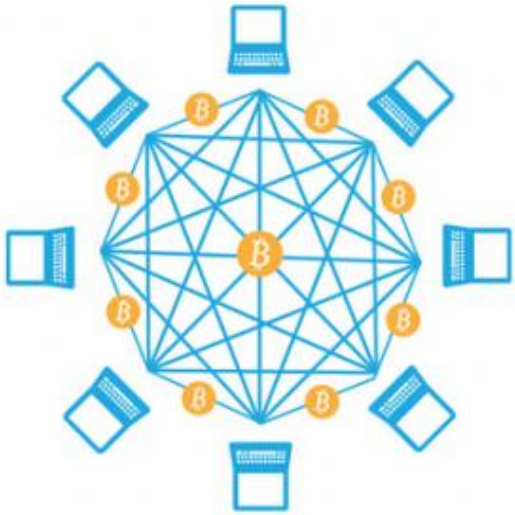
KdG Karel de Grote Hogeschool



Blockchain in Financiële Sector

"WELKE CRITERIA KAN EEN FINANCIËLE INSTELLING HANTEREN OM EEN PRODUCT OF PROCES AF TE HANDELEN VIA BLOCKCHAIN."

Kristoff De Clerck | Bachelorproef | 11 mei 2018

Toegepaste Informatica Blended

Woord vooraf

Deze bachelorproef liet me toe om de opgedane kennis in de studie Toegepaste Informatica te koppelen aan mijn werkervaring. IT gebruiken om efficiënter te werken was ook de drijfveer om deze extra studie aan te vangen. Na een uitgebreid onderzoek naar blockchain is me duidelijk dat deze technologie de financiële sector een pak efficienter kan laten werken.

Ik begon aan deze bachelorproef met de beperkte kennis dat blockchain de achterliggende technologie was voor bitcoin. Deze cryptomunten zouden het financiële systeem zoals we het nu kennen het vuur aan de schenen leggen en dus eerder een bedreiging dan een zegen zijn voor de banken. Mijn interesse was dan ook direct gewekt!

Samen met de stage is de bachelorproef een einde van intensieve studie toegepaste informatica. Dank aan de docenten van KdG om me te vormen in de verschillende IT domeinen. Bijzondere dank aan bachelorproef-begeleider Wim De Keyser, voor de aanzet en de begeleiding voor deze scriptie.

Tenslotte grote appreciatie naar mijn vrouw Sonja en mijn twee dochters. Zij hebben de laatste vier jaar mijn studie volledig gesteund en hierdoor papa toch wel wat moeten missen. Bedankt.

Kristoff De Clerck

Samenvatting

Bitcoin en bij uitbreiding blockchain kan voor financiële instellingen als bedreiging worden aanzien. Aan de hand van de technologische kenmerken van blockchain onderzocht ik of blockchain ook kan toegepast worden door financiële instellingen en welke criteria hiervoor in acht moeten genomen worden.

Door grondige analyses van algemene use cases en cases uit de financiële sector stelde ik vast dat blockchain wel degelijk een meerwaarde kan bieden. Dankzij enkele samenwerkingsverbanden onder koepel van Hyperledger en Corda en tussen verschillende banken onderling zijn reeds heel wat concrete succesvolle pilootprojecten opgezet.

Een blockchain is niet voor elke toepassing de ultieme oplossing (in vergelijking met tradionele databanken). Een succesvolle blockchain kan oplossing bieden wanneer meerdere partijen een databank wensen te delen om acties uit te voeren die met elkaar verbonden zijn en deze databank niet willen toevertrouwen aan één van de partijen of een derde tussenpersoon. Een extra argument is de transparantie die een blockchain biedt hetgeen de regulator tegemoet komt op gebied van audit. Blockchain kan tevens risicoscore beperken door decentralisatie van data, mindere blootstelling aan fraude en lager tegenpartijrisico. Smart contracts laten een betere efficiëntie toe.

Naast deze eerste criteria zal het vooral de omgeving (cliënten, concurrenten, nieuwkomers) zijn die financiële instellingen zal verplichten bestaande processen te automatiseren om deze sneller en goedkoper af te handelen. Dit is een win-win voor zowel de financiële instelling als client.

Inleiding

Een aantal jaar geleden was blockchain quasi onbekend. De jongste maanden en weken is de term bijna dagelijks terug te vinden in financiële berichtgeving. Het aantal hits loopt bijna samen op met de koers van de bitcoin. Deze cryptocurrency is immers gebaseerd op blockchaintechnologie en wordt in één adem uitgesproken. De link met de financiële sector is dus snel gelegd. Nochtans is de bitcoin niet de onderzoeksvraag in deze scriptie, wel de onderliggende technologie. Deze opent immers opportuniteiten voor verwerking van gegevens. Betrouwbare opslag van deze gegevens is voor financiële instellingen bijzonder belangrijk. Banken hebben in het verleden het vertrouwen van stakeholders opgebouwd met bestaande systemen. In hoeverre kan blockchain een alternatief zijn?

Ik ben zelf actief binnen de financiële sector, meer bepaald langs de beleggingskant. De jongste maanden kreeg ik meerdere vragen of investeren in Bitcoin opportuun was en hoe de bank hier tegenover stond. Dit wekte mijn nieuwsgierigheid om bitcoin te ontdekken en vooral ook hoe een bank hiermee omgaat. Hoewel voor bitcoin de meningen sterk uiteen lopen is de interesse in de achterliggende blockchaintechnologie wel zeer groot. Mijn werkgever blijkt zelfs een voorloper te zijn.

Deze scriptie is geen bitcoinverhaal, maar gaat na welke criteria een financiële instelling kan hanteren om een blockchaintoepassing op te zetten. Om een antwoord te vinden op deze onderzoeksvraag focus ik me vooral op de analyse van use cases. Extra aandacht wordt besteed aan concrete implementaties.

Na een toelichting over het ontstaan van blockchain en de technische kenmerken wordt ten eerste **bitcoin** verder toegelicht. Het **Ethereum** platform maakt met de mogelijkheid van smart contracts ook de brug van publieke naar private blockchains. In Hoofdstuk 4 bekijken we de mogelijkheden om blockchain in het **bedrijfsleven** te integreren. Door het specifieke karakter van de financiële sector wordt hier een aparte sectie aan gewijd. Vervolgens diepen we de mogelijkheden verder uit door enerzijds algemene use cases te analyseren en anderzijds de financiële cases uitgebreider te belichten. Dit laat toe de meest gebruikte criteria op te lijsten. Deze worden in Hoofdstuk 5 verder verfijnd via effectieve **implementaties**. Tenslotte staan we nog even stil of blockchain wel altijd de ultieme oplossing is aangezien er toch ook enige **beperkingen** zijn.

Ik **besluit** met het antwoord op de onderzoeksvraag "*Welke criteria kan een financiële instelling hanteren om een product of proces af te handelen via blockchain*".

Inhoudsopgave

1. Blockchain

1.1. Introductie

Bij de ontwikkeling van blockchain was de uitdaging om digitale informatie te kunnen verspreiden, maar niet te kopieren.

> *"Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. "*
> *[1]*

Zo omschrijft Harvard Business Review blockchain. Hoewel bitcoin als cryptocurrency de eerste wijdverspreide toepassing van blockchain was, zou het verkeerd zijn om in de definitie van blockchain al te verwijzen naar bitcoin of enige andere vorm van cryptocurrency. Blockchain kan je dan ook definiëren door enkele kernwoorden die in deze definitie terugkomen:

Centraal hierin is **distributed ledger**. In het recente verleden was bij transacties een centrale derde partij betrokken. Deze partij kreeg als functie de betrouwbare tussenpersoon te zijn tussen partij A en partij B. Afhankelijk van de onderliggende transactie was dit een bank, notaris, de overheid. De transactie kan doorgaan omdat deze derde partij de transactie goedkeurde en beide partijen vertrouwen hadden in deze tussenpersoon.

Bij een gedistribueerd grootboek valt deze tussenpersoon weg en wordt de transactie goedkeurd door het netwerk van participanten. Het grootboek wordt gekopieerd naar een veelvoud van gebruikers en de groep als geheel bevestigt de authenticiteit van het grootboek. Het volledige grootboek wordt gedistribueerd naar alle computers en kan onmiddellijk **geverifieerd** worden.

Belangrijk verschil bij een gedistribueerd grootboek is dat er enkel toevoegingen (record transactions) kunnen gebeuren aan het grootboek en nooit wijzigingen noch verwijderingen. In IT termen is enkel Create beschikbaar, maar niet Update noch Delete (uiteraard ook Read). Elke aanvulling is dan ook **permanent**.

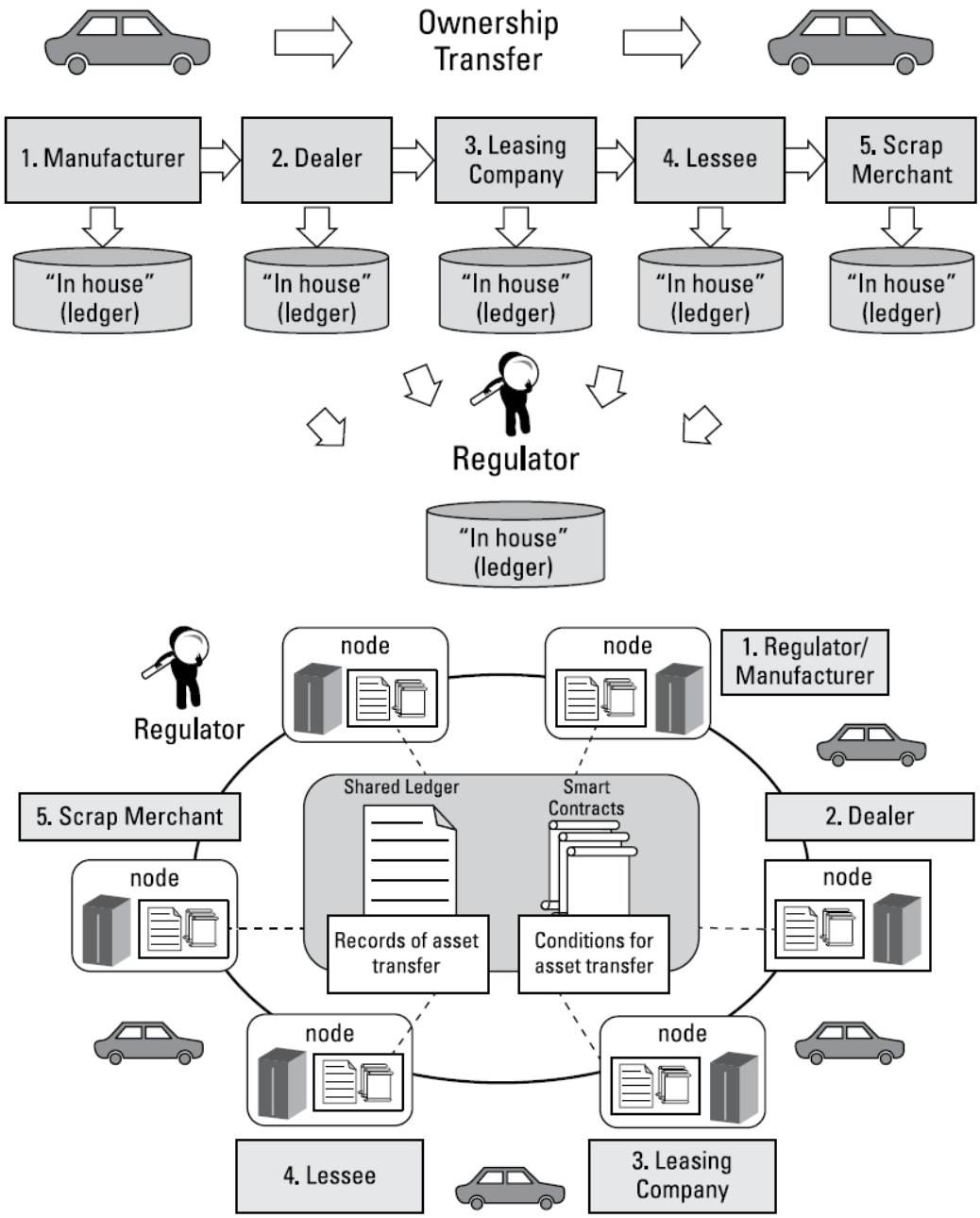
Iedere toevoeging van informatie kan aanzien worden als een blok dat toegevoegd wordt aan de reeds bestaande blokken. Deze blokken worden aaneengekoppeld zodat de blockchain geboren is. Door het continu aaneenschakelen van blokken is er tevens een spoor mogelijk naar de volledige historiek van transacties.

De evolutie van het internet heeft de ontwikkeling van blockchain gefaciliteerd. Een netwerk van computers dat regelmatig met elkaar communiceert over het grootboek is immers cruciaal in het gedeeld grootboek.

De voordelen van een dergelijk gedeeld grootboek worden duidelijk in afbeelding 1. [2] Dit proces volgt de levensloop van een wagen van producent tot recyclagebedrijf. In de eerste tekening houdt elke tussenpersoon een eigen bestand bij hetgeen geen enkele communicatie mogelijk maakt tussen de verschillende partijen. Een derde partij die toegang nodig heeft tot

elke tussenstap dient bovendien naast alle aparte toegangen ook een eigen database aan te leggen met consolideerde gegevens.

De tweede tekening maakt gebruikt van een gedeeld grootboek. Bij elke transactie wordt deze toegevoegd aan het grootboek en geeft deze dus steeds een correct beeld van eigendom van de wagen. De overheid heeft te allen tijde zicht op de eigendomstitel van de wagen.



Afbeelding 1 *Eigendom wagen opvolgen zonder (tekening boven) en met blockchain (tekening onder)*
Bron: Blockchain for Dummies pagina8

De belangrijkste kenmerken van een blockchain kunnen samengevat worden als: [3]

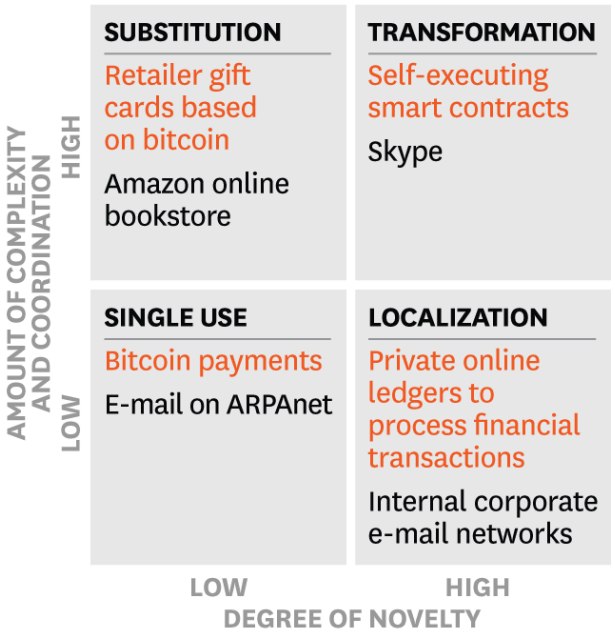
- Meestal financiële transacties
- Vermenigvuldiging van data over meerdere systemen
- Meestal peer-to-peer netwerk
- Versleuteld via cryptografie en digitale handtekening
- Moeilijk om historische transactie te wijzigen

1.2. Evolutie van blockchain

In 2008 publiceert Satoshi Nakamoto een paper van slechts 9 pagina's met als titel "Bitcoin: a peer-to-peer electronic cash system". In deze paper wordt de basis gelegd van de technologie achter blockchain met als eerste concrete toepassing de bitcoin. [4]

Het is dan ook niet verwonderlijk dat blockchain en bitcoin dikwijls samen vermeld worden. Marco Iansiti en Karim R Lakhani illustreren in Harvard Business Review de link tussen blockchain en bitcoin op een mooie manier (zie afbeelding 2). [5] Voor het ontstaan van het internet werd communicatie tussen tussen twee partijen voornamelijk afgehandeld tussen directe verbinding tussen deze twee partijen. Met de komst van het TCP/IP protocol werd dit doorbroken. De overdracht van data werd in pakketjes verdeeld die telkens de adresgegevens bevatte van de tweede partij. Eén van de eerste concrete toepassingen van deze vernieuwende technologie was e-maildienst op ARPAnet (1972). Pas eind jaren 80 werd deze technologie ook in het bedrijfsleven geïmplementeerd, vooral via interne diensten. Half jaren 90 was het wereld wijde web voldoende matuur geworden voor een doorbraak bij het grote publiek en dankzij oa webbrowers konden ondernemingen businessmodellen bouwen op de nieuwe technologiën. Het hele proces heeft echter meer dan 30 jaar gevergd.

De auteurs vergelijken de blockchain als technologie met de ontwikkeling van TCP/IP protocol hetgeen heel wat concrete toepassingen mogelijk maakt. Bitcoin kan snel geïmplementeerd worden en legt basis voor verdere ontwikkelingen. In dezelde logica zullen bedrijven de nieuwe technologie verder implementeren, in eerste instantie voor interne processen.



Afbeelding 2 De aanvaarding van nieuwe technologiën. *The truth about blockchain by Marco Iansiti and Karim R. Lakhani. [Online afbeelding]. Gedownload op 9 december 2017, van https://hbr.org/resources/images/article_assets/2016/12/R1701J_IANSITI_FOUNDATIONALTECHHOLD.png*

Het kwadrant kan als leidraad dienen voor managers om te identificeren in welk stadium een mogelijke toepassing valt en welke uitdagingen dit zou kunnen brengen.

Single use

In dit eerste kwadrant bevinden zich goedkope en sterk gespecialiseerde toepassingen. E-mail was een goedkoop en snel alternatief voor telefoon- en faxverkeer. Hoewel het totaal aantal bitcoin transcaties vergeleken met het totale betalingsverkeer nog beperkt is, biedt het de gebruikers wel rechtstreeks voordeel.

Localization

Dit tweede kwadrant omvat toepassingen die sterk vernieuwend zijn, doch een beperkt aantal gebruikers impacteert. Ondernemingen besteden hier de meeste aandacht aan en de financiële sector leidt de dans. Nasdaq werkt samen met chain.com en heel wat grote financiële instellingen zoeken toepassingen in domeinen zoals trade finance, foreign exchange, cross-border settlement en securities settlement.

In deze scriptie zullen een aantal toepassingen verder uitgewerkt worden.

Substitution

Weinig vernieuwend maar moeilijker te implementeren worden gegroepeerd in derde kwadrant. Hogere barrières stellen zich in aanpassen van gewoontes van gebruikers, maar ook regulatie. Het gebruik van cryptomunten, gebaseerd op bitcoin is een voorbeeld. Een studie van MIT toonde de trage aanvaarding van cryptomunten aan. In 2014 kregen ca 4500 studenten voor $100 tegenwaarde bitcoin. 30% van de studenten schreef zich nooit in om het gratis geld te aanvaarden en 20% zette de bitcoin binnen enkele weken om naar cash geld.

Transformation

Tenslotte bevatten het vierde kwadrant applicaties die onze huidige manier van werken volledig veranderen. Alle spelers moeten akkoord zijn over de processen en sociale, legale en politieke aanpassing zijn onontbeerlijk. De afwikkeling van contracten kan via smart contracts helemaal aangepast worden. Niet alleen valt de tussenpartij weg, maar ook intern kan heel wat wijzigen (denk bv aan aanpassing contract wanneer gps signaal opgevangen wordt bij koper).

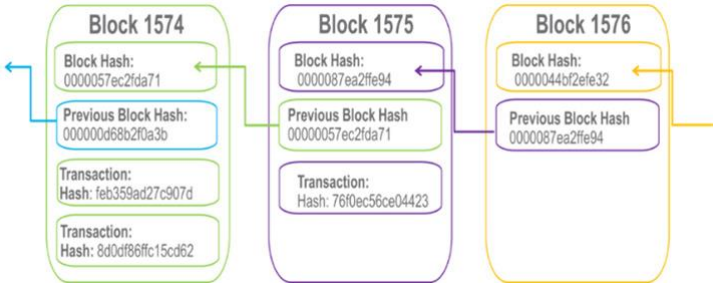
1.3. Blockchain technologie

Blockchain dankt zijn naam aan combinatie van 'block' en 'chain'. [2] Meerdere blokken worden gekoppeld aan een keten. **Afbeelding 3**[1] geeft de gekoppelde blokken weer alsook de verschillende onderdelen van een blok. Elke blok bestaat uit:

Block Hash: een digitale vingerafdruk of uniek id.

Transaction: de inhoud van één of meerdere transacties die op hetzelfde tijdstip gebeurden.

Previous Hash: de unieke code van de vorige blok.



Afbeelding 3 *Blockchain als gekoppelde blokken Bron: Blockchain for dummies, IBM limited Edition, pagina 14*

Omdat in block 1575 verwezen wordt naar block 1574 is het onmogelijk om tussen deze twee blocks een andere te plaatsen. Elke nieuwe blok verwijst dus weer naar de vorige block die ook weer verwijst naar vorige blok,... Op deze manier wordt de ketting steeds versterkt.

De digitale vingerafdruk wordt gemaakt door de inhoud van het block zelf. Hierbij wordt gebruik gemaakt van algoritmes. Deze vingerafdruk zorgt er ook voor dat de hele blockchain consistent is. Indien enige data zou gegewijzigd worden dient de unieke id gewijzigd te worden, alsook alle gekoppelde blocks.

Nieuw block

Wanneer een transactie wordt afgesloten dient een nieuw block aangemaakt te worden. [6] Deze transactie wordt gegroepeerd met andere transacties die plaatsvonden gedurende de laatste 10 minuten. Tenslotte wordt deze block crypothografisch gesloten. Het block wordt pas toegevoegd aan de blockchain op voorwaarde dat 51% van alle computers in het network akkoord zijn met deze block (valideren).

Miners

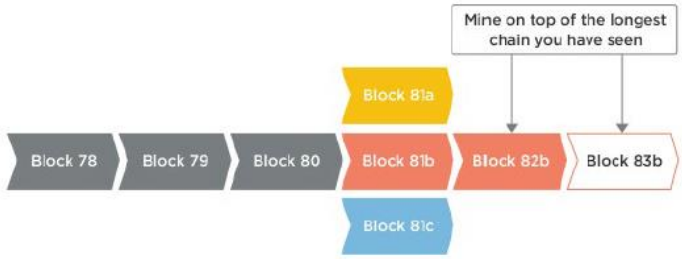
Van zodra een kandidaat block gepubliceerd wordt moet dit block gevalideerd worden. [7] Dit gebeurt door het oplossen van een complex algoritme. Voor het oplossen van deze puzzels is enorm veel rekenkracht nodig en wordt meer en meer gecentraliseerd. Computers die deze taak uitvoeren noemt men miners en meerdere miners zijn in competitie om de puzzel op te lossen. Hoewel deze puzzel enorm complex is om op te lossen is eens de oplossing gevonden het antwoord bijzonder logisch. De miner die als eerste de oplossing vindt publiceert dit op in het network waar andere miners de

[1] Blockchain for dummies, IBM limited Edition, pagina 14

oplossing kunnen controleren. Indien voldoende miners akkoord zijn wordt het block toegevoegd aan de blockchain en ontvangt de miner een beloning. Bij bitcoin bedroeg de beloning bv 25 bitcoins begin 2015, terwijl deze momenteel 12.50 bitcoins bedraagt. Elke 210.000 blocks halveert de beloning immers.[2] De uitbetaling volgt pas nadat 99 blocks zijn toegevoegd aan de blockchain. Dit geeft alle miners incentive om zoveel mogelijk transacties te valideren.

Longest chain rule

Door het groot aantal gecreëerde blocks is het niet onmogelijk dat meerdere miners ongeveer tegelijk een nieuw block ontginnen. Welk block wordt dan opgenomen in de keten en hoe wordt een creatie van verschillende ketens vermeden? De 'Longest Chain Rule' lost dit conflict op [3]. In afbeelding 4 ontginnen drie miners ongeveer tegelijk een block 81 (81a, 81b en 81c). Op dat moment is onduidelijk welk block het meest correcte is. Miners kunnen block 82a, 82b of 82c ontginnen. Zodra echter bv 82b beschikbaar is, vervallen opties 82a en 82c en wordt verder gewerk aan 83b.



Afbeelding 4 *Nieuwe blocks - Longest Chain Rule*

[2] http://www.bitcoinblockhalf.com/

1.4. Blockchain kenmerken

1.4.1. Beveiliging

Het gedistribueerde model heeft nog enkele belangrijke beveiligingsvoordelen. [8] Doordat talloze computers in het netwerk (Node) een kopie van de database bijhouden is er geen probleem als één van deze nodes uitvalt. Het systeem blijft steeds beschikbaar hetgeen niet van toepassing is in een centraal model.[3]

Ook hacking wordt moeilijker via een decentraal systeem. Bij een traditioneel centraal systeem hoeft een hacker maar op één plaats in te breken. Het is zinloos één van de nodes te hacken en de informatie te wijzigen. De andere nodes zullen onmiddellijk zien dat deze informatie niet correct is en de wijziging verwerpen.

Tenslotte worden de gegevens ook minder blootgesteld aan een beperkte groep medewerkers die de gegevens kunnen aanpassen. Het is immers niet ondenkbaar dat in een goed beveiligde database medewerkers van een bedrijf kwaadwillige bedoelingen hebben.

1.4.2. Publiek vs privaat

Cryptomunten draaien meestal op een publieke blockchain: iedereen kan eraan deelnemen. In dit systeem dient een vorm van vertrouwen ingebouwd worden. Crypografie in combinatie met belonen van gebruikers die zich aan de regels houden zijn hierbij noodzakelijk.

Private blockchains zijn beperkt tot een groep gebruikers (bv bedrijf). Doordat dit systeem enkel gebruikt wordt door vooraf goedgekeurde leden is het extra werk voor controle van het vertrouwen niet nodig.

Een mengvorm van publieke en private blockchain is de consortiumblockchain. Dit is een gedeeltelijk gecentraliseerd systeem waarbij meerdere partijen bv bepaalde processen gezamenlijk verwerken. Het samenwerkingsverband tussen meer dan 70 banken wereldwijd: R3 is hier een voorbeeld van.

[3] Ook voor een centraal systeem is replicatie mogelijk via het gebruik van master/slaves

2. Bitcoin

2.1. Introductie

In hoofdstuk 1.2 werden bitcoin en blockchain in dezelfde wieg gelegd. De bitcoin is uitgevonden door Satoshi Nakamoto. [9] Er bestaan verschillende theoriën over Nakamoto. Er bestaan geen foto's en niemand heeft de persoon ooit ontmoet. In april 2011 schreef hij in een e-mail: "I have moved on to other things", waarna sindsdien niets meer van hem gehoord is.

Dit kan verwondering wekken aangezien hij ca 1 miljoen bitcoin in digitale portefeuilles heeft zitten. Omgerekend naar koers dd 9 december 2017 is dit 12,5 miljard euro! Anderzijds valt dit te rijmen met de doelstelling van bitcoin om onafhankelijk te zijn van een centrale bank en het systeem in stand te houden zonder enige inmenging. Tevens zou enig bedrijf van Nakamoto verbonden aan bitcoin snel in het vizier komen van critici.

Andere bronnen beweren dat de code van bitcoin zo sterk is dat het onmogelijk is dat dit door één persoon gecreëerd is. Bijgevolg zou Satoshi Nakamoto een pseudoniem zijn voor een groep.

In oktober 2008 ontstond blockchain als onderdeel van Bitcoin met als doel een virtuele munt te creëren.

2.2. Ontstaan bitcoin

De opzet van Nakamoto was de mogelijkheid voorzien om online geld over te maken van partij A naar partij B zonder tussenkomst van een financiële instelling. Een eerste deel van de oplossing was gebruik te maken van digitale handtekeningen, maar om het probleem te omzeilen dat centen meer dan één keer uitgegeven konden worden maakte hij gebruik van van een peer-to-peer netwerk.

In de traditionele wereld bevestigt een betrouwbare derde partij (bank) dat partij A gelden op de rekening maar één keer kan uitgeven. Nakamoto wou echter een betaalsysteem creëren waar deze derde partij overbodig was. De enige sluitende manier om te verifiëren of een transactie reeds plaatsgevonden heeft (geld is reeds uitgegeven) is kennis te hebben van *alle* voorgaande transacties. Enkel de eerste geldt als correct, eventueel andere zijn 'double spending'.

Hashing

In dit scenario moeten enerzijds alle transacties openbaar worden gemaakt en dient er een afspraak gemaakt te worden over de volgorde van transacties. Bitcoin maakt gebruikt van een gesophisticeerd 'timestamp' systeem gebaseerd op Adam Back's

hashcash. Van een ingewikkelde vergelijking heeft men reeds de meeste parameters en we weten dat de oplossing moet beginnen met een bepaalde tekenreeks (0). Er ontbreekt echter nog een gedeelte dat toegevoegd worden. Door de complexiteit kan dit gedeelte enkel gevonden worden door ontelbare keren te gokken. Bij bitcoin is volledig block gekend (inclusief vorige hashcode), dient er **x** worden toegevoegd zodat de oplossing van de hashfunctie kleiner is dan pre-gedefinieerd getal.

find **x** such that
f(block + **x**) < t
(crytographic hash)

Bij bitcoin dient de oplossing te beginnen met '000'. De functie die gebruikt wordt is SHA-256[4] (Secure Hash Algorithm, 256 bits), ontworpen door NSA van Amerika en 64 tekens bevat, waarvan de eerste drie dus 'nul' dienen te zijn om als oplossing van de puzzel te dienen.

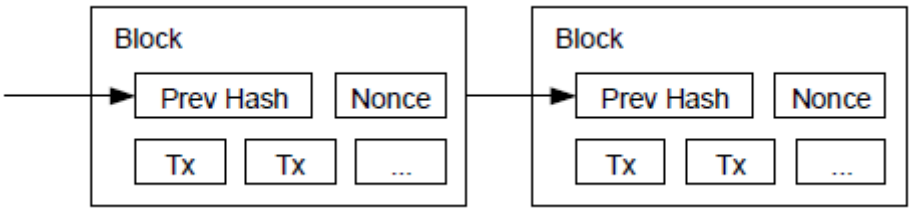
Een voorbeeld[5]

Veronderstel dat gegeven deel "Hello, world!" is. We zouden dan aan het gegeven telkens een extra cijfer kunnen toevoegen, hashen en zien of de oplossing begint met 3x0. In afbeelding x wordt de oplossing gevonden na poging 4251 door het getal 4250 toe te voegen, hetgeen uitzonderlijk snel is. Sha256("Hello, world!4250")=0000c3...

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Bitcoin gebruikt in werkelijkheid een meer complexe versie omdat in de header van het block een *Merkle Tree*[6] is opgenomen, een dubbele SHA256 functie. Dit is buiten scope van deze scriptie.

De gevonden oplossing wordt als Nonce (woord dat maar één keer gebruikt wordt) toegevoegd aan het block zodat het ook wordt afgesloten. Afbeelding 5 komt uit de originele nota van Nakamoto en geeft het afgesloten block weer.



Afbeelding 5 *Proof of work*

[4] https://en.wikipedia.org/wiki/SHA-2
[5] https://en.bitcoin.it/wiki/Proof_of_work
[6] https://en.bitcoin.it/wiki/Protocol_documentation#Merkle_Trees

Netwerk

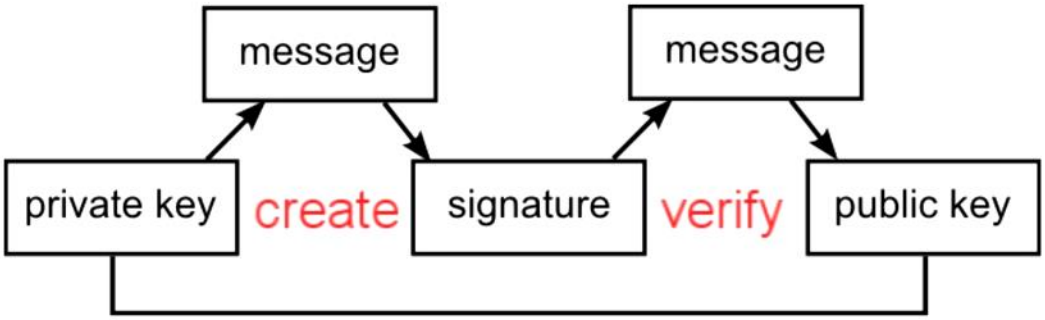
Het afhandelen van een transactie verloopt als volgt:

1. Nieuwe transacties worden doorgestuurd naar alle nodes in het netwerk.
2. Elke node verzamelt de transacties in een block.
3. Elke node zoekt het proof-of-work voor het eigen block.
4. Wanneer een node een proof-of-work gevonden heeft, wordt dit verstuurd naar alle andere nodes.
5. Andere nodes accepteren het block op voorwaarde dat de transacties correct zijn en nog niet uitgegeven zijn.
6. Het block wordt aanvaard doordat andere nodes werken aan het volgende block (waarin de hash van de vorige block is opgenomen).

Keys

Het afhandelen van transacties kan plaatsvinden dankzij het gebruik van publieke en private sleutels (public & private keys). [10]

Via private key (enkel door jou gekend) kan een publieke key aangemaakt worden. Deze kan in het bitcoinnetwerk gebruikt worden om een transactie af te sluiten. Doordat enkel jijzelf de private key hebt kan je de publieke key claimen en de opbrengst van de transactie toevoegen aan persoonlijke portefeuille (wallet).



Afbeelding 6 Combinatie van private en publieke sleutel. Bron: www.imponderablethings.com en https://www.youtube.com/watch?v=Lx9zgZCMqXE

2.3. Zwakheden van bitcoin

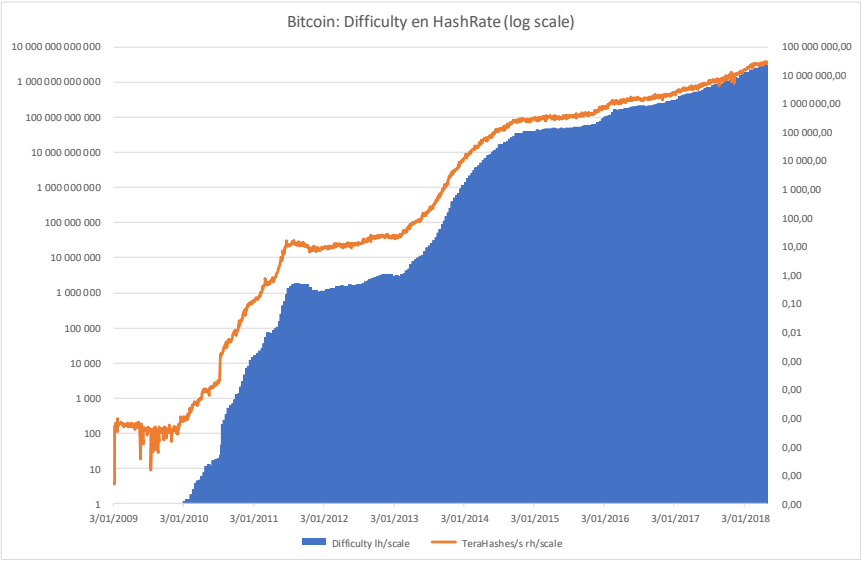
Hoewel in het minen van bitcoins belangrijke incentive is opgenomen om pas na 99 blocks uit te betalen ligt een belangrijke zwakheid in het consolideren van rekenkracht. De oorzaak is te zoeken bij de moeilijkheid om een nieuw block te vinden. [11]

Bitcoin difficulty

Elke 2016 blocks (ca elke 2 weken) wordt de 'bitcoin mining network difficulty' herberekend. De nieuwe waarde wordt herrekend naar een waarde die gelijk is aan een waarde zodat er om de 10 minuten een nieuw block ontdekt zou zijn. Doordat er sinds ontstaan van van bitcoin steeds miners zijn bijgekomen is deze waarde exponentieel gestegen. Afbeelding 7 geeft in een (logaritmische! schaal) de sterke groei van de hashrate en difficulty level.[7]

Deze evolutie heeft ervoor gezorgd dat het steeds moeilijker wordt om een block te ontginnen. In 2009 volstond een eenvoudige computer met een Intel Core i7 (33 MH/s). Vervolgens werd de rekenkracht steeds groter door gebruik te maken van: [12]

- Grafische kaarten (beter in cryptografische vraagstukken) – 650 MH/s
- Mini-farms van grafische kaarten (koppelen van grafische kaarten)
- Field Programmable Gate Array (beter elektriciteit verbruik) – 25,2 GH/s
- Application Specific Integrated Circuit Miners (specifiek) – 1.500 GH/s
- Data Centers (koppeling van ASIC)



Afbeelding 7 https://blockchain.info/nl/charts/hash-rate?timespan=all&scale=1 en https://blockchain.info/nl/charts/difficulty

7 Liefhebbers van begrip difficulty kunnen dit theoretisch verder onderzoeken via : https://en.bitcoin.it/wiki/Difficulty

Het is dus bijna onmogelijk geworden voor particulieren om bitcoins te ontginnen. Steeds meer wordt gebruik gemaakt van datacenters met een groot aantal computers. Een tweede mogelijkheid is om meerdere pc's te koppelen als pool.

Beide oplossingen staan stilaan haaks op de opzet van bitcoin, met name het opzetten van een decentraal systeem. Immers door centralisatie van de rekenkracht zou het mogelijk zijn om voldoende capaciteit te combineren om aan 51% van het netwerk te geraken en op deze manier een hack te doen. In juni 2014 had de pool Ghash.IO kort deze grens overschreden waarop meerdere leden switchten naar andere pool.

De data centers vergen ook een grote hoeveelheid energie om de systemen draaiende te houden en de computers te koelen. Dit stelt enerzijds de milieuvriendelijkheid van de digitale munt in twijfel maar tevens de centralisatie. Landen met voldoende goedkope energiebronnen kunnen de datacenters naar zich toe trekken hetgeen dit land een sterk comparatief voordeel kan bezorgen. Ijsland met grote geothermische bronnen en koel klimaat profiteer hier thans van [13]. Landen met minder goede bedoelingen kunnen hier in de toekomst duidelijk misbruik van maken.[8]

Bitcoin Halvering

Het maximaal aantal bitcoinblocks is 21 mio. Het aantal gedelfde munten halveert elke 210.000 blocks. Bijgevolg daalt ook de beloning periodiek. Dit is nodig om inflatie van de munt onder controle te houden. Initieel (2009) was de beloning voor een blok 50 BTC. Na twee halveringen bedraagt de beloning eind 2017 12.50 BTC per block. Aangezien er ca 144 blocks per dag gedelfd worden en er nog 128.573 blocks te gaan zijn tot volgende halvering zal deze in juni 2020 plaatsvinden.

[8] http://money.cnn.com/2017/12/12/technology/north-korea-bitcoin-hoard/index.html

Hacking

Cryptobeurs is dik 400 miljoen euro kwijt.[9]
Bitcoin: $64m in cryptocurrency stolen in sophisticate hack, exchange says.[10]

Recente titels in de media verwijzen naar hacking van bitcoins. Dit staat een beetje haaks op de sterke bescherming die is ingebouwd in de bitcoin zelf. De hackers slaan echter niet toe op de bitcoin zelf maar op platformen waar bitcoins verhandeld of bewaard worden.

De geciteerde cryptobeurs is Coincheck. Deze beurs zet zichzelf in de markt als 'The Leading Bitcoin and Cryptocurrency Exchange in Asia'. Begin 2018 verloor ze echter ca 435 miljoen dollar aan NEM Munten. De NEM [14] is in Japan één van de meest populaire cryptomunten en staat voor New Economic Movement.

Deze hack is dubbel vervevelend. Enerzijds beschouwt NEM zichzelf als veiliger alternatief dan Bitcoin en Ethereum. Tevens wordt geschermd met betere doorlooptijden, nl honderden transacties per seconden. Tevens bieden ze een verbeterd alternatief voor smart contracts van Ethereum: smart assets.

Anderzijds is de hack ook een tegenvaller voor de Japanse overheid. In tegenstelling tot andere overheden wil die de handel in virtuele munten net stimuleren.

Per eind januari was deze hack de grootste. Andere recente grote hacks:

- Mt. Gox, bitcoin exchange: $350 mio
- NiceHash, mining markt: $78 mio
- Tether hack, start-up offering dollar backed digital tokens: $30 mio
- Bitfinex hack, bitcoin exchange: $72 mio

De hacks hebben als doel de private keys achter de wallets te stelen. Hoewel de bitcoin decentraal is, worden deze keys door de getroffen bedrijven of beurzen centraal bewaard. Onvoldoende beveiliging van de eigen systemen blijkt de grootste kwetsbaarheid te zijn. Voor Mt. Gox is er naast de hack mogelijks ook grootschalige fraude gebeurd. Het onderzoek loopt echter nog.[11]

[9] Tijd, zaterdag 27 januari 2018, pagina 3
[10] https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords
[11] https://www.reddit.com/r/Bitcoin/comments/5cvc3t/how_exactly_was_mt_gox_hacked/

Andere cryptomunten

Bij opstart was bitcoin de enige cryptomunt. Enige mogelijkheid om te handelen via cryptomunt verliep dus altijd via bitcoin en door wetmatigheid van grote vraag en klein aanbod ging de koers steeds hoger. Sindsdien is het aanbod van cryptomunten geëxplodeerd en nemen andere munten een deel van de marktvraag in. Zolang de markt in z'n geheel sterk stijgt kan de vraag naar alle munten toenemen. Zodra de vraag stilvalt kan de prijs fors dalen.

Volgens coinmarketcap.com zijn er per 27 januari ca 1500 cryptomunten in omloop met een totale marktkapitalisatie van ongeveer $543 mrd (gelijk aan marktkapitalisatie van Royal Dutch Shell, dat per 31/12/2017 het 17de grootste beursgenoteerd bedrijf ter wereld was volgens marktkapitalisatie[12]). De Top Tien wordt weergegeven in tabel 1. De 10 grootste cryptomunten hebben een marktaandeel van 80%.

#	Cryptomunt	Symbool	Marktkapitalisatie	Prijs
1	Bitcoin	BTC	$ 187 094 518 679	$ 11 117,00
2	Ethereum	ETH	$ 103 988 374 156	$ 1 069,36
3	Ripple	XRP	$ 46 395 934 388	$ 1,20
4	Bitcoin Cash	BCH	$ 27 027 721 350	$ 1 596,00
5	Cardano	ADA	$ 15 702 133 949	$ 0,61
6	Stellar	XLM	$ 11 048 213 781	$ 0,62
7	Litecoin	LTC	$ 9 725 274 180	$ 177,00
8	EOS	EOS	$ 9 005 382 413	$ 14,27
9	NEO	NEO	$ 8 839 285 000	$ 135,99
10	NEM	XEM	$ 7 716 788 999	$ 0,86
	TOTAAL		$ 426 543 626 895	

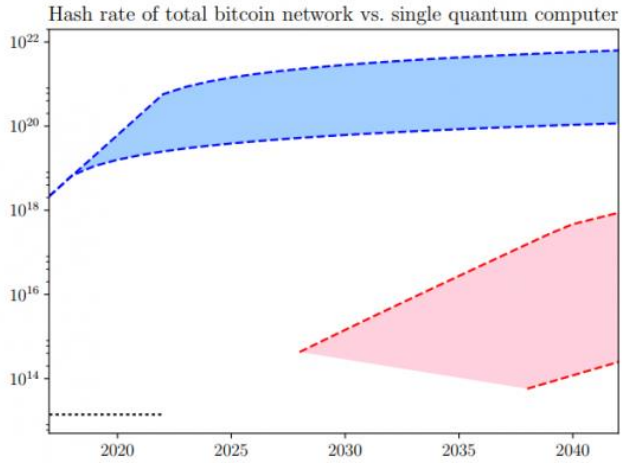
Tabel 1 *Top 10 Cryptomunten volgens marktkapitalisatie; https://coinmarketcap.com/all/views/all/ (27/01/2018)*

[12] http://dogsofthedow.com/largest-companies-by-market-cap.htm

Quantum computing

Eén van de beveiligingen van bitcoin is het gebruik van de hashcode. Om deze complexe puzzel op te lossen werken momenteel tal van ASIC's (zie bitcoin difficulty) samen om de puzzel op te lossen. Het block wordt goedgekeurd als de meerderheid van het netwerk (van computers) akkoord is. Meerderheid van netwerk is in praktijk beschikbare rekenkracht. Met de komst van quantumcomputers zou deze meerderheid wel eens kunnen overhellen naar quantum computers en kan de blockchain naar eigen hand gezet worden. [15].

De eerste quantum-computers zouden binnen 10 jaar gebouwd kunnen worden. Allicht zal de conventionele rekenkracht van het netwerk voorlopig nog superieur blijven.



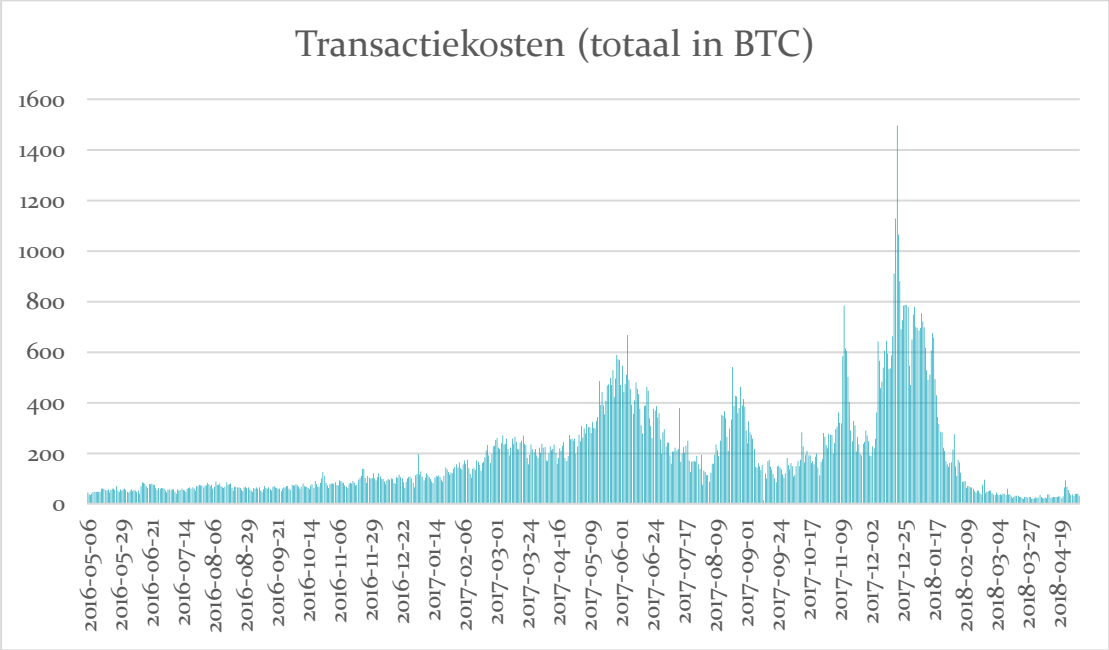
Afbeelding 8 *Hash rate van total bitcoin netwerk vs enkele quantum computer - https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/*

Volgens Forbes is een groter gevaar dat deze computers worden ingezet voor het kraken van public en private keys. [16] Gebruikers van bitcoin genereren via een private key een public key om het netwerk te kunnen handelen. Met huidige computers is het onmogelijk om de private key te berekenen via publiek key. Quantum computers kunnen dit wel. Ook dit gevaar wordt door specialisten echter geminimaliseerd. Enerzijds is de quantumtechnologie gebaseerd op instabile qubits. Anderzijds wordt de kostprijs van de eerste machines geschat op 50 mio dollar.

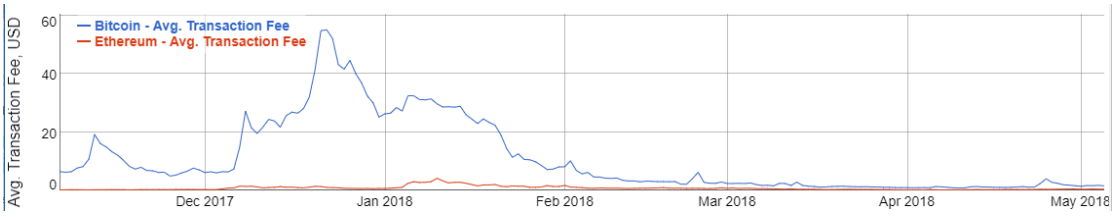
Kostprijs

Voor het uitvoeren van een transactie in bitcoin worden transactiekosten aangerekend. Eind 2017 rezen de transactieskosten in Bitcoin de pan uit. [17]. CNBC verzamelde voorbeelden als $16 transactiekost op overboeking $25 tegenwaarde in BTC van één naar een ander adres. Op de grafiek is de sterke stijging eind 2017 goed te zien. Deze verhoogde transactiekost viel samen met de langere wachtijd om een transactie in een blok goed te keuren.

Om de congestie van bitcoin op te lossen, stappen gebruikers voor een deel over naar andere cryptocurrencies. Een tweede oplossing zou 'Lightning Network' zijn. Dit zou gebruikers toelaten meerdere transacties te versturen naar buiten de blockchain en van buitenaf naar de blockchain.



Afbeelding 9 *Totale transacties van Bitcoinnetwerk, uitgedrukt in bitcoin. Bron: https://blockchain.info/nl/charts*



Afbeelding 10 *De stijgende transactiekosten eind 2017 waren niet zichtbaar bij Ethereum. Bron: https://bitinfocharts.com/comparison/transactionfees-btc-eth.html#6m*

3. Ethereum

In tabel 1 staat Ethereum gelisteerd als tweede belangrijkste cryptomunt. Deze scriptie heeft niet tot doel de belangrijkste cryptomunten te bespreken, Ethereum is echter de link tussen de eenvoudige blockchain die dienst doet als technologie voor een cryptomunt naar uitgebreide blockchain die bedrijven toelaat toepassingen te creëren gebaseerd op blockchain.

Ethereum deelt met Bitcoin volgende elementen [18]:

- Open source
- Blockchain gebaseerd
- Decentraal platform

Ethereum verschilt echter fundamenteel doordat proof-of-work ASIC's niet toelaat (centralisatie van minen kan dus niet). Bovendien omvat het netwerk van Ethereum meer dan enkel de eigen cryptomunt (Ether) en worden meerdere cryptomunten verhandeld. Tenslotte kan Ethereum ook andere data bijhouden. Dit biedt toegang tot Smart Contracts.

"Blockchain app platform" is de subtitel van Ethereum op www.ethereum.org. Op dezelfde website wordt via de missie van Ethereum Foundation (Zwitserland) deze doelstelling verder toegelicht: *"promote and support Ethereum platform and base layer research, development and education to bring decentralized protocols and tools to the world that empower developers to produce next generation decentralized applications (dapps), and together build a more globally accessible, more free and more trustworthy Internet."*

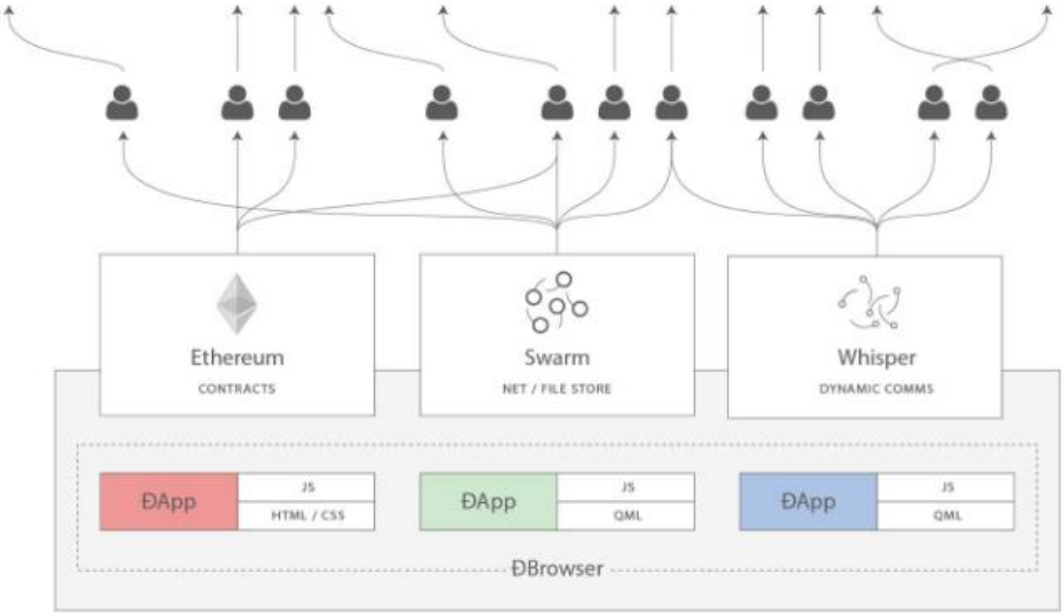
Melanie Swan [19] grijpt terug naar het oorspronkelijke plan van Satoshi Nakamoto om te werken met drie stappen:

- Blockchain: het decentrale publiek dagboek
- Bitcoin protocol: het transactiesysteem om waarde te verhandelen tussen twee partijen zonder tussenkomst van een derde partij
- Turing completeness – meer robust scripting systeem: de mogelijkheid om eender welk betaalmiddel, protocol of blockchain te gebruiken

Bitcoin maakt gebruik van de eerste twee stappen. Doordat Ethereum eerder een infrastructuur platform aanbiedt, zijn andere blockchains en protocollen mogelijk. Elke node in het Ethereum netwerk draait Ethereum Virtuele Machine waarop gedistribueerde programma's werken.

Ethereum gebruikt een eigen gedistribueerd econsysteem inclusief delen van bestanden (file serving), berichtendienst (messaging) en bevestiging van reputatie (reputation vouching)

- **Contracts**: decentralized logic
- **Swarm**: decentralized storage
- **Whisper**: decentralized messaging



Afbeelding 11 *Ethereum Swarm en Whisper [20]*

In afbeelding 11 wordt het decentraal bewaren van bestanden afgehandeld door Ethereum-Swarm. De berichtendienst noemt Ethereum-Whisper. Deze afbeelding introduceert tevens het begrip DApp.

Dapp is de afkorting van Decentralized application. Dit is een applicatie die op een decentraal netwerk draait, met deelnemers waarvan de informatie beveiligd is en enige transacties eveneens decentraal gebeuren. Hiervoor zijn drie kenmerken van toepassing:

- Applicatie moet volledig open source zijn en volledig autonoom kunnen werken. De data moet in een publieke decentrale blockchain bewaard worden.
- Applicatie moet aan de hand van standaard algoritmes tokens aanmaken. Deze tokens kunnen gebruikt worden om deelnemers te belonen.
- Enige aanpassing (verbetering) aan de applicatie kan enkel mits de meerderheid van de gebruikers hiermee akkoord gaan.

Aanvullend op Dapp zijn nog noemenswaardig: DAO (decentralized autonomous organization) en DAC (dencentralized autonomous corporations).

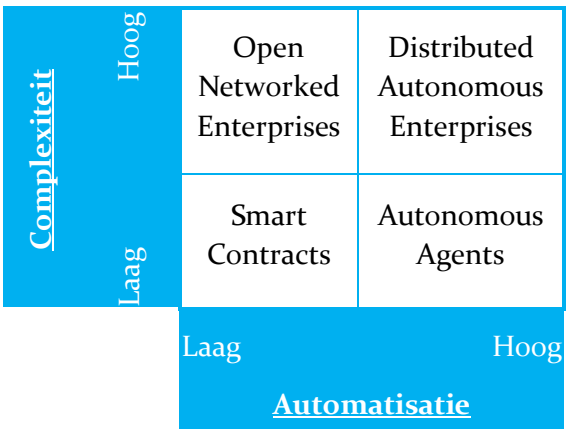
Een voorbeeld: twee personen kunnen een gok wagen op de maximum temperatuur van morgen. Dit contract kan automatisch afgehandeld worden door een software programma dat morgen autonoom de officiële temperatuur gaat controleren via een weerapi.

Andere voorbeelden worden weergegeven in tabel 2

Project	URL	Activiteit	Te vergelijken met
OpenBazaar	https://openbazaar.org	Aan- en verkopen van produkten	Craigslist
LaZooz	http://lazooz.org	Autodelen (ritdelen)	Uber
Twister	http://twister.net.co	Sociaal netwerk	Twitter/Facebook
Gems	http://getgems.org	Sociaal netwerk	Twitter/SMS
Bitmessage	https://bitmessage.org	Berichtendienst	SMS
Storj	http://storj.io	Opslagdienst	Dropbox

Tabel 2 *Lijst van Dapps (overgenomen van Melanie Swan)*

Volgens Tapscott en Tapscott [21] kunnen de innovaties van Smart Contracts tot autonome Dapps weergegeven worden in een matrix met als twee assen: complexiteit en automatisatie. Uit de matrix valt af te leiden dat het gebruik van Smart contracts de eenvoudigste toepassing is van de verdere mogelijkheden van blockchain.



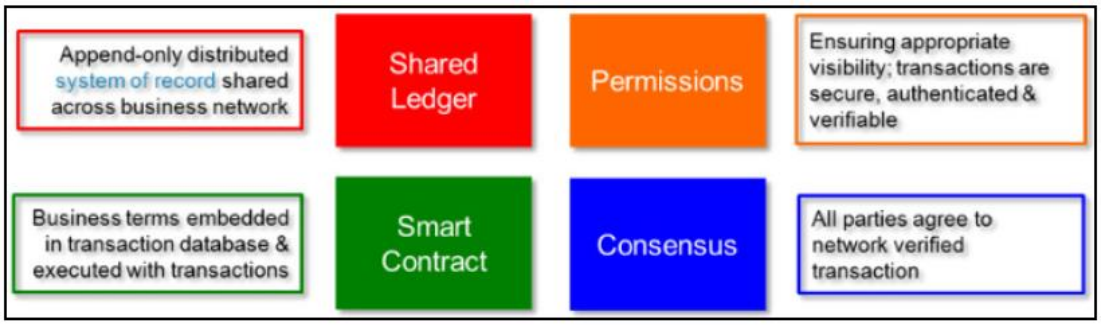
4. Blockchain 2.0

4.1. Blockchain in het bedrijfsleven

4.1.1. Algemeen

De verwevenheid van blockchain en bitcoin is zeer sterk, doch een aantal basisprincipes maken duidelijk dat er belangrijke verschillen zijn. Deze laten ook toe om bepaalde bedrijfsprocessen te optimaliseren.

In *Blockchain for dummies* haalt Manav Gupta vier belangrijke elementen aan die blockchain kenmerken. Afbeelding 12 kadert deze begrippen. Waar toepasselijk wordt het verschil met bitcoin toegelicht.



Afbeelding 12 *Kenmerken blockchain*

Shared Ledger

In tegenstelling tot huidige centrale systemen heeft bij een shared ledger elke participant een volledige copie van de database. Het systeem laat enkel toevoegingen toe, geen wijzigingen of verwijderingen. Het is net omdat iedereen een copie van het dagboek heeft dat iedereen ook alles kan zien of kan schrijven (zie permissions).

Permissions

Blockchains kunnen 'permissioned' of 'permissionless' zijn; vrij vertaald 'met toestemming' of 'geen toestemming nodig'. Bij een permissioned blockchain kan aan de hand van identiteiten specifieke data afgeschermd worden of kunnen bepaalde gebruikers meer of minder rechten toebedeeld krijgen. Een derde partij kan bijvoorbeeld wel zien dat er een transactie heeft plaatsgevonden tussen A en B, maar ziet niet de details. Een auditor kan meerdere rechten toegewezen krijgen zodat deze wel alle details kan raadplegen.

Consensus

Bij bedrijven kennen de tegenpartijen elkaar. Transacties kunnen goedgekeurd worden door:

- Proof of stake: goedkeuring dient te gebeuren door een bepaald percentage van totale waarde van netwerk
- Meerdere handtekeningen: afspraak dat bv 3 van de 5 validators akkoord moeten zijn
- Practical Byzantine Fault Tolerance[13] (PBFT): een algoritme speciaal ontworpen om discussies tussen verschillende participanten te regelen.

Smart Contracts

Een 'intelligent contract' omvat een geheel aan regels verbonden aan een transactie, wordt bewaard op een blockchain en kan automatisch uitgevoerd worden als aan bepaalde regels voldaan is. De uitvoering van de transactie kan op deze manier sneller en goedkoper verlopen dan via traditionele contracten.

Verschillen met bitcoin blockchain [22]

Onderliggende assets: voor bedrijven kan blockchain toegepast worden op ontelbare materiële en immateriële activa en is dus veel uitgebreider dan enkel een digitaal betaalmiddel. Enkele voorbeelden: verkoop van wagens, huizen, voedingsketen, overdracht aandelen, tracking diamanten,…

Anonimiteit: bitcoin is een anoniem netwerk. Hoewel alle transacties voor iedereen zichtbaar zijn, zijn de achterliggende partijen verhuld in aantal nietszeggende digits. Regelgeving legt bedrijven echter op om clienten te identificeren. Hoewel leden van het netwerk herkenbaar moeten zijn, moeten de transacties wel afgeschermd zijn. Deze vereiste vraagt een aangepaste blockchain.

Consensus: in het bitcoinnetwerk wordt consensus bereikt door proof of work: het harde werk van alle miners in het netwerk die de klok rond complexe vraagstukken oplossen en als beloning bitcoins ontvangen. Het enorme verbruik aan rekenkracht en energie is voor een bedrijfsnetwerk overbodig. Door het vastleggen van aantal regels wie wanneer welke transactie goedkeurt is deze proof of work overbodig.

[13] https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

4.1.2. Financiële sector

De vraag stelt zich of de financiële sector anders dient om te springen met blockchain dan andere bedrijfsectoren. SWIFT en Accenture hebben een studie gemaakt in hoeverre blockchain een intrede kan doen in de financiële sector. [23] SWIFT is in deze goed geplaatst aangezien het samenwerkingsverband is van ruim 11.000 leden uit de financiële sector. In het verleden heeft SWIFT een leidende rol gespeeld in het uitwerken van standaarden en conventies voor haar leden.

De studie stelt vast dat de steile opmars van DLT voornamelijk het resultaat is van de cryptomunten die verhandeld worden tussen consumenten. De oplossing is dan ook gericht op C2C (Consumer-to-Consumer). In het bedrijfsleven is de benadering B2B hetgeen andere vereisten heeft. Door de sterke regulering van financiële instellingen zijn de voorwaarden nog strenger.

De vereisten worden grafisch weergegeven in afbeelding 13. Elke voorwaarde wordt onderzocht in hoeverre deze vandaag de nodige score haalt en welke maatregelen nodig zijn om het minimum te behalen.

Afbeelding 13 *Noodzakelijke vereisten van een DLT in de financiële sector (bron: Swift Position Paper)*

Cryptomunten hameren op een volledig decentraal systeem dat zichzelf volledig in stand houdt en met complete transparantie (permissionless). Een oplossing is een permissioned ledger, maar mits de nodige garanties welke partijen wat kunnen zien (granulariteit)

Data is meestal confidentieel. In het DLT wordt alle data gedeeld over alle partijen. Hoewel de transacties beschermd zijn door anonieme adressen, moeten banken de clienten achter deze adressen kennen. Na enige tijd zijn de anonieme adressen dus gekend…

Enige aanpassing van gebruik aan systemen kan pas als financiële instellingen nog steeds voldoen aan de geldende wetten en regels. Zullen de regels aangepast moeten worden of dienen er compleet nieuwe regels te komen ?

Voor correcte uitwisseling van gegevens baseren FI zich op standaarden (ISO, ISDA,…). Verschillende DLT's zijn niet altijd compatibel met elkaar.

Voor financiële transacties moeten partijen gekend zijn. Een specifieke vereiste binnen de financiële industrie is KYC (Know Your Customer). Vooralsnog is het niet mogelijk om volledig zeker een key te koppelen aan een identiteit. Bovendien is het onduidelijk wat er kan gebeuren als key verloren gaat of gestolen wordt.

Open ledgers beschermen zich tegen malafide aanvallen door cryptografische algoritmes. De kostprijs hiervoor is proof of work hetgeen veel rekenkracht vergt, teveel om enig voordeel te hebben in financiële sector. Een oplossing dient gezocht te worden voor beveiliging van lokale versies van het ledger.

Huidige systemen behalen een betrouwbaarheidsgraad van 99%. Betrouwbaarheid wordt opgevolgd door een centrale adminstrator. Dit valt bij een DLT weg en wordt de verantwoordelijkheid van de verschillende participanten.

Hoewel het bitcoin netwerk reeds goed ingeburgerd is, blijft het aantal transacties per seconde laag en niet te vergelijken met het veelvoud van transacties in de sector.

Swift concludeert dat er momenteel nog teveel onzekerheden zijn die een directe doorbraak van blockchaintechnologie in de financiële sector afremt. Niet alleen is er vandaag nog te weinig een alomvattende oplossing, maar de integratie met bestaande systemen dient verder uitgewerkt te worden. Swift stelt zicht tenslotte vragen over de positie van de regulator.

Ze besluiten door te stellen dat DLT geen superoplossing is, maar dat elke use case apart dient geanalyseerd te worden om te verifiëren of de technolgie hiervoor in aanmerking komt. Deze Use Cases worden in het volgende hoofdstuk verder toegelicht.

Afbeelding 14 *Hoe matuur is blockchain om door Financiële Instellingen in te voeren? Bron: Swtift Position Paper (zie geciteerde werken)*

4.2. Use Cases

IBM heeft begin 2018 een 40tal usecases opgelijst die kunnen profiteren van blockchaintechnologie. De meest actuele lijst kan geraadpleegd worden op : https://www.ibm.com/blockchain/use-cases/. In tabel 3 zijn deze use cases per sector weergegeven. Merk op dat ongeveer de helft van de usecases zich situeren in de financiële sector! Aan de hand van deze usecases kunnen we afleiden wanneer een blockchain interessant is om toe te passen. Dit helpt ons de criteria te bepalen die financiële instellingen kunnen hanteren.

Ik groepeer de use cases die niet gelieerd zijn aan financiële diensten samen in hoofdstuk 4.2.1.

Hoofdstuk 4.2.2 zal de usecases van de financiële instellingen behandelen. Een aantal usecases worden in detail belicht. Het Wereld Economisch Forum heeft in een paper: *"The future of financial infrastructure"* een aantal usescases geselecteerd waar de blockhain volgens haar leden baanbrekend zal zijn.

Nr	Industry	Solution Area	Case
01	Chemical and Petroleum	Supply chain	Blockchain transforms supply chain networks in chemicals and petroleum industry
02	Consumer	Food safety and traceability	Walmart's food safety solution built on IBM Blockchain Platform
03	Consumer	Food safety and traceability	IBM announces major blockchain collaboration for food safety
04	Electronics	Supply chain	Blockchain for electronics: taming complexity with better supply chain visibility
05	Energy & Utilities	Carbon credit management	Energy-blockchain labs and IBM create carbon credit management platform
06	Energy & Utilities	Distributed energy source integration	TenneT unlocks distributed flexibility with IBM Blockchain
07	Government	Supply chain, asset registration, identity services, fraud prevention and compliance	IBM Blockchain government point of view
08	Health Care	Person and owner-mediated health data exchange	FDA partners with blockchain for secure exchange of healthcare data
09	Health Care	Supply chain	IBM and Heija launch blockchain-based supply chain financial services platform

10	Health Care	Supply chain	IBM Blockchain and SAP IoT solution for the pharmaceutical cold chain
11	Health Care	Healthcare payments	Healthcare payments reimagined with blockchain
12	Health Care	Clinical trial management, outcome-based contracts, patient consent and health data exchange	IBM Blockchain healthcare point of view
13	Travel & Transportation	Asset registration	Applying blockchain to asset management
14	Cross Industry	Trade and supply chain finance	Blockchain on IBM Z Systems
15	Cross Industry	Visibility	Trust in trade toward stronger supply chains
16	Cross Industry	Dispute resolution	IBM Global Financing uses blockchain to resolve financial disputes
17	Cross Industry	Dispute resolution	Improve dispute resolution in commercial financing with blockchain
18	Cross Industry	Payment and digital currency	Increase visibility and cross-border transactions with blockchain
19	Cross Industry	Trade and supply chain finance	Streamlining trade finance with IBM Blockchain
20	Cross Industry	Supply chain	Blockchain for electronics: taming complexity with better supply chain visibility
21	Cross Industry	Customs declarations	Applying blockchain to customs declarations
22	Banking & Financial Markets	Dispute resolution	Blockchain, the next disruptor for finance
23	Banking & Financial Markets	KYC and identity	Building a digital identity ecosystem on blockchain
24	Banking & Financial Markets	Reference data	London stock exchange group develops data blockchain solution
25	Banking & Financial Markets	Unlisted securities	Northern Trust: blazing a path for blockchain in banking
26	Banking & Financial Markets	Payment and digital currency	Streamlining procurement of contingent labor with blockchain
27	Banking & Financial Markets	Dispute resolution	Distributed ledger technology and guarantees for commercial property leasing
28	Banking & Financial Markets	Bank guarantees	Multiple banks secure successful blockchain trial for guarantees
29	Banking & Financial Markets	Post trade	Blockchain for the banking industry with CLS Group
30	Banking & Financial Markets	Trade and supply chain finance	Using blockchain to disrupt trade promotions

31	Banking & Financial Markets	Trade and supply chain finance	How Mizuho bank leverages blockchain for trade finance
32	Banking & Financial Markets	Trade and supply chain finance	IBM and banks advance an open, blockchain-based trade finance platform
33	Banking & Financial Markets	Trade and supply chain finance	Trade and supply chain finance: expanding bank trade financing
34	Banking & Financial Markets	Payment and digital currency	IBM announces major blockchain solution to speed up global payments
35	Banking & Financial Markets	Payment and digital currency	IBM's universal blockchain payments solution
36	Insurance	Complex risk coverage	Building a multinational insurance policy using blockchain
37	Insurance	Group benefits	IBM introduces industry platform designed specifically for insurers

Tabel 3 *Praktische Blockchain use cases*

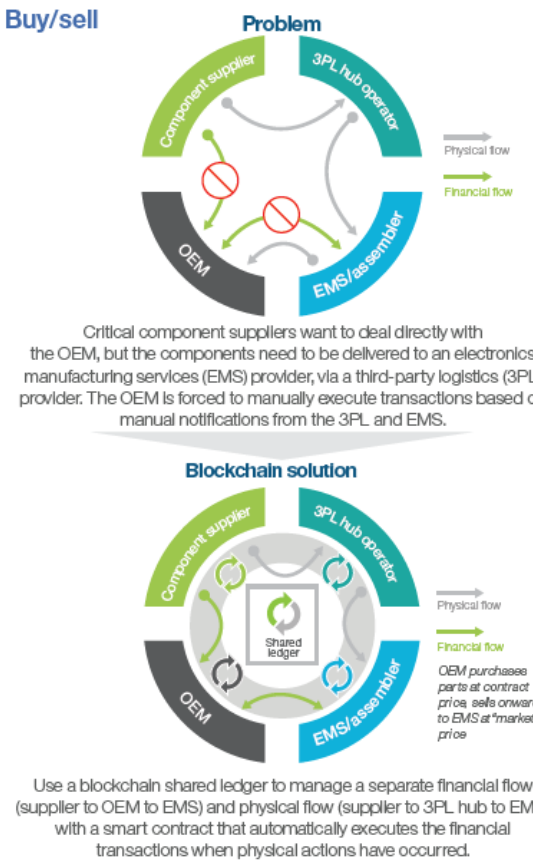
4.2.1. Algemene Use Cases

In de **supply chain** sector houden de deelnemers van het proces allemaal een aparte boekhouding bij en dient deze bij elke transactie aangepast worden. Vervolgens wordt deze informatie ook nog eens gedeeld met derden die op hun beurt deze informatie weer moeten verwerken. Dit neemt niet alleen tijd in beslag, maar manuele verwerking leidt ook tot hogere foutenmarges. Het verlies aan tijd wordt nog versterkt wanneer een derde partij controles dient uit te voeren. Het aanhouden van eigen database is:

- Inefficiënt: elk contract wordt door elke partij ingebracht
- Duur: administratiekost, maar ook auditkost
- Kwetsbaar: fout in een database kan hele transactie in gevaar brengen. Aanleiding kan fraude, cyberaanval of gewone fout zijn.

Bij een crisis in de **voedingsector** is de eerste reactie om het besproken product direct schuldig te bevinden en geen risico te nemen. Vervolgens wordt de herkomst van het product uitgeplozen. Doordat deze zoektocht via systemen die niet op elkaar zijn afgestemd of zelfs in bepaalde gevallen nog op papier gebeuren duurt dit meestal meerdere dagen. Blockhain heeft het potentieel om dit te herleiden tot enkele minuten! Bovendien geeft dit snel volledige transparantie over het product. Directe voordelen zijn het sneller indijken van het probleem, onnodige verspilling van voedsel en aanzienlijke kostenbesparing.

De uitdaging in de **elektronicasector** is om alle componenten in apparatuur optimaal met elkaar te laten samenwerken. Aangezien steeds meer componenten extern aangeleverd worden is opvolging van deze componenten steeds belangrijker. Ten tweede speelt data ook een grotere rol. Deze data betrouwbaar houden en kennis op peil houden vergt steeds complexere processen. Figuur 15 geeft het complexe samenspel weer tussen enerzijds de fysieke goederenoverdracht en anderzijds de financiële flow tussen de verschillende tussenpersonen. De bovenste voorstelling is de traditionele oplossing, de onderste is een blockchainoplossing. Volgens een proof-of-concept van UBS Financial Services zou door ontkoppeling van het financiële luik (facturen, contracten en letters of credit afhandelen via blockchain -> zie 4.3.2) de traditionele doorlooptijd van 7 dagen kunnen reduceren tot 1 uur. [24]



Afbeelding 15 *OEM complexiteit Elektronicasector; oplossing zonder en met blockchain [24]*

China werkt samen met IBM om blockchaintechnologie in te zetten in de strijd tegen CO_2 uitstoot. De **nutsector** dient immers aanzienlijke inspanningen te leveren om de klimaatdoelstellingen te halen. Blockchain helpt de sector via:

- Digitale samenwerking van meerdere organisaties, in combinatie met smart contracts
- Beveiligde en niet te wijzigen gegevens op de blockchain verhoogt kredietwaardigheid van de markt.
- Hogere transparantie en snellere controles bevordert het voldoen aan wettelijke verplichtingen.

De opkomst van hernieuwbare energie (zonnepanelen, windenergie) zorgt voor grotere onevenwichten in het elektriciteitsnet. Productie en consumptie van energie zijn niet altijd in evenwicht, nochtans moet de lamp altijd kunnen branden. Een aantal partijen (Tennet, Sonnen, Vandebron, IBM) gebruiken de blockchain om vele kleine spelers toe te voegen aan het decentrale grootboek. Thuisbatterijen en de batterijen van elektrische wagens kunnen bij stroompieken worden bijgeladen en bij stroomtekort ontladen worden.

De **overheid** kan op verschillende aspecten gebruikmaken van blockchaintechnologie:

- Een beter voorraadbeheer en minder verspilling van eigen produkten (bv apparatuur technische dienst)
- Registratie van eigendom (bv wagen, vastgoed, gronden) kan efficiënter door éénmalig in gemeenschappelijk register te noteren.
- Identiteitsbeheer voor toepassingen als paspoorten, rijbewijzen maar ook medische dossiers.

Blockchain kan de **farmasector** vooruithelpen door verschillende organisaties aan elkaar te koppelen. Enerzijds heeft vandaag de patient moeilijk toegang tot de eigen gegevens doordat deze zeer verspreid zitten in verschillende databases. Anderzijds helpt het centraliseren van deze gegevens de sector in z'n geheel om de data beter te analyseren en trends te onderzoeken. Eerdere pogingen om data te delen liepen vaak mis op het gevaar van dataveiligheid en privacy schending. 70% van bedrijven actief in de sector verwachten dat blockchain een oplossing is voor bijhouden van klinische studies, medische gegevens en naleving van de wetgeving.

In China wordt blockchain gebruikt om de trage terugbetaling van apotheken door ziekenhuizen te versnellen. De blockchain volgt nauwgezet het traject van geneesmiddelen en laat snelle betaling van apothekers toe.

SAP en IBM hebben voor farmabedrijven een systeem opgezet dat product kan opvolgen van zodra order in SAP wordt ingeput (farmabedrijf) tot aankomst in het ziekenhuis. Dankzij gebruik van smart contracts kunnen extra voorwaarden worden ingebouwd (bijvoorbeeld temperatuur van produkt moet in bepaalde zone blijven, zoniet moet het produkt worden teruggestuurd naar fabrikant. De blockchain detecteert automatisch de fout in temperatuurzone en zal ook automatisch een return order aanmaken in het SAP systeem van de client.

Betalingen tussen verschillende participanten in de geneeskundige verstrekking kunnen geoptimaliseerd worden (Patient – ziekenhuis – verzekeringsmaatschappij – mutualiteit – overheid) :

- Vooraf goedkeuren dat een bepaalde ingreep mag uitgevoerd worden. Voorwaarden voor uitvoeren worden vastgelegd in een smartcontract
- Te laat ingediende claims kunnen verjaren door het logge papieren proces. Via blockchain is administratie verwerkt zodra de verstrekker de gegevens toegevoegd aan de blockchain.
- Geweigerde claims doordat niet alle data is ingevuld kunnen vermeden worden.

Tenslotte kan blockchain toegevoegde waarde leveren voor :

- Volgen van klinische studies en aantoonbaarheid aan derden vergroten
- Outcome-based contracts; dit houdt in dat kost van zorgverstrekking nauwkeurig wordt bijgehouden, zodat mogelijke kosten die worden aangerekend aan de patient beter op elkaar afgestemd kan worden.

De belangrijkste pijnpunten in de **transportsector** zijn :

- Informatie is verspreid over verschillende systemen (tussenpersonen)
- Moeilijk om verschillende databases aan elkaar te koppelen omwille van verschillende schema's
- Traag, complex en gefragmenteerd proces
- Niemand heeft een volledige kijk op transactionele updates.

Dit leidt tot corrupte data, verschillen tussen meerdere databases en grote kostprijs om deze fouten te corrigeren.

Een aantal usecases zijn sectoroverschrijdend. Ze worden in deze sectie maar kort aangehaald om volledig te zijn. De uitgebreidere bespreking komt aan bod bij de hoofdsector;

- Supply chain – Trade Finance: Traditionele trade finance process omvat meer dan 10 partijen, en 30 documenten die meestal op papier verwerkt worden. Blockchain met slimme contracten kan dit proces aanzienlijk verbeteren. Tevens optimaliseert de blockchain het vertrouwen aangezien elke partij steeds up-to-date informatie ter beschikking heeft.

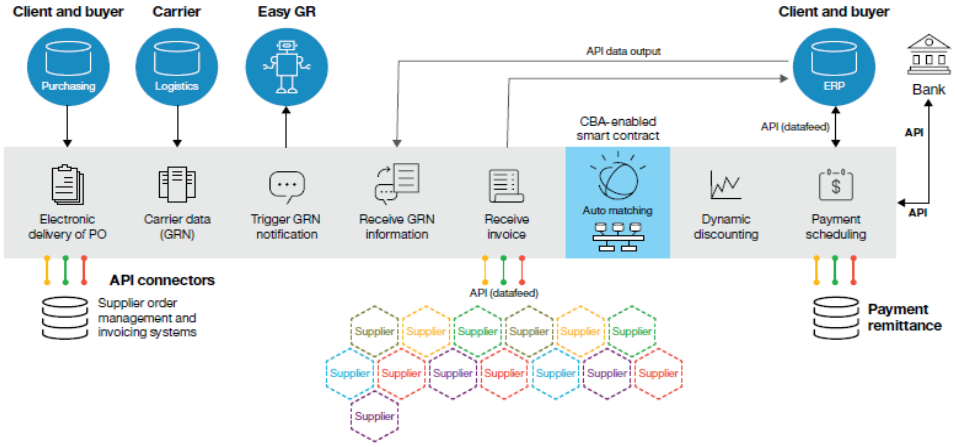
Afbeelding 16 *Blockchain toepassing bij Supply chain; bron: https://www.youtube.com/watch?v=0DSNdLDOZ5w&feature=youtu.be*

- IBM Global Finance stelt blockchain ter beschikking die verschillende partijen uit een transactie aan elkaar linkt. Door gebruik van dit systeem is het aantal discussies dat tussen deze partijen kan ontstaan sterk verminderd en is het aantal dagen om discussies op te lossen gereduceerd van 40 dagen tot minder dan 10 dagen. Er is tevens een aanzienlijke financiële opbrengst doordat ongeveer 40% minder geld geblokkeerd blijft tijdens deze discussies.

- Internationale transacties en de hieropvolgende geldstromen kunnen geoptimaliseerd worden door hogere transparantie en snelheid via het verrekenen van transacties in Nostro/Vostro rekeningen. Dit is een kluwen van rekeningen die banken internationaal aanhouden bij buitenlandse banken in meerdere munten.

Afbeelding 17 *Blockchain toepassing bij Nostro Vostro rekeningen bij Internationale handel. Bron: https://www.youtube.com/watch?v=Y77Bj9kUdt8*

- Handelsschulden kunnen geoptimaliseerd worden via blockchain. Doordat verkoper en koper dezelfde databank gebruiken kunnen, is straight through processing van facturen mogelijk. Dit reduceert de kostprijs per factuur met 60 tot 80%. De snellere omloop zorgt er dan weer voor dat het werkkapitaal beter kan benut worden of zelfs kan verminderen.



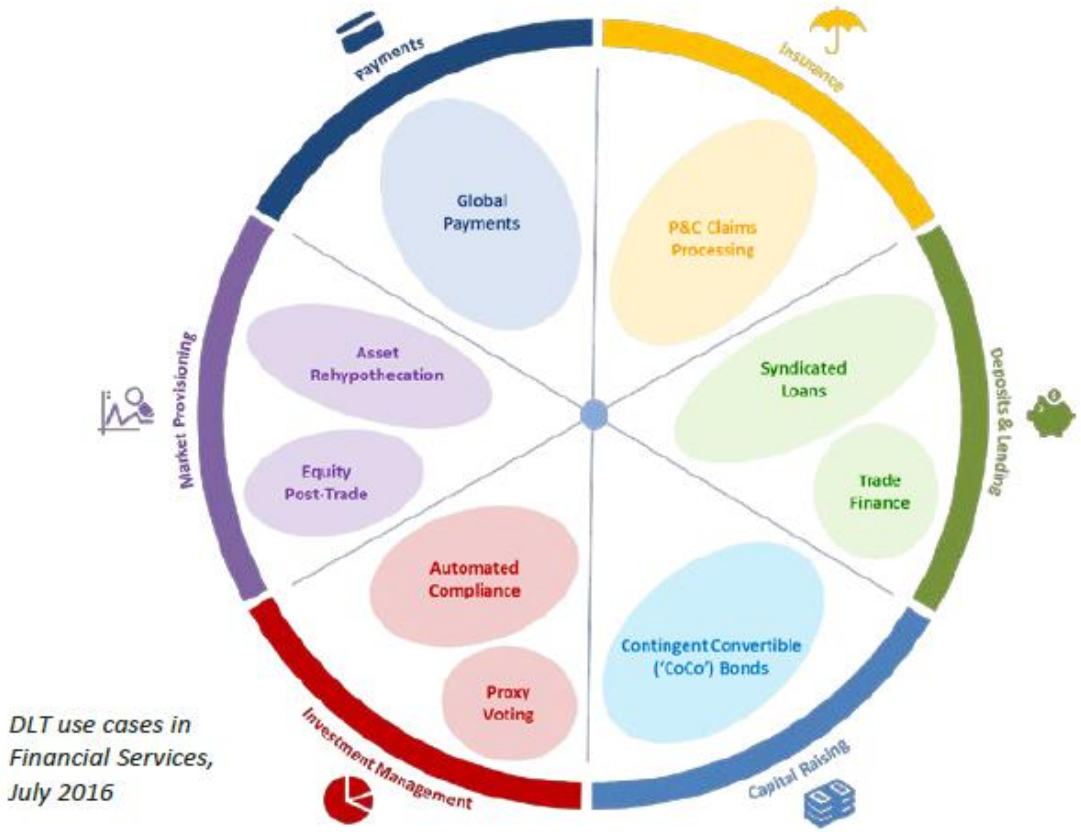
Afbeelding 18 *Blockchain toepassing bij handelsschulden. Bron: Blockchain, the next disrupter for finance (https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=MBW03045USEN)*

Deze algemene use cases delen alvast enkele belangrijke kenmerken:

- Er is steeds sprake van **meerdere partijen** in het proces
- Tracking – audit – **transparantie** is een belangrijke troef van het blockchainproces.
- Blockchain handelt het proces **sneller** af dan het bestaande proces.
- Door automatisatie en snellere afwikkeling wordt er **efficiënter** gewerkt met lagere kosten als gevolg.

4.2.2. Financiële Use Cases

Het Wereld Economisch Forum voerde een 12 maanden durende studie uit over de mogelijkheden van gedistribueerde opslag. De titel van de paper is treffend voor deze bachelorproef: ***'An ambitious look at how blockchain can reshape financial services'***. Een aantal IBM usecases worden in deze paper uitvoerig besproken. [25]



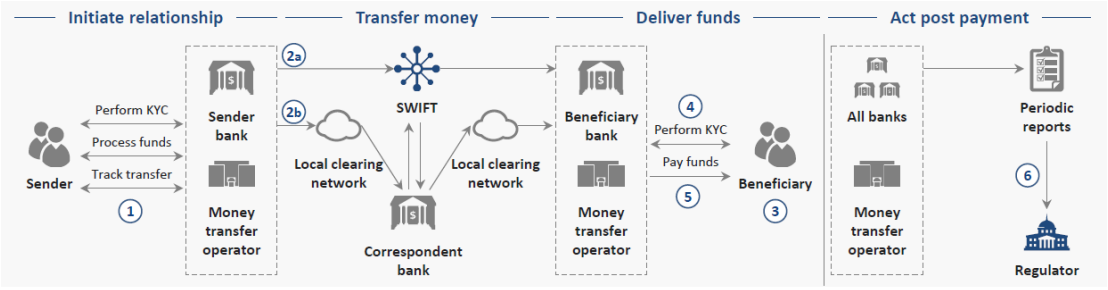
Afbeelding 19 *Geselecteerde use-cases in de financiële sector; bron World Economic Forum [25]*

4.2.2.1. Internationale betalingen

Internationale betalingen is een snelgroeiende wereldwijd gegeven. De jaarlijkse groei bedraagt ca 5% en in 2016 bedroeg het wereldwijd volume 601 mrd USD. Voor financiële instellingen is dit een belangrijke inkomstentak. De gemiddelde kostprijs van een internationale betaling bedraagt ca 7.68% van het getransfereerde bedrag.

Moody's berekende onlangs welke landen relatief veel betalingen uitvoeren tov BNP. De impact op de banken van deze landen is dan ook groter. Na twee uitschieters (Luxemburg en Hong Kong) volgen het VK, België en en Zwitserland.

Huidige proces



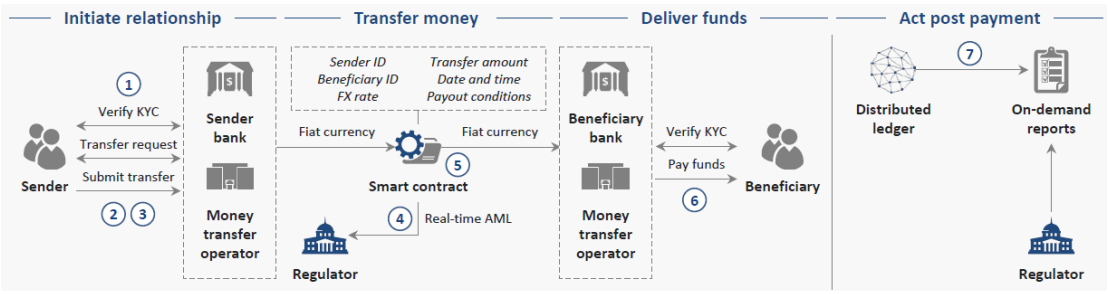
Afbeelding 20 *Global Payments - Huidige proces*

De betaler geeft instructie aan eigen bank die – na interne controles – de gelden ofwel via Swift ofwel via een lokaal netwerk doorstuurt naar de bank van de tegenpartij. De bank van de begunstigde zal na controle de gelden op rekening van begunstigde storten.

Nadelen

Voor het aanvaarden van de betalingsopdracht is extra informatie nodig van de betaler. Dit wordt dikwijls manueel en herhaaldelijk gedaan. De transfers tussen de twee banken kan tot 5 dagen duren, bovendien wordt elke transactie per bank gecontroleerd en wordt deze bij de minste twijfel verworpen. Banken dienen onderling Nostro/Vostro rekeningen aan te houden (zie boven). Tenslotte zijn de rapporteringen naar de regulator tijdsintensief. De opgevraagde gegevens worden door alle partijen apart bijgehouden in verschillende formaten.

Blockchain toepassing



Afbeelding 21 *Global Payments - Alternatief via gedistribueerde opslag*

De blockchain maakt het mogelijk in de transactie tussen verkoper en koper een smartcontract op te stellen. In dit contract wordt de verplichting opgenomen dat opdrachtgever gelden dient over te maken aan de begunstigde. Zodra aan de voorwaarden voldoen worden de gelden real-time overgemaakt met een minimum aan kosten, zonder corresponderende bank.

Voordelen

Beide partijen zijn gekend op de blockchain en hebben een gekende risicoprofiel (vetrouwen). Regulering kan ingebouwd worden in het contract. Automatische opvolging is hierdoor gewaarborgd. Bij post trade controles is de informatie direct uniform beschikbaar. Tenslotte wordt de internationale transfer real-time afgehandeld met een aanzienlijke kostenbesparing.

Voorwaarden

- Standaard KYC (Know Your Customer) proces. Deelnemers van de blockchain dienen gebruik te maken van een gestandaardiseerd KYC proces. Een convergentie is niet eenvoudig, bovendien werken verschillende banken met verschillende lokale regelgeving.
- Regulators, centrale banken en betrokkenen uit verschillende landen moeten samenwerken om tot een centraal geaccepteerd legaal framework te komen.
- Overeenkomst over de centrale database is nodig zodat schaalvoordelen gerealiseerd kunnen worden

Bemerkingen:

- Wie dient initiatief te nemen ? Wereldwijde correspondentenbanken hebben de beste kaarten.
- IT platformen zullen doorslaggevend zijn. IT leveranciers kunnen de sleutel in handen hebben.
- Omzettingen naar vreemde munten en het aanhouden van Nostro/Vostro rekeningen kan opgelost worden door het gebruik van cryptomunten. De volatiliteit van deze munten leidt thans echter tot hogere hedgingkosten.

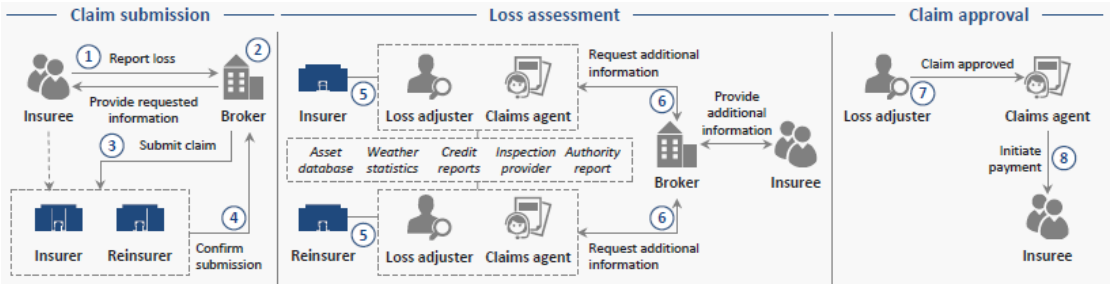
Conclusie:

- Real-time afwikkeling is mogelijk
- Minder fraudegevoelig
- Digitale contracten = minder fouten

4.2.2.2.Schadeverzekering

Schadeverzekeringen zijn na ziekteverzekering en levensverzekering de grootste verzekeringstak. De markt zal in 2018 een totale premieontvangst hebben bijna 900 mrd USD. De afwikkeling van schades is een intensief proces waarvan de kostprijs oploopt tot ca 11% van de onderschreven premies.

Huidige proces



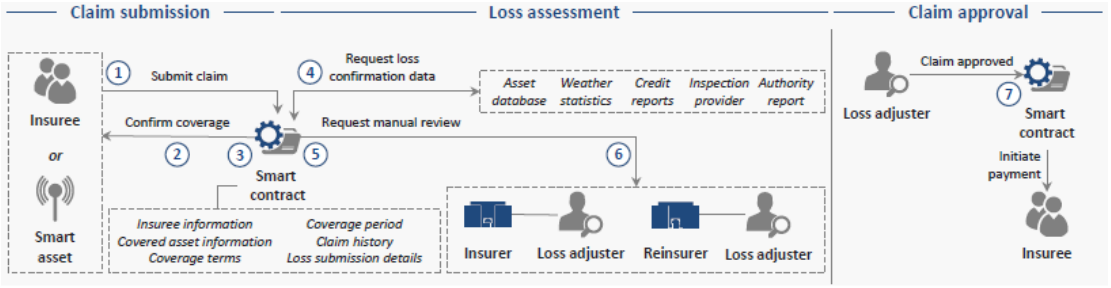
Afbeelding 22 *Schadeverzekering - Huidig proces afwikkeling schadeproces*

De schadelijder signaleert schade aan de makelaar of rechtstreeks aan maatschappij. Eventueel wordt extra argumentatie opgevraagd. Na bevestiging ontvangst zal de verzekeringsmaatschappij de schade onderzoeken. Hiervoor is soms extra informatie nodig van externe bronnen (zoals bv inspectierapport, rapport van de overheid) of extra informatie van de schadelijder. Tenslotte zal de maatschappij de claim ontvankelijk verklaren en tot uitbetaling overgaan.

Nadelen:

De gehanteerde schadeformulieren kunnen zeer uitgebreid en moeilijk in te vullen zijn. De eiser dient veelal de bewijzen fysiek in te dienen of bij te houden. Indien er gewerkt wordt met een makelaar is er een extra tussenstap nodig. De verzekeringsmaatschappijen bekijken schadeafhandeling allen apart. Ze delen geen gegevens onder elkaar hetgeen fraude in de hand kan werken. De hele claimafhandeling gebeurt manueel.

Blockchain toepassing



Afbeelding 23 *Schadeverzekering - Blockchain oplossing*

De eiser kan nog steeds een schadeclaim indienen, maar de claim kan ook geïnitieerd worden via een smart contract. Dit laatste kan getriggerd worden via het gebruik van sensoren of via externe databronnen (weerberichten, overstromingen,...). Dankzij het inbouwen van bepaalde regels kan de claim automatisch ontvankelijk verklaard worden. Aansluitend kan ook het bedrag berekend worden dat kan worden uitgekeerd. Dit laatste kan meteen worden uitgebetaald via het smart contract.

Voordelen:

- Claim kan automatisch worden ingediend
- Noodzaak om te werken met tussenpersonen wordt kleiner en leidt tot snellere afwikkeling
- Efficientiewinst doordat niet elke claim individueel onderzocht moet worden
- Minder fraudegevallen doordat historische gegevens beschikbaar blijven op de het gedistribueerde opslag.
- Uitbetaling kan sneller gebeuren

Voorwaarden:

- Verschillende spelers dienen samen de historiek van claims op de blockchain te plaatsen
- Standaarden tussen verzekeringsmaatschappijen en regulator dienen afgesproken worden
- Legaal kader dient uitgewerkt te worden.

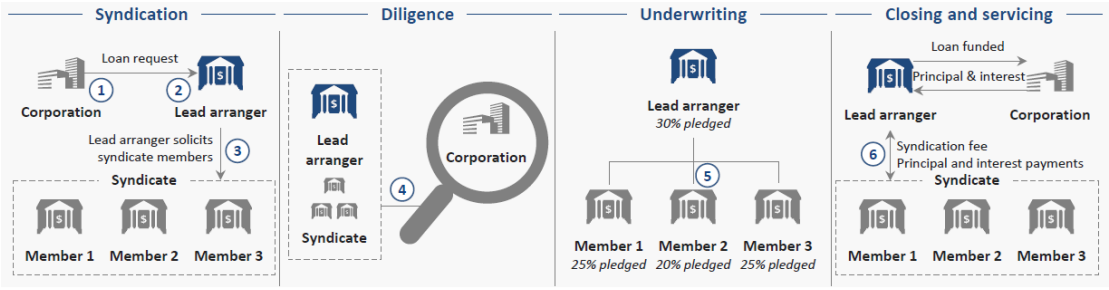
Conclusie:

- Automatisatie van claimafhandeling wordt mogelijk
- Minder kans op fraude

4.2.2.3. Gesyndiceerde lening

Gesyndiceerde leningen zijn leningen die gedragen worden door meer dan één investeerder. Eén partij treedt op als lead manager en zorgt ervoor dat de volledige lening geplaatst wordt bij andere investeerders. De lead manager verzorgt eveneens de administratie en rekent de fee aan.

Huidige proces

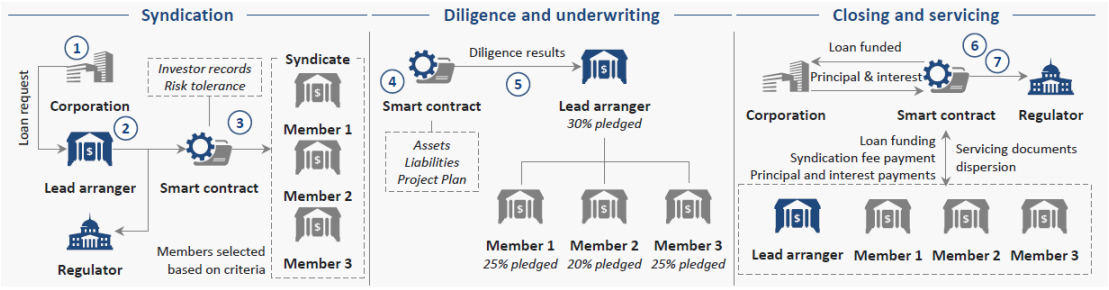


Afbeelding 24 *Gesyndiceerde lening - Huidige proces*

Een bedrijf vraagt lening aan Financiële Instelling. Deze zal optreden als lead manager en aantal andere financiële spelers contacteren om de lening mee te onderschrijven. Vervolgens zal deze de risico's van de lening analyseren en de verdeling doen tussen de andere onderschrijvers. Van zodra de lening loopt, verlopen de rentebetalingen ook via de lead manager.

Nadelen:

Zowel het zoeken naar syndicaatleden als het verifiëren van kredietwaardigheid van de vennootschap die lening aanvraagt is tijdsintensief en voornamelijk een manueel proces. Ook het de verdeling tussen de onderschrijvers is tijdsintensief en manueel. Elke instelling hanteert eigen databanken die niet op elkaar zijn afgestemd. Tenslotte zijn voor uitbetaling van fondsen heel wat tussenpartijen betrokken die de geldstromen met vertraging verwerken.



Afbeelding 25 *Gesyndiceerde lening - Blockchain oplossing*

De financiële instelling die kredietaanvraag binnenkrijgt heeft direct zicht op financiële cijfers en sterkte door digitale identiteit op het gedistribueerd ledger. Dankzij deze financiële cijfers kan ook sneller een match gevonden worden met andere potentiële leden van het syndicaat. In het onderschrijvingsmandaat worden een aantal regels bepaald die vastgeklikt worden in een smartcontract. Dit laat toe om toekomstige betalingen automatisch te laten verlopen zonder extra tussenpersonen. Regulator kan ten alle tijden het centrale register controleren.

Voordelen:

- Vorming van syndicaat kan automatisch gebeurden
- Regulator kan real time controleren
- Tijd om boekenonderzoek te doen wordt drastisch verminderd
- Verschillende partijen krijgen toegang tot uniforme gegevens.
- Snelheidswinst bij betalingsopdrachten.
- Verlaging van risico (tegenpartijen) door incorporatie via smartcontracts

Voorwaarden:

- Standardisatie is nodig tussen financiële instellingen
- Tegenpartijen moeten uniform risicobeheersing opstellen en dit willen delen met elkaar

Conclusie:

- Automatisatie is mogelijk en laat toe meer informatie met elkaar te delen
- Aanzienlijke kostenbesparing mogelijk door tijdswinst bij het opzetten van de lening, alsook bij afhandeling tijdens de lening.

4.2.2.4. Handelsfinanciering

Handelsfinanciering (Trade Finance) is het proces waarbij importeurs en exporteurs risico beheersen dankzij derde partijen. De verkoper wil zeker zijn dat goederen betaald worden en de koper wil vergoed worden indien de goederen niet correct geleverd worden. Financiële instellingen verzorgen deze stroom van documenten en de details worden gebundeld in een documentair krediet (letter of credit).

Huidig proces

Afbeelding 26 *Handelsfinanciering - Huidig proces*

Koper en verkoper bereiken verkoopsovereenkomst hetgeen wordt bevestigd via een factuur. De koper (importeur) vraagt op basis van factuur handelskrediet aan FI die via een documentair krediet contact opneemt met de bank van de verkoper (exporteur). Deze laatste kan nu de goederen versturen die na de nodige douaneformaliteiten bij de de verkoper toekomen. Na bevestiging goede ontvangst kan bank van importeur via corresponderende bank betaling uitvoeren naar bank van exporteur.

Nadelen:

- Manueel proces voor opmaken van documenten en controleren van documenten
- Extra kredietrisico door gebruik van facturen van meerdere partijen
- Goederen kunnen pas verstuurd worden na akkoord van meerdere tussenspelers
- Bank van exporteur dient bank van importeur te controleren
- Elke tussenpersoon gebruikt verschillende platform
- Betalingstromen worden sterk vertraag.

Afbeelding 27 *Handelsfinanciering - Blockchainoplossing*

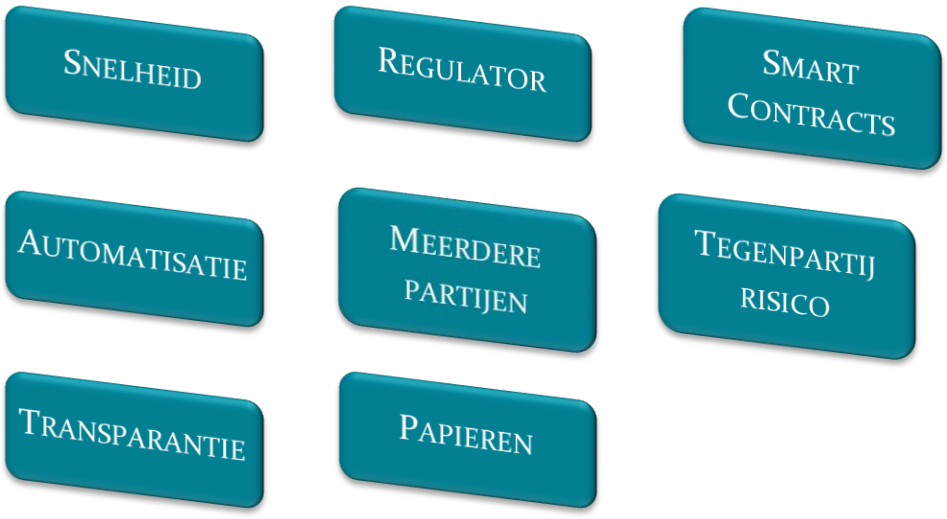
De verkoopsovereenkomst wordt opgenomen in een smartcontract. De bank van de importeur maakt nog steeds een kredietbrief op die ter beschikking van de bank van exporteur wordt gesteld. De voorwaarden van kredietbrief worden toegevoegd aan het smart contract. Contracten worden digitaal ondertekend en tussenpersonen bevestigen tussenstap in het smartcontract: Exporteur bevestigt verzending, douane bevestigt inspectie,... Wanneer importeur tenslotte ontvangst van goederen bevestigt wordt betaling automatisch uitgevoerd.

Voordelen:

- Financiële documenten worden toegevoegd aan digitale ledger
- Facturen kunnen real time gelinkt worden aan handelstransactie
- FI hebben geen tussenpersoon meer nodig (corresponderende bank)
- Minder tegenpartijrisico omdat ook vrachtbrieven ed worden toegevoegd aan digitaal ledger
- Grotere transparantie van het hele proces
- Automatische tracking

Voorwaarden:

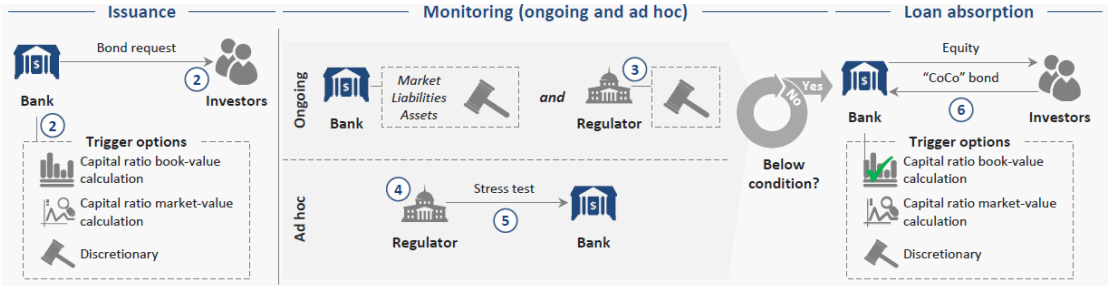
- Grotere transparantie tussen verschillende spelers (met zicht op verschillende documenten)
- Opstellen van decentraal systeem dat toegankelijk en connecteerbaar is door verschillende financiële instellingen
- Wetgevend kader dient uitgewerkt te worden



4.2.2.5. Contingent Convertible Bonds

Een bufferobligatie of coco (afkorting van het Engelse contingent convertible bond) is een tussenvorm tussen een langlopende achtergestelde lening en een aandeel, die verwant is aan de al langer bestaande converteerbare obligatie, en die wordt uitgegeven door banken met een vast relatief hoog rentepercentage. Als de bank door vooraf duidelijk aangegeven vermogenslimieten zakt, de zogenaamde trigger, dan wordt de obligatie omgezet in aandelen, of volgens van tevoren gemaakte afspraken geheel of gedeeltelijk afgeschreven.[14] De koersfluctuatie van deze leningen is bijzonder hoog.

Huidig proces



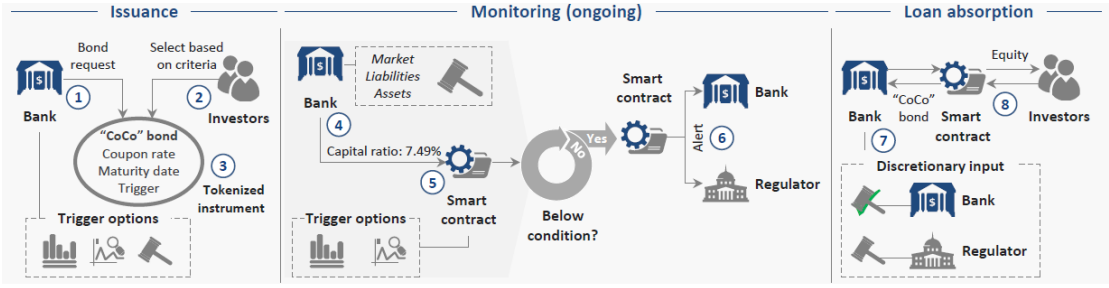
Afbeelding 28 *Bufferobligaties - huidig proces*

Uitgevende bank bepaalt trigger die omzetting van lening naar kapitaal teweeg brengt. Vervolgens wordt deze coco naar de markt gebracht en wordt deze door verschillende partijen aangekocht. Tijdens de looptijd evalueert de bank regelmatig of de buffer overschreden wordt. Ook de regulator kan ad-hoc stress tests bepalen die onderzoeken of de buffer overschreden wordt. Als de trigger bereikt wordt, zal de lening worden omgezet in kapitaal.

Nadelen:

- Markt van coco's is niet heel liquide
- Onduidelijk hoe berekend wordt wanneer de trigger doorbroken wordt
- Berekeningen gebeuren doorgaans op historische (gepubliceerde balans) data
- Regulator holt achter de feiten aan
- Omzetting naar kapitaal gebeurt altijd later dan het doorbreken van de trigger

Blockchain oplossing



Afbeelding 29 *Bufferlening - Blockchain oplossing*

[14] https://nl.wikipedia.org/wiki/Bufferobligatie

Alle voorwaarden mbt de nieuwe coco worden opgenomen in het smartcontract en op de decentrale ledger geplaatst. De berekening dient nog altijd te gebeuren of de trigger geraakt wordt of niet. Elke berekening wordt toegevoegd aan het centrale ledger zodat er real time opvolging mogelijk is bij participanten (beleggers en regulator). Het smart contract verwittigt automatisch iedereen wanneer de grens doorbroken wordt. Dit zorgt er ook voor dat de lening automatisch kan omgezet worden naar kapitaal.

Voordelen:

- Vertrouwen stijgt door gebruik te maken van real time informatie en betrouwbare historiek. Hierdoor trekt de markt ook meer investeerders aan.
- Berekeningen kunnen frequenter gebeuren en zijn ook meer betrouwbaar
- Regulator wordt real time verwittigd wanneer trigger bereikt wordt
- Kapitaalbuffers zijn real time beschikbaar voor regulators. Hierdoor moeten er minder adhoc stress tests uitgevoerd worden.
- Cocobond kan sneller omgezet worden in kapitaal

Voorwaarden:

- Financiële instellingen en regulators moeten framework uitwerken om uniforme data te gebruiken.
- Regulators en banken dienen transparant en gelijke berekening uit te voeren van kapitaalbuffers
- Proces om automatisch alle actoren te verwittigen bij triggers dient uitgewerkt te worden.

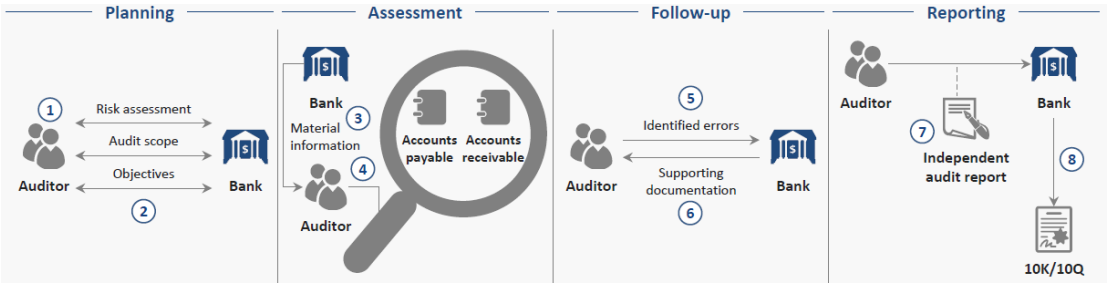
Conclusie:

- Real time informatie
- Hoger vertrouwen van investeerders

4.2.2.6. Automatische Compliance

Financiële instellingen spenderen veel tijd aan het opvolgen van transacties in het bedrijf. Deze kunnen zowel intern gebeuren als extern. Verplichting van de regulator licht aan de basis. Taken bestaan uit oa KYC (Know Your Customer), taks audits, opvolging van betalingen, ad hoc ondervragingen van de wetgever,... Ook het jaarlijkse boekenonderzoek valt onder deze regulering.

Huidige proces



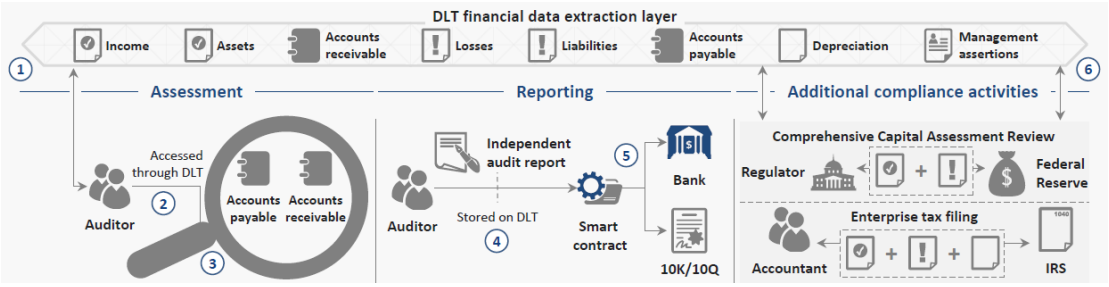
Afbeelding 30 *Automatische compliance - Huidige proces*

Auditors werken samen met de bank om te bepalen welke domeinen geauditeerd worden. De auditors krijgen toegang tot de informatie die ze nodig hebben om de controles te kunnen uitvoeren. Ze verifiëren correctheid en volledigheid van de data. Tenslotte stellen ze een rapport op, hetgeen bank kan toevoegen aan de kwartaal- en of jaarcijfers.

Nadelen:

- Opzetten van de audit vereist mankracht van auditors, maar ook van bank zelf. De personeelsleden kunnen tijdens de audit minder accuraat job uitoefenen.
- Het controleren van de bank is zeer arbeidsintensief. Bank moet data ter beschikking stellen en auditor moet deze data verifiëren.
- Dikwijls wordt data gedupliceerd om de audit te kunnen voltooien.
- Opgeleverde rapport is niet integreerbaar in het jaarrapport van de bank.

Blockchain oplossing:



Afbeelding 31 *Automatische compliance - Blockchain oplossing*

Bij de blockchainoplossing is de te verifieren informatie beschikbaar op de blockchain. De auditafspraken dienen niet steeds opnieuw gemaakt te worden, de nodige data moet enkel toegankelijk gemaakt worden voor de auditors. Er moet ook geen extra personeel van de bank aangesteld worden om data aan te leveren aan auditors aangezien zij rechtstreeks toegang hebben tot gegevens. Deze directe link levert het extra voordeel dat kans op fouten veel kleiner wordt door het vermijden van manueel werk. Duplicatie is niet meer nodig doordat smart contract ervoor kan zorgen dat bepaalde informatie doorstroomt naar het jaarrapport.

Voordelen:

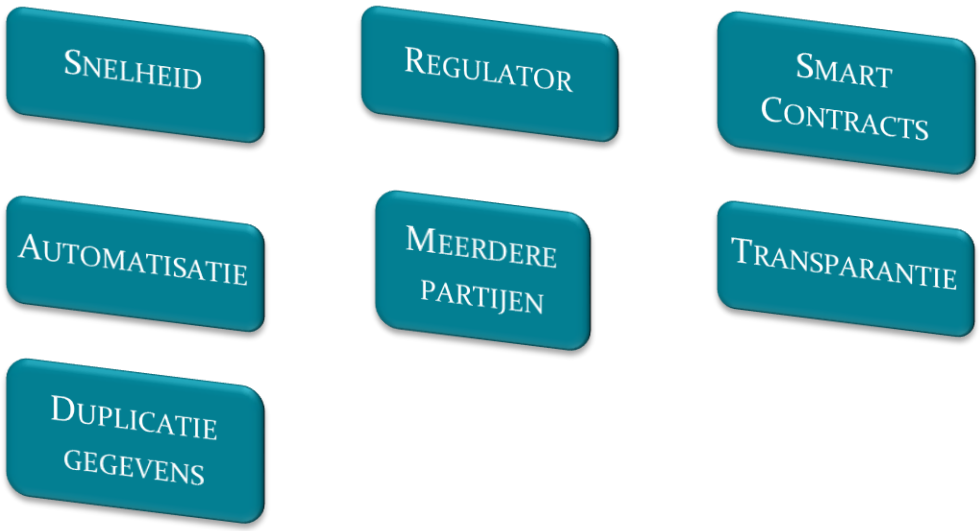
- Onwijzigbare en transparante informatie direct beschikbaar
- Audit software kan automatische controles uitvoeren
- Lagere foutenmarge
- Geïntegreerde systemen

Voorwaarden:

- Bepaalde data moet gefragmenteerd ter beschikking gesteld kunnen worden aan derden
- Platformen van verschillende participanten dienen op elkaar afgestemd worden
- Financiële instellingen en regulators dienen voorbereid te worden op real time verwerking en controle van gegevens

Conclusie:

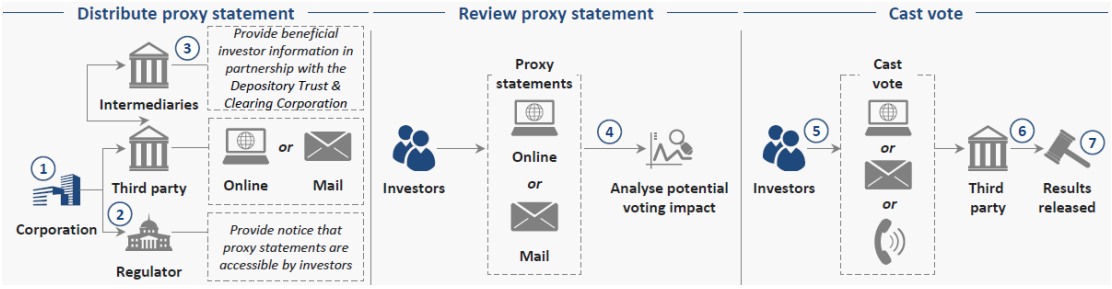
- Hogere transparantie
- Snellere controle
- Kostenbesparing



4.2.2.7. Beheer van vermogen: Stemmen per volmacht

Aandeelhouders hebben het recht op algemene vergadering te stemmen voor de verschillende punten die ter stemming worden voorgelegd. In praktijk is het niet altijd mogelijk om fysiek op iedere stemming aanwezig te zijn. Particuliere investeerders maken gemiddeld maar 28% gebruik van het stemrecht. Stemmen per volmacht (proxy voting) is een mogelijke oplossing die door blockchain ondersteund kan worden.

Huidige proces



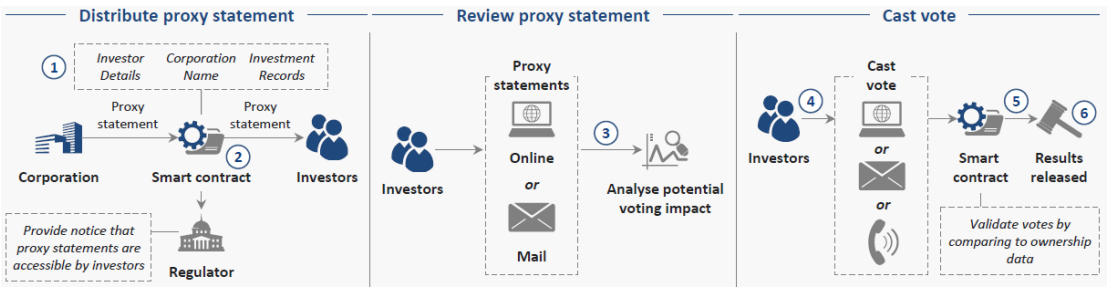
Afbeelding 32 *Stemmen per volmacht - Huidige proces*

Een bedrijf stelt documenten op die de volmacht regelt en stelt deze ter beschikking aan derde partij. Investeerders krijgen inzicht in de documenten en kunnen online, per brief en telefonisch stem meedelen aan derde partij. Deze zal de stemmen toevoegen aan de stemming op de jaarvergadering.

Nadelen:

- Duur systeem aangezien de meeste documenten geprint en per post verstuurd worden.
- Niet alle documenten kunnen met elke investeerder gedeeld worden
- Documenten die verspreid worden zijn een samenvatting van de informatie die gedeeld wordt op de algemene vergadering en kan dus een verkeerd beeld schetsen
- Ook voor elke investeerder is het een groot manueel proces om de documenten door te nemen en met kennis van zaken te handelen.
- Uiteindelijk nemen nog steeds weinig aandeelhouders deel aan de stemming

Blockchain oplossing



Afbeelding 33 *Stemmen per volmacht - Blockchain oplossing*

Van zodra een investeerder een aandeel koopt van een bedrijf wordt de informatie bewaard in het DLT. Wanneer het bedrijf een proxy statement opmaakt wordt dit via een smart contract automatisch elektronisch bezorgd aan investeerders. Ook de regulator wordt automatisch verwittigd. Investeerders krijgen nog steeds de mogelijkheid om de documenten door te nemen en stem per brief, online of telefonisch uit te brengen. Deze frontend systemen dienen gekoppeld te worden aan DLT. Het smartcontract kan controleren of correspondent geldig gestemd heeft (aantal stuks) en resultaten zijn real time beschikbaar.

Voordelen:

- Geen aparte overeenkomsten meer nodig met andere partijen. Het smart contract kan deze rol vervullen
- Lagere kosten door besparing op printen en posten
- Automatische validatie
- Hogere transparantie
- Hogere participatie

Voorwaarden:

- Beurzen en bedrijven dienen aangesloten te zijn op DLT om investeerders te kunnen identificeren
- Ontwerpen van systemen die stemmen per mail en telefoon kunnen converteren naar het DLT
- Standardisatie dient uitgewerkt te worden tussen bedrijven zodat investeerders over de verschillende bedrijven een uniform systeem kunnen hanteren

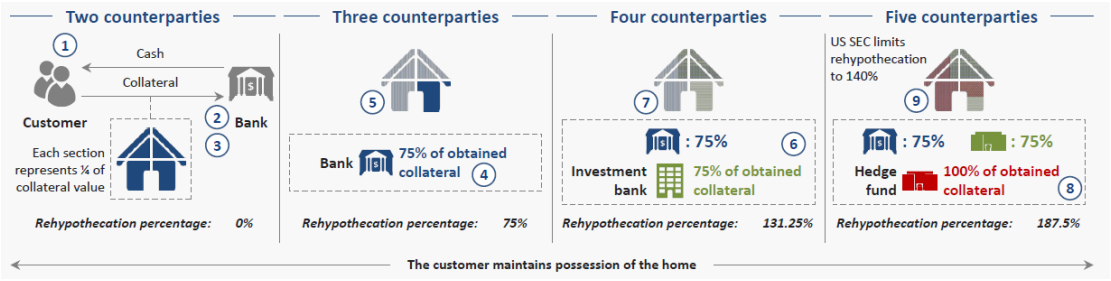
Conclusie:

- Minder manueel werk
- Automatisatie van stemmen

4.2.2.8. Herverpakken van hypotheekleningen

Financiële instellingen herverpakken hypotheekleningen om te gebruiken als onderpand voor andere financiële transacties. Omdat de kostprijs om elke individuele lening apart te verpakken te groot is worden meerdere leningen samen genomen. Het compleet en accuraat zicht op deze verpakte leningen wordt minder transparant. De wetgever wil hier dan ook de nodige controles op uitvoeren.

Huidige proces



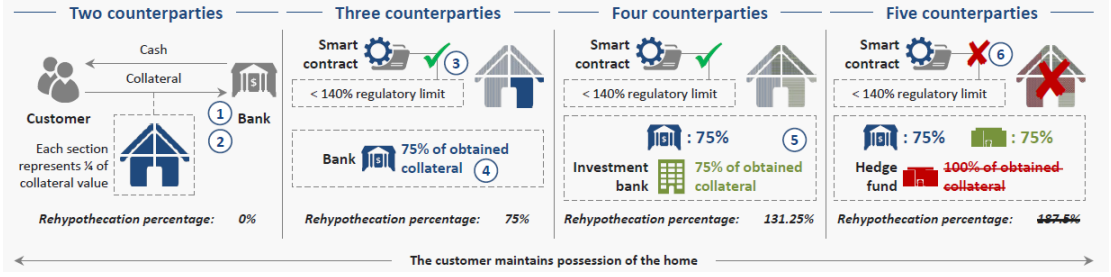
Afbeelding 34 *Herverpakken van hypotheekleningen - huidige proces*

Een client koopt een woning en financieert aankoop via hypothecair krediet. Doordat client toestemming geeft om lening te herverpakken verkrijgt deze een goedkopere rente. De bank groepeert verschillende leningen en kan met deze groep leningen ca 75% van het onderliggende gebruiken als werkkapitaal. Investeringsbank doet dit nog eens over zodat onderliggend een hefboom gecreëerd wordt van 75% + (75%x75%) = 131.25%. In het voorbeeld wordt dit alles nog eens doorverkocht aan een hedgefund die de constructie herhaalt.

Nadelen:

- Bij het herverpakken van de lening gaat gedetailleerde informatie van de oorspronkelijke hypotheek verloren
- Het tegenpartijrisico wordt onduidelijk
- Regulator heeft geen zicht op historiek
- Moeilijk om waarde van onderliggende effecten correct te bepalen
- Bij systeemfalen wordt een volledige ketting geraakt

Blockchain toepassing



Afbeelding 35 *Herverpakken van hypotheekleningen - Blockchain oplossing*

De hypotheeklening wordt inclusief details toegevoegd aan het DLT. Deze worden toegevoegd aan een smartcontract zodat deze informatie steeds beschikbaar is bij alle volgende transacties. Enige investeerders verkrijgen dus altijd een correct en compleet beeld van het onderliggende. Regulators krijgen real time informatie en kunnen bv restricties opleggen dat er een maximale limiet is van 140%.

Voordelen:

- Transparantie
- Tegenpartij risico wordt drastisch verlaagd
- Automatisatie van onderliggende processen
- Regulator heeft zicht op volledig proces

Voorwaarden:

- Versleutelen van oorspronkelijk hypotheek dient gestandardiseerd worden
- Het verhandelen van deze versleutelde hypotheken dient op een uniforme manier te gebeuren
- DLT dient ontworpen te worden

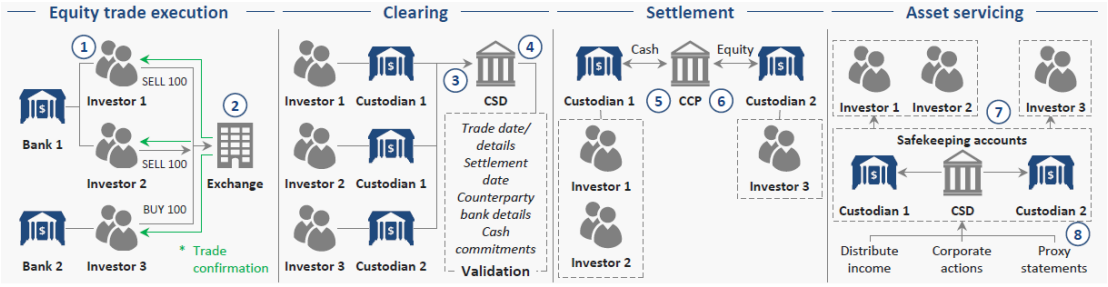
Conclusie:

- Hypotheekleningen kunnen versleuteld worden en digitaal op DLT geplaatst worden
- Transparantie neemt toe hetgeen een beter toezicht toelaat
- Verschillende partijen zullen veel nauwer moeten samenwerken

4.2.2.9. Afhandeling aandelenorders

Het proces na aan- of verkoop van een aandeel omvat oa uitwisseling van gegevens van verkoper en koper, aanpassingen van databanken (wie wordt nieuwe eigenaar van de aandelen) en transfers van gelden. In dit proces komen meerdere tussenpersonen tussen zoals depositarissen en clearinghuizen. De Amerikaanse beurs NYSE verhandelt dagelijks miljoenen orders zodat use case aanzienlijk is.

Huidige proces



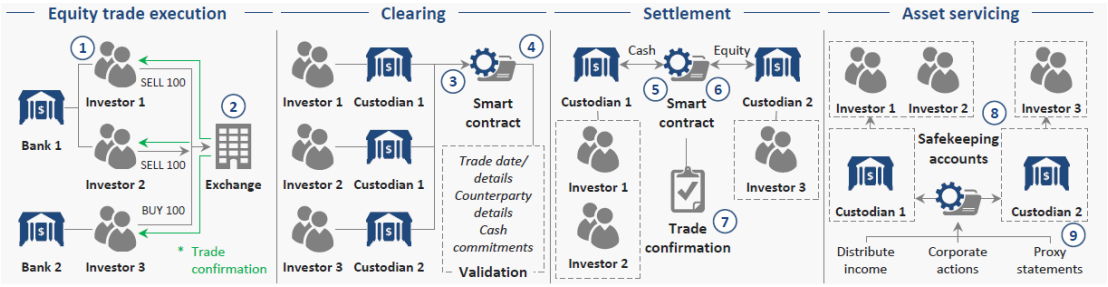
Afbeelding 36 *Afhandeling aandelenorders - Huidige proces*

Clienten voeren via interface van eigen bank transacties uit. De beurs bevestigt uitvoering en start afhandeling van de transactie op. De eerste fase is 'clearing'. In eerste instantie wordt gehandeld met een centrale tegenpartij die vervolgens doorstuurt naar verschillende clearingagenten. Vervolgens wordt de transactie gesettled. Dit houdt de juridische overdracht van de effecten in en betaling van de stukken. Tegelijk worden de effecten overgemaakt naar bewaarhoudende instellingen (custodians) waar de bank mee samenwerkt. Tenslotte wordt na de initiële transactie verdere dienstverlening geleverd zoals bijvoorbeeld het uitbetalen van dividenden.

Nadelen:

- Hoewel een transactie op enkele seconden uitgevoerd en bevestigd is, duurt de totale afwikkeling voor de meeste beurzen 2 dagen (uitgedrukt als D+2)
- De hoeveelheid aan transacties leidt tot inconsistente data
- Zoveel verschillende partijen die tussenkomen vergroot tegenpartijrisico
- Verschillende depositarissen werken op verschillende methoden zodat bevestigingen naar clienten (banken) op meerdere manieren verloopt
- Banken contacteren verschillende depositarissen voor financiële nazorg
- Meerdere tussenpersonen verhogen de totale kosten

Blockchain alternatief



Afbeelding 37 *Afhandeling beursorders - blockchain oplossing*

Clienten geven nog steeds orders door via toepassing van de bank en het order wordt door de beurs bevestigd aan client. De bank stuurt details door naar custodians die transactie op DLT plaatsen en dit in een smart contract verwerken. Dit contract kan verdere afhandeling verzekeren: gelijktijdige overdracht van effecten en contanten, details van depothoudende bank en verdere afhandeling van enige acties verbonden aan het effect.

Voordelen:

- Standardisatie van datavalden
- Automatische validaties door smartcontracts
- Minder inconstitenties
- Lager tegenpartijerisico
- Snellere afhandeling
- Kostenvoordelen door minder tussenpersonen
- Transacties kunnen sneller 'genet' worden: het samenvoegen van verschillende aan- en verkopen alvorens volledig af te handelen

Voorwaarden:

- Custodian banken en regulator dienen af te spreken op welke manier transacties correct genet kunnen worden
- Beurzen, banken, regulators dienen een platform op te zetten dat in staat de stroom van miljarden dollars per dag te beheersen
- Datavelden dienen geharmoniseerd te worden

Conclusie:

- Automatisatie leidt tot sneller afwikkeling
- Kostenbesparing door minder tussenpersonen of minder werk door tussenpersonen
- Minder risico

4.2.3. Conclusie Use Cases

Voorgaande use cases hebben een aantal duidelijke kenmerken gemeen die het gebruik van een blockchain toelaten. Voor de financiële cases zijn de meest toepasbare telkens aan de use case toegevoegd. De samenvatting is te vinden in tabel 4.

5 Criteria komen in meer dan 75% van de besproken casussen terug. De interactie tussen **meerdere partijen** komt overal terug. Dit hoeft ook niet te verwonderen aangezien we in onze oorspronkelijke definitie van blockchain reeds verwezen naar twee partijen. Nagenoeg even belangrijk zijn de mogelijkheid om **smart contracts** te gebruiken en **automatisatie**. Het eerste is een duidelijk voordeel van blockchain in het bedrijfsleven, het tweede hangt nauw samen met efficiëntiewinsten die gerealiseerd kunnen worden en hieruit voortvloeiende kostenbesparingen.

Tenslotte biedt blockchain een belangrijke **snelheidswinst** op vergeleken met traditionele systemen. De aanwezigheid van een **regulator** of de mogelijheid om deze te laten 'inpluggen' in de blockchain is eveneens een criterium dat in meer dan de helft van de gevallen aanwezig is.

Criterium/ Use Case	1	2	3	4	5	6	7	8	9	Aantal
Meerdere partijen	x	x	x	x	x	x	x	x	x	9
Smart Contract		x	x	x	x	x	x	x	x	8
Automatisatie		x	x	x	x	x	x	x	x	8
Snelheid	x	x	x	x	x	x	x		x	8
Regulator	x		x	x	x	x		x	x	7
Transparantie				x	x	x	x	x		5
TegenpartijRisico			x	x					x	3
Fraude	x	x								2
Papieren				x						1
Duplicatie Gegevens						x				1

Tabel 4 *Samenvattende tabel van criteria van use cases.*

4.3. Drijfveren voor Financiële instellingen

Don Tapscott en Alex Tapscott waarschuwen in hun boek "How the technology behind bitcoin is changing money, business and the world" [21] dat de dagen van het tweede oudste beroep ter wereld geteld zijn, behalve voor diegenen die de opportuniteit grijpen. Financiële sector draait op decennia oude technologie, is traag en onbetrouwbaar, is exclusief (niet iedereen heeft toegang tot het systeem) en is door centralisatie van data kwetsbaar voor hacking. Volgens de auteurs wordt de sector op z'n kop gezet door :

- **Vertrouwen**: banken zullen niet meer het alleenrecht hebben om tegenpartij te identificeren als te vertrouwen.
- **Kosten**: volgens Spaanse bank Santander kan alleen al met rechtstreekse betalingen ruim $20 mio bespaard worden.
- **Snelheid**: bij bewegingen tussen verschillende banken dienen er meerdere databases aangepast te worden. Zelfs voor eenvoudige transacties duurt dit soms dagen.
- **Risico management**: Settlement risico, tegenpartij risico.
- **Open source**: laat toe om veel sneller technologie up to date te houden.

Ze kaarten enkel ook aan dat er opportuniteiten voor de sector zijn. De use cases uit het vorige hoofdstuk laten een aantal duidelijke criteria optekenen die een financiële instelling kan bewegen om gebruik te maken van een blockchaintoepassing. Enisa (European Union Agency For Network And Information Security) bekijkt het gebruik van blockchain vanuit veiligheidsaspect. In een paper uit 2016 [26] onderzoekt dit agentschap de voordelen en uitdagingen vooor financiële instellingen. De grootste drijfveren kunnen samengevat worden als:

- **Kostenbesparingen**: Enerzijds kan dit financiële instellingen toelaten om verouderde systemen af te bouwen of het aantal verschillende lagen die data lezen te reduceren. Anderzijds doordat data meteen gedeeld wordt op een decentraal ledger is er later ook minder reconcialiatie nodig.
- **Riscobeheersing**: Doordat gebruik wordt gemaakt van gestandardiseerd framework kunnen risico's van complexe produkten zoals afgeleide produkten beter beheerst worden.
- **Regulatory compliance**: Bepaalde legale verplichtingen kunnen voor een deel geautomatiseerd worden.

De auteurs gaan dieper in op het specifieke kader waarin financiële instellingen opereren en de verschillende verplichtingen die ze moeten nakomen. Om hieraan te voldoen maken ze gebruik van een 'governance toolkit':

- **Regulation**: Een beperkt aantal personen en/of orgaan wordt toegelaten om op bepaalde markten te handelen. De kosten om nieuwe reglementering op te

volgen die na de bankencrisis van 2008 zijn ingevoerd lopen op tot meer dan $4Bn per jaar voor bepaalde instellingen.

- **Audit**: Op regelmatige tijdstippen dient bepaalde informatie aan de wetgever doorgegeven worden.
- **Interne controles**: Instellingen volgen de verschillende afdelingen of ze nog in lijn zijn met kapitaal- en risicoparameters.
- **Technologie**: Huidige technologische implementaties zijn niet in staat om volledige integratie te bekomen met achterliggende systemen. Er is dus veel 'oplapwerk' nodig en onderhoud.

Bovenstaande 'as-is' situatie is kwetsbaar doordat medewerkers moedwillig misbruik kunnen maken van het systeem, data onbewust verkeerd inbrengen en de technologische belemmeringen. Het agentschap gaat ervan uit dat blockchain een technologische oplossing kan zijn om deugdelijk bestuur beter te kunnen naleven. Wetgeving, audit en interne controles kunnen rechtstreeks samen met de transacties worden vastgelegd:

- **Wijzigingen in wetgeving**: Van zodra een wijziging in wetgeving ingebracht is in DLT, is deze informatie direct beschikbaar voor alle tegenpartijen, zonder enige technische aanpassing.
- **Audits**: Bestaande audits gebeuren op een bepaald tijdstip en geven enkel een momentopname weer. Via DLT is continue monitoring mogelijk.
- **Business logica**: smart contracts laten toe om logica op te nemen in de transactie. Dit zou latere afhandeling via back office veel eenvoudiger laten verlopen.
- **Interne opvolging**: afhandeling van transacties kan via blockchain via software zelf verlopen. Enkel opvolgen of het smart contract correct is uitgevoerd dient nog intern opgevolgd te worden.
- **Onzekerheid**: consensus kan bereikt worden door de logica die in het contract verwerkt wordt, zelfs wanneer de tegenpartij niet volledig vertrouwd wordt.

5. Blockchain implementaties

In de toelichting rond Ethereum zijn kort enkele concrete bedrijfstoepassingen aangekaart. In dit hoofdstuk gaan we dieper in op een aantal voorbeelden en bespreken we uitvoerig de genomen initiatieven in de financiële sector.

5.1. Hyperledger

De officiële website van Hyperledger[15] omschrijft zichzelf als *"Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chain, manufacturing and technology."* De subtitel vat het echter snel samen: "Blockchain Technologies For Business". Doelstelling is om Hyperledger als basis in de markt te positioneren met een kwalitatieve openbron code die als veilige basiscomponent gebruikt kan worden door bedrijven om modulair verder te bouwen.

Onder Hyperledger zijn er momenteel tal van frameworks en tools ter beschikking die door bedrijven als basis gebruikt kunnen worden. In tabel 5 en 6 worden de beschikbare frameworks en tools opgelijst. De componenten zijn overgenomen van www.hyperledger.org en behouden de Engelse toelichting.

HYPERLEDGER SAWTOOTH	Hyperledger Sawtooth is a modular platform for building, deploying, and running distributed ledgers. Hyperledger Sawtooth includes a novel consensus algorithm, Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption.
HYPERLEDGER IROHA	Hyperledger Iroha is a business blockchain framework designed to be simple and easy to incorporate into infrastructural projects requiring distributed ledger technology.
HYPERLEDGER FABRIC	Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. (IBM)
HYPERLEDGER BURROW	Hyperledger Burrow is a permissionable smart contract machine. The first of its kind when released in December, 2014, Burrow provides a modular blockchain client with a permissioned smart contract interpreter built in part to the specification of the Ethereum Virtual Machine (EVM).
HYPERLEDGER INDY	Hyperledger Indy is a distributed ledger, purpose-built for decentralized identity. It provides tools, libraries, and reusable components for creating and using independent digital identities rooted on blockchains or other distributed ledgers for interoperability.

***Tabel 5** Hyperledger Frameworks (bron: https://www.hyperledger.org/projects)*

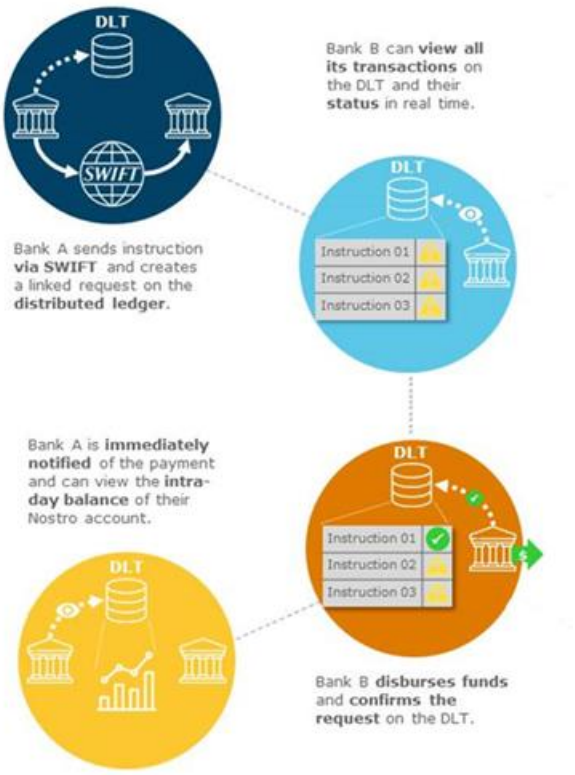
[15] https://www.hyperledger.org/

HYPERLEDGER CALIPER	Hyperledger Caliper is a blockchain benchmark tool, which allows users to measure the performance of a specific blockchain implementation with a set of predefined use cases.
HYPERLEDGER CELLO	Hyperledger Cello aims to bring the on-demand "as-a-service" deployment model to the blockchain ecosystem to reduce the effort required for creating, managing and terminating blockchains.
HYPERLEDGER COMPOSER	Hyperledger Composer is a collaboration tool for building blockchain business networks, accelerating the development of smart contracts and their deployment across a distributed ledger.
HYPERLEDGER EXPLORER	Hyperledger Explorer can view, invoke, deploy or query blocks, transactions and associated data, network information, chain codes and transaction families, as well as any other relevant information stored in the ledger.
HYPERLEDGER QUILT	Hyperledger Quilt offers interoperability between ledger systems by implementing ILP, which is primarily a payments protocol and is designed to transfer value across distributed ledgers and non-distributed ledgers.

Tabel 6 *Hyperledger Tools (bron: https://www.hyperledger.org/projects)*

Proof Of Concept – Internationale betalingen

Hyperledger laat toe om enkele Use Cases uit hoofdstuk 4.2.2 te concretiseren naar een Proof Of Concept. ANZ Banking en Wells Fargo hebben met succes het internationale betalingsysteem omgezet naar een DLT oplossing. [27] Deze is minder doorgedreven vergeleken met use case 4.2.2.1, maar praktisch toepasbaar en gelinkt aan bestaande systeem. In het POC werd een gedeeld DLT opgezet dat toeliet efficiënter en sneller internationale betalingen uit te voeren. Beide banken beklemtonen dat de oplossing parellel draait met het huidige systeem en dat de oplossing niet enkel intern helpt, maar ook de sector in het algemeen vooruithelpt. Aangezien beiden lid zijn van Linux Foundation is Hyperledger Fabric gekozen als technologie.



Afbeelding 38 *Internationale betalingen - Proof of Concept (bron: https://bluenotes.anz.com/posts/2016/09/how-blockchain-will-change-correspondent-banking)*

In de motivatie om de POC uit te werken verwijzen de instellingen naar twee belangrijke redenen. Enerzijds voelen de banken de hete adem van de competitie en uitdagers in de markt om snellere en goedkopere oplossingen aan te bieden. Anderzijds verwacht ook de client een snellere en goedkopere afhandeling van internationale betaling.

Proof of Concept – Escrow Accounts

ABN Amro heeft succesvol een blockchain ontwikkeld voor afhandeling van te blokkeren gelden tijdens een transactie tussen twee partijen. Volgens de bank is het grote voordeel het verminderen van administratieve kosten voor organisaties die fondsen van cliënten beheren zoals beurzen, pensioenfondsen, notarissen. Dankzij de blockchain kan elke individuele client gelinkt worden aan de blockchain. De test is begin 2018 van start gegaan met één client (Nxchange) die samen met ABN Amro verdere functionaliteiten zal uitwerken. [28]

Proof of Concept – Optimalisatie processen

Japan Net Bank, de eerste Japanse online bank, heeft een pilootproject opgezet gebaseerd op mijin en Hyperledger blockchain om over te schakelen naar een papierloze contract administratie. Het process bestond uit het versturen van papieren documenten en e-mails. De kans op fouten en vervalsingen van documenten was reëel. POC bestond erin om een dubbele blockchain op te zetten om backup van gegevens te hebben. [29]

Demo – Altoros Distributed Clearing Platform for Derivatives

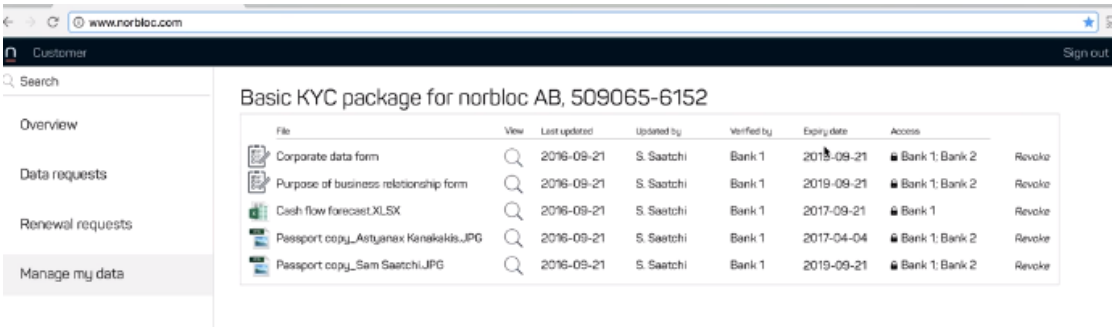
Bij het afsluiten van derivaten volgt een aanzienlijke werklast (post trade): margin bepalen en stellen, cash flows uitwisselen, eventuele tegengestelde trades neutraliseren, risico op falingen incalculeren. Een aantal taken worden manueel (papier/fax) afgehandeld en/of via een clearing house. Altoros (consultancy firm) biedt oplossingen aan gebaseerd op Hyperledger ecosysteem. Door het gebruik van smart contracts op de Hyperledger blockchain kunnen ze de post trade afhandeling veiliger en goedkoper afwikkelen.

Demo – Altoros Uitgifte en handelen van obligaties

'Catastrophe bond' is een obligatie die een aantrekkelijke coupon betaalt, maar hoofdsom vervalt wanneer een ramp zich voordoet. Een zakenbank stelt de voorwaarden op en brengt de emittent (verzekeraar) en investeerder samen. Albatros voorziet een oplossing die zakenbank vervangt door blockchain met smart contracts. De blockchain zelf wordt geïnstalleerd bij elke deelnemer, maar vereist in tegenstelling met publieke blockchains slechts beperkte rekenkracht. Veiligheid wordt voorzien door geavanceerde cryptografie. Tenslotte wordt gebruik gemaakt van derden (bv Swift) om betalingen te kunnen uitvoeren.

Piloot – Isabel Group en Norbloc organiseren piloot met blockchain KYC-platform

Norbloc heeft op basis van hyperledger een blockchain ontwikkeld die toelaat clientendata te delen tussen verschillende banken. De 4 grootste Belgische banken (Belfius, BNP Paribas, ING en KBC) hebben aan Isabel Group de opdracht gegeven om blockchainplatform uit te werken. Dit platform heeft het potentieel om een tijdrovend en vaak nog steeds papieren registratie te vervangen. [30]



Afbeelding 39 *Beeld van client die gegevens kan wijzigen en toegang kan verlenen aan meer dan één bank. (Bron: https://www.youtube.com/watch?v=hyADGKP9XbQ&feature=youtu.be)*

Volgens Tom De Block, Blockchain solution architect bij SettleMint, is deze use case een goed voorbeeld van het toekomstig model voor banken. [31] In het interview dat ik had met een van de weinige blockchain specialisten in België waarschuwt hij de bankensector voor de komst van PSD2. Deze richtlijn schrijft voor dat financiële instellingen clientendata ter beschikking moeten stellen aan derden (op voorwaarde dat client hiertoe instemt). De komst van andere spelers (buiten de banksector), maar ook jongere gestroomlijnde banken uit Oost-Europa staan klaar om de markt te veroveren. Het wordt tijd dat de Belgische banken wakker geschud worden en in actie komen. Een taak die in de toekomst voor de bank weggelegd is, is net het identificeren van cliënten. In bovenstaand voorbeeld wordt de bank die als eerste identificeert door de volgende banken vergoed voor dit identificatieproces.

5.2. Corda – R3

Corda[16] is een platform opgemaakt om afspraken tussen tussen verschillende partijen op te slaan, beheren en automatisch te laten afhandelen. Het is een initiatief dat genomen is door R3[17], een software bedrijf opgericht door meer dan 200 banken, financiële instellingen, regulators en technologiebedrijven. Aan de basis lag een frustratie dat verschillende generaties van technologische ontwikkelingen niet goed samenwerken, inefficiencies veroorzaken en steeds hogere kosten meebrengen. R3 is dankzij de vele partners actief op 6 continenten en beweert het grootste samenwerkingsverband te zijn in de blockchainwereld.

Nochtans is Corda niet echt een blockchain, maar eerder een berichten protocol (messaging protocol). Transacties kunnen gebeuren op verschillende nodes die niet op de hoogte zijn van de transacties op andere nodes. De verschillende nodes zijn wel aan elkaar verbonden, maar er geen distributie van alle transacties naar alle nodes. Enkel de informatie die gedeeld moet worden, wordt uitgezonden.

Corda onderscheidt zich ook door zich vanaf de start te richten op financiële sector. Hierdoor is sinds opstart rekening gehouden met strenge regulering en privacy criteria. Er is geen sprake van cryptomunten of consensus gebaseerd op mining. Bovendien kan het direct geïntegreerd worden in bestaande systemen.

Corda maakt gebruik van **gedistribueerd ledger** bewaard in Corda Vault en **Smart Contracts.** Dit contract bevat de businesslogica en kan autonoom afgehandeld worden.

***Afbeelding** 40 Corda - point-to-point (bron: https://www.corda.net/wp-content/uploads/2017/10/Corda-Solution-Guide.pdf)*

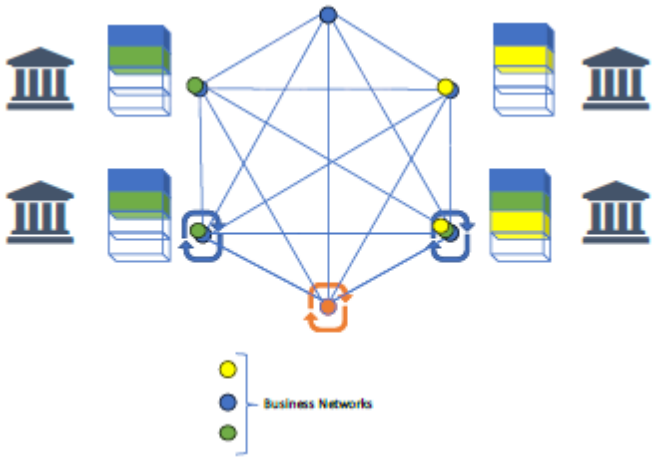
Corda zorgt voor verhoogde veiligheid, hoge beschikbaarheid en prestaties. Voor verhoogde veiligheid maakt Corda gebruik van SGX technologie van Intel (volledige privacy van transacties) en laat bedrijven toe eigen cryptografische sleutels te beheren (Hardware Security Module).

[16] www.corda.net
[17] www.r3.com

Corda integreert met bestaande netwerken en systemen zoals:

- SQL Server, Oracle, SQL Azure
- Advanced Message Queueing Protocol
- Lightweight Directory Access Protocol (LDAP° en Active Directory
- SWIFT en Financial products Markup Language (FpML)

De code zelf draait op Java Virtual Machine (JVM).



Afbeelding 41 *Integratie met bestaande infrastructuur (bron: https://www.corda.net/wp-content/uploads/2017/10/Corda-Solution-Guide.pdf)*

Ook via R3 zijn reeds meerdere concrete proof of concepts uitgewerkt en aantal concrete projecten gestart. In de toelichting op de jaarcijfers stelt CEO Ralph Hamers dat ING zich de komende tijd vooral wil bezighouden met blockchaintechnologie[18]. De reeds behaalde resultaten zijn in samenwerking met andere partners: “Deze mijlpalen staan symbool voor de samenwerking die inherent is aan het succes van blockchain”, dixit Hamers.

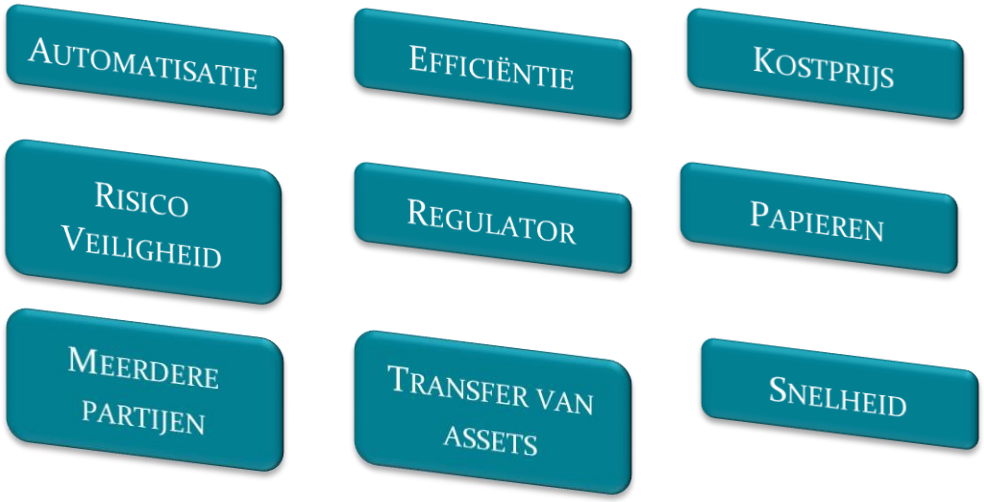
Samen met R3, 12 andere banken en trading platform **TradeIX** bouwde ING een gedistribueerd ledger platform dat handelsfinanciering voor traders automatiseert voor en na verscheping. [32] Manuele processen zoals het controleren van documenten wordt vervangen door smart contracts. Dit laat alle partijen toe om gelijktijdig dezelfde informatie te raadplegen. In de ontwikkeling wordt rekening gehouden met geografische verschillen en de koppeling aan specifieke API’s en technologische tools. Zowel de betrokken banken als de verkopers en kopers hebben baat bij deze grotere transparantie. De focus lag in deze piloot op het uitwerken van gestandaardiseerde smart contracts mbt handelsfinanciering. Eerder werd design van infrastructuur reeds geoptimaliseerd. In een latere fase wordt de piloot uitgerold naar meerdere partijen.

Easy Trading Connect Blockchain is een prototype ontwikkeld door ING en Société Générale samen met trading house Mercuria. [33] Doelstelling is blockchain technologie in te zetten om live oliecontracten te verhandelen. De eerste testen leverden snelheidswinst op, gecombineerd met lagere kosten en risico’s. Concreet werd een lading Afrikaanse olie, onderweg naar China, tijdens de reis drie keer verkocht. Alle tussenpartijen (traders, banken, agenten, inspecteur) handelden direct op de blockchain. De uitdaging lag vooral in het vervangen van het volledige papierwerk. De transactietijd voor ING alleen kon gereduceerd worden van gemiddeld 3 uur tot ca 25 minuten. Tegenpartij Société Générale verwijst naar het opgebouwde data record dat een gemakkelijke audit toelaat.

Afbeelding 42 *Grootste voordelen van Easy Trading Connect. Bron: https://www.youtube.com/watch?v=kDnBkAnsp1k*

[18] https://www.emerce.nl/nieuws/ing-meer-doen-blockchain

In een update van het project eind 2017 zijn reeds enkele grote energiebedrijven betrokken in het project en wordt verwezen dat de technologie beschikbaar zal gesteld worden aan alle marktpartijen in de energiehandel.



Het **Easy Trading Connect** platform werd begin 2018 ook succesvol toegepast op landbouwhandel. Samen met ABN Amro, Société Générale en handelaar Louis Dreyfus Company (LDC) werd de eerste blockchain transactie uit deze sector opgezet. Dankzij het wegvallen van papieren proces werd een verkoop van LDC aan een Chinese koper afgehandeld in 4 dagen vergeleken met het traditionele proces van 11 tot 14 dagen. Naast deze snelheidswinst worden aangestipt: minder kans op fraude, lagere kosten, hogere veiligheid en de mogelijkheid om real-time de transactie te volgen. Een volledige infografiek is terug te vinden in Bijlage 2; video van het proces via https://youtu.be/GobHxOoglcE. De criteria zijn dezelfde als vorige use case van Easy Trading Connect zodat ze hier niet herhaald worden.

Tenslotte zette ING samen met Credit Suisse de eerste **blockchain effectentransactie** op. [34] De twee banken wisselden liquide activa uit met een onderliggende waarde van 25 mio euro. De swap gebeurde dankzij een achterliggend waarborgplatform van fintechbedrijf HQLA[x]. Banken houden liquide effecten aan omwille van Basel III liquiditeitsnormen. Nochtans is een actief beheer hiervan onontbeerlijk zodat banken regelmatig effecten uitwisselen. Volgens Ivar Wiersma, head of ING Wholesale Banking Innovation, maakt deze blockhain-innovatie financiële dienstverlening niet alleen sneller, gemakkelijker en efficiënter, maar wordt de hele industrie hier beter van. Er wordt immers een meer transparante marktplaats beschikbaar. Ook in deze piloot wordt expliciet verwezen naar de directe lijn die regulator heeft naar de volledig historiek van de transactie.

ING CEO Hamers verwees eerder al naar sterke samenwerking tussen partners om van blockchain een succes te maken. Een duidelijk bewijs ligt in de ontwikkeling van **zero-knowledge range proof (ZKRP)**. [35] Het blockchain team van ING heeft een belangrijke doorbraak gerealiseerd in het beschermen van data. Doordat informatie door elke participant zichtbaar is op het ledger was deze informatie niet altijd geheim. De ZKRPcode voegt een extra cryptografische laag toe aan de blockchaintechnologie die toelaat om de waarheid te bewijzen, zonder teveel aan informatie zichtbaar te moeten maken. Voor aanvraag van een lening is dit bijvoorbeeld het bewijs dat loon voldoende hoog is om lening te kunnen krijgen, zonder het exacte bedrag te moeten opgeven. Voor een betaling kan akkoord gegeven worden dat rekening voldoende saldo heeft zonder het exacte saldo kenbaar te maken.

De ZKRPoplossing blijkt 10 keer efficiënter te zijn dan gelijkaardige technologieën, terwijl de basisprincipes blijven gelden: compleet, soliditeit en volledige geheimhouding. De technologie wordt beschikbaar gesteld als open source zodat anderen hiervan gebruik kunnen maken en zelfs de code kunnen verbeteren.[19]

[19] De code is beschikbaar op github: https://github.com/ing-bank/zkrangeproof

5.3. Blockchain in praktijk

De concrete implementaties via Hyperledger en R3-Corda tonen aan dat financiële instellingen actief participeren in de uitbouw van blockchain. Ook Charles Sanders stelt in financieel-manegement.nl [36] vast dat de Nederlandse banken volop inzetten op blockchain, terwijl volgens sommige experts de komst van blockchain financiële instellingen overbodig dreigt te maken. De auteur haalt een aantal zelfde pilootprojecten aan en concludeert dat banken wel degelijk een toekomst hebben door oa het efficiënter uitvoeren van payment processen, efficiënter maken van processen in de supply chain, identity management om fraude en witwaspraktijken tegen te gaan, checken van documenten, assetmanagement, concurreren met bedrijven die eigen wallets en payment services beginnen. Sanders beklemtoont het vertrouwen dat banken genieten bij de bevolking. Geld wordt straks data. Cliënten vertrouwen banken bij de opslag van geld, dus dat zal ook gelden bij opslag van gegevens.

De belangrijkste criteria die in de praktijk use cases zijn gehanteerd zijn samengevat in tabel 7. De top 5 uit de use cases komen terug in de concrete implementaties. Het gebruik van smart contracts en de link met de regulator blijkt echter minder sterk door te wegen in de implementaties. Aantal andere criteria gelijken sterk op elkaar (veiligheid-fraude, efficiëntie-automatisatie) of zijn eerder een gevolg van de toepassing dan wel een criterium (lagere kosten).

Implementaties	1	2	3	4	5	6	7	8	9	Aantal
Meerdere partijen	x	x		x	x	x	x	x	x	8
Automatisatie			x	x	x	x	x	x		6
Efficiëntie			x			x	x	x	x	5
Kostprijs				x		x	x	x		4
Snelheid	x							x	x	3
Veiligheid				x	x			x		3
Clienten	x	x								2
Smart Contract					x		x			2
Regulator								x	x	2
Concurrentie	x									1
Nieuwkomers	x									1
Fraude			x							1
Transparantie									x	1

Tabel 7 *Samenvattende tabel van criteria van implementaties*

6. Blockchain als ultieme oplossing?

Blockchain heeft het potentieel om bedrijfsprocessen compleet te veranderen. De technologie staat echter nog in de kinderschoenen en kent nog heel wat beperkingen.

Tevens is blockchain niet de modeloplossing voor alle use cases. Door de hype rond blockchain is het aantrekkelijk geworden om een blockchainoplossing te voorzien om extra budgetten los te krijgen. Waar we in Hoofdstuk 4 en 5 eerder criteria toelichten die gelden voor een valabele blockchain toepassing bekijken we ook even wanneer dit net niet van toepassing is.

6.1. Beperkingen

6.1.1. Technologische beperkingen

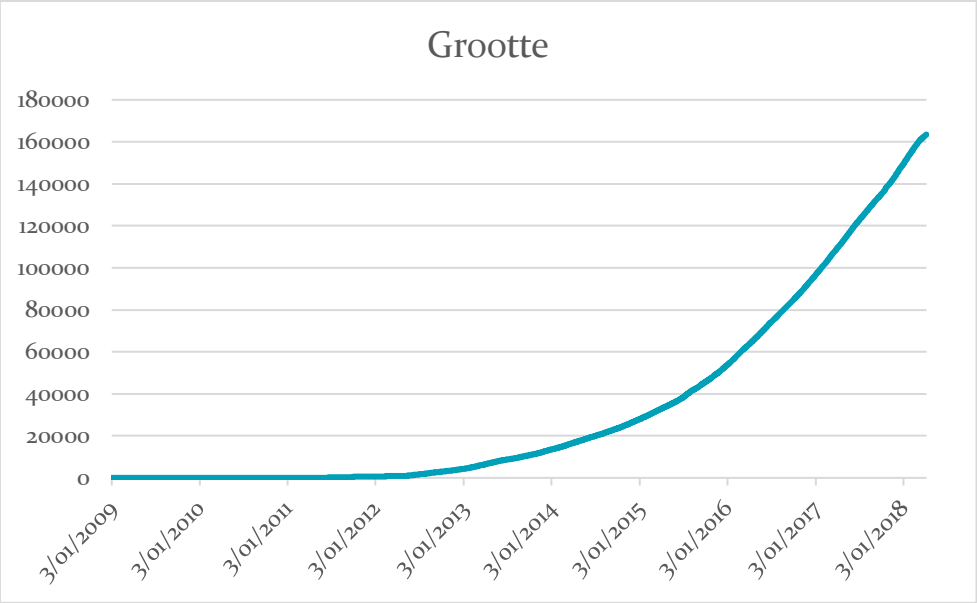
In hoofdstuk 4.2.2 is het bepalen van standaarden tussen verschillende spelers en/of de regulator een belangrijke voorwaarde om de usecase te laten slagen. Binnen blockchain zijn ondertussen al verschillende mogelijkheden. Ten eerste verwijzen specialisten naar de bitcoin blockchain als de enige echte. Nochtans toont het Ethereum netwerk dat blockchain ook op alternatieve netwerken kan slagen. De derde grootste cryptomunt Ripple werkt tenslotte zonder blockchain[20] .

Melanie Swan somt in "Blockchain, blueprint for a new economy" enkele technologische belemmeringen op [19]. De meeste belemmeringen zijn gelieerd aan bitcoin:

- **Throughput**: Gemiddeld verwerkt het bitcoin netwerk maar 1 transactie per seconde. Theoretisch ligt het maximum op 7 transacties per seconden. Hoewel dit volgens ontwikkelaars verhoogd kan worden (door blocks te vergroten) verbleekt dit in het niets als we verglijken met bv Visa (2000 tps) en Twitter (5000 tps).
- **Latency**: Elke transactie duurt ongeveer 10 minuten om bevestigd te worden. Visa doet er ca 1 seconde over.
- **Size and bandwidth**: Melanie Swan noteert in haar boek nog 25 GB als grootte van de bitcoin blockchain. In 2015 zou deze met 14 GB zijn aangegroeid. Door exponentiële groei is de bitcoin blockchain per begin april 2018 reeds 163 GB groot. Bijgevolg wordt de initiële doelstelling dat elke partij een volledige copie van het grootboek lokaal bijhoudt steeds moeilijker. In praktijk runnen slechts een 7.000 servers wereldwijd een volledige copie van de bitcoin blockchain. Afbeelding 43 geeft de exponentiële groei van de grootte weer.
- **Security**: Doordat de bitcoinblockchain moet goedgekeurd worden door de meerderheid van de nodes is de aanval op het netwerk met meer dan 50% rekenkracht een reëel gevaar.

[20] https://www.want.nl/ripple-xrp-cryptocoin-investeren

- **Wasted resources**: het proof-of-work concept zorgt voor de betrouwbaarheid van het bitcoinnetwerk. Het delven van nieuwe blocks vergt echter enorm veel energie die compleet verloren gaat. De krant The Guardian[21] schatte eind 2017 het verbruik op ca 30 TWh per jaar. Dit is meer dan het jaarlijks verbruik van 19 Europese landen. Niet alleen gaat er veel rekenkracht verloren die mogelijks een nieuw medicijn tegen kanker had kunnen opleveren, maar zorgt ook voor een enorme ecologische voetafdruk. Voor elke dollar die computer verbruikt aan elektriciteit is ook een halve dollar nodig om deze te koelen. Kan het schaarse water gebruikt worden om pc's te koelen ?
- **Usability**: De API om te werken met Bitcoind is minder gebruiksvriendelijk dan doorsnee REST-API.



***Afbeelding 43** Grootte (in MB) van bitcoin blockchain (https://blockchain.info/nl/charts/blocks-size?timespan=all)*

6.1.2. Business model uitdagingen

Ondernemingen hanteren business modellen die gedurende meerdere decennia ontwikkeld zijn. Het is niet evident om deze modellen plots opzij te schuiven. Bovendien worden bepaalde modellen volledig onderuit gehaald door de komst van blockchain. In vele use cases wordt de rol van tussenpersoon geëlimineerd. Tussenpersonen kunnen dus weigerachtig staan om nieuwe technologie te implementeren.

6.1.3. Schandalen en publieke opinie

Het bitcoinnetwerk en achterliggende blockchaintechnologie zijn neutraal. Het is echter mogelijk om illegale activiteiten te ontwikkelen en zich te verschuilen achter de

[21] https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland

anonimiteit van het netwerk. Bitcoin komt regelmatig negatief in het nieuws doordat hackers ransomware installeren op pc's en pas vrijgeven wanneer betaald is via bitcoin.

Hoofdstuk 2.3 schetste bij de zwakheden van bitcoin de mogelijkheid tot hacking. Het blijft voor de publieke opinie moeilijk vatbaar dat na de hack van MtGox zoveel bitcoins verloren zijn, terwijl het netwerk net bijzonder transparant blijkt te zijn.

Tenslotte voorspellen doemdenkers een volledige instorting van het gebruik van cryptomunten. Eerdere technologische beperkingen kunnen aan de basis liggen of zelfs een nog niet te voorspellen oorzaak. In praktijk stellen we vast dat het gebruik continu stijgt (zie tabel 1, hoofdstuk 2.2) en dat meer en meer grote bedrijven gebruik maken van digitale munten.

Cryptomunten blijven alvast polariseren. Warren Buffet, het orakel van Omaha, noemde op de aandeelhoudersvergadering van Bershire Hathaway de cryptomunten 'rattenvergif in het kwadraat'. Volgens Buffet hebben cryptomunten geen intrinsieke waarde, de enige waarde die we eraan verbinden volgt uit hun vermeende schaarste. [37]

6.1.4. Overheidsvoorschriften

In hoofdstuk 4.2 bespraken we meerdere use cases waarbij de regulator betrokken partij is, enerzijds als controle-orgaan, anderzijds als rechtstreekse participant. De verdere evolutie van gebruik van digitaal geld heeft echter nog andere effecten.

Het zal veel moeilijker worden als overheid om belastingen te heffen. Als decentraal wereldwijd actief netwerk wordt het voor een lokale overheid niet eenvoudig om een taks op te leggen. Het stelsel van BTW is ook voorzien dat elke tussenpersoon de nodige BTW aanrekent en verrekent via de jaarrekening. Uitschakelen van deze tussenpersonen verandert dit systeem volledig. Onrechtstreeks heeft dit bv ook effect op groeicijfers omdat de basis voor het berekenen van Bruto Binnenlands Product cijfers (GDP) wijzigt.

De overheid wordt zelf ook sterk geraakt als tussenpersoon. Indien het DLT erin slaagt om de gegevens die nu door overheidsdiensten worden verwerkt, op te slaan met nodige transparantie voor wie hier toegang toe heeft, wordt de overheid voor een groot deel buitenspel gezet.

6.1.5. Privacy

De vrees om persoonlijke gegevens uitsluitend in een decentrale database ter beschikking te stellen, zonder een centraal orgaan om op terug te vallen schrikt velen af. Indien toegang verkregen wordt tot persoonlijke codes is het mogelijke verlies (diefstal!) onherroepelijk en kan er geen beroep gedaan worden op een mogelijke backup.

6.2. Kritisch over blockchain

In de studie naar blockchain in het bedrijfsleven en specifiek naar usescases binnen de financiële sector is veel documentatie te vinden dat ter beschikking gesteld wordt door verkopers van blockchain toepassingen. Het hoeft dan ook niet verwonderen dat een blockchainplatform als ideale oplossing uit te bus komt. In Hoofdstuk 4 zijn de niet-financiële use cases gebaseerd op onderzoek van IBM (een 'vendor' van blockchain), doch de financiële use cases zijn gebaseerd op het Wereld Economisch Forum, aangevuld met een studie van Swift. Ook de reële implemenaties via Corda vinden oorsprong bij financiële instellingen zelf. Het bronnenonderzoek is dus uitgebreider dan verkooppraat.

Toch blijven we even kritisch stilstaan bij de opgesomde criteria uit voorgaande hoofdstukken en kijken we na of er nuances nodig zijn.

Antony Lewis[22], Director of Research Lab & Research Centre Singapore bij R3, en een autoriteit op gebied van blockchain stelt in zijn blog Bits on blocks een aantal nieuwe vragen voor die toelaten na te kijken of blockchain wel een oplossing kan zijn. [38] en [39]

Bij analyse van use cases uit 2016 stelt hij vast dat meerdere proof of concepts niet zijn doorgebroken tot reële toepassingen omdat enerzijds de technologie onvoldoende ontwikkeld was of anderzijds de use case eigenlijk onecht was. Deze waren teveel gebaseerd op bitcoin netwerk en te weinig gecorreleerd met bedrijfsleven. Men ging uit van noodzaak om **veel deelnemers** te hebben, alles wat **datasharing** nodig had was goed genoeg voor blockchain (gebruik gewoon webportal), en als iets leek op **smart contract** was de case compleet.

Een meer genuanceerde checklist is :

- **B2B workflows**: een beperkt aantal deelnemers die elke partij de garantie geeft dat iedereen met dezelfde data werkt en dezelfde regels respecteert. De data wordt pas bewaard als iedereen hiermee akkoord is en niet nadien.
- **Industry utilities**: een DLT laat toe dat geen enkele partije volledige controle krijgt over een database, een ultiem voordeel vgl met een centrale database die door één van de partijen beheerd wordt.
- **Centralisatie risico**: door toegenomen cybercriminaliteit is decentralisatie van van infrastructuur meer en meer van belang.

In een ander artikel vatte de auteur de eerste twee punten treffend samen: *"Blockchains are great when multiple parties need to read the same information but for whatever reason there can't be or shouldn't be any specific individual party in control of that data."*

[22] https://bitsonblocks.net/my-story/

Ook Gideon Greenspan[23], CEO en Founder Coin Sciences (bedrijf achter Multichain open source blockchain platform) heeft enkele posts gepubliceerd die waarschuwen voor de wildgroei aan blockchaintoepassingen. Ik toets mijn criteria ook aan zijn bevindingen.

Volgens Greenspan zijn heel wat cases ook op te lossen via relationele databases. Indien dit mogelijk is moet je dat ook doen! Traditionele databanken zoals Oracle, MySQL, SQL Server ed hebben een bewezen trackrecord terwijl blockchain nog in de kinderschoenen staat. Hij heeft een checklist opgesteld met criteria waaraan voldaan moet zijn [40]:

- Database; er moet nood zijn aan een gedeelde database.
- Meerdere partijen die schrijven; meerdere partijen moeten de database kunnen wijzigen.
- Gebrek aan vertrouwen; dit is niet alleen van toepassing tussen verschillende ondernemingen maar kan ook tussen departementen van ondernemingen zijn.
- Disintermediatie; bovenstaande drie kenmerken zouden opgelost kunnen worden door bv een bank een centrale database te laten beheren. Indien het uitschakelen van deze tussenpersoon leidt tot lagere kosten, snellere afhandeling van transacties, nieuwe wetgeving,… dan loont dit.
- Interactie tussen transacties; er is een link tussen verschillende transacties die plaatsvinden op de database. Bij blockchain kunnen verschillende transacties gelijktijdig plaatsvinden.
- Regels; doordat meerdere partijen data kunnen wegschrijven in de database dient elkeen zich te houden aan afgesproken regels. Een regel kan bv zijn dat de som van alle activa voor en na een transactie gelijk moet blijven.
- Transactie log met validatie; dit laat een nieuwe node toe de actuele toestand van de database op te bouwen. Bovendien garandeert dit dat alle nodes naar dezelfde waarheid convergeren. Doordat nieuwe transacties niet in een bepaalde volgorde toegevoegd worden is er een validatie nodig van deze transacties. Bij bitcoin nemen de miners dit voor hun rekening, Corda werkt bv met notaries.
- Garantie; volg op wie achter de digitale activa zit. Als ik een bepaalde activa op een blockchain claim, waar kan ik deze eis in het 'echte' leven hard maken?

Vooral de eerste 5 criteria zijn doorslaggevend. Indien hier niet aan voldaan is kan net zo goed een andere oplossing dienen:

- Gewone dataopslag
- Centrale database
- Master-slave database replicatie
- Meerdere databases waarop geconnecteerd kan worden

[23] https://www.linkedin.com/in/gidgreen/

Hij vergelijkt blockchains verder met een centrale database. [41] De voor- en nadelen worden samengevat in tabel 8.

Vanuit standpunt van **wegvallen van een tussenpersoon** is blockchain duidelijk in het voordeel tov centrale database. Ook al zou je een tussenorganisatie vertrouwen om het centrale register te beheren, dan blijft er een potentieel gevaar dat menselijke tussenkomst (opzettelijk of per vergissing) de database aanpast. Ook al zijn de personeelsleden van de tussenpartij ter goeder trouw brengt deze tussenstap altijd extra kosten met zich mee.

Doordat elke node zicht heeft op alle transacties is een blockchain minder **confidentieel** dan een centrale database. Geavanceerde cryptografische technieken trachten te verhinderen dat elke node ook alle informatie kan inzien (zie ZKPC in 5.3), doch dit gaat ten koste van performance en snelheid.

In een blockchain heeft elke node een volledige copie van het register. Dit resulteert in een continue **beschikbaarheid** van de database en het wegvallen van één of meerdere nodes heeft geen implicaties op het functioneren van de blockchain. Een centrale database 100% bereikbaar houden impliceert een hogere kostprijs aan infrastructuur.

In een blockchain dient elke transactie apart geverifieerd te worden via publiek-private sleutels. Alvorens een block definitief wordt toegevoegd aan de blockchain dienen alle nodes hierover akkoord te zijn. Dit houdt intensief uitwisselen van gegevens in. Tenslotte verwerken alle nodes alles transacties hetgeen meer rekenkracht vergt. Bijgevolg scoren blockchains minder goed op **prestatie**.

En smart contracts ? Die zouden in een relationele database opgevangen kunnen worden via stored procedures.

Criterium	Blockchain	Centrale database
Disintermediatie	✔	✘
Vertrouwelijkheid	✘	✔
Stevigheid	✔	✘
Prestatie	✘	✔

Tabel 8 *Vergelijking voor- en nadelen blockchain met centrale database (bron: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases)*

7. Besluit

Nadat we eerst enkele technische elementen van blockchain via de historiek van blockchain, Bitcoin en Ethereum ander de knie kregen doken we vanaf hoofdstuk 4 in de zoektocht naar criteria die een blockchain succesvol maken. Een studie van Swift stelde vast dat de technologie voor – de specifieke eisen van - financiële instellingen nog in de kinderschoenen staat en elke case individueel bekeken moet worden.

De algemene use cases (niet specifiek gelinkt aan financiële sector) lijsten alvast op dat voor een succesvolle blockchain er **meerdere partijen** betrokken moeten zijn, het proces enige **transparantie** nodig heeft, er een noodzaak is om **sneller** te handelen en bijgevolg ook veel **efficiëntiewinst** mogelijk is.

Deze criteria gelden evenzeer voor financiële instellingen, doch worden uitgebreid met verdere **automatisatie** en een noodzaak vanuit regulatorstandpunt. De financiële sector is sterk gereguleerd en wordt ook sterk geaudit. Blockchain biedt een duidelijke meerwaarde aan bedrijf en **regulator** om deze audit uit te voeren.

Experts waarschuwen de bankensector trouwens om niet op de lauweren te rusten en de technologie te omarmen en zien voordelen mbt **risicomanagement** (tegenpartijrisico, maar ook data bescherming) en zien dit als aanzienlijke **kostenbesparing**.

De vele pilootprojecten via Hyperledger en Corda (R3) tonen aan dat de financiële sector blockchain omarmd heeft en de technologie eerder als troef ziet dan als concurrent. De reeds aangehaalde criteria blijken dan ook toegepast te worden in het opzetten van de proof of concepts en pilootprojecten.

Tenslotte controleerden we in hoofdstuk 6 of de toegepaste criteria genuanceerd dienden te worden. Dit levert ons volgende oplossing voor de hoofdvraag van deze scriptie:

Welke criteria kan een financiële instelling hanteren om een product of proces af te handelen via blockchain:

- In het proces zijn meerdere partijen betrokken, die een zekere vorm van wantrouwen ten opzichte van elkaar hebben die
- Een database willen delen en hiervoor niet afhankelijk willen zijn van een tussenpersoon die deze data beheert en waar
- Een interactie is tussen deze partijen via transacties die aan elkaar gelinkt zijn.
- Het proces vergt een zekere transparantie, dit voor zowel interne audits als door regulering die wordt opgelegd
- Verplichting door de cliënt: Nieuwkomers (zullen aan)bieden nieuwe diensten aan die goedkoper en/of sneller zijn dan het bestaande proces. De instelling kan maw een aanzienlijke snelheidswinst of kostenbesparing realiseren door toepassing blockchain.

- Automatisatie: blockchain laat een grotere automatisatie toe van bestaande processen.
- Veiligheid: bescherming van data door cybercriminaliteit, maar ook fraudemogelijkheden in het bestaande proces door intervenianten of personeelsleden.
- Smart Contracts: Blockchain is vernieuwend door het toevoegen van intelligente contracten aan transacties. Eenvoudige iteratieve taken die vandaag een grote personeelskost vergen kunnen in de transactie ingeschreven worden.

8. Verklarende woordenlijst

API
Application Programming Interface, 52
bitcoin
is een cryptovaluta en een globaal betaalmiddel, 6
Bitcoind
programma dat het Bitcoin protocol implementeert (volledige node van alle code), 52
consortiumblockchain
Een combinatie van publieke en private blockchain, nl een samenwerking van meerdere partijen op één blockchain maar niet opengesteld aan iedereen, 10
distributed ledger
een database die verspreid is over verschillende computers die telkens een exacte kopie bijhouden en onafhankelijk kunnen werken, 4
DLT, 45
Digital Ledger Technology, 45
Mining
Valideren en vastleggen van transacties die op blockchain gebeurd zijn, 8
node
Computer die deel uitmaakt van het netwerk, 10
publieke blockchain
Een blockchain waar alle gebruikers zonder restricties kan deelnemen, 10
Ripple
httRipple is niet alleen een cryptocoin, maar ook een betaalprotocol. Het gaat om een valutanetwerk dat officieel bekend staat als het Ripple Transaction Protocol (RTXP). Het systeem is gebouwd op een open source en gedistribueerde basis. De bijbehorende munteenheid heet XRP, ook wel bekend als Ripples, en die kun je dus ook kopen. Het overkoepelende systeem streeft om veilig, instant en bijna gratis wereldwijd transacties uit te voeren, zonder terugboekingen, 52
Satoshi Nakamoto
De uitvinder van bitcoin, 11

9. Geciteerde werken

[1] M. S. A. P. C. Catalini, „blockchain-explained," 25 05 2017. [Online]. Available: http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/.

[2] M. Gupta, Blockchain for dummies IBM limited edition, Hoboken, USA: John Wiley & Sons, Inc, 2017.

[3] A. Lewis, „bravenewcoin," [Online]. Available: https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf. [Geopend 21 12 2017].

[4] S. Nakamoto, „bitcoin.org," [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Geopend 09 12 2017].

[5] M. I. a. K. R. Lakani, „hbr," harvard business review, 01 2017. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain. [Geopend 9 12 2017].

[6] C. Thompson, „The Blockchain Review," 2 10 2016. [Online]. Available: https://medium.com/blockchain-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093. [Geopend 28 12 2017].

[7] L.S., „The Economist," 20 01 2015. [Online]. Available: https://www.economist.com/blogs/economist-explains/2015/01/economist-explains-11. [Geopend 28 12 2017].

[8] S. V. e. P. Smit, Blockchain, de technologie die de wereld radicaal verandert, Den Haag: Einstein Books, 2017.

[9] L.S., „The Economist," 02 11 2015. [Online]. Available: https://www.economist.com/blogs/economist-explains/2015/11/economist-explains-1. [Geopend 09 12 2017].

[10] S. Driscoll, „How Bitcoin Works Under The Hood - youtube," http://www.imponderablethings.com/, 14 07 2013. [Online]. Available: https://www.youtube.com/watch?v=Lx9zgZCMqXE. [Geopend 31 12 2017].

[11] „Bitcoinmining," [Online]. Available: https://www.bitcoinmining.com/#bw. [Geopend 28 12 2017].

[12] „forklog.net," The Brief History of Bitcoin Mining: How It All Started, 18 07 2016. [Online]. Available: http://forklog.net/bitcoin-mining-past-present-and-future/. [Geopend 28 12 2017].

[13] J. V. Eerten, „Bitcoins delven lukt nergens beter dan in IJsland," *De Tijd,* p. 10, 16 11 2017.

[14] P. Saaim, „Profit Confidential," 30 11 2017. [Online]. Available: https://www.profitconfidential.com/cryptocurrency/nem/xem-price-forecast-2018-consider-tether-hack/. [Geopend 27 01 2018].

[15] E. T. f. t. arXiv, „MIT Technology Review," MIT, 8 11 2017. [Online]. Available: https://www.technologyreview.com/s/609408/quantum-computers-pose-imminent-threat-to-bitcoin-security/. [Geopend 27 1 2018].

[16] A. Castor, „Forbes," Forbes, 25 08 2017. [Online]. Available: https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-a-long-way-off/. [Geopend 27 01 2018].

[17] R. Browne, „cnbc.com," 19 12 2017. [Online]. Available: https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html. [Geopend 04 05 2018].

[18] Diversen, „Wikipedia," Wikipedia, 13 01 2018. [Online]. Available: https://nl.wikipedia.org/wiki/Ethereum. [Geopend 27 01 2018].

[19] SwanMelanie, Blockchain, blueprint for a new economy, Sebastopol, CA 95472: O'Reilly Media, 2015.

[20] T. Gerring, „ethereum.stackexchange.com," 22 01 2016. [Online]. Available: https://ethereum.stackexchange.com/questions/375/what-is-swarm-and-what-is-it-used-for. [Geopend 18 02 2018].

[21] D. T. a. A. Tapscott, Blockchain Revolution - How the technology behind bitcoin is changing money, business and the world, USA: Penguin Random House, 2016.

[22] M. Lucas, „The difference between Bitcoin and blockchain for business," 09 05 2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/. [Geopend 29 12 2017].

[23] S. a. Accenture, „www.swift.com," 20 04 2016. [Online]. Available: https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services. [Geopend 11 04 2018].

[24] Meerdere auteurs, „www.ibm.com," 02 2017. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03809USEN. [Geopend 22 02 2018].

[25] W. E. Forum, „The future of financial infrastructure," 2016.

[26] D. W. K. Hon, „www.enisa.europa.eu," 18 01 2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Geopend 05 12 2017].

[27] J. K. &. L. F. Chris T'en, „bluenotes.anz.com," anz, 26 09 2016. [Online]. Available: https://bluenotes.anz.com/posts/2016/09/how-blockchain-will-change-correspondent-banking. [Geopend 11 04 2018].

[28] onbekend, „www.finextra.com," 15 02 2018. [Online]. Available: https://www.finextra.com/newsarticle/31681/abn-amro-moves-escrow-accounts-to-the-blockchain/wholesale. [Geopend 12 04 2018].

[29] I. Allison, „www.ibtimes.co.uk," 6 02 2018. [Online]. Available: https://www.ibtimes.co.uk/japan-net-bank-tests-blockchain-mijin-hyperledger-1659181. [Geopend 13 04 2018].

[30] P.-J. Crombez, *Isabel Group en norbloc organiseren piloot met blockchain KYC-platform (persbericht),* Brussel, Stockholm, 15 maart 2018.

[31] T. De Block, Interviewee, *Blockchain solution expert.* [Interview]. 06 03 2018.

[32] ING, „R3," 26 09 2017. [Online]. Available: https://www.r3.com/news/r3-and-tradeix-develop-open-account-trade-finance-dlt-business-network/. [Geopend 01 05 2018].

[33] ING, „www.ingwb.com," 22 02 2017. [Online]. Available: https://www.ingwb.com/insights/news/2017/compelling-results-for-blockchain-oil-trade-test-ing-and-societe-generale. [Geopend 10 05 2018].

[34] ING, „www.ing.com," 01 03 2018. [Online]. Available: https://www.ing.com/Newsroom/All-news/Blockchain-set-to-transform-collateral-lending.htm. [Geopend 09 05 2018].

[35] ING, „www.ing.com," 16 11 2017. [Online]. Available: https://www.ing.com/Newsroom/All-news/Blockchain-transactions-just-got-a-whole-lot-safer.htm. [Geopend 09 05 2018].

[36] C. Sanders, „financieel management," 07 02 2018. [Online]. Available: https://financieel-management.nl/artikel/blockchain-in-de-praktijk-wat-doet-ing-al. [Geopend 09 05 2018].

[37] B. Serrure, „Buffet:'Cryptocurrencies? Rattenvergif in het kwadraat'," *De Tijd,* 06 05 2018.

[38] A. Lewis, „bitsonblocks," 24 07 2017. [Online]. Available: https://bitsonblocks.net/2017/07/24/avoiding-blockchain-for-blockchains-sake-three-real-use-case-criteria/. [Geopend 10 05 2018].

[39] A. Lewis, „bitsonblocks.net," 19 07 2016. [Online]. Available: https://bitsonblocks.net/2016/07/19/so-you-want-to-use-a-blockchain-for-that/. [Geopend 10 05 2018].

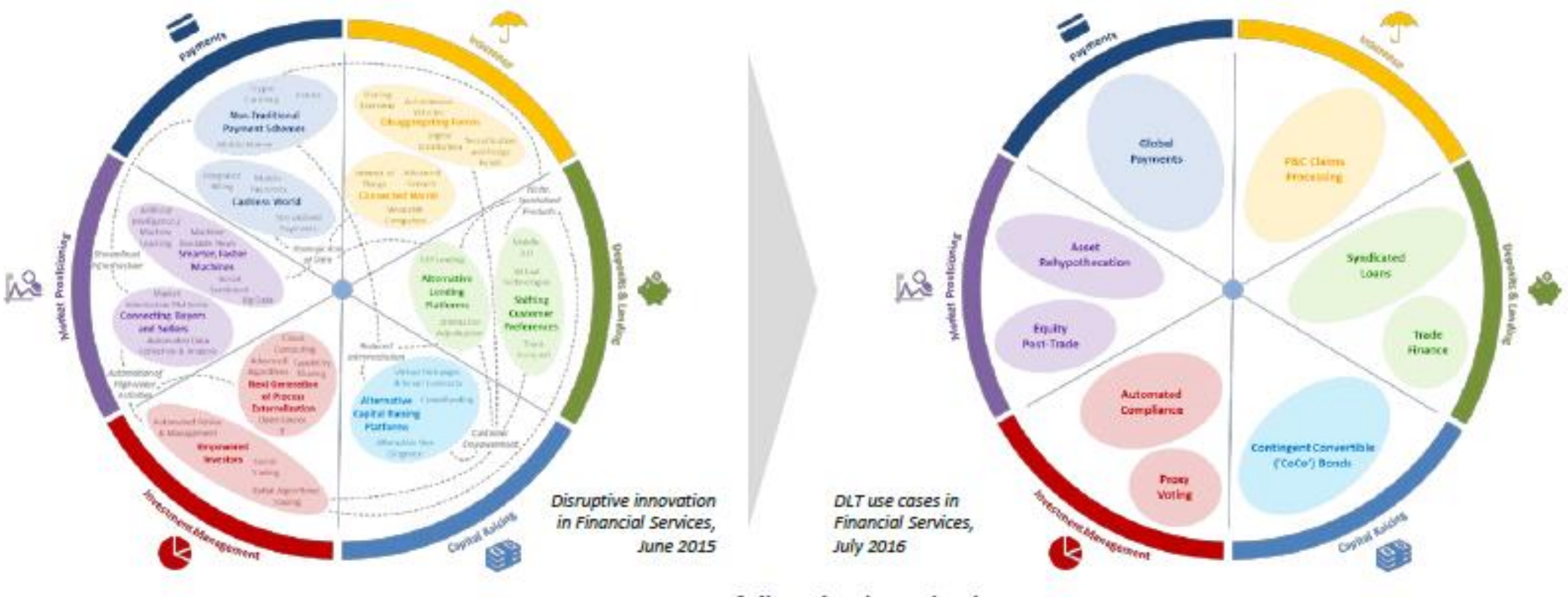
[40] G. Greenspan, „www.multichain.com," 22 11 2015. [Online]. Available: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/. [Geopend 10 05 2018].

[41] G. Greenspan, „www.multichain.com," 17 03 2016. [Online]. Available: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/. [Geopend 10 05 2018].

10. Lijst van afbeeldingen en tabellen

11. BIJLAGEN

11.1. Bijlage 1 Use Cases World Economic Forum; gebaseerd op Rapport van 2016



11.2. Bijlage 2 Easy Trading Connect Platform Infografiek