BLOCKCHAIN: VAN HYPE NAAR HYMNE?

Wat is blockchain en hoe kun je het gebruiken?

Sinds de DotCom-periode is geen technologie meer zo gehypet als blockchain-technologie. Blockchain-adepten noemen het een nog fundamentelere technologie dan TCP/IP was voor het internet. Wat is blockchain-technologie, waar is het voor bedoeld en vooral, wat zal dan die fundamentele maatschappelijke verandering zijn?

The Internet of Everything needs a Ledger of Everthing
The blockchain is a truly open, distributed, global platform that fundamentally changes what we can do online, how we do it, and who can participate. Call it the world wide ledger.

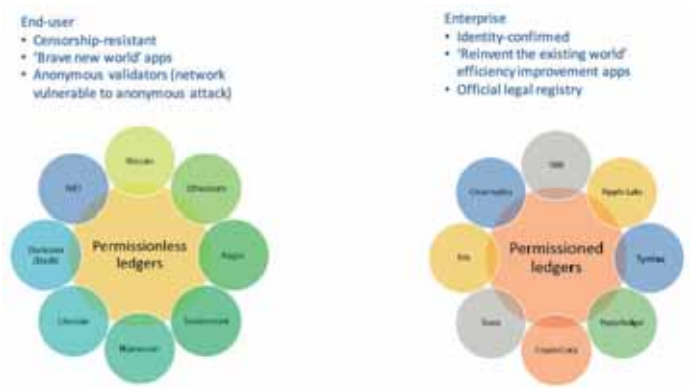
- Don & Alex Tapscott [1]

Er is niet één blockchain

Er wordt veel gepraat over 'de blockchain', alsof er maar één blockchain bestaat. Echter, er zijn verschillende soorten blockchains. Elk met een eigen signatuur en bijbehorende consensusprotocollen, die ontworpen zijn voor bepaalde use-cases. De Bitcoin-blockchain en het bijbehorend 'proof of work' consensusprotocol bijvoorbeeld, lossen het zogenaamde 'double spend'-probleem op bij digitaal geld. Het zorgt ervoor dat eenzelfde digitale munt niet twee keer kan worden verhandeld of uitgegeven. Het zijn met name cryptocurrencies waarmee blockchain-technologie bekend geworden is en waarvan Bitcoin veruit de populairste en het meest bekend is. Cryptocurrencies gebruiken overwegend publieke blockchain-technologie.

Naast publieke blockchains zijn er ook private blockchains. Een andere term die je in dit verband vaak hoort is 'permissionless' en 'permissioned' blockchains, ook wel ledgers genoemd.

Public & permissionless betekent dat de actoren en de hardware waarop de blockchain draait onbekend c.q. anoniem zijn. Private-permissioned ledgers daarentegen draaien op bekende en beheerde hardware en de actoren/deelnemers zijn geïdentificeerd en geauthenticeerd door bijvoorbeeld een KYC- (know your customer) of andere onboarding procedure.



T. (0215). Consensus as a service: a brief report on the emergence of permissioned, distributed ledger systems htttp://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distribute-ledgers.pdf

Permissioned ledgers

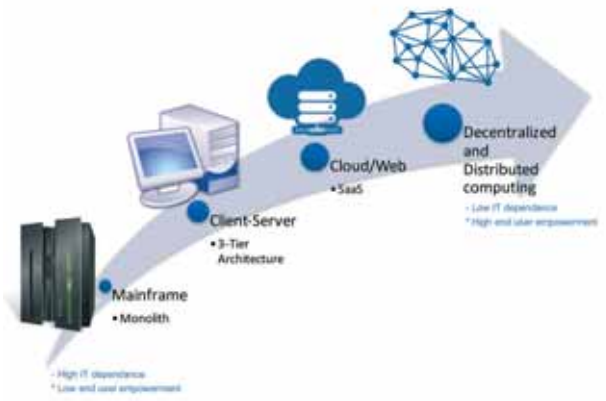
Er zijn ook private-permissioned blockchain-technologieën die zonder cryptocurrencies werken. Bijkomend voordeel voor het bedrijf is dan dat de CFO niet gedwongen wordt om niet-gereguleerd geld in z'n financieel overzicht op te nemen. Veelal kunnen dit soort systemen enorme transactievolumes verwerken.

Een ding hebben alle blockchains gemeen; ze zijn ontworpen om de noodzaak voor de Trusted Third Party (TTP) in ketens of processen te elimineren. De blockchain vormt dan het trustcenter. Daardoor ontstaat optimalisatie in de keten/het proces en wordt vertrouwen op een hoger plan getild en kan het gebruikt worden om processen verder te automatiseren (smart contracts).

De ontwikkeling van netwerkarchitectuur

De afgelopen decennia heeft de netwerkarchitectuur verschillende ontwikkelstadia gehad, elk met hun eigen karakter qua informatiebeveiliging. Het ging van een gecentraliseerd model, via een client-server model naar het huidige cloudcomputing-model. Dit laatste zou je ook een gecentraliseerd model kunnen noemen. De ontwikkeling wordt mogelijk gemaakt door een drietal factoren;

1. **Dalende kosten hardware**
2. **Stijgende rekenkracht**
3. **Virtualisatie**



Distributed computing

Volgens Peter Levine, partner bij Venture Capital bedrijf Andreesen Horowitz, is het einde van het cloudcomputing-tijdperk al weer in zicht [2]. Zijn stelling is dat in 2020 naar een volledig gedistribueerd model wordt gegaan onder invloed van Internet of Things en machine-learning. Hij noemt dit Edge Computing. Dit is geheel in lijn met de ontwikkeling van blockchain-technologie als vitaal onderdeel in gedistribueerde computing.

Qua informatiebeveiliging kan voor de verschillende stadia van netwerk architectuur het volgende model gehanteerd worden:

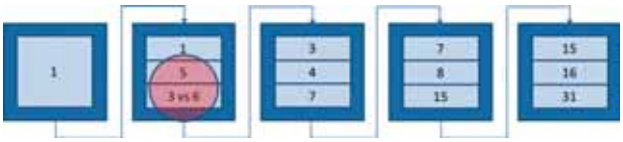
Soort	kwetsbaarheid	Niveau kwetsbaarheid	Kosten Informatiebeveiliging
Mainframe	-	Admin	--
Client/Server	++	Admin, end-user hardware (patch)	++
Cloud computing	+	Admin end-user	+
Distributed and Edge computing	--	enduser	-

Kwetsbaarheden

Volgens dit model dalen de kosten voor informatiebeveiliging bij een gedistribueerd model, omdat de invloed van onder andere de admin, als trusted third party, wordt verminderd.

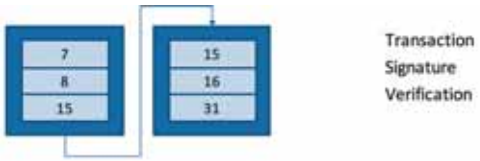
De blockchain en hoe het werkt?

Waarom het de blockchain heet, weet niemand. Het bekt lekker, maar het hadden ook cirkels of rechthoeken kunnen zijn, maar dat terzijde.



De karakteristiek van de blockchain is dat de output van het eerste blok, de input vormt voor het tweede blok enzovoorts. Het eerste blok wordt het zogenaamde Genesis-blok genoemd. Het is de eerste transactie die wordt vastgelegd in de blockchain. Elk blok is volledig versleuteld, gehashed en omdat alle blokken aan elkaar gerelateerd zijn, is het onmogelijk om de ketting te verbreken door één blok te hacken zonder alle andere blokken te herschrijven. Daarvoor heb je onder andere de private-key van anderen nodig. Omdat de blockchain niet op één node draait, maar bijvoorbeeld in het geval van Bitcoin op meer dan 17.000 nodes, moet een aanvaller dus op 17.000 nodes op hetzelfde tijdstip een volledige herschrijving van de blockchain zien te bewerkstelligen om één transactie te manipuleren. Dat is met de huidige computerkracht onmogelijk. Wellicht dat quantum computing roet in het eten kan gooien, maar ook hiertegen zijn inmiddels 'quantumproof' algoritmes op de markt.

Reinier van der Drift is co-founder van Tymlez. Sinds midden jaren '90 heeft Reinier zich toegelegd op sterke authenticatie en identity management. In 2015 verkocht hij zijn softwarebedrijf Authasas aan het Engelse beursgenoteerde Microfocus. Sindsdien houdt Reinier zich bezig met Tymlez, een bedrijf dat een enterprise ready blockchain development platform ontwikkelt en op de markt brengt. Reinier is bereikbaar via reinier.vanderdrift@tymlez.com.



sign("Hello World", User 's private key) = n67n54n6l10xf15
sign("Hello World!", User's private key) = vk34jxl140501025

verify("n67n54n6l10xf15", "Hello World", User 's public key) = valid or invalid

Consensusprotocollen

De integriteit en het onderhoud van blockchains wordt gedaan door consensusprotocollen. Er zijn verschillende consensusprotocollen en naast het eerder aangehaalde 'proof of work'-protocol, zijn de twee belangrijkste 'proof of stake' en 'majority voting'. Het concept van consensusprotocollen in computernetwerken is niet nieuw. De inmiddels bijna vijftig jaar oude Boeing 747 heeft vijf boordcomputers die elk individueel de koersbewegingen van de piloot analyseren en via een 'majority voting' consensusprotocol tot overeenstemming komen alvorens de koersbeweging wordt ingezet. De consensusprotocollen kunnen per use-case verschillen. De protocollen zorgen ervoor dat de transacties worden gevalideerd en bijgeschreven in de blockchain. In het geval van cryptocurrencies wordt dat gedaan door zogenaamde miners. Miners zetten daarvoor hun krachtige computers in, wat geld kost natuurlijk. Via een loterijsysteem, wordt een pool van miners gevraagd om een cryptografische puzzel op te lossen. Voor hun diensten worden zij betaald in de betreffende currency, die ze vervolgens kunnen verhandelen.

Mining

'Mining' is een gedistribueerd consensussysteem dat wordt gebruikt om transacties in de blockchain op te nemen. Het dwingt een chronologische volgorde in de blockchain af, beschermt de neutraliteit van het netwerk, en maakt het mogelijk dat verschillende computers overeenstemming bereiken over de toestand van het systeem. Om te worden bevestigd, moeten de transacties worden verpakt in een blok dat aan zeer strikte cryptografische regels moet voldoen die door het netwerk worden gecontroleerd. Deze regels voorkomen dat voorgaande blokken kunnen worden gewijzigd, omdat daarmee alle volgende blokken ongeldig zouden worden. 'Mining' creëert ook het equivalent van een concurrerende loterij en verhindert daarmee dat een individu zelf nieuwe blokken kan laten opnemen in de blockchain. Op deze manier kan een individu geen controle krijgen over wat wordt opgenomen in de blockchain of delen van de blockchain vervangen om de eigen transactie terug te draaien.

Dus wat is de blockchain?

Een nieuwe vorm van informatietechnologie, een gedecentraliseerd systeem van 'checks and balances', een infrastructuur, een organisatiesysteem dat universeel is en op wereldschaal [3].

Wat kunnen we met blockchain-technologie?

Zoals eerder gezegd, richt blockchain-technologie zich primair op het elimineren van de Trusted Third Party. Het is een peer-to-peer technologie die de TTP uitsluit. Daardoor kunnen (business)processen opnieuw worden ingericht en kan een grote mate van efficiency bereikt worden. Een goed voorbeeld daarvan is de financiële sector.
Jan wil graag €100 overmaken naar Piet. Op dit moment loopt dat via de bank die, als TTP, de feitelijke transactie namens partijen uitvoert en daarvoor betaald krijgt. In geval van blockchain-technologie is de uitkomst nog steeds dat Jan €100 overmaakt aan Piet, maar de hele keten van banken en correspondent banken wordt uitgesloten. Jan maakt rechtstreeks het geld van zijn wallet over naar die van Piet. Voor de bank betekent dit dat zij haar directe invloed op de klant kwijtraakt. Zij weet niet alles meer over haar klant en daarmee wordt zij in het hart geraakt van haar businessmodel.

Als men kijkt naar de basisfunctionaliteit van blockchain-technologie dan zijn dit drie functies:

1. Data logging
2. Smart contract
3. Digitaal eigenaarschap

Met deze drie functionaliteiten kan men in de business processen herdefiniëren en –inrichten.

http://www.amazon.com/Bitcoin-Blueprint-New-World-Currencey/dp/1491920491

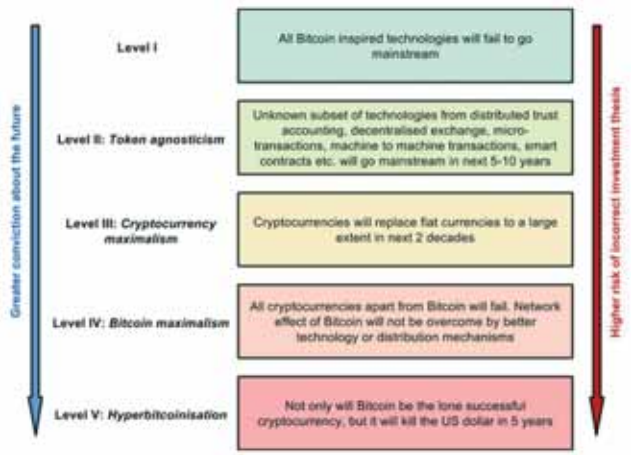
Business processen

Het grootste voordeel komt te liggen bij de gebruiker. Hij krijgt de controle. Hij gaat bepalen aan wie, waarvoor, wanneer en voor hoelang hij data beschikbaar gaat stellen. Dat gaat huidige businessmodellen volledig op zijn kop zetten. De Facebooks en Googles van deze wereld kunnen hun borst nat maken. Maar ook bedrijven als Microsoft en SAP moeten zich achter de oren gaan krabben. Disruptie gaat nu eenmaal

gepaard met snelheid van handelen. Voor je het weet ben je je marktpositie kwijt.

Toekomst

Hoe gaat de toekomst eruitzien en wat kunnen we op korte en langere termijn verwachten?
Meher Roy [4], een ingenieur bij Novartis, heeft een model waarin hij vijf niveaus heeft uitgewerkt waarlangs de crypto-kolonisatie van de maatschappij zich zou kunnen voltrekken.



Niveaus crypto-kolonisatie (Meher Roy)

Op dit moment focust de ontwikkeling zich op niveau 2 & 3. Er wordt behoorlijk geïnvesteerd door overheden, banken en venture capital-maatschappijen om deze niveaus te bereiken. Het andere model van Roy plaatst de vijf niveaus in perspectief van technologie en risico's.

Belief / bet	Platform opportunities	Incremental risk	Advantages
Level I	Not Applicable	Not Applicable	Not Applicable
Token agnosticism	Hyperledger, Eris, Codius, Ripple / Stellar	-Lack of solutions for identity and Private Key management -Regulatory uncertainty resulting from end-users controlling transactions -Platform specific flaws like weak consensus algorithm	-Applicable to all assets including fiat money, shares and cryptocurrencies -Can replicate all applications pioneered by cryptocurrency community -Relative compatibility with existing regulations
Cryptocurrency maximalism	Bitcoin, Ethereum, Tendermint, Pebble, Ripple / Stellar (partially) etc.	-Societal inertia to new forms of value holds massive network effect -System that possesses sound monetary policy and consensus method, fast transaction speed and is scalable appears late -Associated political ideologies prevent mainstream growth	-Market segment dissatisfied with conventional banking system is a ready market -Significant public interest for the time being
Bitcoin maximalism	Sidechains	-New technologies that improve on network maintenance cost, transaction speed and scalability outcompete Bitcoin	-Significant first mover advantage for Bitcoin
Hyperbitcoinisation	Not Applicable	-Opinion proves to be a delusion	-None

Technologiën en risico's (Meher Roy)

Dus het korte termijnperspectief ligt bij de permissioned blockchain, terwijl maximalisatie van cryptocurrencies op langere termijn wordt voorzien.

De blockchain als concept zal disruptief blijken voor veel bestaande business-modellen

Conclusie

De blockchain als concept zal disruptief blijken voor veel bestaande businessmodellen. Trust gaat op een nieuwe manier georganiseerd worden. Voor de ICT-community gaan spannende en interessante tijden aanbreken. Welke reuzen gaan ten onder en welke nieuwe toekomstige giganten gaan opstaan? Het begint bij het ontdekken van de mogelijkheden van deze technologie. En juist daarom worden er nu zoveel pilots en PoC's gedaan met blockchain. Welke keuzes gaat u maken?

Referenties

[1] www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=nl
[2] http://a16z.com/2016/12/16/the-end-of-cloud-computing/
[3] www.melanieswan.com/documents/BlockchainThinking_SWAN.pdf
[4] https://medium.com/@Meher/a-model-to-makes-sense-of-beliefs-and-associated-crypto-finance-platforms-f761a7d782cb#.qdj2kwp4x

Links

Explaining Bitcoin Mining: https://youtu.be/iyq4od8MBoE
De blockchain uitgelegd: https://youtu.be/gKC2oelL878
De blockchain is eating Wall Street (TED Talk Alex Tapscott)_: https://youtu.be/WnEYakUxsHU
Website van Melanie Swan: www.melanieswan.com
State of the blockchain: http://www.coindesk.com/research/state-of-blockchain-q3-2016/
EB84 – Tim Swanson: Permissioned Ledgers And The Case For Blockchains Without Bitcoin : https://youtu.be/k3pM8vB2QYc