarheid en de transparantie van de gegevens die zijn opgeslagen in de blockchain. Daarnaast draagt de hogere transparantie bij tot een betere controleerbaarheid (Zheng, Xie, Dai, Chen, & Wang, 2018).

3.3.4 Vertrouwen

Vertrouwen in de blockchain wordt gecreëerd door de interacties tussen de verschillende *nodes* van het netwerk. Elke transactie wordt geverifieerd door het netwerk via een consensusmodel dat de regels bevat voor het valideren van de transacties. De gebruikers van het blockchainnetwerk vertrouwen op het netwerk zelf en zijn zo onafhankelijk van een derde partij om de transacties te faciliteren (Lo et al., 2017).

4 Het ontwerp van blockchain

In dit hoofdstuk wordt er dieper ingegaan op het ontwerp van de blockchain. Het is belangrijk om te weten dat er verschillende ontwerpen van een blockchainapplicatie mogelijk zijn. Indien overheden dergelijke applicaties willen benutten, zullen zij naargelang de toepassing rekening moeten houden met het ontwerp. Zo zijn er talloze keuzemogelijkheden over technische aspecten zoals cryptografiestandaarden, *peer-to-peer*-regelingen, gegarandeerde distributiebenaderingen, gedeeltelijke cryptografie, programmeertalen, communicatieprotocollen, etc. (Mainelli & Smith, 2015). Het is belangrijk dat men beseft dat blockchain toepassingen in vele verschillende ontwerpen kunnen worden geïmplementeerd. Het is belangrijk dat men er zich van bewust is dat blockchain veel verschillende ontwerpen kent. Er wordt echter een grove opdeling van de verschillende soorten blockchain ontwerpen gehanteerd. Hierbij is de voornaamste keuze enerzijds tussen 'publiek' of 'privaat' en anderzijds tussen '*permissionless*' of '*permissioned*' blockchains (Swan, 2015). Indien er gesproken wordt over de toegang tot de gegevens gaat het over publiek versus privaat. Wanneer het handelt over toegang tot transactieverwerking (gegevens toevoegen en verifiëren) gaat het over *permissionless* versus *permissioned* blockchains (Ølnes et al., 2017). Zowel publiek en *permissionless* als privaat en *permissioned* worden in de literatuur vaak als synoniemen gebruikt. Desondanks is dit niet volledig correct. Dit is mogelijks te wijten aan het gebrek aan standaarden omtrent de terminologie. In realiteit werken de meeste *permissionless* blockchains met een publieke toegang tot de gegevens en de transactieverwerking, terwijl *permissioned* blockchains deze toegang juist beperken. Om deze reden wordt deze sectie beperkt tot het onderscheid tussen *permissionless* en *permissioned* blockchains. Toch is het van belang om aan te halen dat een *permissioned* blockchain bijvoorbeeld niet uitsluitend privaat moet zijn. Ten slotte is het ook mogelijk om de toegang tot de gegevens verder in te perken (bv. gebruiker ziet enkel zijn eigen gegevens en niet van iedereen) (BitFury Group, 2015).

4.1 Permissionless blockchain

Permissionless blockchains, zoals bijvoorbeeld Bitcoin en Ethereum, laten vrije toegang tot alle gegevens toe. De gebruikers kunnen op autonome wijze transacties voorstellen en verifiëren en nemen op deze manier deel aan het netwerk. Dit creëert resistentie tegen censuur; geen enkele actor kan vermijden dat een transactie wordt toegevoegd aan de blockchain.
De integriteit van de gegevens op de blockchain worden onderhouden door de *nodes* van het netwerk. Deze komen door het uitvoeren van *Proof-of-Work* tot een consensus (Walport, 2015). Dit consensus mechanisme zorgt voor het vertrouwen tussen twee wederzijds wantrouwende partijen en stelt hun in staat onderling transacties uit te voeren (Berryhill et al., 2018).
Door gebruik te maken van *Proof-of-Work* kent een *permissionless* blockchain een groot nadeel. Elke node in het netwerk moet immers het *Proof-of-Work* probleem oplossen om de databases te synchroniseren. Bijgevolg is er nood aan een aanzienlijke hoeveelheid rekenkracht en dus energie om de blockchain te onderhouden. Dit zorgt voor een afname in efficiëntie en bemoeilijkt het uitbreiden naar een grotere schaal.

Daarnaast impliceert het publieke aspect van dit soort ontwerp dat de privacy voor transacties minimaal is (Jayachandran, 2017). Beide aspecten zorgen ervoor dat het gebruik van een *permissionless* blockchain minder interessant is voor de meeste bedrijfstoepassingen aangezien bedrijven vaak met vertrouwelijke informatie werken en dit liefst privaat houden. Om deze reden is het gebruik van *permissioned* blockchains beter geschikt voor interne activiteiten zoals bijvoorbeeld databasemanagement of auditing.

4.2 Permissioned blockchain

Het netwerk van een *permissioned* blockchain bezit over een bepaalde toegangscontrole. Het doel van een dergelijk netwerk is het beperken van de toegang tot transactieverwerking. Dit soort ontwerp laat toe dat men kan specifiëren wie onder andere betrokken wordt in het consensus mechanisme, wie transacties en *smart contracts* kan publiceren en wie bepaalde functies van deze *smart contracts* kan activeren (Verslype, 2017). Op deze manier kunnen enkel geautoriseerde entiteiten de blockchain onderhouden. *Permissioned* blockchains kunnen bijvoorbeeld iedereen toestaan de gegevens op de blockchain te lezen of kunnen de toegang tot informatie beperken tot slechts enkele bevoegde personen. Dit soort ontwerp kan evenwel iedereen toelaten om transacties te publiceren of de toegang hiervoor te beperken tot de geautoriseerde gebruikers (Yaga, Mell, Roby, & Scarfone, 2018).

Om dit te realiseren, is het noodzakelijk om de gebruikers en deelnemers van het netwerk te identificeren. De gebruiker is iemand die toegang tot de gegevens heeft en een deelnemer heeft betrekking tot het verifiëren van transacties (consensusmechanisme). Er kunnen namelijk geen regels of beperkingen aan een individu worden opgelegd in verband met het 'gebruiken' of toevoegen van gegevens indien de gebruikers en de deelnemers niet geïdentificeerd kunnen worden.

Om deze reden vereist een *permissioned* blockchain netwerk een uitnodiging om deel te nemen. Zowel de gebruikers als de deelnemers worden goedgekeurd door de oprichter van het netwerk of door een aantal regels dat door deze autoriteit werd opgelegd (Jayachandran, 2017). Echter kan het controlemechanisme, nodig om toegang te verkrijgen, verschillen van het bovenstaande. Zo zouden bijvoorbeeld bestaande deelnemers van een netwerk de toekomstige deelnemers kunnen bepalen. Een andere mogelijkheid is dat een regulerende instantie vergunningen tot het netwerk verleent (Jayachandran, 2017).

Naast de beperkingen die kunnen worden opgelegd binnen dit soort netwerk, kan men gebruik maken van een eenvoudiger consensus mechanisme, namelijk *Proof-of-Authority*. In tegenstelling tot *Proof-of-Work*, wat erg veel middelen vergt, vereist *Proof-of-Authority* enkel de identificatie van de deelnemers. *Proof-of-Authority* zou net zoals *Proof-of-Work* de integriteit van de gegevens moeten behouden. De deelnemers die de blockchain onderhouden, hebben namelijk onderling reeds een bepaalde vertrouwensband; zij zijn allen geautoriseerd om transacties te publiceren en verifiëren. Daarnaast kan hun autorisatie worden ingetrokken indien ze zich misdragen (Yaga et al., 2018). Het eenvoudigere consensusmechanisme zorgt ervoor dat *permissioned* blockchains doorgaans veel efficiënter en sneller werken. Omwille van bovenstaande redenen vormt een *permissioned* netwerk waarschijnlijk de meest geschikte optie voor de publieke sector.

Ondanks dat *permissioned* blockchain in de literatuur vaak geassocieerd wordt met een privaat netwerk kan men ook een publieke *permissioned* blockchain ontwerpen. Een dergelijk ontwerp zou de verantwoordingsplicht aanzienlijk kunnen vergroten aangezien iedereen, al dan niet in beperkte mate, toegang heeft tot de gegevens. Echter kunnen enkel geautoriseerde deelnemers gegevens toevoegen. Dit soort ontwerp is zeer interessant voor bepaalde toepassingen zoals supply chain management, financiële verslaggeving van de overheid of bedrijven, etc.
De regels met betrekking tot het functioneren van *permissioned* blockchains kunnen op voorhand vastgelegd en geprogrammeerd worden. Op deze manier kunnen bijvoorbeeld de regels en wetten, opgelegd door de overheid, in rekening worden gebracht binnen het netwerk. Uiteraard is het van belang dat het ontwerpen van zo een toepassing met grote zorgvuldigheid gebeurd. De toepassingen worden voornamelijk ontworpen door experts waarbij hun verantwoordingsplicht ten opzichte van het publiek in vraag kan gesteld worden. Hoewel men met blockchain technologie vaak de toegang tot gegevens wil 'democratiseren', zou dit mogelijks een averechts effect teweeg kunnen brengen. De experten die het systeem ontwerpen, vormen namelijk een minderheid. Zij kunnen in principe regels opleggen aan zowel de gebruikers als de deelnemers en slechts enkelen zouden in staat zijn deze regels te veranderen. Men kan ervan uitgaan dat een bepaald ontwerp de belangen van de betrokken actoren zal vertegenwoordigen. Om deze reden moet er een zorgvuldig beleidsproces worden gevoerd dat geleid wordt door de maatschappelijke behoeftes en niet door de behoeftes van enkele besluitmakers. De motivaties achter elke ontwerpkeuze moeten verantwoord kunnen worden aan de samenleving (Ølnes et al., 2017). Ten slotte zijn overheden genoodzaakt om onderling in overleg te gaan. Zo kan er besproken worden welk soort ontwerp het beste aansluit bij een bepaalde toepassing, rekening houdend met de voordelen en *trade-offs* van elk type ontwerp.

5 Framework

De mogelijkheden die het gebruik van blockchain technologie biedt, worden in veel verschillende domeinen erkend. Dit zorgt ervoor dat er veel middelen worden geïnvesteerd in het ontwikkelen en onderzoeken van mogelijke toepassingen van deze technologie (Chung & Kim, 2016). In deze sectie wordt er een framework besproken dat een eerste evaluatie kan vormen van de toepasbaarheid van blockchain voor de verschillende applicaties. Zo kunnen organisaties en overheden relatief snel inzicht verkrijgen of het gebruik van blockchain technologie al dan niet voordelig is voor een bepaalde toepassing. In deze thesis wordt voor de evaluatie van de toepassingen van blockchain aanleuning gezocht bij het framework beschreven in het artikel van Lo, Xu, Chiam en Lu (Lo et al., 2017). Het proces om de geschiktheid van blockchain te evalueren, omvat zeven criteria (Lo et al., 2017). Het behandelde framework wordt gebruikt om de verschillende toepassingen, besproken in de casestudy's te toetsen. Het is echter belangrijk om te vermelden dat dit framework als een soort vuistregel dient, maar dat niet alle mogelijke aspecten hierin verwerkt zijn. Er is namelijk nog nood aan verdere ontwikkeling en experimentatie om het volledige potentieel van blockchain in kaart te brengen en aan de hand hiervan een meer nauwkeurig framework op te stellen.

5.1 Meerdere partijen

In eerste instantie moet men nagaan of er meerdere partijen in het scenario betrokken worden. Normaliter worden transacties tussen partijen geregeld door tussenpersonen. Supply chain management (SCM) is hier een goed voorbeeld van. Het vereist complexe, dynamische en *multi-party* communicatie tussen de verschillende entiteiten zoals leveranciers van grondstoffen, producenten ter vorming van een eindproduct, magazijnen voor opslag en distributiecentra voor de aflevering van het product aan handelaren (Dictionary, 2019). SCM kent echter regelgevende en logistieke beperkingen aangezien de samenwerking verspreid ligt over verschillende rechtsgebieden (Lo et al., 2017). In zo een geval kan blockchain een gedeelde infrastructuur bieden met een neutraal karakter waar geen enkele van de deelnemende partijen zelf iets kan bepalen. Blockchain kan voordelen bieden in scenario's waarbij meerdere partijen en eventueel tussenpersonen betrokken worden. Dit zou zorgen voor een reductie van de grote hoeveelheid informatie onder controle van individuele partijen en tegelijkertijd het proces efficiënter en transparanter maken (Lo et al., 2017). Indien er een systeem nodig is binnen één enkele organisatie is het minder voordelig om blockchain te implementeren en bestaan er goedkopere en snellere alternatieven.

5.2 Vertrouwde autoriteit

Een tweede vraag naar de toepasbaarheid van blockchain is of er al dan niet nood is aan een vertrouwde autoriteit zoals banken en overheden. Het probleem dat zich stelt bij een vertrouwde autoriteit is dat dit mogelijks een 'single point of failure' kan betekenen. Indien zo een vertrouwde autoriteit problemen ervaart, worden alle gebruikers van zijn service getroffen. Blockchain

technologie is geschikt voor toepassingen waar er een gebrek is aan een vertrouwde autoriteit of waar de huidige autoriteit gedecentraliseerd kan worden (Lo et al., 2017). Het gebruik van blockchain technologie kan de rol van deze vertrouwde autoriteit vervangen. Het vertrouwenselement verdwijnt echter niet. De gebruikers verschuiven enkel hun vertrouwen van de centrale autoriteit naar de blockchain software en de correcte werking van de *nodes*. Het gebruik van blockchain zorgt ervoor dat men niet langer afhankelijk is van vertrouwde derden om de database te onderhouden. Het wordt daarom ook wel 'gedistribueerd vertrouwen' genoemd.

5.3 Gedecentraliseerde werking

Het derde criterium toetst de nood aan een gecentraliseerde werking. Een op blockchain gebaseerd systeem zorgt er immers voor dat geen enkele partij het systeem bestuurt, maar dat elk individu de controle heeft over zijn eigen gegevens en bezittingen, wat bijgevolg uitdagingen creëert voor het bestuur van het systeem. "*The management of the evolution of blockchain-based systems is more like diplomacy than traditional risk management or conventional product management"* (Lo et al., 2017). Daarom is de huidige configuratie van blockchain niet geschikt voor een systeem dat een gecentraliseerde werking vereist. Denk maar aan toepassingen waarbij bijvoorbeeld regelmatig gegevens worden gewijzigd of verwijderd of wanneer men te maken heeft met zeer gevoelige gegevens. Men zou in principe wel een gecentraliseerde blockchain kunnen ontwerpen, maar dit zou net de onderliggende bedoeling van blockchain dwarsbomen.

5.4 Data transparantie versus vertrouwelijkheid

Een vierde vraag die men moet stellen, is of er datatransparantie of vertrouwelijkheid vereist is. Blockchain biedt een neutraal platform waar alle gebruikers de gepubliceerde gegevens kunnen zien. Doordat al deze gegevens gepubliceerd zijn, kunnen de transactievereisten worden nagegaan door de *nodes*. Zo gebruiken de *nodes* van het Bitcoin netwerk de publieke gegevens om na te gaan of de zender genoeg middelen beschikbaar heeft om de transactie te verrichten. Het versleutelen van gegevens vooraleer ze op de blockchain worden opgeslagen, kan de vertrouwelijkheid vergroten maar zou de prestaties, transparantie en onafhankelijke controleerbaarheid verminderen. Men kan er ook voor kiezen om slechts een referentie of *hash* van de gegevens in de blockchain op te slaan en deze te linken met de werkelijke, 'ruwe' gegevens die ergens anders (*off-chain*) bewaard worden. Deze *hash* verwijst enkel naar de gegevens zonder ze werkelijk op de blockchain op te slaan. Dit zou de vertrouwelijkheid en prestaties ten goede komen, maar ondermijnen toch gedeeltelijk het voordeel van blockchains bij het leveren van gedistribueerd vertrouwen (Lo et al., 2017). De belangrijkste *trade-off* bestaat dus tussen de voordelen van het delen van gegevens binnen eenzelfde groep en het behouden van vertrouwelijkheid jegens concurrenten of privacy waar nodig.

5.5 Gegevensintegriteit

Het volgende aspect dat men moet nagaan is of de integriteit van de transactiegeschiedenis vereist is. De integriteit van de gegevens is van cruciaal belang voor het tracken van fysieke activa doorheen de verwerking en de verandering in eigendom van deze producten. Om deze reden past het gebruik van blockchain goed binnen bijvoorbeeld supply chain management. Echter kan het gebruik van blockchain om enkel integriteit te bereiken relatief kostelijk zijn in vergelijking met andere mechanismes. Zo zijn er reeds bestaande mechanismes beschikbaar om de oorsprong van gegevens te bewijzen zoals *hashing* technologie (Lo et al., 2017). Een systeem dat reeds zo een tracking mechanisme heeft ingebouwd, haalt mogelijks geen extra voordeel uit de 'herkomstinformatie' die wordt toegevoegd door het gebruik van blockchain maar zal bijkomende voordelen genieten zoals een betere gegevensuitwisseling en meer transparantie.

5.6 Onveranderlijkheid van de gegevens

De zesde vraag heeft betrekking tot de onveranderlijkheid van de gegevens. In economieën waar externe dienstverleners niet altijd betrouwbaar zijn en waar veel corruptie heerst, kan het gebruik van blockchain veel voordelen genereren. Blockchain voorziet in de nood aan onveranderlijkheid en niet-weerlegbaarheid door de blokken cryptografisch aan elkaar te linken. In praktijk kunnen de gegevens op de blockchain niet veranderd worden aangezien de gegevens voortdurend gedupliceerd en verspreid worden over veel verschillende locaties en organisaties. Pogingen om de gegevens te veranderen in één locatie zal door de andere deelnemers worden geïnterpreteerd als een 'aanval' op de integriteit en zal bijgevolg afgewezen worden. Dit wordt doorgaans gezien als een goede eigenschap, toch kan dit voor problemen zorgen. Indien we gebruik gaan maken van blockchain in de 'echte' wereld zullen er zich verschillende problemen voordoen: betwiste transacties, incorrecte adressen, het blootstellen of verliezen van de private sleutel, fouten bij het invoeren van de gegevens of het bevel van de rechter om bepaalde inhoud te verwijderen van de blockchain. Echter is deze onveranderlijkheid niet geheel onontkoombaar. In een *permissioned* netwerk is het mogelijk om een veranderlijkheidsprotocol te voorzien; zo kunnen er eventueel dingen gewijzigd of verwijderd worden indien de *nodes* tot een consensus komen omtrent de betwiste transactie.
De implicaties rond de onveranderlijkheid van transactiegeschiedenis moeten zorgvuldig overwogen worden bij het ontwerpen van het blockchainsysteem. Het onveranderlijke karakter zorgt ervoor dat blockchain minder flexibel is dan conventionele technologieën die beheerd worden door vertrouwde externe organisaties die bijvoorbeeld *rollback* ondersteunen (Lo et al., 2017).

5.7 Hoge verwerkingscapaciteit

Tenslotte moet men zich afvragen of een hoge verwerkingscapaciteit vereist is voor de toepassing in kwestie. Blockchains (voornamelijk *permissionless)* zijn momenteel moeilijker schaalbaar in

vergelijking met conventionele middelen. Toch is dit geen inherente beperking vermits deze schaalproblemen in de nabije toekomst overwonnen kunnen worden. *Permissioned* blockchains met een zorgvuldig ontwerp en *performance tuning* hebben reeds veel betere prestaties ten opzichte van *permissionless* ontwerpen. Echter is blockchain waarschijnlijk niet geschikt voor het opslaan van 'Big Data' vanwege de grote hoeveelheden en de *high velocity* van de dataverwerking (Lo et al., 2017). Deze eigenschappen gaan niet goed samen met het feit dat elke *node* van het netwerk een volledige kopie bezit van de gedeelde gegevens. De huidige oplossing voor dit probleem is om de grote hoeveelheden van gegevens *off-chain* te bewaren en slechts een referentie of link op te slaan in de blockchain. Zo kan men voorkomen dat in elke node een kopie van alle gegevens wordt opgeslagen (Lo et al., 2017).

6 Uitdagingen van blockchain binnen de publieke sector

Het gebruik en de implementatie van blockchain technologie brengt uiteraard wat uitdagingen met zich mee. In dit hoofdstuk worden de voornaamste uitdagingen met betrekking tot de implementatie, ontwikkeling en het bestuur van blockchain besproken. Daarnaast worden ook nog de technologische beperkingen behandeld.

6.1 Onveranderlijkheid data en privacy

Zoals eerder besproken is de onveranderlijkheid van de gegevens een van de kerneigenschappen van blockchain. Hoewel deze eigenschap belangrijke voordelen biedt, is het tegelijkertijd ook een van de grootste beperkingen van blockchaintoepassingen. In tegenstelling tot de traditionele databases, kan men bij blockchain geen gegevens verwijderen of veranderen zodra ze in de blockchain zijn opgeslagen. Blockchain is dus geen goede keuze wanneer er regelmatig gegevens gewijzigd of verwijderd moeten worden.
Echter zorgt de onveranderlijkheid van de gegevens ook voor juridische conflicten. In 2016 werd door de Europese Unie een nieuwe regulering goedgekeurd inzake gegevens privacy, namelijk de '*General Data Protection Regulation'* ofwel GDPR genoemd (Europese Unie, 2016). Deze wet heeft als doel om alle EU-burgers beter te beschermen tegen onder andere privacy- en datalekken. Artikel 17 van de GDPR bevat het 'recht om vergeten te worden'-principe. Dit principe bepaalt dat een individu, onder bepaalde voorwaarden, het recht heeft om de verwijdering van persoonlijke informatie te eisen (Europese Unie, 2016). Dit zou mogelijks ook bepaalde overheidsdocumenten of databases omvatten. Nu wordt al snel de discrepantie duidelijk tussen de onveranderlijkheid van de gegevens en de GDPR. Het gebruik van blockchain voor dergelijke informatie zou ervoor zorgen dat het 'recht om vergeten te worden'-principe onmogelijk afdwingbaar wordt. Binnen de publieke sector zou dit probleem slechts relevant zijn in een beperkt aantal gevallen. Zo hebben burgers niet het recht om de verwijdering van hun informatie te eisen uit alle overheidsdatabases. Ze mogen uiteraard niet aan de overheid vragen om hun identiteitsinformatie of juridische feiten te verwijderen. In een wereld waar privacy en bescherming van persoonlijke gegevens steeds belangrijker wordt, zullen overheden goed moeten overwegen welke gegevens op de blockchain worden opgeslagen en welke gegevens *off-chain* bewaard worden. Bij het ontwerpen van de blockchain is het uitermate belangrijk dat deze privacyaspecten door de overheden worden gerespecteerd.

6.2 Dataopslag en kwaliteit

Publieke en private instellingen maken vaak gebruik van een database om grote hoeveelheden gegevens op te slaan zoals documenten, foto's, video's, software, etc. Blockchain is in het algemeen meer een lijst van transacties en bevat hoogstens kleine hoeveelheden gegevens om *smart contracts* uit te voeren en te begeleiden (Berryhill et al., 2018). Zoals eerder vermeld zijn blockchains niet geschikt voor het opslaan van grote hoeveelheden gegevens. Men kan echter wel de grote

hoeveelheid gegevens *off chain* bewaren en slechts een *hash* opslaan in de blockchain (Yaga et al., 2018). Indien men enkel opzoek is naar gegevensopslag is blockchain technologie waarschijnlijk niet de geschikte keuze. Indien overheden echter opzoek zijn naar een manier om een gedeeld en betrouwbaar transactieoverzicht te behouden, kan blockchain eventueel een oplossing bieden. Het is bovendien zeer goed mogelijk dat er een hybride aanpak nodig is, waarbij men blockchain technologie in combinatie met een oplossing voor de gegevensopslag (bv. traditionele database) benut. Zo zou men de transacties op de blockchain kunnen linken met gegevens die buiten de blockchain worden opgeslagen (Berryhill et al., 2018).
Vanzelfsprekend hangen de kwaliteit van de gegevens af van degene die deze oorspronkelijk heeft ingevoerd. Men moet er dus op toezien dat de gegevens accuraat en zorgvuldig worden ingevoerd in de blockchain.

6.3 Uitdagingen bij het Proof-of-Work consensusmodel

In dit gedeelte worden twee limieten van het *Proof-of-Work* consensusmodel besproken, de energieconsumptie en de schaalbaarheid. Zoals eerder aangehaald zullen overheden echter meestal *permissioned* netwerken verkiezen en bijgevolg ook gebruik maken van een efficiënter consensusmodel zoals *Proof-of-Authority*. Toch is het belangrijk om de limieten van *Proof-of-Work* toe te lichten aangezien deze vaak als argument worden aangehaald tegen het gebruik van blockchain terwijl deze limieten enkel van toepassing zijn op blockchainnetwerken met een *Proof-Of-Work* model.

6.3.1 Energieconsumptie

Blockchainnetwerken met *Proof-Of-Work* eisen veel computerkracht om de transacties te verifiëren. Momenteel wordt het jaarlijks verbruik van het grootste *Proof-of-Work* netwerk, Bitcoin, geschat op zo'n 52 terrawattuur (TWh) en piekte zelfs tot 72 TWh in November 2018 tijdens de 'crypto-hype' (Digiconomist, 2019). Om dit even in perspectief te zetten: België verbruikte volgens cijfers van Statbel in 2017 zo'n 82 TWh (Statbel, 2019). Het huidige jaarlijks verbruik van 52 TWh is het equivalent van het verbruik van bijna 5 miljoen Amerikaanse gezinnen. Het elektriciteitsverbruik voor één enkele transactie van Bitcoin zou één Amerikaans huishouden kunnen voorzien van 17 dagen stroom (Digiconomist, 2019). Deze cijfers maken duidelijk dat dit elektriciteitsverbruik onhoudbaar is.
In de toekomst zullen software en hardware echter verbeteren waardoor men efficiënter (minder energieverbruik) kan *minen*. Aan de andere kant blijven blockchainnetwerken ook steeds groeien en eisen bijgevolg meer energie. Een ander aspect dat men ook in rekening moet brengen, is dat bij de creatie van een nieuwe *node* de volledige blockchaingeschiedenis gedownload moet worden (Yaga et al., 2018). Begin 2019 bedroeg de volledige dataset van Bitcoin ongeveer 197 GB (Statista, 2019). Het opstellen van een nieuwe *node* vergt dus ook een grote downloadcapaciteit.

Nogmaals, dit extreme energieverbruik geldt enkel voor blockchain platformen die gebruik maken van *Proof-of-Work*. Aangezien de overheid meestal met *permissioned* netwerken en *Proof-of-Authority* zal werken, vormt het energieverbruik geen probleem.

6.3.2 Schaalbaarheid

Permissionless netwerken die een *Proof-Of-Work* consensusmodel hanteren, stuiten op schaalproblemen. Dit doet zich voor wanneer het netwerk zijn maximale verwerkingscapaciteit bereikt heeft en dus niet meer in staat is de transacties snel genoeg te verwerken. Zo kan het Bitcoin netwerk bijvoorbeeld slechts zeven transacties per seconde verwerken. Dit is zeer traag in vergelijking met Visa die gemiddeld een 2.000 transacties per seconde verwerkt en een 'topsnelheid' van 56.000 transacties per seconde kan behalen (Croman et al., 2016). De schaalbaarheid van een netwerk wordt een steeds groter probleem naarmate het populairder wordt. Zo zullen meer gebruikers uiteraard voor meer transacties zorgen en bijgevolg moeten de gegevens voor deze transacties ook verspreid worden doorheen het groeiende netwerk (Berryhill et al., 2018). Zonder oplossingen zal een blockchain met *Proof-of-Work* nooit kunnen concurreren op vlak van verwerkingscapaciteit met bewezen technologieën zoals bijvoorbeeld van Visa. De problemen in verband met schaalbaarheid zijn, nogmaals, enkel van toepassing op *permissionless* netwerken. *Permissioned* netwerken behalen tegenwoordig al veel hogere prestaties. Zo verwerkt de *Hyperledger Fabric* van IBM ongeveer 3.500 transacties per seconde (IBM Research Editorial Staff, 2018). In de toekomst zou de *Hyperledger* zelfs opnieuw ontworpen kunnen worden om te schalen tot wel 20.000 transacties per seconde (Gorenflo, Lee, Golab, & Keshav, 2019).

6.4 Beleid

Een van de meest aangehaalde voordelen van blockchain is dat het de behoefte aan een centrale autoriteit overbodig maakt. Dit is echter niet helemaal correct, ook niet voor *permissionless* blockchains waar iedereen toegang tot heeft en transacties op kan uitvoeren. Blockchains ontstaan namelijk niet zomaar. Ze moeten ontworpen en bestuurd worden door programmeurs, ingenieurs en andere besluitvormers die belast worden met belangrijke rollen bij de ontwikkeling. Deze ontwikkelaars vormen in principe ook een centrale autoriteit en hun samenstelling, acties en beslissingen geprogrammeerd in de blockchain zijn mogelijks minder transparant dan de transacties zelf (Berryhill et al., 2018). Naarmate de samenleving steeds meer verantwoording eist, is het van groot belang wie de eigenaar is van de gegevens, wie de blockchain bestuurt en op welke manier dit gebeurt.

De mogelijke voordelen die blockchain te bieden heeft, maakt de technologie aantrekkelijk voor overheden en andere organisaties. Toch brengt de gedistribueerde aard van blockchain en de nood aan beslissingen met betrekking tot het ontwerp enkele moeilijkheden met zich mee. De gedistribueerde aard van blockchain vereist een transformatie van de overheid om alle mogelijke voordelen te realiseren. Terwijl traditionele systemen relatief eenvoudig te besturen zijn, vergt de gedistribueerde aard van blockchain veranderingen in verantwoordelijkheden en nieuwe

benaderingen met betrekking tot het bestuur. Het implementeren van blockchain zonder deze veranderingen zou mogelijks weinig bijkomende voordelen opleveren (Ølnes et al., 2017).

6.4.1 Auditing toepassingen

Uiteindelijk zullen overheidsinstanties vertrouwd moeten worden met het coderingsproces, zelfs wanneer het echte codeerwerk in verband met de toepassingen wordt geoutsourcet. De overheid moet namelijk de geschiktheid van de code van het blockchainproject evalueren en neemt zo ook de eindverantwoordelijkheid op zich (Berryhill et al., 2018). De overheid zal dus een soort van audit moeten uitvoeren. Waar de traditionele audit focust op het controleren van transacties, zal in dit soort omgeving de nadruk verschuiven naar een audit op het systeemniveau. In de blockchainomgeving dienen zowel de software als de algoritmes gecontroleerd te worden. Zo kan men het correct functioneren ervan garanderen en analyseren of de software en algoritmes de wetgeving naleven (Ølnes et al., 2017). De algoritmes die in de software zijn ingebouwd, bepalen of er aan de regels voldaan wordt en de transacties correct zijn. Deze algoritmes worden steeds meer autonoom en 'onzichtbaar' waardoor het moeilijk wordt voor het publiek om deze met een kritisch oog te bekijken (Janssen & Kuk, 2016). Daarom is het zeker belangrijk dat deze algoritmes gecontroleerd worden. Hoewel open-source software (Bitcoin, Ethereum, *Hyperledger*,…) de 'broncode' van de software publiek toegankelijk maakt, is er hoe dan ook nood aan externe, objectieve controle (Ven, Verelst, & Mannaert, 2008). De onderliggende algoritmes zijn namelijk vrij complex waar gespecialiseerde expertise noodzakelijk is en waar men niet zomaar beroep kan doen op het publiek om de codes en algoritmes te herzien. Het publiek neemt aan dat ze kunnen vertrouwen op de correcte werking van de software en algoritmes.

6.4.2 Rol van de overheid

Zoals eerder vermeld hebben blockchaintoepassingen het potentieel om bepaalde rollen van de overheid te vervangen zoals het opslaan van officiële documenten en het beschikbaar stellen van gegevens. Indien men blockchain wil toepassen in de publieke sector zal dit een transformatie vergen van de overheid. De toepassingen moeten niet enkel geauditeerd worden, maar het systeem moet ook door iemand worden ontworpen, bediend en onderhouden. De overheid neemt haar plaats in als vertrouwde beheerder van een register die de transactieregels bepaalt en toepassingen controleert om de juiste werking ervan te waarborgen. De nieuwe rol van de overheid zal meer betrekking hebben tot het creëren van infrastructuur en het besturen van de blockchain om de juiste datakwaliteit te kunnen garanderen. Overheden zullen dus waarschijnlijk verantwoordelijk blijven voor het besturen van de toepassingen en zullen ook aansprakelijk gesteld kunnen worden in geval van storing of problemen met de datakwaliteit (Ølnes et al., 2017).
Vermits er geen uniforme oplossing bestaat, is het noodzakelijk dat de overheid experimenteert. Blockchain kan namelijk verschillende vormen aannemen met elk hun eigen voordelen en kenmerken. Het implementeren van blockchain is geen lineair of rationeel proces. Er zijn nog veel onzekerheden en er is nog verder onderzoek nodig om de technologie en zijn beperkingen volledig

in kaart te brengen. Bovendien zorgen nieuwe technologieën vaak voor een verandering van menselijk gedrag dat op zijn beurt weer de technologische toepassingen beïnvloedt (DeSanctis & Poole, 1994). Een belangrijk aspect van experimenteren, is dat de toepassingen kunnen worden aangepast aan veranderende omstandigheden. Dit aanpassingsvermogen wordt vaak als bepalende factor beschouwd voor het succes van IT-systemen. Dan rest nog de vraag of blockchain voldoende aanpassingsvermogen bezit om updates met betrekking tot de implementatie en het bestuur aan te pakken. Kleinschalige experimenten zijn noodzakelijk om de interactie tussen de technologische kenmerken van blockchain en de specifieke eisen van overheidsprocessen te onderzoeken. Indien men op termijn overschakelt naar grootschalige experimenten zal er behoefte zijn aan een zekere mate van standaardisatie om interoperabiliteit te garanderen. Toch moet men hier mee opletten; een 'onrijpe' technologie standaardiseren zou de ontwikkeling ervan kunnen belemmeren (Ølnes et al., 2017). Daarnaast zal er waarschijnlijk een combinatie van technologieën nodig zijn om blockchain geschikt te maken voor gebruik binnen de overheid (van Engelenburg, Janssen, & Klievink, 2017). Zoals eerder vermeld zouden bijvoorbeeld de transacties kunnen worden opgeslagen in de blockchain met enkel een referentie (*hash*) naar de onderliggende gegevens die in een ander systeem worden opgeslagen. Bij implementatie van blockchain in de publieke sector zal men echter ook rekening moeten houden met de institutionele aspecten. Zo kan er mogelijks discussie ontstaan rond de geografische locatie van de verschillende *nodes*. Sommige overheden zullen waarschijnlijk eisen dat de *nodes* zich in hun rechtsgebied bevinden. Indien dit niet het geval is bestaat de kans dat er andere wetten van toepassing zijn (Ølnes et al., 2017).

6.4.3 Regelgeving

Het gebruik en de ontwikkeling van blockchain vereist een doordachte toepassing van de huidige wettelijke kaders in combinatie met nieuwe wettelijke oplossingen. Voorstanders van gedecentraliseerde systemen strijden voor een toekomst waar informatie en interactie niet beperkt wordt door een centrale autoriteit. Zij stellen dat het contraproductief zou zijn om blockchain in dit vroege en innovatieve stadium te reguleren. De geschiedenis van *peer-to-peer* technologie toont aan dat het waarschijnlijk een aantal jaar zou duren voordat het volledige potentieel duidelijk wordt. Daarom wordt er aanbevolen dat beleidsmakers nog niet ingrijpen met strenge reguleringen of normen die de innovatie mogelijks kunnen verstikken. Er moet eerder gezocht worden naar manieren om de nieuwe benaderingen binnen de huidige wettelijke kaders op te nemen en de ontwikkeling van blockchain te stimuleren (Yeoh, 2017). Anderen zijn van mening dat een overmatige afhankelijkheid van de automatisering van bijvoorbeeld wetten, contracten en informatiestromen zou kunnen leiden tot een 'tirannie van codes' (De Filippi, 2014) (Lee, 2015). Hoe beleidsmakers juist moeten omgaan met de ontwikkeling en implementatie van blockchain is niet geheel duidelijk. Volgens een rapport van de OESO kunnen we drie soorten regelgevende posities onderscheiden (OECD, 2018).

- **"Study-and-Wait-and-See"**: Aangezien blockchain een nieuwe complexe technologie is, bevinden de meeste beleidsmakers zich in deze positie. Net zoals de meeste personen en instituties proberen beleidsmakers de technologie en de bijhorende socio-economische

effecten volledig te begrijpen en te conceptualiseren. Aan de ene kant is dit een goede aanpak want overhaaste en strikte reguleringen zouden de innovatie kunnen afremmen. Anderzijds is er binnen de sector echter nood aan een duidelijke wetgeving om nieuwe businessmodellen te proberen.

- **"Nieuwe wet- en regelgeving"**: Doordat de technologie nog in zijn kinderschoenen staat, is er een gebrek aan algemeen aanvaarde terminologie en normen in verband met blockchain. Toch zijn verschillende landen begonnen met nieuwe wetten en regels te implementeren. Zo heeft Rusland een regulerend raamwerk aangekondigd voor *Initial Coin Offerings* (ICO's) en staat Frankrijk toe dat *crowdfunding*-records worden bijgehouden op de blockchain. Ook verschillende staten in Amerika hebben staatswetten uitgevaardigd met betrekking tot *smart contracts*, digitale handtekeningen en de juridische toelaatbaarheid van blockchain-grootboeken als bewijsmateriaal (OECD, 2018). De kans bestaat echter dat een nieuwe wetgeving een averechts effect heeft en uiteindelijk gewijzigd moet worden. Het feit dat er geen algemeen aanvaarde terminologie is, kan daarnaast ook juridische verwarring veroorzaken.

- **"Begeleiding en *sandboxing*"**: Gezien de nadelen van de bovenstaande aanpakken concluderen sommige beleidsmakers dat het enerzijds te vroeg is voor een nieuwe regelgeving. Anderzijds vinden zij het te riskant om de kat uit de boom te kijken. Daarom hebben zij ervoor gekozen regelgevende begeleiding te bieden over hoe de nieuwe technologie past binnen de bestaande wettelijke kaders. Daarnaast bieden zij ook '*sandbox*' mogelijkheden om te experimenteren met nieuwe modellen. *Sandboxing* betekent dat er een juridisch veilige omgeving is voor blockchainontwikkelaars om hun producten te testen. Hiervoor worden er vaak een aantal wettelijke uitzonderingen gemaakt. De producten worden onder nauwlettend toezicht geïmplementeerd op een gecontroleerde schaal voor een beperkte periode. In 2016 heeft de *Financial Conduct Authority* (FCA) in het Verenigd Koninkrijk groen licht gegeven voor *sandboxes* met betrekking tot FinTech-services, waaronder ook blockchain. Ook Canada, Australië, Singapore, Zwitserland en Luxemburg hebben soortgelijke initiatieven aangekondigd. In 2017 heeft de Europese Commissie een verklaring uitgegeven waarin *sandboxing* in FinTech-services wordt erkend als een aanvaardbaar regelgevingsinstrument (OECD, 2018). Deze aanpak zou naar verwachting veel voordelen voor beide partijen opleveren omdat de innovatie en kennisopbouw gestimuleerd worden.

Naast de verschillende soorten regelgevende posities vermeldt het rapport van de OESO dat een van de belangrijkste regelgevende initiatieven geleid wordt door een samenwerking tussen de *International Organization for Standardization* (ISO) en *Standards Australia*. Zij hebben een *taskforce* opgericht om te werken aan blockchain-standaarden en aan standaarden over de interoperabiliteit van aparte blockchains. Zonder diep in te gaan op technische specificaties zou de normalisatie drie cruciale gebieden omvatten:

- **"Terminologie"**: Zoals eerder vermeld gebruiken mensen verschillende termen om hetzelfde te benoemen. Zelfs de technologie kent verschillende benamingen zoals blockchain, *distributed ledger, shared ledger, public ledger,* etc. Er is eensgezindheid nodig om verwarring te voorkomen.

- **"Architectuur"**: Dit heeft voornamelijk te maken met standaarden omtrent protocollen voor gegevensopslag, gegevensverspreiding en toegangsrechten, consensusmechanisme, *smart contracts*, etc.

- **"Bestuur"**: Het bestuur heeft betrekking tot de procedures en regels over hoe een blockchain wordt geïnitieerd en beheerd. Het bepaalt de regels en procedures, het netwerklidmaatschap, het managen van de *permissions*, software updates, wettelijke verslaggeving en bescherming tegen cyberrisico's.

Na implementatie van de juiste normen rest er enkel een transparante dialoog tussen de beleidsmakers en de experten. Hierdoor voorkomt men een onstuimige regelgeving die de technologische vooruitgang mogelijks zou belemmeren. Zowel de kennis van bestaande technologieën als een blik op toekomstige trends zorgen voor de mogelijkheid om een effectieve regulering in te voeren (OECD, 2018).

Casestudy's

7 Casestudy Estland: e-Health

Estland is een technologisch geavanceerd land en staat relatief ver op vlak van blockchaintoepassingen. Zij experimenteren reeds sinds 2011 met blockchain en zijn een erkende leider op vlak van *e-Government*. De Estse overheid maakt gebruik van een bepaald ontwerp van blockchain om hun gegevens te beveiligen, namelijk de *Keyless Signature Infrastructure* (KSI)-blockchain. De KSI-blockchain werd ontwikkeld door *Guardtime*, een Estlands bedrijf dat in 2008 werd opgericht met als doel het elimineren van de nood aan vertrouwen binnen het overheidsnetwerk (Guardtime, 2019). In eerste instantie dient de KSI-blockchain om de integriteit en beveiliging van de gegevens te garanderen. Daarnaast maakt Estland gebruik van X-Road als ruggengraat voor hun digitaal systeem. Hiermee wordt gegevensuitwisseling tussen zowel openbare als particuliere sectordatabases mogelijk gemaakt. Alhoewel KSI-blockchain en X-Road geen concrete toepassingen van blockchain vormen, is het gebruik van beide een belangrijke factor binnen het digitalisatieproces. Om deze reden worden KSI en X-Road eerst besproken. Hierna volgt een veelbelovende toepassing met betrekking tot de *e-Health* records die als casestudy wordt uitgediept.

7.1 KSI blockchain

Na een nationale cyberaanval in 2007 erkende Estland dat een nieuwe aanpak nodig was om het vertrouwen in hun digitaal systemen te herstellen. Om deze reden werd er in 2008 samen met *Guardtime* een schaalbaar en veilig systeem voor digitale handtekeningen ontwikkeld, namelijk de KSI-blockchain.

KSI is een methode en een netwerkinfrastructuur voor de uitgifte en verificatie van KSI-handtekeningen. In tegenstelling tot de traditionele digitale handtekening zoals *Public-key Infrastructure* (PKI) die gebruik maken van asymmetrische sleutelcryptografie, is KSI enkel gebonden aan de *hash* functies. Dit wil zeggen dat het verificatieproces voor deze digitale handtekening enkel berust op de veiligheid van deze *hash* functies (en de beschikbaarheid van een database), waardoor het systeem makkelijker te schalen is. Een gebruiker kan met het KSI-systeem interageren door de *hash* waarde van zijn te ondertekenen gegevens (document) in te dienen. Vervolgens ontvangt hij zijn digitale handtekening die de tijd van de handtekening, de integriteit van de gesigneerde gegevens en de oorsprong van deze handtekening bewijst (Guardtime, 2019).

Het gebruik van KSI kent enkele voordelen. Zo is het systeem makkelijk schaalbaar tot op industrieel niveau; het systeem groeit niet lineair in functie van het aantal transacties, maar neemt lineair toe in functie van de tijd (onafhankelijk van aantal transacties). Zo kunnen KSI-handtekening tot op exabyte (1 miljard gigabytes) schaal worden gegenereerd. Ter illustratie: er zouden ongeveer een biljoen documenten (van 1MB) per dag ondertekend kunnen worden met behulp van KSI zonder dat hier significante rekenkundige-, opslag- of netwerkkosten aan verbonden zijn.

De KSI-blockchain is een *permissioned* netwerk met een snellere verwerkingstijd, doorgaans minder dan één seconde. Bovendien zijn de gesigneerde gegevens makkelijk overdraagbaar; het is mogelijk ze te verifiëren zelfs nadat ze organisationele of geografische grenzen hebben overschreden. Verder is de cryptografie achter de KSI-handtekeningen bestand tegen *quantum computing*, wat de (toekomstige) veiligheid ten goede komt. Ten slotte wordt de privacy van de gegevens gegarandeerd. Het KSI-systeem neemt namelijk nooit klantgegevens op; het systeem is gebaseerd op een éénrichting cryptografische *hash* functie. Dit wil zeggen dat de *hash* waardes op een unieke manier de gegevens representeren zonder dat men de gegevens kan reconstrueren uitgaande van de *hash* waardes. Dit zorgt voor de vertrouwelijkheid van de gegevens (Guardtime, 2019).
Door middel van KSI kunnen burgers de correctheid van hun eigen gegevens in overheidsdatabases verifiëren. Daarnaast is het voor bevoorrechte 'insiders' onmogelijk om binnen de overheidsnetwerken onopgemerkt illegale handelingen uit te voeren. Op deze manier worden de burgers verzekerd dat hun gegevens veilig én accuraat worden bijgehouden. Zo worden de *e-Health* records van alle burgers beheerd met behulp van de KSI-technologie.
Kortom, KSI wordt gebruikt om netwerken, systemen en gegevens te beveiligen en garandeert de privacy van de gegevens. Door de implementatie van de KSI-blockchain in overheidsnetwerken kan niemand onopgemerkt wijzigingen doorvoeren in gegevens en kan men de authenticiteit van de gegevens wiskundig bewijzen. De KSI-blockchain wordt voor zowel interne als externe processen gebruikt om de integriteit van de gegevens te onderhouden en maakt het mogelijk om zowel opzettelijke als onopzettelijke wijzigingen te detecteren.

7.2 X-Road

X-Road is een *open source* oplossing voor gegevensuitwisseling en biedt een veilige manier voor overheden en organisaties om diensten te leveren en te gebruiken (Amet, 2019). Het is de ruggengraat van het Estse digitale systeem. Het laat de verschillende *e-Service* informatiesystemen van de publieke en de private sector in harmonie coöpereren. Estland biedt een groot gamma van digitale diensten aan zoals *e-Tax, i-Voting, e-Health, e-Residency*, etc. Aangezien elke afdeling zijn eigen informatiesysteem benut, maken zij allen gebruik van de X-Road om interoperabiliteit tussen de verschillende organisaties te garanderen. Hierdoor werven zij een vlotte samenwerking en moeten de gegevens van elke burger slechts eenmaal worden geregistreerd. X-Road heeft zich verder ontplooid tot een systeem dat zowel data kan toevoegen aan meerdere informatiesystemen, grote gegevenssets kan verzenden als meerdere informatiesystemen gelijktijdig kan doorzoeken. Momenteel maken 52.000 organisaties indirect gebruik van X-Road. Hierdoor zou X-Road naar verluidt de Estlanders 1.400 jaar arbeidstijd per jaar besparen (e-Estonia, z.d.). Omgerekend is dit ongeveer 0,4 arbeidsdagen per inwoner per jaar.

7.3 e-Health records

7.3.1 Situatieschets

Het belang van gezondheidszorg kan nauwelijks overschat worden. Echter maken beleidsmakers wereldwijd zich zorgen over de toekomstige draagbaarheid van het systeem. De kosten in verband met de gezondheidszorg volgen de laatste jaren een sterk stijgende trend (Europese Commissie, 2017). Dit valt deels te wijten aan de vergrijzing; er is een toenemende behoefte aan dienstverlening voor de ouderen die ook steeds ouder worden. Tegelijkertijd is er een kleiner aantal werkende mensen die het financieringssysteem van de gezondheidszorg kunnen ondersteunen. Naast de veroudering van de bevolking stijgt ook de kost van de gezondheidszorg door nieuwe en vaak duurdere technologieën of behandelingen (Schokkaert, 2016). Beide factoren creëren een enorme druk op de begrotingen van overheden (Phi, 2017). Om deze reden zijn overheden en bedrijven op zoek naar innovatieve manieren om het leveren van gezondheidszorg efficiënter en minder kostelijk te maken.
De gezondheidszorgsector is een op data gefocust domein waar een enorme hoeveelheid gegevens worden gegenereerd, geraadpleegd, opgeslagen en verspreid. De blockchain technologie kan met gemakkelijk overdraagbare gegevens, toezicht, interoperabiliteit en zorg- en leveringsbeheer mogelijks een antwoord bieden op verschillende toekomstige uitdagingen van de gezondheidszorg (Esposito, De Santis, Tortora, Chang, & Choo, 2018). De voornaamste effecten van blockchain in de gezondheidszorg zullen betrekking hebben tot het verschaffen van het veilig beheer van medische gegevens.

7.3.2 Toetsing aan de hand van het framework

- **"Meerdere partijen"**: Een elektronisch patiëntendossier bevat medische gegevens van patiënten. Deze gegevens omvatten onder andere de volledige medische voorgeschiedenis van de patiënt, zoals doorgemaakte ziekten, chronische aandoeningen, de ondergane operaties en behandelingen, etc. Bij uitwisseling van deze gegevens zijn meerdere partijen uit verschillende organisaties betrokken. Enkel door een goede wisselwerking/samenwerking is een efficiënte zorgverlening mogelijk. Blockchain biedt een gedeelde, neutrale infrastructuur waar geen enkele betrokken actor macht over kan uitoefenen.

- **"Vertrouwde autoriteit"**: Bij een toepassing zoals een EPD is er naast de neutrale infrastructuur nood aan vertrouwde autoriteiten met toegang tot de gegevens. Deze personen, namelijk de behandelende artsen, zijn bevoegd om gegevens toe te voegen en wijzigingen aan te brengen in het dossier van de patiënt. Andere zorgverleners, zoals verpleegkundigen hebben enkel zicht op de EPD's van de patiënten aan wie zij zorg verlenen. Verpleegkundigen kunnen echter geen gegevens toevoegen of wijzigen. Over het algemeen is de vertrouwde autoriteit binnen het EPD in feite ook gedecentraliseerd: de behandelende artsen uit verschillende ziekenhuizen zijn bevoegd om toegang tot het EPD te verkrijgen.

- **"Gecentraliseerde werking"**: Toepassingen die een gecentraliseerde werking vereisen, zijn niet geschikt om te berusten op blockchain. Een EPD vergt echter geen gecentraliseerde werking. De gedecentraliseerde werking zorgt ervoor dat geen enkele (afzonderlijke) partij controle heeft over het systeem, maar wel dat elke gebruiker controle heeft over zijn eigen gegevens. Dit creëert echter wel uitdagingen voor het bestuur van het systeem. De huidige EPD's zijn informatiesilo's die niet verbonden zijn met andere systemen. Dit bemoeilijkt de gegevensuitwisseling en zorgt ervoor dat veel informatie op één enkele plaats wordt opgeslagen waardoor het systeem vatbaar wordt voor cyberaanvallen.

- **"Transparantie versus vertrouwelijkheid"**: Blockchain voorziet een neutraal platform waar alle deelnemers inzage hebben in de gepubliceerde gegevens. Bij implementatie van een EPD blijft de gegevenstransparantie een van de struikelblokken; het bevat namelijk gevoelige gegevens die niet zomaar openlijk gedeeld mogen worden. In eerste instantie is blockchain door zijn transparante aard minder geschikt voor toepassingen die vertrouwelijkheid van de gegevens vereisen. Echter kan men dit omzeilen door enkel de *hash* waardes van de gegevens in de blockchain op te slaan en de werkelijke gegevens off-chain te bewaren. Hierdoor blijft de informatie vertrouwelijk en wordt de privacy van de patiënt gerespecteerd. Echter stapt deze aanpak verder weg van de kerngedachte achter blockchain.

- **"Gegevensintegriteit en onveranderlijkheid"**: Blockchain kan zijn nut bewijzen bij applicaties waar een hoge gegevensintegriteit gewenst is. EPD's bevatten belangrijke gezondheidsgegevens die in principe niet aangepast mogen worden zonder dat dit door een arts of gezondheidsexpert herzien is. Met behulp van blockchain kan de accuraatheid van de geschiedenis en de afkomst van deze gegevens eenvoudig worden aangetoond. Deze nauwkeurig bijgehouden, onveranderlijke geschiedenis kan op zijn beurt gebruikt worden voor controledoeleinden.

- **"Verwerkingscapaciteit"**: EPD's vereisen in mindere mate real-time data updates, waardoor de iets lagere verwerkingscapaciteit van blockchain geen grote invloed zal hebben op de werking van het EPD.

Het framework stelt dat blockchain mogelijks interessant kan zijn voor een toepassing met betrekking tot een EPD. Blockchain zou bevorderlijk zijn voor de gegevensuitwisseling en voor de veiligheid van de gegevens. Echter moet er rekening gehouden worden met de privacyaspecten van de patiënt en moet het systeem conform zijn aan de GDPR.

7.3.3 Bevindingen

Het zorgstelsel van Estland is revolutionair veranderd door innovatieve, digitale oplossingen. Niet enkel patiënten en artsen, maar ook ziekenhuizen en de overheid profiteren van de eenvoudige toegang en besparingen die *e-Services* reeds hebben opgeleverd.

Elke persoon in Estland die een arts heeft bezocht, heeft een online *e-Health* record dat kan worden gevolgd. Identificeerbaar door middel van de elektronische ID-kaart, wordt de gezondheidsinformatie volledig beveiligd bewaard en is tegelijkertijd enkel toegankelijk voor bevoegde personen.
In het elektronisch patiëntendossier (EPD) worden gegevens van de verschillende zorgverleners van Estland geïntegreerd om zo een gemeenschappelijk dossier te creëren dat de patiënt in kwestie online kan raadplegen. Het *e-Health* record vraagt via de X-Road gegevens op bij verschillende providers, die mogelijks verschillende systemen gebruiken, en presenteert het in een standaardstructuur via het *e-Patient portal*. Hierdoor kunnen artsen eenvoudig toegang verkrijgen tot patiëntendossiers vanuit één enkel elektronisch bestand. Zo kunnen ze testresultaten en medische beeldvorming, zoals bijvoorbeeld röntgenfoto's, raadplegen vlak na registratie, zelfs indien deze gegevens uit een 'afgelegen' ziekenhuis afkomstig zijn. In geval van nood kunnen artsen ook tijdskritieke informatie opvragen via de ID-code van de patiënt, zoals allergieën, bloedgroep, recente behandelingen, huidige medicatie of zwangerschapsinformatie. Daarnaast verzamelt het systeem ook gegevens voor nationale statistieken zodat de overheid gezondheidstrends en epidemieën kan volgen. Hierdoor verkrijgen ze meer inzicht in de efficiëntie van hun zorgverlening en kunnen ze ervoor zorgen dat hun middelen op een verantwoorde manier worden besteed (e-Estonia, z.d.-b).
Om de gegevensintegriteit te waarborgen en om het toegangslogboek bij te houden, maakt men gebruik van de KSI-blockchain technologie. Patiënten hebben zowel toegang tot hun eigen gegevens en de gegevens van hun minderjarige kinderen alsook toegang tot de gegevens van mensen die hun toestemming hiervoor hebben gegeven. Door zich met hun elektronische ID-kaart in te loggen in het *e-Patient portal* kunnen patiënten doktersbezoeken en huidige voorschriften herzien en nagaan welke zorgverleners hun gegevens hebben geraadpleegd.
Een belangrijke innovatie, die gepaard gaat met het elektronisch patiëntendossier, zijn de *e-Prescription*s. Zij berusten op een gecentraliseerd, 'papierloos' systeem voor het uitgeven en verwerken van medische voorschriften. Artsen schrijven geneesmiddelen elektronisch voor aan de hand van een online formulier. De patiënt moet bij de apotheek slechts zijn ID-kaart afgeven (e-Estonia, z.d.-a). Zo kan de apotheker de voorschriften opvragen en de geneesmiddelen voorzien
Een ander aspect dat de administratieve lasten zou reduceren, is het feit dat het *e-Prescription* systeem gebaseerd is op gegevens van het nationale ziekenfonds. Hierdoor zullen alle medische terugbetalingen ook verschijnen en wordt dit in mindering gebracht van de prijs van het geneesmiddel. Een ander groot voordeel is dat er geen doktersbezoeken meer nodig zijn voor een herhaalvoorschrift; de patiënt kan simpelweg de arts contacteren via e-mail, Skype of telefoon. De arts kan dan met slechts een paar klikken een voorschrift 'hernieuwen' en de patiënt kan het geneesmiddel bij de dichtstbijzijnde apotheek ophalen. Tegenwoordig worden 99% van alle voorschriften elektronisch verstrekt (e-Estonia, z.d.-a). Dit zorgt uiteraard voor een tijdswinst voor zowel patiënten als artsen en vermindert de administratieve last op ziekenhuizen.
In feite verbindt X-Road de verschillende ziekenhuizen en organisaties. Het zorgt voor een uniform EPD waarbij de zorgverlener de nodige informatie over de patiënt kan raadplegen en de privacy van de patiënt toch waarborgt. De KSI-blockchain wordt op zijn beurt gebruikt voor het beveiligen van deze gegevens.

7.3.4 Uitdagingen en beperkingen

Er zit veel potentieel in de ontwikkeling van een blockchainplatform voor een veilig, onveranderlijk, eenvoudig toegankelijk medisch dossier. Toch zijn er enkele uitdagingen die men het hoofd moet bieden. De gegevens binnen de gezondheidszorg bevatten uiteraard persoonlijke en gevoelige informatie van de patiënt die niet openlijk gedeeld mag worden. Deze gegevens kunnen dus best niet in de blockchain worden opgeslagen. Daarom worden enkel de *hash* waardes van de (gevoelige) gegevens opslaan. Men kan die *hash* waardes beschouwen als een digitale vingerafdruk van de oorspronkelijke gegevens. Zoals reeds enkele keren vermeld, representeren deze *hash* waardes de oorspronkelijke gegevens op een unieke manier. Het is echter onmogelijk om slechts op basis van de *hash* waarde de gegevens in kwestie te bekomen. Op deze manier is het onbelangrijk wie de gegevens op de blockchain kan inkijken, aangezien men er toch geen betekenisvolle gegevens uit kan opmaken. Toch zullen overheden de privacy rechten van de patiënt sterk moeten overwegen bij de implementatie van dergelijk systeem. Zo zal de overheid moeten garanderen dat de toestemming van de patiënt vereist is vooraleer hun gegevens geraadpleegd worden. Daarnaast moeten de patiënten eigenaar zijn van en controle hebben over hun eigen gegevens. Ten slotte zal het opschalen van dergelijk systeem naar nationaal of globaal niveau een algemene aanvaarding vereisen omtrent de protocollen voor het coderen van medische gegevens. Het aanzetten van individuen, zorgverleners en verzekeringsmaatschappijen om één enkel systeem aan te nemen, zal waarschijnlijk een moeizaam en kostelijk proces zijn.

7.3.5 Belgische context

De gezondheidsuitgaven in België zijn in de laatste 10 jaar sterk toegenomen en overtreffen deze van de meeste EU-landen. In 2015 besteedde België 3.568 EUR per capita aan gezondheidszorg, vergeleken met het EU-gemiddelde van 2.797 EUR. Dit komt overeen met 10,5% van het Belgische BBP, tegenover 9,0% in 2005 (OESO, 2017). Enerzijds is dit toe te schrijven aan de vergrijzing. Anderzijds zorgen technologische ontwikkelingen en innovaties voor duurdere behandelingen. Bovendien is veiligheid ook van uitermate belang bij een toepassing zoals een elektronisch medisch dossier. Het bevat zeer gevoelige, persoonlijke informatie van de patiënt. Het is moeilijk te bepalen wat voor effecten een dergelijk systeem in België zou kunnen teweegbrengen. De voornaamste voordelen zijn meer transparantie en controle voor de patiënt, een verlaging van de administratieve kosten, een betere gegevensuitwisseling en een betere veiligheid van de gegevens.
België heeft de afgelopen jaren ook meer aandacht besteed rond *e-Health*. Zo werd er een veilig en patiëntgericht portaal gerealiseerd waar men gepubliceerde informatie over de gezondheid van de patiënt kan terugvinden. In november 2018 werden er 4,4 miljoen elektronische voorschriften uitgegeven door 16.000 verschillende artsen. Dit is ongeveer de helft van alle voorschriften. Ook wordt er steeds meer elektronisch informatie uitgewisseld; 2,7 miljoen patiënten hebben een Sumehrs (elektronische samenvatting van medische patiëntgegevens) en 36.000 artsen gebruiken de hub (een regionaal uitwisselingsnetwerk) om informatie uit te wisselen. Er werd een acceleratorprogramma met betrekking tot het EPD gestart, met als gevolg dat meer dan de helft van de algemene ziekenhuizen een actieplan heeft opgestart voor de implementatie van een dergelijk

EPD (eGezondheid, 2019). Een bekende speler op deze markt is Nexuzhealth, een joint venture van UZ Leuven en Cegeka. Nexuzhealth helpt klanten met de implementatie, optimalisatie en verdere ontwikkeling van het klinisch werkstation (KWS), een volledig geïntegreerd elektronisch patiëntendossier. Ze willen de kwaliteit van de patiëntenzorg vergroten door de samenwerking tussen verschillende ziekenhuizen op een transparante en eenduidige manier aan te reiken. Dit zorgt ervoor dat alle disciplines bijdragen aan hetzelfde patiëntendossier en dat elke patiënt slechts één dossier heeft ongeacht het ziekenhuis of de zorgverlener. Daarnaast wordt de informatie op dezelfde wijze geïnterpreteerd door de verschillende instellingen en wordt belangrijke kennis tussen ziekenhuizen gedeeld. Artsen en andere zorgverleners kunnen een dossier inkijken op voorwaarde dat ze direct bij de behandeling betrokken zijn. Via een toegangscontrole wordt bijgehouden wie wanneer welk deel van een bepaald dossier inkijkt of bewerkt. De patiënten kunnen de verslagen, afspraken, testresultaten en medische beeldvorming, facturen en persoonlijke gegevens online raadplegen door in te loggen met hun *e-ID*. Ten slotte is het systeem volgens Nexuzhealth ook streng beveiligd en worden de privacy rechten van de patiënt gegarandeerd (NexuzHealth, 2019). Indien een EPD zoals KWS algemeen wordt toegepast, is het van groot belang dat overheid de veiligheid hiervan grondig analyseert en test om zich tegen cyberaanvallen, zoals in 2017 te weren.

Eens een systeem zoals KWS in België wordt geïmplementeerd, zullen de verwachte baten sterk gelijken op die van Estland. Het grootste verschil is dat zij de KSI-blockchain gebruiken voor het beveiligen van de medische gegevens en X-Road benutten voor de toegankelijkheid en uitwisselbaarheid van de gegevens. Het Estse systeem is dus mogelijks beter beveiligd tegen cyberaanvallen.

Het initiatief achter de ontwikkeling van het EPD in België heeft reeds veel tijd en geld gekost aan zowel de overheid als private bedrijven. Het zou daarom onverstandig zijn om nu aan artsen en ziekenhuizen te vragen om van hun huidig systeem af te stappen en een volledig op blockchain gebaseerd systeem te implementeren. Nochtans is het van uitermate belang dat de veiligheid van een EPD-systeem kan aangetoond worden. Naar de toekomst toe kan blockchain mogelijks gebruikt worden om de medische gegevens te beveiligen en het toegangslogboek bij te houden zoals in Estland. Indien een van de huidige EPD's door elke zorgverlener wordt gebruikt (om de gegevensuitwisseling te garanderen) én voldoende beveiligd is, kent de ontwikkeling van een volledig nieuw systeem op basis van blockchain weinig nut.

8 Casestudy Zweden: kadaster

8.1 Situatieschets

Ook Zweden is gestart met het verkennen van blockchain technologie. Zo werkt het *Lantmäteriet*, de Zweedse autoriteit voor land registratie, samen met *Chromaway* en *Telia Company* om de technologie te gebruiken bij het ondersteunen van vastgoedtransacties. Met behulp van blockchain hopen zij het proces van de aankoop van een woning aanzienlijk efficiënter, veiliger en transparanter te maken voor alle betrokken partijen.
Onroerend goed in Zweden is momenteel meer dan 1 biljoen euro waard, bijna drie keer de waarde van het bbp van Zweden. Voor veel Zweden, net zoals de doorsnee mens, zijn hun huizen zowel hun meest waardevolle bezit alsook de grootste bron van persoonlijke schuld, met bijna 300 miljard euro aan hypotheken op de Zweedse markt (Juliet McMurren, 2018). Ondanks het enorme economische belang zijn de processen voor landoverdracht vaak traag, kwetsbaar voor fouten en niet transparant. Vanaf de ondertekening van het contract kan het drie tot zes maanden duren vooraleer de titel wordt overgedragen aan de nieuwe eigenaar. Het officiële Zweedse kadaster was in de jaren zeventig een van de eerste overheidsinstanties in de wereld die zijn kadaster digitaliseerde. Hoewel de database van het kadaster nu gedigitaliseerd is, is het proces van de landsoverdracht dat echter niet.
Onder het huidige kadastersysteem wordt de officiële autoriteit *Lantmäteriet* pas betrokken in het overdrachtsproces wanneer de bank van de koper de titelregistratie aanvraagt en de verkoopakte en de (mogelijke) aanvraag voor een nieuwe hypotheek aan hun bezorgt (Juliet McMurren, 2018). Hierdoor wordt de overdracht pas geregistreerd in het kadaster nadat de contracten werden getekend. Aangezien de officiële autoriteit de meeste vertrouwde actor is binnen het overdrachtsproces zorgt zijn afwezigheid in de beginfase van het proces voor minder transparantie en vertrouwen. Bovendien is het een langzaam proces dat veel tijd en inspanning vergt bij de voorbereiding van de documenten en bij de authenticatie en de verificatie ervan. Zo duurt een overdracht vanaf de ondertekening van de verkoopakte tot de overdracht gemiddeld vier maanden (Kairos Future, 2017). Ondanks de digitale registratie van het kadaster worden de accuraatheid en de efficiëntie van de huidige overdrachten van onroerende goederen belemmerd door de wetgeving die papieren transacties en fysieke handtekeningen vereist. Het ondertekenen van een verkoopakte kan snel twee uur duren en het verifiëren van de documenten en de identiteit van ondertekende moet manueel gedaan worden. Ten slotte zorgt de grote hoeveelheid vereiste documenten en herhaalde gegevensinvoer voor een hoger risico op fouten. Zo moet vier tot zeven procent van de aanvragen opnieuw worden ingediend vanwege een fout in het overdrachtsproces (Juliet McMurren, 2018). Om deze reden is de *Lantmäteriet* mogelijke blockchaintoepassingen voor onroerende goederen gaan verkennen. Zij hebben in samenwerking met enkele private bedrijven een prototype ontwikkeld. Deze werkt als volgt: op het moment dat er een overeenkomst tot verkoop wordt bereikt, wordt de vastgoedtransactie vastgelegd in de blockchain. Deze blijven onveranderlijk totdat de grondtitel opnieuw overgedragen wordt. Het nieuwe systeem probeert de informatieasymmetrie te beperken door alle partijen (bank, kadaster, makelaars, kopers en verkopers) toe te laten de vooruitgang van de transactie te volgen.

8.2 Toetsing aan de hand van het framework

- **"Meerdere partijen"**: Bij de overdracht van een eigendomstitel zijn er heel wat partijen betrokken: kopers, verkopers, de bank, makelaars, de kadasterautoriteit, etc. Blockchain kan hier dus een gedeelde, neutrale infrastructuur bieden voor alle actoren in het proces.

- **"Vertrouwde autoriteit"**: Voor het overdragen van eigendomstitels is er nood aan een vertrouwde autoriteit die erop toeziet dat alles juist verloopt en op een correcte manier wordt opgeslagen. Echter wordt deze vertrouwde autoriteit pas relatief laat in het proces betrokken waardoor de voorgaande stappen in het overdrachtsproces minder transparant zijn. Blockchain kan dit verhelpen door transparantie te verschaffen aan alle actoren gedurende het gehele proces.

- **"Gecentraliseerde werking"**: Een toepassing met betrekking tot het kadaster vereist in principe geen gecentraliseerde werking. De verschillende geautoriseerde *nodes* zouden de transacties (en hun voorwaarden) kunnen verifiëren waardoor er minder kans is op frauduleuze transacties of foutieve aanvragen.

- **"Data transparantie versus vertrouwelijkheid"**: Een hoge gegevenstransparantie met betrekking tot het kadaster is uiteraard gewenst. Momenteel worden de overdrachten pas relatief laat opgenomen in het kadaster. Aangezien de officiële autoriteit pas in een later stadium betrokken wordt, zorgt dit voor minder transparantie en vertrouwen in de eerdere fases van het proces. Het is bovendien van groot belang dat iedereen inzage heeft in wie welk eigendom bezit en dat deze eigendomsrechten eenvoudig aantoonbaar zijn.

- **"Gegevensintegriteit en onveranderlijkheid"**: Het is vanzelfsprekend dat er binnen het kadaster een hoge gegevensintegriteit gewenst is. In het huidige systeem kan er informatie ontbreken door een deels verkeerd gelopen registratieproces. Dit valt te wijten aan het feit dat de gegevens manueel en meerdere keren moeten worden ingevoerd. Met behulp van blockchain is de overdracht van de titel onveranderlijk totdat deze opnieuw wordt overgedragen, waardoor er minder kans is op fraude. Daarnaast moeten gegevens niet meerdere keren worden ingevoerd waardoor de kans op fouten in het overdrachtsproces verkleind wordt.

- **"Hoge verwerkingscapaciteit"**: Een blockchaintoepassing met betrekking tot het kadaster vereist in principe geen hoge verwerkingscapaciteit. Momenteel duren de overdrachtsperiodes ettelijke maanden. De lengte van deze periode valt niet te wijten aan een te lage verwerkingscapaciteit maar wel aan het lange en moeizame administratief proces. Informatie moet op meerdere plekken opgevraagd en gecontroleerd worden. Zo moet de vastgoedmakelaar bijvoorbeeld de eigendomstitel controleren om na te gaan of de beoogde verkoop wel mogelijk is. Blockchain zou ondanks zijn lagere verwerkingscapaciteit toch veel efficiëntiewinsten boeken doordat de informatie eenvoudig beschikbaar is voor alle partijen in het overdrachtsproces.

Uit de toepassing van het framework is gebleken dat een blockchaintoepassing binnen het kadaster hoogstwaarschijnlijk nuttig zal blijken. Een systeem op basis van blockchain zou mogelijks het overdrachtsproces efficiënter maken, administratieve lasten verlagen en zorgen voor transparante en eenvoudig aantoonbare eigendomsrechten.

8.3 Bevindingen

Het opzet van dit project was het creëren van een op blockchain gebaseerd, veilig, efficiënt en vertrouwd proces voor landoverdracht dat volledig (*end-to-end*) digitaal was. Het doel was om de tijd tussen het tekenen van de verkoopakte en de registratie van de eigendomstitel te reduceren van gemiddeld vier maanden tot slechts enkele dagen. Dit werd bereikt door het elimineren van een aantal stappen en door het verminderen van vertragingen veroorzaakt door de nood aan herhaalde controles en fysieke handtekeningen. Zo zou het signeren van de verkoopakte en het registreren van de landtitel uiteindelijk min of meer in real-time kunnen gebeuren. De koper verkrijgt de *pending* eigendomstitel waardoor het eigendom geen tweede keer verkocht kan worden door de verkoper (McMurren, Young, & Verhulst, 2018).
Bovendien vergroot deze blockchain oplossing het vertrouwen in de eigendomsoverdracht omdat de wettelijk noodzakelijke informatie door het systeem wordt vastgelegd en voor alle partijen zichtbaar is voordat de contracten worden ondertekend. Ook het risico dat de overdracht niet succesvol verloopt wordt hierdoor sterk verkleind. Het proces wordt dus minder vatbaar voor fouten en fraude (Kairos Future, 2017). De volledige digitalisering van het proces zorgt er voor dat fysieke archieven van contracten en documenten onnodig worden. Zo vermoedt de kadasterautoriteit dat Zweden meer dan 100 miljoen euro zou kunnen besparen door snellere transacties, meer accurate gegevens, het elimineren van papieren processen en de toegenomen veiligheid die het gebruik van blockchain met zich meebrengt (Kairos Future, 2017).
Het gebruik van blockchain zou echter nog meer voordelen kunnen realiseren binnen ontwikkelingslanden waar veel fraude en corruptie heerst. Het hebben van een betrouwbare registratie en de mogelijkheid om grondbezit veilig te stellen, kan men haast beschouwen als noodzakelijke voorwaarde voor het ontwikkelen van een land.

8.4 Uitdagingen en beperkingen

De belangrijkste hindernis om het blockchainsysteem breder te implementeren, heeft betrekking tot de onzekerheid over de geldigheid van digitale handtekeningen. Tot nu toe vereist de Zweedse wet fysieke handtekeningen voor vastgoedcontracten. Echter is het voor een effectieve implementatie van cruciaal belang dat de geldigheid van de digitale handtekeningen onomstreden is. Ondanks dat zowel het Zweedse als het Europese recht steeds meer elektronische identificatie toe laten, is de juridische status van digitale handtekeningen voor vastgoed niet bij de rechtbank vastgesteld (Juliet McMurren, 2018).
In het huidige project zijn reeds veel actoren betrokken: de overheidsinstelling (*Lantmäteriet*), projectmanagers (*Kairos Future*), zakelijke partners voor de technologie (*Chromaway* en *Telia Company*) en banken voor de transacties. Echter zullen er bij uitbreiding naar grotere schaal ook

andere partijen betrokken moeten worden zoals makelaars, kopers en verkopers. Daarnaast is er nood aan aanvullende technische partners voor het leveren van cloud-oplossingen, dataopslag en netwerkcapaciteit. Een framework voor het gegevensbeheer en de integratie van deze partijen moet nog worden opgesteld. Er zijn veel mogelijkheden om nieuwe oplossingen en diensten te ontwikkelen met behulp van de gegevens en het ontwikkelde platform. Daarom is het belangrijk dat de verschillende mogelijkheden besproken worden en dat het besluitvormingsproces omtrent wijzigingen aan het systeem zorgvuldig onderzocht moeten worden (Kairos Future, 2017).

8.5 Belgische context

Een assumptie die we hier kunnen maken is dat de Belgische situatie sterk gelijkaardig is met deze in Zweden. In België waren er geen beschikbare gegevens omtrent de gemiddelde overdrachtsperiode. Echter heeft het Kadaster en het NVM (Nederlandse Vereniging van Makelaars) onderzoek gevoerd naar de overdrachtsperiode in Nederland, die gemiddeld iets meer dan drie maanden duurt (Kadaster.nl, 2018). In de huidige situatie lopen de erelonen van notarissen bij de verkoop van een woning hoog op. Er moeten veel documenten (bodemcertificaat, energieprestatiecertificaat etc.) worden opgevraagd bij verschillende instanties, wat een zeer tijdrovend en kostelijk proces is. Dit genereert overbodige, additionele kosten die bij de volledige digitalisering van het proces via een smart contract bespaard kunnen worden. Het gebruik van blockchain kan de administratieve lasten voor burgers terugdringen en een deel van de administratieve procedures automatiseren. Hierdoor zal de functie van de notaris meer verschuiven naar een advies verlenende rol. Bovendien is er nog nood aan iemand die de correctheid van de ingevoerde gegevens controleert.

Het is zeer lastig om de verwachte effecten van het gebruik van blockchain technologie bij het kadaster te gaan kwantificeren. Zo schatte het *Lantmäteriet* dat de Zweedse belastingbetalers samen wel meer dan 100 miljoen euro per jaar kunnen besparen door de snellere transactiesnelheid, het verdwijnen van papierwerk en de reductie van fraude of fouten (Kairos Future, 2017). Zowel het huidige overdrachtsproces, het bbp als de populatie zijn sterk gelijkaardig tussen Zweden en België. Men zou dus vereenvoudigd kunnen stellen dat de implementatie van een dergelijk systeem in België ook 100 miljoen euro of meer zou kunnen besparen. Daarnaast werden er ook opmerkelijke verbeteringen geconstateerd omtrent het proces voor hypotheekaktes. In België bereikte het uitstaande bedrag aan particuliere hypothecaire leningen eind 2016 ongeveer 217 miljard euro. Op Europees niveau bedraagt de totale som een kleine 7 biljoen (EMF, 2017). Indien de bank dus zeker kan zijn dat het vastgoed (onderpand) betrouwbaar wordt vastgelegd en dat dit eenvoudig aantoonbaar is, zou hun risico en bijgevolg mogelijks de rentevoet kunnen dalen. Een vermindering van de rentevoet met 0,1%, zou al een baat van 217 miljoen euro voor Belgische en 700 miljard euro voor Europese kredietnemers genereren.

Volgens deze casestudy is het zeker interessant om ook in België onderzoek te voeren naar het gebruik van blockchain bij het kadaster. Het zou veel administratief werk besparen, snellere overdrachten verwezenlijken en kostenbesparing voor de burger en de overheid realiseren.

9 Casestudy Walmart: supply chain management

9.1 Situatieschets

Dr. Margaret Chan, de directeur-generaal van de *World Health Organisation*, pleit voor meer aandacht naar voedselveiligheid*. "Food safety is a hidden, and often overlooked, problem."* (Chan, 2014) Zo worden meer dan 200 ziektes verspreid door middel van voedsel. Dit wordt veroorzaakt door micro-organismes (virussen, bacteriën, etc.) en door chemicaliën, radioactiviteit en fysische agentia. Bovendien lopen vooral kinderen, zwangere vrouwen en oudere mensen meer risico op ernstige gevolgen na contact met besmet voedsel. Globaal gezien worden er jaarlijks 600 miljoen mensen ziek waarvan er 420.000 sterven. In Europa vallen jaarlijks meer dan 23 miljoen mensen ziek waarvan 5.000 overlijdens. Volgens het WHO vertegenwoordigen kinderen (< 5 jaar) 13% van de zieken en 14% van de sterfgevallen (WHO, 2015). Deze zieken en sterfgevallen brengen natuurlijk veel kosten met zich mee. Dit zijn niet enkel directe kosten zoals medische kosten, maar ook indirecte kosten zoals productiviteitsverlies (ziekteverzuim), vervoerskosten, daling in levenskwaliteit, etc. Zo wordt er in een rapport van de *United States Department of Agriculture* (USDA) geschat dat de kosten van voedsel overgedragen ziektes in de Verenigde Staten ongeveer een $ 15,6 miljard (€ 14 miljard) bedragen (USDA, 2014).

Wanneer een ziekte, veroorzaakt door besmet voedsel, uitbreekt, kan het dagen of zelfs weken duren voordat de bron wordt achterhaald. Indien men niet naar een specifieke boerderij kan verwijzen als oorzaak, adviseert de overheid meestal om producten van een bepaald gebied of zelfs het type product geheel te vermijden. Op deze manier wordt er dus zeer veel voedsel verspild en gaat het vertrouwen bij de consument verloren. Hierdoor dragen dus alle boeren de gevolgen, zelfs indien hun producten niet besmet waren. Een betere en snellere traceerbaarheid zou veel levens kunnen redden doordat bedrijven en overheden sneller kunnen ingrijpen. Het huidig onvermogen om producten in de supply chain efficiënt te traceren is te wijten aan ongelijkaardige methodes voor het bijhouden van de gegevens. Daarnaast wordt er over het algemeen de "One up, one down" (OUOD) aanpak gehanteerd; deelnemers van de voedsel supply chain kennen enkel hun directe leverancier (*one up*) en hun directe klant (*one down*) (Kamath, 2018). Deze aanpak is gewoonweg niet voldoende in een complexe supply chain die grote gevolgen kan hebben op de volksgezondheid.

Bij vermoede besmettingen wordt de papieren documentatie stap voor stap onderzocht. Dit is een zeer tijdrovend proces; verkeerde of onvolledige gegevens kunnen het onderzoek nog verder vertragen. Daarnaast kunnen voedingsmiddelen en bulkcontainers met meerdere ingrediënten, elementen bevatten uit verschillende bronnen en uit meerdere landen, wat de traceerbaarheid nog complexer maakt. Momenteel wordt er uit voorzorg volledige containers weggegooid onder het OUOD-systeem (Welt & Blanchfield, 2012).

Daarom heeft retail gigant Walmart ervoor gekozen om in samenwerking met IBM een blockchain-pilot voor de 'herkomst' van hun voedsel te ontwikkelen en implementeren. Walmart maakt hiervoor gebruik van IBM zijn *Hyperledger Fabric* en heeft twee blockchain-pilots getest, het traceren van varkensvlees in China en het traceren van mango's in Amerika.

9.2 Toetsing aan de hand van het framework

- **"Meerdere partijen"**: De supply chain sector omvat alle processen gepaard gaande met de productie en distributie van goederen. Zowel het bewerkingsproces van ruwe grondstoffen tot afgewerkte producten als het leveren van deze producten aan de consument worden hierbij opgetekend. Supply chain management (SCM) omvat het structurele beheer van zowel goederen- en informatiestromen als de organisaties die hiervoor instaan (Vandooren, z.d.). Het is een zeer complex systeem met meerdere partijen zoals bijvoorbeeld landbouwers, fabrieken, logistieke deelnemers, retailers, etc.

- **"Vertrouwde autoriteit"**: Binnen het SCM is er nood aan een vertrouwde autoriteit. De gegevensuitwisseling berust op de vraag of de gegevens wel op een correcte manier verzameld zijn en of de gegevens beschikbaar worden gesteld door de informatiesystemen van de verschillende stakeholders. Hierdoor steunt het systeem dus op het vertrouwen dat elke stakeholder de correcte informatie communiceert.

- **"Gecentraliseerde werking"**: Een gecentraliseerde werking is zeker en vast geen vereiste voor SCM. Zo zou deze sector voordeel halen uit een gedecentraliseerd systeem. De activiteiten binnen de supply chain liggen namelijk verspreid over alle deelnemende organisaties. Bovendien is het noodzakelijk voor de gegevensuitwisseling dat de verschillende systemen van de stakeholders in staat zijn de gegevens op een correcte manier te registreren en te delen met de andere informatiesystemen.

- **"Transparantie versus vertrouwelijkheid"**: Een hoge graad van transparantie binnen het SCM is gewenst. De deelnemers moeten op een eenvoudige en duidelijke manier kunnen nagaan waar het product zich binnen de supply chain bevindt opdat ze zich kunnen voorbereiden op hun eigen rol binnen het systeem. Bovendien zal op die manier ook meer vertrouwen gecreëerd worden binnen de keten.

- **"Gegevensintegriteit en onveranderlijkheid"**: Een hoge integriteit van de transactiegeschiedenis en onveranderlijkheid van de gegevens zijn uiteraard ook gewenst binnen het SCM. Hiermee kan de herkomst en de staat van de overgedragen goederen worden gecontroleerd zonder dat afzonderlijke organisaties hier mee kunnen knoeien. Echter blijft de correctheid van de gegevensinvoer cruciaal voor een eerlijk systeem.

- **"Hoge verwerkingscapaciteit"**: De huidige systemen binnen het SCM, zeker deze die nog met papieren documenten werken, worden niet in real-time bijgewerkt. In deze omstandigheden kan men zich bij implementatie van blockchain korte vertragingen veroorloven. Men kan stellen dat de iets lagere verwerkingscapaciteit van blockchain systemen verwaarloosbaar zijn in de context van een toepassing binnen de supply chain sector.

Volgens dit framework is de toepassing van blockchain binnen het SCM veelbelovend. Het SCM zal mogelijks veel voordelen kunnen realiseren door de digitale, gedistribueerde aard van blockchain. Het zou mogelijks bijdragen tot een hogere graad van transparantie en vertrouwen binnen de keten.

9.3 Bevindingen

9.3.1 Varkensvlees

Het eerste project was gericht op het verzekeren van de supply chain van varkensvlees in China. China is zowel de grootste importeur als de grootste producent van varkensvlees. De kleinschalige varkensvleesproducenten worden steeds meer vervangen door grote geïndustrialiseerde varkensvleesproductiesystemen (Gale, 2017).
75% van de Chinese burgers is van mening dat voedselveiligheid een van de belangrijkste *Quality-of-Life* indicatoren is. Bovendien werden 95% van de 133.225 deelnemers al eens geconfronteerd met voedselveiligheidsproblemen, waarvan 50% zich zorgen maakt over de voedselveiligheid in China (Galvin, 2017). Daarom riepen overheidsinstanties de varkensvleesindustrie op om het productiesysteem te moderniseren van boer tot bord. De Chinese overheid heeft zwaar geïnvesteerd in haar voedselsysteem; ze hebben de voedselinspecties en veiligheidsmethodes verhoogd, ze zetten druk op productiesystemen en werken samen met grote retail giganten. Toch heeft ongeveer 60% van de Chinese burgers geen vertrouwen in deze nieuwe acties om de voedselveiligheid te verbeteren (Galvin, 2017). Aangezien de consumentenfocus verschoven is naar voedselveiligheid en -kwaliteit is vertrouwen van cruciaal belang voor aankoopbeslissingen. Gezien de zeer grote populatie en de hoge consumptie van varkensvlees (34kg per capita/jaar) in China, had Walmart een nieuwe stimulans om nieuwe technologieën te verkennen om vertrouwen te creëren in de origine van het varkensvlees op de Chinese markt (Statista, 2018).
Het proces begint bij de stallen waar elk varken wordt voorzien van een streepjescode, die het product helemaal volgt tot bij de verpakking. Er wordt gebruikt gemaakt van radiofrequentie-identificatie (RFID) en camera's in de slachthuizen om het gehele productieproces vast te leggen (Kamath, 2018). De vrachtwagens voor transport zijn uitgerust met temperatuur- en vochtigheidsgraadsensoren samen met een gps. Zo kan men verzekeren dat het vlees onder veilige omstandigheden bij de winkels aankomt; Walmart kan de locaties van de vrachtwagens achterhalen en de omstandigheden in elke koelwagen monitoren. Indien de omstandigheden bepaalde drempels overschrijden (bv. te hoge temperatuur), krijgt Walmart een waarschuwingsnotificatie opdat ze snel corrigerende maatregelen kunnen treffen (Gale, 2017). Met behulp van blockchain kunnen aankoopmanagers op afstand alle informatie, van vervaldatums tot magazijntemperaturen, traceren. Informatie over de herkomst van de boerderij, batchnummers en verwerkingsgegevens kunnen worden geüpload op een elektronisch certificaat en gekoppeld aan het productpakket via een QR-code. Op deze manier wordt er meer vertrouwen in het systeem gecreëerd waar dat vroeger een ernstig probleem was. Walmart en IBM hebben gemeld dat deze pilot een verbeterde snelheid en accuraatheid aangaf bij de toegang tot de relevantie informatie van de boerderij tot het verkooppunt (Kamath, 2018). Blockchain technologie kan bijdragen aan een hogere voedselveiligheid door het hebben van een betrouwbare bron van gegevens die snel en veilig kunnen worden gecommuniceerd

tussen verschillende partijen. Wanneer een bepaald voedselproduct besmet wordt, kan blockchain helpen met het identificeren van de specifieke producten die uit de verkoop moeten worden genomen in plaats van de gehele productlijn uit de verkoop te verwijderen. Het gebruik van blockchain heeft het potentieel om kosten te besparen bij het terughalen van producten, het verminderen van procesinefficiënties en retailers toe te laten de varkensvleesproducten te traceren in enkele seconden in plaats van enkele dagen (Kamath, 2018).

9.3.2 Mango's

Naast varkensvlees heeft Walmart ook een pilot uitgevoerd om gesneden mango's te traceren van de producenten in Zuid- en Centraal-Amerika tot de winkels in Noord-Amerika. Mango's evenals hun derivaten worden wereldwijd verzonden en zijn vatbaar voor Salmonella-verontreinigingen (Andrews, 2012). Daarom beoogde deze pilot het demonstreren van hoe blockchain de traceerbaarheid van een product over nationale grenzen heen mogelijk zou maken. Vooraleer ze de pilot startte, zijn ze opzoek gegaan naar een referentiepunt. Zo werd er een pak gesneden mango's gekocht bij een Walmart vestiging in Amerika. Vervolgens probeerden ze zo snel mogelijk het product te traceren tot de oorsprong, de fruitboer. Na veel e-mails en telefoontjes hadden ze eindelijk hun antwoord, bijna zeven dagen later. Deze tijd was zeker niet slechter dan de industriestandaard. Toch was er nog veel ruimte voor verbetering. Na de succesvolle pilot was men in staat de tijd van het traceren te reduceren van 7 dagen tot slechts 2,2 seconden (Champion, Stevens, & Ward, 2018). Net zoals bij het varkensvlees zou blockchain ook hier kostenbesparingen kunnen realiseren door een veel sneller en accurater systeem.

Naast een snellere traceerbaarheid verwacht men echter dat het gebruik van blockchain nog enkele andere voordelen met zich meebrengt. Zo is het productieproces bij mango's zeer veeleisend waardoor producenten zich mogelijks onethisch gaan gedragen; vervuilde meststoffen, kinderarbeid, hongerlonen, uitbuiting, etc. De werkers hebben geen contracten of vakbonden om hun rechten te verdedigen. Blockchain kan helpen met aan de bel te trekken bij dergelijke praktijken.

Importeurs van mango's en de retail distributeurs inspecteren op kwaliteit, meten en registreren zendingen, documenteren correcte certificaten, meten temperatuur, etc. (The National Mango Board, 2014). Al deze gegevens zou men in de blockchain kunnen opslaan en traceren. Bij de distributie zouden smart sensors, verbonden met de blockchain, uiteindelijk in staat zijn productschade door temperatuur of vochtigheid te registreren (Gantait, Patra, & Mukherjee, 2017). Ten slotte zouden klanten in staat zijn feedback te geven omtrent de kwaliteit, die dan ook weer gelinkt kan worden met specifieke producenten (Kamath, 2018).

De twee pilots hebben aangetoond dat blockchain helpt bij het voorzien van meer transparantie, eerlijkheid en vertrouwen in de voedselindustrie. Daarnaast kunnen leden van de supply chain onmiddellijk maatregelen nemen indien er zich problemen voordoen. Om hun blockchain toepassing te verbeteren en toe te passen op het globaal voedselsysteem, hebben IBM en Walmart hun samenwerking uitgebreid met *Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, Mclane Company, Nestlé, Tyson Foods* en *Unilever* (IBM, 2017). Naar aanleiding van de grote E. Coli uitbraak in Romeinse sla in 2018, vraagt Walmart nu dat zijn leveranciers van bladgroentes hun

producten volledig (tot de boerderij) traceren door middel van blockchain technologie. Er wordt verwacht dat de leveranciers eind 2019 het systeem hiervoor hebben geïmplementeerd.

9.4 Uitdagingen en beperkingen

Zowel Walmart als IBM benadrukken de noodzaak om verder onderzoek te voeren naar hoe men dergelijke blockchain systemen kan schalen en implementeren over de volledige voedsel supply chain. Blockchain technologie heeft zeker het potentieel om een veilig, *end-to-end* beeld te bieden van de gegevens in de supply chain. Om zo een systeem te vertrouwen is het echter belangrijk dat de gegevens afkomstig zijn van een gevalideerde en vertrouwde 'oorsprong'. Zo stelt Mitchell Weinberg, oprichter van het detectie- en preventiebedrijf voor voedselfraude *Inscatech*: *"Blockchain is only as good as the person who's entering the information"* (McKenzie, 2018). Hierop erkende Brigid McDermott, vice-president van IBM *Food Trust*, dat de gegevens in eerste instantie niet van betere kwaliteit zouden zijn dan dat momenteel het geval is. Het toegenomen toezicht door de gegevens op de blockchain te registreren, zou op termijn een kwaliteitsverbetering teweegbrengen en een betere tracering van fouten en fraude mogelijk maken (McKenzie, 2018). Er dient nog onderzoek te gebeuren naar de manier waarop men de herkomst van de gegevens op de blockchain kan verifiëren. Daarnaast is er behoefte aan afgesproken bestuursbeginselen en -structuren om de nodige gegevensuitwisseling tussen alle belanghebbenden te beheren.
Blockchain kan met andere woorden enkel de toegang en het correct delen van gegevens in de voedsel supply chain veilig beheren indien het systeem werkt met bekende en geaccepteerde standaarden. Bovendien is het noodzakelijk dat de gegevens op de blockchain van een geverifieerde bron afkomstig zijn. Ten slotte vereist een succesvolle, globale implementatie deelname van alle actoren binnen het systeem.

9.5 Belgische context

Een toepassing van blockchain in de voedselketen lijkt veelbelovend. Ook in België zijn er de laatste jaren regelmatig voedselschandalen; zo heeft de supermarktgroep Colruyt zeer recent nog 39 rundvlees producten moeten terugroepen omdat ze mogelijk besmet waren met de E. coli-bacterie. De besmette producten waren te koop in 95 van de 239 Colruyt winkels. Het is echter nog niet bekend hoeveel deze terugroepactie ging kosten (Cardinaels, 2019). Half mei 2018 raakte bekend dat zo een 14 schoolkinderen werden opgenomen in het ziekenhuis voor salmonellavergiftiging na het eten van producten, geleverd door traiteur Esthio. Het was zeer groots nieuws aangezien het aantal besmette kinderen bleef toenemen. Eind mei waren er 453 zieke kinderen in 44 verschillende scholen gerapporteerd (FAVV & Zorg en Gezondheid, 2018). Een ander bekend voorbeeld is het wereldwijde fipronil-schandaal anno 2017; pluimveebedrijven gingen nonchalant om met de schadelijke insecticide fipronil. In totaal zouden 45 landen besmette producten ingevoerd hebben waardoor dit zich wereldwijd verspreidde. Hierdoor moest er enkel en alleen in België al een kleine 80 miljoen eieren vernietigd en 2 miljoen kippen geruimd worden (De Standaard, 2017).
Deze schandalen maken wel duidelijk dat een blockchain systeem in de voedselketen enkele voordelen kan realiseren. Zo zou het zeker een tijdswinst boeken; producten kunnen sneller en

accurater getraceerd worden. Bijgevolg kan men in geval van besmetting ook sneller maatregelen nemen en is het onnodig om mogelijks niet besmet voedsel uit de verkoop halen. Aan de kant van de consument zal er meer vertrouwen zijn door de hogere transparantie en door het feit dat er niet geknoeid kan worden met gegevens.

Het is zeer moeilijk om deze effecten te gaan monetariseren. Wat wel mogelijk is, is kijken naar de ziektelast van voedsel gerelateerde pathogenen. Deze ziektelast wordt uitgedrukt in *Disability Adjusted Life Years* (DALY's), een internationaal gehanteerde maat voor het aantal gezonde levensjaren die verloren gaan aan ziekte of overlijden (WHO, 2019).

Een onderzoek van het Rijksinstituut voor Volksgezondheid en Milieu (RVIM) in 2016 schat dat de ziektelast door besmetting via voedsel in Nederland 4.708 DALY's bedraagt. Zij hebben de hiermee gepaard gaande kosten, zowel de directe (medische kosten) als de indirecte (reiskosten, werkverzuim, etc.), geschat op zo een 171 miljoen euro (MJ, IHM, JA, & W). Deze resultaten maken duidelijk dat de ziektelast door voedselbesmetting niet onbelangrijk is in termen van volksgezondheid. Het is tenslotte de overheid haar plicht om de voedselveiligheid te beschermen en te controleren. Indien er aangenomen wordt dat de Belgische situatie hiermee vergelijkbaar is, kan men met behulp van een blockchain-systeem een betere voedselveiligheid bekomen.

Echter kan de ontwikkeling van dergelijke systemen deels aan de private markt worden overgelaten. Zij halen namelijk ook voordeel uit het ontwikkelen van een transparante en veilige supply chain. Zo zijn enkele verwachte baten van Walmart: meer vertrouwen bij de eindconsument, een verbeterd houdbaarheidsmanagement, minder frauduleuze producten (die pr-ramp kunnen veroorzaken), etc. (Galvin, 2017). Idealiter ondersteunt de overheid de private markt om dergelijke initiatieven te ondernemen door samenwerkingsverbanden op te stellen om de innovatie en ontwikkeling te stimuleren.

10 Casestudy Zwitserland: digitale identiteit

10.1 Situatieschets

De stad Zug in Zwitserland staat tegenover dezelfde uitdagingen met betrekking tot digitale identiteit als de rest van de overheden. Officiële identiteiten zijn gefragmenteerd; verschillende overheidsdiensten vragen verschillende identificatiebewijzen en de afgeschermde informatie in de aparte databases zorgen voor administratieve lasten {Young, 2018 #384}.
Zo bestaan er reeds enkele digitale identiteiten, maar deze stuitten allemaal op hetzelfde probleem: de persoonlijke gegevens worden opgeslagen op centrale servers en kunnen bijgevolg gestolen worden. Bovendien worden onze persoonlijk gegevens in handen van grote zoekmachines en sociale media gebruikt om winst mee te maken. Daarnaast ontbreekt er voor individuen een alternatief voor een beveiligde, zelf bestuurde en geauthentiseerde digitale identiteit die veel waarde zou kunnen bieden in een alsmaar meer digitale samenleving. Steeds meer digitale applicaties in de private en publieke sector vereisen een eenduidige, vervalsingsvrije identificatie die niet enkel gebaseerd is op een wachtwoord. Momenteel ligt de focus enkel op gecentraliseerde oplossingen, zoals de 'Suisse ID', een digitaal paspoort en handtekeningsysteem. Echter zijn deze oplossingen tot nu toe niet geaccepteerd. Dit valt volgens sommigen te wijten aan het feit dat ze relatief moeilijk te gebruiken zijn en dat ze technisch gezien reeds als verouderd beschouwd kunnen worden (Young & Verhulst, 2018).
Zug heeft om deze reden het heft in eigen handen genomen en heeft een pilotproject opgestart. Het doel van het project was het creëren van één enkele elektronische identiteit voor allerlei toepassingen, zoals een digitaal paspoort. Daarnaast wouden ze dat de digitale identiteit niet centraal werd opgeslagen in Zug, maar dat het zich op de blockchain bevond. De burgemeester, Dolfi Müller, voegde hier nog aan toe dat hun rol enkel het verifiëren en bevestigen van de identiteit (van een persoon) omvat (Offerman, 2018).

10.2 Toetsing aan de hand van het framework

- **"Meerdere partijen"**: Een digitale identiteit of *e-ID* wordt door meerdere partijen gebruikt. Zo zou een burger zijn digitale identiteit voor verschillende diensten in zowel de publieke als de private sector kunnen gebruiken.

- **"Vertrouwde autoriteit"**: Bij een *e-ID* is er nood aan een vertrouwde autoriteit die de identiteit van een persoon kan verifiëren. Dit kan bijvoorbeeld de overheid zijn die door uitgave van een elektronische identiteitskaart ervoor zorgt dat de burgers zich digitaal kunnen identificeren. Echter wordt Facebook ook gebruikt om de identiteit online te bevestigen. Daarnaast verzamelen bedrijven zoals Facebook of Amazon immens veel gegevens, die voor winstbejag gebruikt worden zonder expliciete toestemming van de gebruiker. Een *self-sovereign* identiteit op de blockchain zou deze 'vertrouwde' autoriteiten kunnen vervangen. Echter zal er bij het opstellen van een

digitale identiteit een of andere vorm van verificatie nodig zijn om de correctheid van de identiteit na te gaan.

- **"Gecentraliseerde werking"**: Een digitale identiteit eist zeker geen gecentraliseerde werking. Door de identiteit op de blockchain te zetten en dus te decentraliseren, kan men ervoor zorgen dat de burgers zelf controle hebben over hun eigen persoonlijke gegevens en hoe deze gebruikt worden.

- **"Data transparantie versus vertrouwelijkheid"**: Er is nood aan een zekere mate van vertrouwelijkheid bij het gebruik van *e-ID*. Het bevat namelijk persoonlijke gegevens die liefst niet openbaar gemaakt worden. Standaard is blockchain transparant, echter kan men ervoor kiezen om de gegevens op de blockchain te verbergen. Vervolgens is het mogelijk om applicaties selectief toegang te verlenen tot bepaalde gegevens. Zo wordt enkel de noodzakelijke informatie vrijgegeven, vereist voor die specifieke toepassing.

- **"Data integriteit en onveranderlijkheid"**: Blockchain technologie biedt een oplossing voor veel problemen rond digitale identiteit; de identiteit kan worden geauthentiseerd op een onweerlegbare, onveranderlijke en veilige manier. De huidige systemen berusten op wachtwoorden die worden uitgewisseld en opgeslagen op onveilige systemen. Een op blockchain gebaseerd authenticatiesysteem berust op een onweerlegbare identiteitsverificatie met behulp van een digitale handtekening. Bij een identiteit op de blockchain wordt er enkel nagegaan of de transactie al dan niet ondertekend werd door de juiste private sleutel. Hier wordt dus aangenomen dat degene die toegang heeft tot de private sleutel ook de eigenaar is en dat de exacte identiteit van de eigenaar als irrelevant beschouwd kan worden.

- **"Hoge verwerkingscapaciteit"**: Een digitale identiteit vereist geen hoge verwerkingscapaciteit. De tragere verwerkingscapaciteit van blockchain vormt dus geen obstakel voor de implementatie van een dergelijk systeem.

Uit de toepassing van het framework blijkt dat een blockchaintoepassing rond digitale identiteit zeker waarde kan bieden. Een self-sovereign digitale identiteit zou ervoor zorgen dat de burgers terug controle krijgen over hun persoonlijke gegevens. Daarnaast zou een uniforme digitale identiteit de overheid administratieve lasten besparen en stelt het hun in staat om veilig digitale diensten aan de burgers te verlenen.

10.3 Bevindingen

Om de administratieve inefficiënties en het gebrek aan controle van individuen over hun persoonlijke informatie aan te pakken, is er een samenwerkingsverband ontstaan om een nieuwe aanpak te ontwikkelen. Het consortium bestond uit het *Institute for Financial services Zug* (IFZ), het Zwitsers IT-bedrijf *ti&m* en *ConSensys*, het bedrijf achter de *uPort* identiteitsprotocol. Deze actoren ontwikkelden samen met het stadsbestuur van Zug een nieuwe oplossing voor een *self-sovereign*

identiteit voor de inwoners van de stad. Ter verduidelijking: *self-sovereign* verwijst naar een identiteitssysteem dat individuen in staat stelt om te bepalen hoe hun identiteit interageert met verschillende diensten, zonder te vertrouwen op gecentraliseerde identiteitsleveranciers (bv. facebook) (Braendgaard, 2017).
Een artikel gepost door *uPort* beschrijft het proces hoe men de digitale identiteit kan verkrijgen in vijf stappen (uPort, 2017).

- Na het downloaden van de *uPort* app, registreert de burger zijn *uPort-ID* op de Ethereum blockchain.
- Met behulp van hun recent geregistreerde *uPort-ID*, melden de burgers zich aan in het Zug-ID-portaal met behulp van een QR-code.
- Na authenticatie in het webportaal van Zug voert de burger zijn persoonlijke gegevens en zijn bestaande Zug ID-nummer in. Aangezien de persoonlijke gegevens van de burger afkomstig zijn van hun nog niet geverifieerde *uPort-ID*, vereist deze inzending nog een persoonlijke verificatie door een stadsmedewerker.
- Na registratie heeft de burger 14 dagen om persoonlijk naar het kantoor van de Zug-records te gaan met een van zijn officiële identiteitsbewijsdocumenten.
- Eens een ambtenaar van Zug de informatie van de individu verifieert en kruis controleert, wordt de nieuwe *digital citizenship credential* van de bewoner toegevoegd aan hun *uPort-ID*. Deze *credential* vertegenwoordigt een digitale attestering van Zug aan de burger, en claimt hun actieve burgerschap.

De stad is nu bezig met het evalueren van verschillende concrete toepassingen die zullen bouwen op deze nieuwe identiteitsinfrastructuur. Zo zijn enkele voorbeelden van de toepassingen: de toegang tot alle onlinediensten van de stad, fietsverhuur, parkeerbeheer, boeken lenen van de bib en het verzamelen van andere toeslagen. Niet enkel de stad, maar ook derde partijen zouden gebruik kunnen maken van het nieuwe identiteitssysteem, bijvoorbeeld indien iemand een kamer wilt (ver)huren. Het idee erachter is dat kleine vereenvoudigingen het leven van de burger gemakkelijker maakt. Naar de toekomst toe zullen meer complexe toepassingen ontwikkeld worden (Nawfal, 2018). Elke afdeling onderzoekt nu mogelijke toepassingen voor hun eigen domein. Digitalisatie en *e-Government* zijn centrale thema's voor de volgende jaren.

10.4 Uitdagingen en beperkingen

Bij het project zijn er enkele uitdagingen ondervonden. Zo is het blockchain systeem voor identiteit van Zug niet wettelijk erkend. Dit valt te wijten aan conflicten tussen het stadsbestuur en het bestuur op kantonnaal niveau. Hoewel het systeem wordt erkend voor de dienstverlening van de stad zal er verandering moeten komen in de wetgeving op kantonnaal niveau om deze digitale identiteit kracht bij te zetten.
Zoals in het proces beschreven wordt, vereist de creatie van een identiteit op de blockchain nog steeds een persoonlijke identificatie op het stadhuis. Hoewel deze stap belangrijk is om de erkenning

van de identiteit te kunnen verzekeren, zaait deze twijfels over de schaalbaarheid van meer gedecentraliseerde en digitale benaderingen voor het vestigen van een vertrouwde identiteit.
Ten slotte was de invoering relatief traag; slechts 120 inwoners hebben zich geregistreerd in het eerste jaar. Dit kan allicht toegeschreven worden aan zowel het registratieproces als het gebrek aan duidelijke toepassingen. Hoewel de eerste factor waarschijnlijk nog even zal aanhouden, is Zug volop in de weer voor het ontwikkelen van nieuwe toepassingen. Zo gaan ze ook een vergadering voor identiteit-houders organiseren om mogelijke ideeën te gaan verkennen (Young & Verhulst, 2018).

10.5 Belgische context

Het is zeer moeilijk om te voorspellen wat voor effecten een *self-sovereign* digitale identiteit met zich mee zou kunnen brengen in België. Een assumptie die we hier kunnen maken, is dat een digitale identiteit op basis van blockchain ongeveer dezelfde effecten als in Zwitserland met zich mee zou brengen. Volgens *uPort* zou het gebruik van hun oplossing enkele voordelen genereren. Zo is de overheid niet verplicht hun eigen servers of *nodes* op te zetten, maar kan ze gebruik maken van het Ethereum netwerk. Door het eigenaarschap van zowel de identiteit als het attest aan de burgers niet op hun eigen servers op te slaan maar te distribueren, is het systeem minder vatbaar voor cyberaanvallen of gegevensdiefstal. Bovendien is het gebruik van de *uPort-ID* in overeenstemming met de GDPR; bedrijven verifiëren enkel de specifieke informatie die vereist is voor een bepaalde toepassing. Dit vermindert de aansprakelijkheid van service providers aangezien ze enkel de gegevens opslaan die ze gebruiken (Kohlhaas, 2017).
Nu rest de vraag nog of België ook gebruik zou moeten maken van blockchain voor het vestigen van digitale identiteit. Het valt niet te ontkennen dat een eenduidige, vervalsingsvrije identificatie noodzakelijk is voor de digitalisatie van overheidsdiensten. Een succesvolle implementatie van een blockchain systeem kan aanzienlijke gevolgen hebben voor de overheden alsook voor de burgers. Een digitale identiteit wordt steeds belangrijker naarmate de mogelijkheden om toegang tot overheidsdiensten op afstand te verkrijgen, toenemen. Dit potentieel wordt mogelijks nog versterkt indien men op Europees niveau een dergelijk systeem zou kunnen doorvoeren. De Europese eIDAS (*Electronic Identification Authentication and trust Services*) heeft een framework opgesteld voor digitale identiteiten en vertrouwen in heel Europa. Dit framework werd echter ingesteld vóór de meer recente ontwikkelingen in blockchain-technologie met betrekking tot digitale identiteit en houdt geen rekening met het model van *self-sovereign* identiteit dat blockchain mogelijk maakt (Third, Quick, Bachler, & Domingue, 2018). Om deze reden moeten er waarschijnlijk eerst legislatieve veranderingen worden doorgevoerd om een duidelijk en concreet kaderwerk op te stellen.

11 Conclusie

Blockchain is een innovatieve technologie die een nieuwe manier van organiseren biedt binnen verschillende domeinen voor het vastleggen van transacties, gebeurtenissen, certificaten en eigenaarschap. Het is een gedistribueerd systeem waar de centrale autoriteit vervangen wordt door een consensusmechanisme tussen *nodes* van een netwerk. Momenteel zijn de *cryptocurrencies* zoals Bitcoin de populairste toepassing van blockchain technologie. Echter kan het gebruik van de technologie ook binnen de publieke sector opmerkelijke voordelen genereren op vlak van transparantie, efficiëntie en veiligheid.

De technologie creëert eenvoudige en efficiënte methoden voor het opslaan en delen van gegevens. Ook worden de integriteit en de vertrouwelijkheid van de gegevens gegarandeerd door middel van cryptografie. Daarnaast maakt de gedistribueerde aard van de technologie het mogelijk dat de verschillende stakeholders in bezitting zijn van hun eigen gegevens.

Als eerste casestudy werd de toepassing met betrekking tot *e-Health records* binnen de Estse overheid geanalyseerd. Zo maakt Estland momenteel gebruik van de KSI-blockchain om de integriteit en de veiligheid van de gegevens te waarborgen. Daarnaast wordt X-Road benut om de interoperabiliteit tussen verschillende systemen mogelijk te maken. Een gelijkaardig systeem zou in België kunnen toegepast worden. Echter werden er reeds veel middelen gespendeerd aan andere EPD's zoals het KWS, waardoor het overtuigen van alle actoren om over te stappen naar een nieuw systeem moeizaam zou kunnen zijn. Toch zou het gebruik van blockchain binnen de gezondheidszorg verder onderzocht en getest kunnen worden door de overheid. Zo kan er mogelijks een meer ondersteunende rol aan de technologie worden toegeschreven zoals in Estland, waar blockchain instaat voor de beveiliging en de integriteit van de gegevens. Blockchain zou binnen de gezondheidszorg evenzeer gebruikt kunnen worden voor medicatiebeheer, het traceren van geneesmiddelen binnen de supply chain, het opvolgen van de vaccinatiegraad, etc.

Naast de mogelijkheid om een efficiëntere en veiligere gezondheidszorg te bekomen, biedt blockchain mogelijks een nieuwe manier van werken waarbij fouten, fraude en de kosten omtrent het leveren van diensten zou verminderen. Zo bleek uit zowel de casestudy van Zweden als de toetsing ervan aan de hand van het framework dat er zeker potentieel is voor een blockchaintoepassing binnen het kadaster. De hogere efficiëntie- en transparantiegraad van het overdrachtsproces zou significante baten kunnen realiseren zowel voor de overheid als de burger.

Door middel van de casestudy van Walmart werd aangetoond dat het gebruik van blockchain binnen het supply chain management significante efficiëntiewinsten en een hogere transparantiegraad kan verwezenlijken. De implementatie ervan binnen de voedselketen zou zowel de volksgezondheid als het vertrouwen in de voedselindustrie ten goede komen. Bovendien zou een dergelijke toepassing gebruikt kunnen worden voor het opvolgen van geneesmiddelen, van producent tot patiënt.

Het gebruik van digitale overheidsdiensten vereist een elektronisch en streng beveiligd identificatiesysteem. In de casestudy van Zwitserland werd beschreven hoe de inwoners van Zug gebruik konden maken van een *self-sovereign* identiteitssysteem dat berust op blockchain technologie. Op deze manier kunnen de persoonlijke gegevens van de burgers niet misbruikt worden voor winstbejag door bedrijven, maar hebben de burgers controle over hun eigen gegevens. Bovendien kan het gebruikt worden als een veilig, efficiënt en 'eerlijk' identificatiesysteem.

Naast de uitgevoerde casestudy's zijn er veel andere mogelijke toepassingen die nog verder onderzocht moeten worden, zoals bijvoorbeeld belastinginning, het uitkeren van sociale bijstand, digitaal stemmen etc. Hoewel blockchain technologie zich zeer nuttig kan bewijzen voor de overheid zijn er naast verder onderzoek nog enkele uitdagingen te overwinnen. Zoals eerder vermeld zullen toepassingen binnen de publieke sector meestal gebruik maken van *permissioned* (en private) netwerken. *Permissioned* blockchains worden ontworpen en geoptimaliseerd voor specifieke toepassingen en steunen sterk op reeds bestaande vertrouwensbanden. Zo zijn enkel de 'vertrouwde' *nodes* geautoriseerd om gegevens aan de blockchain toe te voegen, ook wel *Proof-of-Authority* genoemd. Dergelijke systemen werken efficiënter, maar hun veiligheidsgaranties moeten vóór implementatie steeds worden nagegaan. De weerstand tegen aanvallen op het netwerk zal afhankelijk zijn van de concrete vertrouwensmodellen en geïmplementeerde beveiligingsmechanismes die gehanteerd worden ter bescherming voor zowel insider- als outsideraanvallen.

Een bijkomende uitdaging is het feit dat blockchain technologie nog steeds in zijn kinderschoenen staat. Keuzes rond het ontwerp van blockchain bepalen hoe de technologie gebruikt kan worden, welke baten worden behaald en welke beperkingen de implementatie ervan heeft. In tegenstelling tot Estland bevinden andere overheden zich hier nog steeds in een zeer vroeg en conceptueel stadium. Er heerst dus nog onzekerheid en discussie over de gerealiseerde voordelen van een geïmplementeerde blockchaintoepassing.

Daarnaast kan de technologie moeilijk als een afzonderlijke component van de IT-infrastructuur geëvalueerd worden. Een kritische beoordeling van de potentiële voordelen van blockchain vereist verder onderzoek naar de socio-economische effecten, gepaard gaande met het creëren van vertrouwen, de organisatorische transformatie en de vorming van nieuwe bestuursmodellen.

Ten slotte vereist de verdere ontwikkeling van de technologie passende bestuursmaatregelen om de positieve effecten van het gebruik van blockchain te stimuleren en mogelijke ongewenste gevolgen voor de samenleving te beperken. Kleinschalige experimenten door de overheid met betrekking tot *e-Government* lijken noodzakelijk om enerzijds een dieper inzicht te verkrijgen in de werking van blockchain, anderzijds om hun eigen rol en functie binnen een veranderend systeem te onderzoeken en bepalen.

12 Referenties

- Ammous, S. (2016). Blockchain Technology: What is it good for?
- Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: BLOCKCHAIN TECHNOLOGY AND ITS USE IN THE PUBLIC SECTOR. In (pp. 1-53). Paris: Organisation for Economic Cooperation and Development (OECD).
- BitFury Group, G., J. (2015). Public versus private blockchains: Part 1: permissioned blockchains.
- Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform.
- Camenisch, J., & Lysyanskaya, A. (2002). *A signature scheme with efficient protocols.* Paper presented at the International Conference on Security in Communication Networks.
- Champion, D., Stevens, B., & Ward, R. (2018). *Can the 'blockchain' contribute to achieving global food security?* Retrieved from https://stfc.ukri.org/files/d-champion-state-of-the-art-review-of-blockchains-in-the-food-sector/
- Chan, M. (2014). Food safety must accompany food and nutrition security. *The Lancet*.
- Chung, M., & Kim, J. (2016). The Internet Information and Technology Research Directions based on the Fourth Industrial Revolution. *KSII Transactions on Internet & Information Systems, 10*(3).
- CoinMarketCap. (2019).
- Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., . . . Wattenhofer, R. (2016). *On Scaling Decentralized Blockchains (A Position Paper)*.
- De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2).
- DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization science, 5*(2), 121-147.
- Dictionaries, O. L. (2019). Definition of blockchain. Retrieved from https://en.oxforddictionaries.com/definition/blockchain?fbclid=IwAR1N1NYDmIecZisg94fmDnaUOhsZEYxV8wXh0gevGFmOjK5QFJTwe0wCEPU
- Dictionary, B. (2019). Definition Supply Chain. Retrieved from http://www.businessdictionary.com/definition/supply-chain.html?fbclid=IwAR1xiKmvMrKruzhuHuoyxx_xopdGUo_wf2DsSv8CAfzNZxy8D5lUbgp7So8
- Digiconomist. (2019). Bitcoin Energy Consumption Index. Retrieved from https://digiconomist.net/bitcoin-energy-consumption
- e-Estonia. (z.d.-a). e-Prescriptions. Retrieved from https://e-estonia.com/solutions/healthcare/e-prescription/
- e-Estonia. (z.d.-b). interoperability services. Retrieved from https://e-estonia.com/solutions/interoperability-services/x-road/
- Europese Commissie. (2017). State of Health in the EU
- België.
- Europese Unie. (2016). {Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation)}. *Official Journal of the European Union, L119*, 1-88. doi:citeulike-article-id:14071352

- Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2019). Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. *arXiv preprint arXiv:1901.00910*.
- Guardtime. (2019). Retrieved from https://guardtime.com
- IBM Research Editorial Staff. (2018). Behind the Architecture of Hyperledger Fabric. Retrieved from https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/
- Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. In: Elsevier.
- Jayachandran, P. (2017). The difference between public and private blockchain. Retrieved from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
- Kairos Future. (2017). The Land Registry in the blockchain - testbed.
- Kohlhaas, P. (2017). Zug ID: Exploring the First Publicly Verified Blockchain Identity. Retrieved from https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702
- Lee, L. (2015). New kids on the blockchain: How bitcoin's technology could reinvent the stock market. *Hastings Bus. LJ, 12*, 81.
- Lo, S. K., Xu, X., Chiam, Y. K., & Lu, Q. (2017). *Evaluating Suitability of Applying Blockchain.* Paper presented at the Engineering of Complex Computer Systems (ICECCS), 2017 22nd International Conference on.
- Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology).
- Manchisi, B. (2018). What is blockchain technology? Retrieved from https://www.ibm.com/blogs/blockchain/2018/07/what-is-blockchain-technology/?fbclid=IwAR2Hx8tP6eA4XnQYDoDh_37RIF6jCHSal7pLd1T2gkhR8VLqSASoJFY2bcc
- McMurren, J., Young, A., & Verhulst, S. (2018). Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers.
- Merriam-Webster. (2019). Definition of blockchain. Retrieved from https://www.merriam-webster.com/dictionary/blockchain?fbclid=IwAR3aC2wh7YyHoXjcwTL_80u6oTtgTuRaSE6gICEGSrhUd0Lj5cDv_5KnYyw
- Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research, 5*, 2541. doi:10.12688/f1000research.9756.1
- OECD. (2018). *Blockchain Technology and Corporate Governance*
- *Technology, Markets, Regulation and Corporate Governance*. Retrieved from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/CA/CG/RD(2018)1/REV1&docLanguage=En
- Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355-364. doi:10.1016/j.giq.2017.09.007
- Phi, G. (2017). Determinants of Health Expenditures in OECD Countries.

- Porru, S., Pinna, A., Marchesi, M., & Tonelli, R. (2017). *Blockchain-oriented software engineering: challenges and new directions.* Paper presented at the Proceedings of the 39th International Conference on Software Engineering Companion.
- Puthal, D., Malik, N., Mohanty, S., Kougianos, E., & Das, G. (2018). *Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems* (Vol. 7).
- Satoshi, N. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System.
- Schokkaert, E. (2016). *De gezopndheidszorg in evolutie: uitdagingen en keuzes*: KVAB Press.
- Statbel. (2019). Energie gebruiksstatistieken. Retrieved from https://bestat.statbel.fgov.be/bestat/crosstable.xhtml?view=e8ce66e8-d75f-4dae-b0d9-b7720dd96be0
- Statista. (2019). Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes).
- Subramanya, S., & Yi, B. K. (2006). Digital signatures. *IEEE Potentials, 25*(2), 5-8.
- Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.".
- Swan, M., & de Filippi, P. (2017). Toward a Philosophy of Blockchain: A Symposium: Introduction. *Metaphilosophy, 48*(5), 603-619. doi:10.1111/meta.12270
- Third, A., Quick, K., Bachler, M., & Domingue, J. (2018). Government services and digital identity. *European Union Blockchain Observatory and Forum*.
- van Engelenburg, S., Janssen, M., & Klievink, B. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent information systems*, 1-24.
- Vandooren, S. (z.d.). Wat is Supply Chain Management? Retrieved from https://www.ubeon.com/nl/ubeon/artikels/wat-is-supply-chain-management?fbclid=IwAR334jTnwPzvVSmNU9aQLjYEiz3ngzcWdTkREbVqgc3M9yJlxe0SMCTlBrs
- Ven, K., Verelst, J., & Mannaert, H. (2008). Should You Adopt Open Source Software? *IEEE Software, 25*(3), 54-59. doi:10.1109/MS.2008.73
- Walport, M. (2015). *Distributed Ledger Technology: Beyond block chain*. Retrieved from
- Weise, J. (2001). Public key infrastructure overview. *Sun BluePrints OnLine, August*, 1-27.
- WHO. (2019). Health statistics and information systems.
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *Draft NISTIR, 8202*.
- Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance, 25*(2), 196-208.
- Zhang, L., Shan, L., & Wang, J. (2012). *Summary of Digital Signature* (Vol. 137).
- Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352-375.