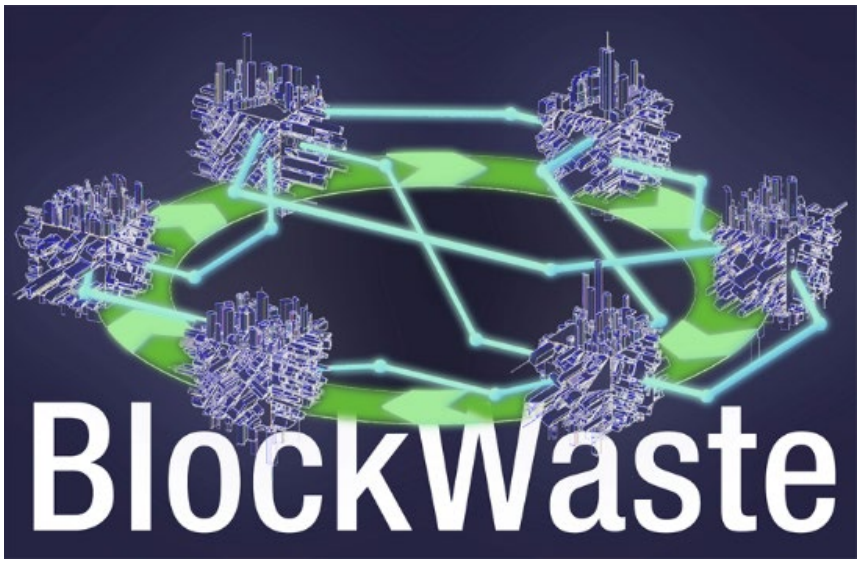
O1.A3 Handboeken voor strategieën voor circulaire economie toegepast op gemeentelijk afvalbeheer met behulp van Blockchain-technologie

Handboek II: Blockchain



Output factsheet:

Financieringsprogramma	Erasmus+ programma van de Europese Unie
Financiering NA	EL01 Stichting Griekse Staatsbeurs (IKY)
Volledige titel van het project	Innovatieve opleiding op basis van Blockchain-technologie toegepast op afvalbeheer - BLOCKWASTE
Veld	KA2 - Samenwerking voor innovatie en uitwisseling van goede praktijken KA203 - Strategische partnerschappen voor het hoger onderwijs
Projectnummer	2020-1-EL01-KA203-079154
Duur van het project	24 maanden
Startdatum project	01-10-2020
Einddatum van het project:	30-09-2022

Uitvoergegevens:

Titel van de output: O1: Leermateriaal voor interdisciplinair Blockchain-MSW

Titel van de taak: O1/A3. Handboeken van strategieën voor circulaire economie toegepast op gemeentelijk afvalbeheer met behulp van Blockchain-technologie

Outputleider: NTUA

Task leader: Saxion UAS

Auteur(s): Christa Barkel, c.barkel@saxion.nl, Saxion UAS, Nederland, Perry Smit, Saxion UAS, p.j.smit.01@saxion.nl, Nederland

Beoordeeld door: Rainer Lenz, rlenz@fh-bielefeld.de, Bielefeld UAS, Duitsland, Paraskevas Tsangaratos, National Technical University of Athens, ptsag@metal.ntua.gr, Greece

Documentcontrole

Versie van het document	Versie	Amendement
V0.1	11/03/2022	Definitieve versie – 29/04/2022

Co-funded by the Erasmus+ Programme of the European Union

Inhoud

Samenvatting v
1 Inleiding 1
1.1 Korte projectbeschrijving 1
1.2 Doelstellingen en methodologische aanpak 2
2 Blockchain grondbeginselen 3
2.1 Inleiding 3
2.1.1 Bitcoin vs bitcoin 4
2.1.2 Peer-to-peer netwerk 4
2.1.3 Client-server-netwerk 5
2.1.4 Hybride netwerken: het geval van Napster 6
2.1.5 Blockchain 7
2.1.6 Dubbele uitgaven 8
2.1.7 Bewijs van werk 9
2.1.8 Decentralisatie 10
2.1.9 Privacy 11
2.1.10 Samenvatting 12
2.2 Blockchain 2.0 en slimme contracten 13
2.2.1 Inleiding 13
2.2.2 Blockchain 1.0 en 2.0 13
2.2.3 Ethereum 13
2.2.4 Ethereum transacties en gas 14
2.2.5 Slimme contracten 14
2.2.6 Gedecentraliseerde toepassingen 15
2.2.7 Gedecentraliseerde autonome organisatie (DAO) 15
3 Soorten Blockchain 17
3.1 Soorten Blockchain volgens het consensusprotocol 17
3.2 Blockchaingovernance en wie met welke rol kan deelnemen 18
3.3 Platforms en consortia 21
4 Cryptocurrencies en tokens 23
4.1 Crypto-economie 23
4.2 Classificatie van Blockchain-tokens 25
4.3 Fondsverwerving tokens 28
5 Gebruik en toepassingen van Blockchain 29
5.1 Bedrijfsmodellen 29

5.2 Blockchaintoepassingen voor ondernemingen 29
5.3 Wanneer heeft welke Blockchain implementatie zin? 34
6 Referenties en bronnen voor verdere lezing 37
Bijlage I - Begrippenlijst 40

Lijst van figuren

Figuur 1: Handboeken BlockWASTE project (de auteurs) 2

Figuur 2: Een weergave van een gedistribueerd netwerk, waarbij de Blockchain is verdeeld over een netwerk van volledige knooppunten (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 1, pagina 14). 4

Figuur 3: Vereenvoudigde beslisboom om al dan niet Blockchain te gebruiken (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 1). 5

Figuur 4: Nieuwsbericht in New York time; Napster moet dicht blijven, 12 juli 2001. 6

Figuur 5: Napster-netwerk. (1) Computer A zoekt op de centrale indexserver van Napster naar Michael Jackson - Billy Jean. De centrale indexserver van Napster zoekt naar computers die op het netwerk zijn aangesloten en het nummer op hun harde schijf hebben staan. (2) Computer B heeft het nummer. Computers A en B leggen een rechtstreekse peer-to-peer-verbinding, waarna computer A het muziekbestand van computer B downloadt. 7

Figuur 6: Vereenvoudigde weergave van een geldig genesisblok en blok #2 met beide blokken aan elkaar geketend met behulp van de block header hash en de vorige hash. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 3). 8

Figuur 7: Schematische weergave van hoe een transactie aan de Blockchain wordt toegevoegd. De mempool is de plaats waar onbevestigde transacties binnenkomen en worden bewaard. Miners kiezen welke van de transacties uit de mempool zij aan het blok willen toevoegen. Vervolgens proberen zij een cryptografische puzzel op te lossen. Eenmaal opgelost, ontvangen ze een blokbeloning in bitcoins.(Bron: Boek: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 4). 9

Figuur 8: Een overzicht van verschillende Blockchain types, uitgedrukt in permissionless, permissioned, private en public (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 9). 20

Figuur 9: Multidisciplinaire aspecten van cryptoeconomie. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 10). 24

Figuur 10: Dubbel formaat van tokens. Aan de ene kant, om tokens te onderscheiden die worden gebruikt om Blockchain-netwerk te onderhouden vs om eigendom aan te tonen en over te dragen. Anderzijds om onderscheid te maken tussen tokens die inwisselbaar vs. niet inwisselbaar zijn. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 10). 25

Figuur 11: Overzicht van 67 live enterprise Blockchain netwerken en in welke sectoren ze vallen (Bron: Rauchs, Blandin, Bear, McKeon, 2019). 30

Figuur 12: Vereenvoudigde beslisboom om al dan niet Blockchain te gebruiken (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021). 36

Lijst van afkortingen

Afkorting	Definitie
CBDC	Centrale Bank Digitale Munt
CBDC	Centrale Bank Digitale Munt
DAO	Gedecentraliseerde autonome organisatie
dApps	Gedecentraliseerde toepassingen
DLT	Gedistribueerde grootboektechnologie
dPoS	Gedelegeerd bewijs van inzet
ERC-20 (protocol)	Ethereum Request For Comments 20 (protocol)
ICO	Initial Coin Offering
IEO	Eerste beursgang
MSW	Beheer van gemeentelijk vast afval
NFT	Niet-fungibele penning
P2P	Peer-to-Peer
PoS	Bewijs van inzet
PvA	Bewijs van autoriteit
SPOF	Eén enkel foutpunt
STO	Security Token Offering
TTP	Vertrouwde derde partij

Samenvatting

In dit handboek wordt Blockchain vanuit een breed scala aan perspectieven benaderd. De verwachting is dat dit de lezer zal helpen de relevantie van Blockchain beter te ontleden en een dieper inzicht te krijgen in de mogelijkheden ervan. De eerste basisbeginselen worden toegelicht met Bitcoin als voorbeeld. Bitcoin is de eerste toepassing die gebruik maakt van Blockchain. Bitcoin maakt gebruik van een gedecentraliseerd netwerk, waarin alle individuen die willen deelnemen aan het Bitcoin-besluitvormingsproces samen deelnemen aan de besluitvorming. De Bitcoin-code is open source, waardoor iedereen de broncode gemakkelijk kan bekijken, kopiëren en bewerken naar eigen inzicht, waardoor nieuwe experimenten met andere, wellicht betere vormen van cryptocurrency of andere toepassingen en andere vormen van consensus kunnen ontstaan. Hoewel Bitcoin wordt gebruikt als voorbeeld ter verduidelijking, is het belangrijk op te merken dat niet alleen het financiële systeem door Blockchain wordt beïnvloed. De onderliggende technologie van Blockchain biedt nieuwe mogelijkheden om andere industrieën te transformeren, waaronder die van het gemeentelijk beheer van vast afval.

Dit handboek begint met een uitleg van Blockchain en de kenmerken ervan. Er wordt een duidelijker onderscheid gemaakt tussen de cryptocurrency Bitcoin en het Bitcoin-netwerk en het consensusmechanisme van Bitcoin, Proof-of-Work, wordt uitgelegd. Naast de basisbeginselen van Blockchain die in dit handboek worden uitgelegd aan de hand van Bitcoin, verschuift de aandacht naar een nieuwere generatie Blockchains die specifiek zijn ontworpen om een overvloed aan andere soorten gedecentraliseerde toepassingen of dApp's te creëren. Een specifieke Blockchain waarop de aandacht wordt gericht is Ethereum, dat als eerste de programmering van Smart Contracts mogelijk maakte. Een Smart Contract is gedecentraliseerde automatisering en kan worden gedefinieerd als een contract met bepaalde voorwaarden die in code zijn vastgelegd. Het contract is self-executing, omdat het passende overeenkomstige acties uitvoert wanneer aan de voorwaarden is voldaan.

Verder worden in dit handboek twee fenomenen van Blockchain kort toegelicht: gedecentraliseerde applicaties (dApps) en gedecentraliseerde autonome organisaties (DAO).

Blockchain kan worden onderverdeeld in zijn types vanuit drie perspectieven, consensusprotocol, governance en types van samenwerking tussen Blockchain-systemen. Consensusprotocollen zijn essentieel om het vertrouwen tussen verschillende deelnemers binnen een gedistribueerd netwerk te waarborgen. Er moet vertrouwen zijn dat de deelnemers niet corrupt zijn en dat de gegevens die onder hen worden gedeeld niet corrupt zijn. Vervolgens moet een Blockchain, zoals elk samenwerkingsverband, worden beheerd en gecontroleerd via een Blockchain-governancestructuur. Keuzes tussen de verschillende soorten Blockchains zijn van invloed op de controle van de organisatie. Hoe meer vertrouwen er is in het gedecentraliseerde karakter van de Blockchain, hoe gemakkelijker het is om deel te nemen. Hoe meer vertrouwen er is dat validators als onbekenden kunnen deelnemen aan de consensusvorming, hoe transparanter het systeem.

Ter afsluiting van de drie perspectieven zijn er verschillende soorten samenwerking tussen Blockchain-systemen. Blockchain waarbij verschillende bedrijven en derden samenwerken zonder dat een centrale gebruiker deze Blockchain controleert, wordt een Enterprise Blockchain genoemd. Om een dergelijke Enterprise Blockchain te bouwen, gebruiken bedrijven Blockchain-platforms. Deze platforms stellen gebruikers in staat om applicaties te schrijven met behulp van bepaalde technologieën. Rond deze platforms zijn verschillende

samenwerkingsverbanden georganiseerd. Platformen zijn de derde en laatste manier waarop we hier naar verschillende soorten Blockchains kijken.

Een van de grote uitvindingen van Satoshi Nakamoto is de combinatie van reeds bestaande technologieën met een beloningssysteem dat een gedecentraliseerd netwerk draaiende houdt: crypto-economie. Het centrale idee achter crypto-economie binnen Blockchain is dat er protocollen worden ontwikkeld die mensen stimuleren om op zo'n manier aan het netwerk deel te nemen dat de waarde van het netwerk voor de deelnemers wordt gemaximaliseerd.

Een crypto-token kan worden gecreëerd op een Blockchain en ook een verhandelbaar activum vertegenwoordigen. Soms worden tokens gecreëerd om een project te financieren. Het proces van tokencreatie wordt tokenization genoemd. Door deze tokens te verhandelen kan het eigendom van de onderliggende activa worden overgedragen. In dit handboek worden verschillende soorten tokens en hun gebruik uitgelegd.

Ter afsluiting worden drie voorbeelden gegeven van het gebruik en de toepassing van Blockchain, inclusief de interpretatie van enkele cruciale voorwaarden voor een succesvolle implementatie van Blockchain.

1 Inleiding

1.1 Korte projectbeschrijving

Het BlockWASTE-project wil de interoperabiliteit tussen afvalbeheer en Blockchain-technologie aanpakken en de juiste behandeling ervan bevorderen door middel van educatieve opleidingen, zodat de verzamelde gegevens worden gedeeld binnen een veilige omgeving, waar geen ruimte is voor onzekerheid en wantrouwen tussen alle betrokken partijen. Daartoe zijn de doelstellingen van het BlockWASTE-project als volgt:

- Onderzoek verrichten naar vast afval dat in steden wordt geproduceerd en hoe het wordt beheerd, zodat een informatiebasis van goede praktijken kan worden gecreëerd, teneinde afval opnieuw in de waardeketen te brengen en het idee van intelligente circulaire steden te bevorderen.
- De voordelen van de Blockchain-technologie binnen het gemeentelijke afvalbeheer (MSW) in kaart brengen.
- Een studieplan opstellen dat de opleiding van docenten en professionals van organisaties en bedrijven uit de sector mogelijk maakt, in de overlapping van de domeinen Afvalbeheer, Circulaire Economie en Blockchaintechnologie.
- Een interactief instrument ontwikkelen op basis van Blockchain-technologie, waarmee het beheer van gegevens afkomstig van stedelijk afval in de praktijk kan worden gebracht, zodat de manier waarop de gegevens in de Blockchain worden geïmplementeerd zichtbaar wordt en gebruikers verschillende vormen van beheer kunnen evalueren.

BlockWASTE wil transnationaal nieuwe onderwijsinhoud implementeren met als doel de studenten in de partnerlanden op te leiden en hen de nodige basisvaardigheden bij te brengen die hen in staat stellen professioneel op te treden als toekomstige werknemers in de sector, waarbij digitale competenties worden toegevoegd die vereist zijn door bedrijven die het proces van digitale transformatie omarmen. In die zin is het project gericht op:

- Ondernemingen en KMO's, IT-professionals, urbanisten en afvalbeheerders.
- Universiteiten (professoren, studenten en onderzoekers).
- Openbare instanties

Het project omvat de volgende vier intellectuele outputs:

- O1. Leermateriaal voor interdisciplinair Blockchain-MSW
- O2. Europees gemeenschappelijk curriculum inzake VHA dat Blockchain-technologieën toepast op Circulaire Economie-strategieën
- O3. E-learning tool gebaseerd op Blockchain-MSW gericht op Circulaire Economie
- O4. BlockWASTE Open Educational Resource (OER)

Dit document beschrijft en verklaart de basisprincipes van Blockchain. Het beschrijft wat Blockchain is, wanneer je het kunt gebruiken, uit welke componenten een Blockchain is opgebouwd, welke Blockchain technologieën worden gebruikt en het geeft een beschrijving van verschillende succesvolle Blockchain toepassingen.

1.2 Doelstellingen en methodologische aanpak

Het doel van dit handboek "Blockchain" is om professionals in de afvalverwerkingssector te begeleiden bij het implementeren van IoT en Blockchain-technologie als strategieën van Circulaire Economie. Daarom is het gericht tot praktijkmensen die de voordelen kennen van het gebruik van Blockchain-technologie. De drie gezamenlijke handboeken van dit Blockwaste-project zijn bedoeld om de lezers voldoende kennis bij te brengen over het potentieel van Blockchain-technologie om bij te dragen aan meer circulariteit in het beheer van gemeentelijk vast afval. Handboek 1 (Blockchain) en handboek 2 (Circulaire economie) moeten worden gezien als een beknopt compendium en geven een overzicht van de essentiële inhoud van handboek 3 (Blockchain gebaseerd afvalbeheer) - zie fig. 1.

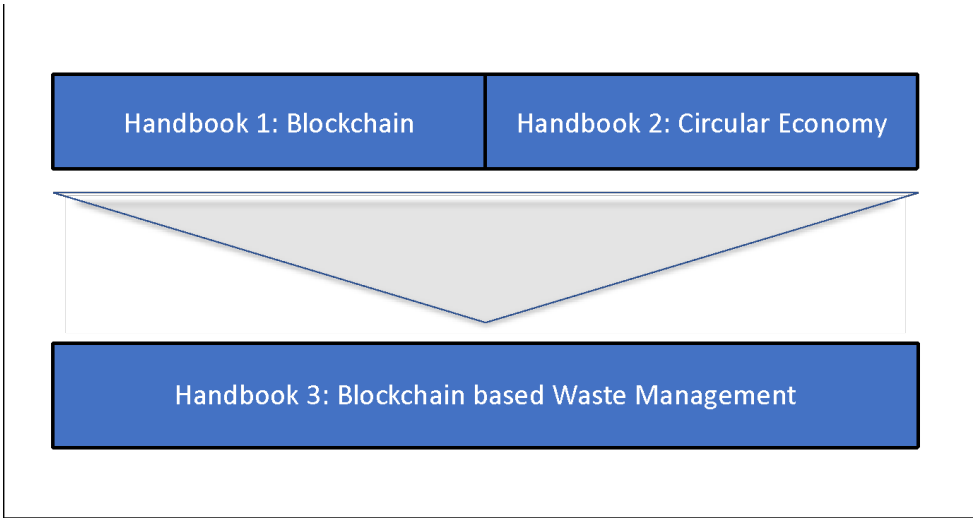


Figure 1:Handboeken BlockWASTE project (de auteurs)

De structuur van het handboek volgt een deductieve logica door in het eerste deel (hoofdstuk 1 tot en met 4) een korte geschiedenis van Blockchain aan de hand van Bitcoin en de basisprincipes van Blockchain-technologie te presenteren Het tweede deel van het handboek (hoofdstuk 5) bevat een duidelijke leidraad voor gebruik en toepassingen van Blockchain-technologie.

2 Blockchain grondbeginselen

Blockchain-principes begrijpen via Bitcoin

"Sorry dat ik een natte deken ben. Een beschrijving schrijven voor dit ding voor een algemeen publiek is verdomd moeilijk. Er is niets om het aan te relateren."
- Satoshi Nakamoto (2010)

2.1 Inleiding

Leerdoelen

- Blockchain op het meest basale niveau door te kijken naar Bitcoin.
- Blockchain is in wezen een gedistribueerd grootboek waarin je gegevens kunt opslaan.
- De verschillen tussen een Blockchain-netwerk en een gecentraliseerd netwerk.

Inleiding

Op 31 oktober 2008 werd onder de naam Satoshi Nakamoto een e-mail gestuurd naar de mailinglijst voor cryptografie.[1] De e-mail bevatte een verwijzing naar een **white paper** met de titel *Bitcoin: A Peer-to-Peer Electronic Cash System*. De white paper die hij bij de aankondiging voegde is een document van slechts 9 pagina's waarin de technische werking van Bitcoin wordt beschreven. Dit systeem maakt het mogelijk om online betalingen naar andere partijen te sturen, zonder dat daar een financiële instelling voor nodig is.

De belangrijkste kenmerken van dit betalingssysteem, volgens Satoshi:

1. Dubbele uitgaven worden voorkomen met een peer-to-peer netwerk.
2. Geen munt of andere vertrouwde partijen.
3. Deelnemers kunnen anoniem zijn.
4. Nieuwe munten worden gemaakt van Hashcash-stijl proof-of-work.
5. De proof-of-work voor het genereren van nieuwe munten voedt ook het netwerk om dubbel spenden te voorkomen.

Technische termen als double-spending, peer-to-peer netwerk, Proof-of-Work, Hashcash, timestamps, hashing, en digitale handtekeningen in de e-mail maken het moeilijk voor het grote publiek om Bitcoin of meer in het algemeen Blockchain te begrijpen. Vooral in die tijd, toen er voor de meeste mensen niets was om het mee in verband te brengen. In dit hoofdstuk bespreken we Bitcoin als middel om de basisbeginselen van Blockchain te begrijpen.

[1] De oorspronkelijke e-mail is te vinden op: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

2.1.1 Bitcoin vs bitcoin

In het algemeen wordt onderscheid gemaakt tussen (kleine letters) bitcoin, het digitale geld dat ook wel cryptocurrency wordt genoemd, en (hoofdletters) Bitcoin, het onderliggende financiële netwerk waarmee bitcoins kunnen worden verstuurd en ontvangen.

2.1.2 Peer-to-peer netwerk

De computers, ook wel ***knooppunten*** genoemd, die dit financiële netwerk beheren, hebben toegang tot een grootboek waarin alle Bitcoin-transacties worden bijgehouden. Dit Bitcoin-grootboek is een register van alle geldige transacties die ooit zijn verzonden naar het netwerk, de onderliggende infrastructuur die bestaat uit de knooppunten die alle Bitcoin-transacties bijhouden, valideren en van een tijdstempel voorzien. Wij noemen dit netwerk een ***peer-2-peer (P2P) netwerk***.

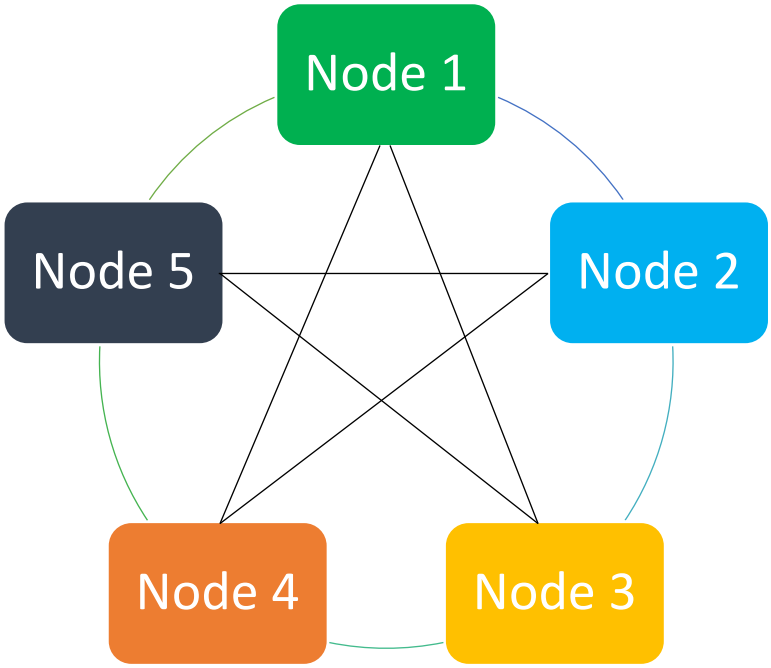


Figure 2: Een weergave van een gedistribueerd netwerk, waarbij de Blockchain is verdeeld over een netwerk van volledige knooppunten (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 1, pagina 14).

Een P2P-netwerk is een netwerk van knooppunten, vaak een computer, die even bevoorrecht zijn. Elk knooppunt kan zowel dienstverlener als dienstafnemer zijn. Iedereen heeft toegang tot het Bitcoin-netwerk en is vrij om een node op het netwerk te beheren. Gespecialiseerde knooppunten op het netwerk, ook wel ***volledige knooppunten genoemd***, houden de hele transactiegeschiedenis bij. Om het hele netwerk en de bijbehorende transactiegeschiedenis plat te leggen, zou men alle nodes moeten uitschakelen, wat bijna onmogelijk is als het netwerk uit veel nodes bestaat.

Elke deelnemer aan het netwerk volgt het Bitcoin-protocol. Het Bitcoin-protocol zijn de procedurele regels die gelden voor het Bitcoin-netwerk. Bovendien is er geen tussenpersoon

tussen twee verschillende knooppunten. Dit betekent ook dat er geen centrale partij is die uw transacties kan regelen, tegenhouden en bevriezen. De eliminatie van dergelijke tussenpersonen maakt efficiëntere en goedkopere transacties mogelijk.

2.1.3 Client-server-netwerk

Dit P2P-netwerk staat in contrast met het ***client-server-netwerk*** (werkstation-server-netwerk).

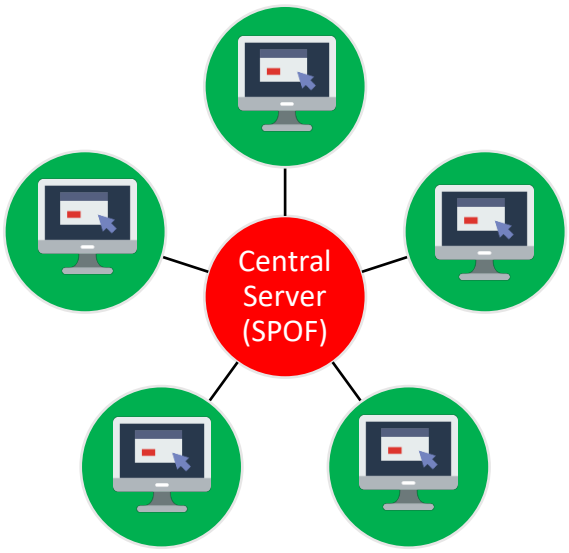


Figure 3:Vereenvoudigde beslisboom om al dan niet Blockchain te gebruiken (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 1).

Een client-server netwerk maakt gebruik van gecentraliseerde servers die diensten, zoals een e-maildienst, verlenen aan de cliënten. De server bevat vaak gegevens en toepassingen. Wanneer cliënten toegang tot deze middelen nodig hebben, kunnen zij een verzoek indienen bij de server. Een zwak punt van client-server netwerken is dat het een ***Single Point Of Failure (SPOF)*** bevat. In dit geval is de SPOF de centrale server. Eenmaal uitgeschakeld, hebben de cliënten geen toegang meer tot de diensten van de server.

De noodzaak om een centrale partij te vertrouwen met uw gegevens en erop te vertrouwen dat de SPOF niet zal falen, maakt het model kwetsbaar. Ook grote gerenommeerde bedrijven kunnen last hebben van een SPOF-netwerkontwerp. Zo was er in 2015 een stroomstoring in één datacenter van PayPal. Als gevolg daarvan hadden veel gebruikers geen toegang meer tot de PayPal-website, konden creditcardtransacties niet meer worden verwerkt, hadden mensen geen toegang meer tot hun persoonlijke rekeninginformatie of werden onjuiste balansen getoond.[2]

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

2.1.4 Hybride netwerken: het geval van Napster

Er bestaan ook hybride netwerken. Een bekend voorbeeld is Napster, een muziekdownloaddienst die eind jaren negentig en begin jaren 2000 bekendheid verwierf.

In 1999 lanceerden de tieners Shawn Fanning en Sean Parker de peer-to-peer dienst voor het delen van bestanden Napster. Napster maakte het mogelijk dat mensen gemakkelijk digitale muziekbestanden van anderen konden delen en downloaden. Het veroorzaakte veel commotie, omdat voor het eerst op grote schaal gratis muziek met elkaar werd gedeeld. Met Napster konden mensen losse nummers downloaden en beluisteren. Voorheen moest je, als je een enkel nummer wilde hebben, een volledig album kopen. In 2001 werd Napster uiteindelijk gesloten na een rechtszaak met de Recording Industry Association of America, omdat het verspreiden en downloaden van digitale muziekbestanden in strijd werd geacht met de auteurswet. Toch staat Napster nog steeds bekend als een revolutionaire dienst die de muziekindustrie heeft ontwricht. In de Verenigde Staten piekte de cd-verkoop in het jaar 2000, waarna er een scherpe daling optrad - mede door Napster en latere diensten als BitTorrent en Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Figure 4:New York time news item; Napster moet dicht blijven, 12 juli 2001.

Het is bekend dat Napster een P2P netwerk gebruikt. Hoe komt het dat de autoriteiten Napster hebben kunnen platleggen, wat met Bitcoin vrijwel onmogelijk is?

Napster gebruikt een centrale index die bijhoudt welke computer welke bestanden heeft om te delen met andere gebruikers. Als een gebruiker (computer A) wil zoeken naar een nummer zoals Michael Jackson - Billie Jean, wordt een verbinding gemaakt met de index en wordt gezocht op welke computers dit nummer staat. Als uit de index blijkt dat computer B dit nummer heeft, wordt een rechtstreekse peer-to-peer-verbinding gemaakt tussen computers A en B, zodat A het nummer rechtstreeks kan downloaden van de computer van B.

Napster is een gemengd model van client-server en peer-to-peer. Het centrale indexelement is client-server, maar de eigenlijke bestanden worden peer-to-peer gedownload. De centrale

indexserver is een ernstige achilleshiel voor Napster gebleken, omdat deze gemakkelijk kan worden afgesloten, waardoor Napster niet meer werkt. Omdat Napster alleen een centrale indexserver heeft, waarop staat welke computers welke deelbare muziekbestanden hebben, heeft Napster zelf geen muziekbestanden op zijn server staan. Het heeft alleen gebruikers gefaciliteerd om peer-to-peer verbindingen te maken en muziek met elkaar te delen.

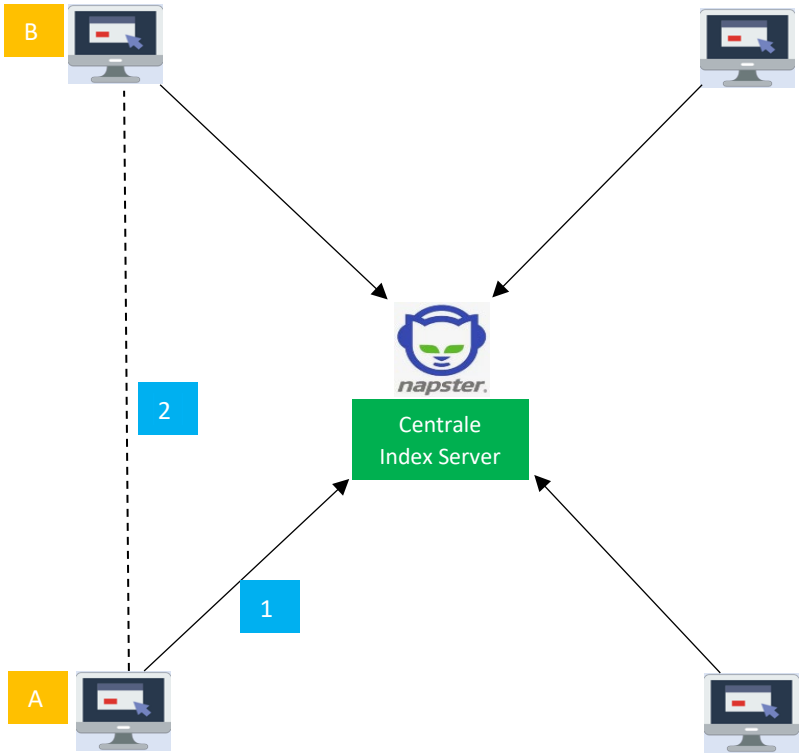


Figure 5:Napster netwerk. (1) Computer A zoekt op de centrale indexserver van Napster naar Michael Jackson - Billy Jean. De centrale indexserver van Napster zoekt naar computers die op het netwerk zijn aangesloten en het nummer op hun harde schijf hebben staan. (2) Computer B heeft het nummer. Computers A en B leggen een rechtstreekse peer-to-peer-verbinding, waarna computer A het muziekbestand van computer B downloadt.

Hoewel het delen van muziekbestanden bij Napster peer-to-peer gebeurt, bevat het ook een centraal serverelement, waardoor het vatbaar is voor aanvallen. In dit geval werd het gesloten door de rechtshandhaving. Bij het Bitcoin-netwerk hebben alle knooppunten een exacte kopie van het openbare grootboek van Bitcoin. Het Bitcoin-netwerk bestaat uit vele knooppunten, die verspreid zijn over de hele wereld, waardoor het moeilijk is ze allemaal te lokaliseren en af te sluiten.

2.1.5 Blockchain

Het openbare grootboek van Bitcoin wordt beschouwd als gedecentraliseerd, omdat het verdeeld is over knooppunten over de hele wereld. Het openbare grootboek van Bitcoin wordt ook wel een keten van blokken of een Blockchain genoemd, die de transactiegegevens bevat. Als we de Blockchain zien als een database waarin informatie wordt vastgelegd, zijn dit de essentiële inherente eigenschappen van een Blockchain:

1. De gegevens worden gerangschikt in gegevensblokken.
2. De blokken zijn oplopend in bloknummers.
3. De gegevens zijn betrouwbaar omdat ze cryptografisch verifieerbaar zijn.

De keten is de transactiedatabase die wordt opgebouwd door knooppunten die deelnemen aan het mijnproces op het Bitcoin-netwerk. De keten wordt onderhouden door een tijdstempelserver, die bewijs genereert voor de chronologische volgorde van transacties. Elk blok bevat een hashverwijzing naar het blok waarop het voortbouwt, waardoor een lineaire volgorde in de tijd ontstaat. Blokken kunnen worden gezien als de afzonderlijke pagina's van een logboek.

Miners verwerken voortdurend transacties tot blokken, die zij aan het einde van de keten toevoegen. Het proces waarbij miners nieuwe blokken aan de keten toevoegen, wordt ook wel ***Proof-of-Work genoemd***. Dit proces voorkomt ***dubbel werk***.

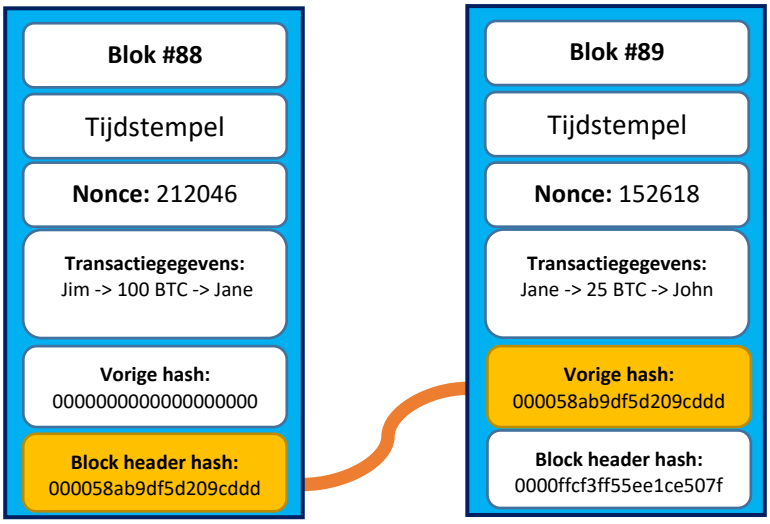


Figure 6:Vereenvoudigde weergave van een geldig genesisblok en blok #2 met beide blokken aan elkaar geketend met behulp van de hash van de block header en de vorige hash. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 3).

2.1.6 Dubbele uitgaven

Een belangrijk probleem dat een peer-to-peer elektronisch financieel systeem moet oplossen, is het probleem van double-spending. Double-spending is het meer dan eens uitgeven van een bitcoin. Bijvoorbeeld, als je 1 bitcoin hebt en die tegelijkertijd uitgeeft aan persoon A en persoon B. Binnen een gecentraliseerd financieel netwerk kan het probleem van double-spending worden opgelost door een ***Trusted Third Party (TTP)*** die het grootboek bijhoudt en alle transacties binnen het grootboek controleert.

Binnen het Bitcoin-netwerk wordt dit probleem opgelost via de economische prikkels en het gebruik van een tijdstempelserver. Miners hebben een sterke prikkel om deze transacties niet in een blok op te nemen, omdat ze het risico lopen dat hun blok door andere miners wordt verworpen, en bovendien medeplichtig zouden zijn aan het plegen van een misdrijf.

2.1.7 Bewijs van werk

Naast het vermijden van dubbel werk is het doel van proof-of-work ook om het netwerk te beschermen tegen aanvallers en om consensus te bereiken over de toestand van het publieke grootboek. Kortom, proof-of-work is een mechanisme waarbij miners computerkracht moeten gebruiken om de juiste waarden te vinden voor een blok waaraan zij werken. Door de juiste hashwaarde te vinden, mogen zij het blok toevoegen aan de Blockchain en ontvangen zij een beloning in bitcoins. Het proces van het vinden van de juiste waarde wordt mining genoemd.

Transacties die naar het netwerk worden gezonden, worden niet rechtstreeks door de miner aan een blok toegevoegd, noch rechtstreeks in het grootboek opgeslagen. Ze komen eerst terecht in een ***geheugenpool*** (mempool) met andere transacties die nog door miners aan een blok moeten worden toegevoegd en die nog door het netwerk moeten worden bevestigd. Je kunt de mempool zien als een wachtruimte voor alle inkomende transacties die nog door het netwerk moeten worden bevestigd. Elke miner heeft zijn eigen mempool en het is mogelijk dat de individuele mempools per miner verschillen. Dat komt omdat er altijd netwerklatentie is binnen een computernetwerk: het duurt altijd even voordat een transactie die naar het netwerk wordt gestuurd, alle miners op het netwerk bereikt.

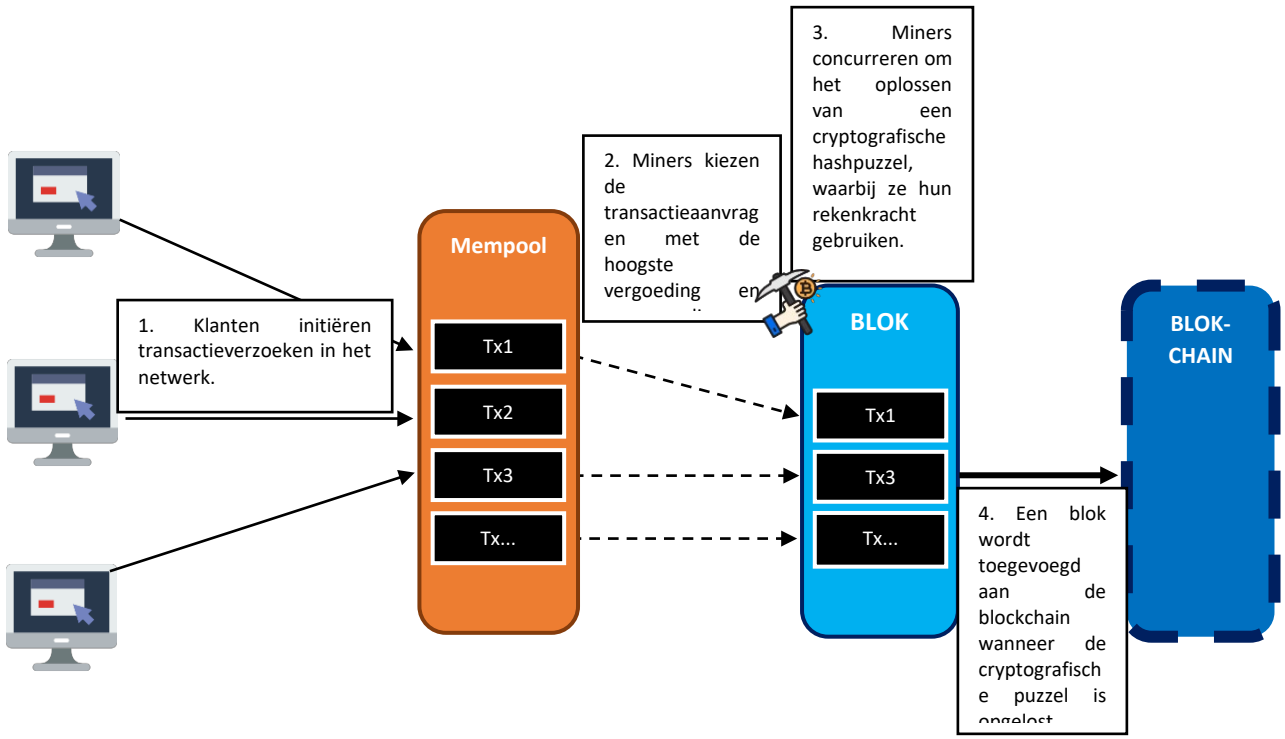


Figure 7:Schematische voorstelling van hoe een transactie wordt toegevoegd aan de Blockchain. De mempool is de plaats waar onbevestigde transacties binnenkomen en worden bewaard. Miners kiezen welke van de transacties uit de mempool zij aan het blok willen toevoegen. Vervolgens proberen zij een cryptografische puzzel op te lossen. Eenmaal opgelost, ontvangen ze een blokbeloning in bitcoins.(Bron: Boek: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 4).

Elke transactie vereist transactiekosten. Miners worden economisch aangemoedigd om de

transacties met de hoogste vergoedingen aan hun blok toe te voegen, omdat zij deze vergoedingen innen wanneer zij als eerste een geldige hash voor het blok vinden. Naast de transactievergoedingen ontvangen mijnwerkers ook een blokbeloning, die elke 210.000 blokken halveert.

Het systeem is veilig zolang eerlijke knooppunten gezamenlijk meer rekenkracht beheersen dan een samenwerkende groep aanvallende knooppunten.

2.1.8 Decentralisatie

De termen "gedecentraliseerd netwerk" en "gedistribueerd netwerk" worden vaak door elkaar gebruikt.[3] Decentralisatie voorziet in een ander belangrijk veiligheidskenmerk met betrekking tot de vernietiging van een enkel knooppunt dat de gegevens als een SPOF host. De gebruikelijke oplossing die ondernemingen hebben is om meerdere kopieën te bewaren voor hun hele systeem/applicatie, gehost in datacentra op meerdere locaties. Dit is een enorme kostenverdubbeling die nodig is voor de beveiliging van gegevens die Bitcoin bereikt alleen al door zijn eigen architectonische ontwerp.

- **Een gedecentraliseerde Blockchain vereist bevestigingen van nieuwe gegevens van andere knooppunten**

Met een gecentraliseerde server is het relatief eenvoudig om nieuwe gegevensinjecties in de database op te nemen. De nieuwe gegevens hoeven slechts door één partij te worden toegevoegd. Bij een gedecentraliseerd netwerk ligt dat anders. Als de nieuwe gegevens aan een Blockchain worden toegevoegd door een miner, moeten deze gegevens nog worden geverifieerd door andere volledige nodes en vervolgens ook worden opgenomen in de Blockchains die door andere nodes worden gehost.

- **Een gedecentraliseerde Blockchain vereist consensus**

Hoe zit het met nieuwe updates van het netwerkprotocol? Een gedecentraliseerde Blockchain vereist consensus voor updates en afspraken over de juiste staat van de Blockchain.

- **Een gedecentraliseerde Blockchain is moeilijk te hacken**

Aangezien de Blockchain wordt bijgehouden op verschillende knooppunten die zich op verschillende plaatsen in de wereld kunnen bevinden, is het moeilijk om de controle over het netwerk over te nemen. Om het netwerk te controleren, moet u de langste keten kunnen creëren, wat alleen kan worden bereikt door een meerderheid aan rekenkracht te hebben. Daarmee kun je sneller geldige blokhashes vinden dan de rest van het netwerk samen. Een aanval gebaseerd op meerderheidsrekenkracht wordt ook wel een ***51%-aanval genoemd***.[4] Met een 51%-aanval kunt u dubbel spenden.

---

[3] Omdat de Blockchain een database is die over verschillende servers is verspreid, wordt deze technologie ook wel een ***Distributed Ledger Technology*** (DLT) genoemd. Blockchain kan worden beschouwd als een DLT, maar een DLT hoeft niet altijd een Blockchain te zijn.

[4] Hoewel de 51%-aanval de bekendste is, zijn er ook vele andere aanvallen mogelijk. Reguliere aanvallen die voorkomen op gecentraliseerde netwerken, zoals corruptie van kernontwikkelaars, bugs in

- **Een gedecentraliseerde Blockchain bemoeilijkt censuur en fraude**

De Blockchain is, mits ver en wijd genoeg verspreid, meer fraudebestendig. Het is echter wel mogelijk om gegevens te veranderen of te verwijderen als er binnen het netwerk consensus bestaat om dit te doen. Als we aannemen dat het netwerk goed gedecentraliseerd is, kunnen we stellen dat censuur van de Blockchain moeilijk te realiseren is.

2.1.9 Privacy

Satoshi Nakamoto verklaarde bij zijn eerste aankondiging van het Bitcoin-netwerk dat bitcoin anoniem is, maar dat is eigenlijk niet waar. Bitcoin is pseudoniem. Dat betekent dat het privé is, maar niet anoniem. Het publiceert alle transacties in duidelijke tekst op een openbare Blockchain, zodat iedereen deze kan controleren en er zaken als machine learning algoritmes op kan loslaten om analyses uit te voeren. Het is echter privé, wat betekent dat tenzij er een noodzaak is om het te weten (zoals een gerechtelijk bevel) en als de gebruiker het gebruikt met de bedoeling zijn financiële transactie privé te houden (door zijn openbare adressen niet meermaals te hergebruiken), de privacy is ingebouwd.

Privacy wordt nog steeds gehandhaafd door de publieke sleutels en het bijbehorende portefeuilleadres pseudoniem te houden. Dankzij het openbare grootboek kan iedereen zien welk adres welke transactie heeft gedaan, maar zolang de adressen onbekend zijn en niet gekoppeld aan uw persoonlijke gegevens, kunt u vrij "anoniem" transacties verrichten.

In de Bitcoin whitepaper vermeldde Satoshi ook dat als extra firewall om de privacy te waarborgen, voor elke transactie een nieuw sleutelpaar moet worden gebruikt om te voorkomen dat ze worden gekoppeld aan een gemeenschappelijke eigenaar. Enige koppeling is nog steeds onvermijdelijk bij transacties met meerdere ingangen, die noodzakelijkerwijs onthullen dat hun ingangen eigendom waren van dezelfde eigenaar. Het risico is dat, als de eigenaar van een sleutel bekend wordt, het koppelen andere transacties aan het licht kan brengen die van dezelfde eigenaar waren.

De gangbare opvatting dat Bitcoin een anonieme munt is, is dus feitelijk onjuist. Integendeel, het werkt als een transparant open grootboek en dat heeft ruimte geschapen voor een hele reeks nieuwe cryptocurrencies die gericht zijn op anonimiteit, zoals monero, zcash en enkele andere. Veel landen werken eigenlijk al actief aan wetgeving.

Het traditionele bankmodel bereikt een niveau van privacy door de toegang tot informatie te beperken tot de betrokken partijen en de vertrouwde derde partij. De noodzaak om alle transacties openbaar aan te kondigen sluit deze methode uit, maar de privacy kan toch worden gehandhaafd door de informatiestroom op een andere plaats te onderbreken: door de publieke sleutels anoniem te houden. Het publiek kan zien dat iemand een bedrag naar iemand anders stuurt, maar zonder informatie die de transactie aan iemand koppelt. Dit is vergelijkbaar met het informatieniveau dat wordt vrijgegeven door effectenbeurzen, waar het tijdstip en de omvang van individuele transacties, de "tape", openbaar wordt gemaakt, maar zonder te vertellen wie de partijen waren.

verkeerd geschreven code, of het stelen van sleutels die toegang geven tot servers komen ook voor bij Blockchains.

2.1.10 Samenvatting

Hoewel er veel verschillende soorten Blockchains zijn en met verschillende niveaus van decentralisatie, kunnen wij concluderen dat in het algemeen een gedecentraliseerd Blockchain-netwerk de volgende kenmerken heeft:

1. Er is geen Single Point of Failure (SPOF).
2. Nieuwe gegevens moeten door andere knooppunten worden bevestigd.
3. Een vorm van consensus is vereist om updates uit te voeren en het eens te worden over de correcte toestand van de Blockchain.
4. Het is moeilijk te hacken.
5. Het maakt het moeilijker om de gegevens op de Blockchain te censureren of te wijzigen.
6. Het is een peer-to-peer netwerk, waarvoor geen vertrouwen in een centrale partij nodig is.

Slotopmerkingen

- Blockchains verschillen van traditionele databases.
- De reden dat Napster faalde is dat het een SPOF had. Een Blockchain daarentegen heeft geen SPOF en is daarom moeilijker uit te schakelen.
- Een Blockchain is een peer-to-peer netwerk.

Gebruikte pictogrammen

Computer gemaakt door Prettycons van www.flaticon.com

De mijne is gemaakt door Strip van www.flaticon.com

2.2 Blockchain 2.0 en slimme contracten

"We willen een hele reeks bedrijven: digitale titels, digitale media-activa, digitale aandelen en obligaties, digitale crowdfunding, digitale verzekeringen. Als je online vertrouwen hebt zoals de Blockchain biedt, kun je veld na veld opnieuw uitvinden."
- Marc Andreessen (2014)

2.2.1 Inleiding

Leerdoelen

- Wat Blockchain 1.0 is en waarom er behoefte is aan Blockchain 2.0.
- Ethereum is een voorbeeld van Blockchain 2.0.
- Wat slimme contracten zijn.
- Wat gedecentraliseerde applicaties (dApps) zijn.
- Wat gedecentraliseerde autonome organisaties (DAO's) zijn.

Inleiding

In het vorige hoofdstuk werden voornamelijk de basisbeginselen van Blockchain besproken aan de hand van Bitcoin. In dit hoofdstuk verschuiven we onze aandacht naar een nieuwere generatie Blockchains die specifiek bedoeld zijn om een overvloed aan andere soorten gedecentraliseerde toepassingen of dApps te creëren. Een specifieke Blockchain waar we ons op richten is Ethereum, dat zichzelf ook aanprijst als 's werelds gedecentraliseerde computer.

2.2.2 Blockchain 1.0 en 2.0

De eerste generatie Blockchains staat ook bekend als ***Blockchain 1.0***, die vooral gericht is op digitaal geld. Vitalik Buterin had het idee om een nieuwe Blockchain te ontwikkelen, Ethereum, waarop men nieuwe coins, contracten met voorwaarden en eisen en zelfs volwaardige ***gedecentraliseerde applicaties*** (dApps) kon creëren. Blockchains met dergelijke mogelijkheden worden ook wel 2e generatie Blockchains genoemd: ***Blockchain 2.0***.[5]

2.2.3 Ethereum

Ethereum werd voor het eerst geïntroduceerd door Vitalik Buterin in "Ethereum White Paper: a next generation Smart Contract & decentralized Application Platform" (2013). In het witboek legt Buterin uit dat Bitcoin kan worden omschreven als een "first-to-file systeem" waarbij de volgorde van de transacties cruciaal is. Technisch gezien kan Bitcoin worden beschouwd als een eenvoudig toestandsovergangssysteem waarbij (a) de "toestand" bestaat uit de eigendomsstatus van alle bestaande bitcoins en (b) de "toestandsovergangsfunctie" die een

[5] Dit zijn Blockchains die een cluster van problemen hebben opgelost waar Blockchain 2.0 zich nog mee bezighoudt. Voorbeelden van dergelijke problemen zijn schaalbaarheid, interoperabiliteit, privacy, en duurzaamheid en governance (Ackermann & Meier, p. 1). EOS, Cosmos, Cardano, Avalanche en Terra zijn voorbeelden van Blockchains die als Blockchain 3.0 kunnen worden beschouwd.

toestand en een transactie neemt en als resultaat een nieuwe toestand produceert. Het is echter moeilijk om contracten uit te voeren met betrekking tot de transactie, die meerdere toestanden kan omvatten. Het is bijvoorbeeld nauwelijks mogelijk om een stuk logica door te geven dat zegt dat Bob zijn geld naar Alice kan sturen, maar dat Alice het pas kan opeisen nadat ze er iets voor terug heeft gegeven. (Buterin, 2013, p. 12)

Het doel van Ethereum is ontwikkelaars de mogelijkheid te bieden toepassingen te ontwikkelen op basis van willekeurige voorwaarden. De speciaal voor Ethereum ontwikkelde programmeertaal heet ***Solidity***.

2.2.4 Ethereum transacties en gas

De onderliggende cryptocurrency van de Ethereum Blockchain is ether (ETH). Voor het doen van een transactie op het Ethereum-netwerk is ***gas nodig***. Gas wordt uitgedrukt in de cryptocurrency Ether. Gas op het Ethereum-netwerk is in principe hetzelfde als transactiekosten. Dit wordt berekend aan de hand van standaardkosten per eenheid rekenkracht x het aantal eenheden. U kunt een specifieke hoeveelheid gas, of transactiekosten, opgeven voor elke transactie die u uitvoert. De gebruiker moet een passende hoeveelheid gas betalen voor de transactie. Als er te weinig gas wordt betaald, is het mogelijk dat de miners de transactie niet in het blok opnemen en deze transactie dus niet wordt uitgevoerd. Naast de blokbeloning ontvangt de miner ook alle gaskosten die bij de transacties in het blok zijn opgenomen.

De crypto-economische reden waarom gas is ingevoerd in het Ethereum-netwerk is dat het prioriteit geeft aan belangrijke transacties. Een blok heeft slechts ruimte voor een beperkt aantal transacties. Het gassysteem zorgt ervoor dat er geen energie wordt verspild aan spam of transacties van lage waarde.

2.2.5 Slimme contracten

Een smart contract is gedecentraliseerde automatisering en kan worden gedefinieerd als een contract met bepaalde voorwaarden die in code zijn vastgelegd. Het contract is self-executing, omdat het passende overeenkomstige acties uitvoert wanneer aan de voorwaarden is voldaan.

Een slim contract zou bijvoorbeeld een arbeidscontract kunnen zijn, waarbij Alice Bob 500 euro wil betalen om een website te ontwikkelen. Het contract zou als volgt kunnen werken:

1. Alice zet 500 euro in op het contract en de fondsen worden vergrendeld.
2. Wanneer Bob de website heeft ontwikkeld, stuurt hij een bericht naar het contract om de middelen aan hem vrij te geven.
3. Het fonds wordt vrijgegeven als Alice akkoord gaat.
4. Als Bob besluit de website niet af te maken, kan Bob zijn opdracht annuleren door een bericht naar het contract te sturen, waarna het fonds automatisch aan Alice wordt teruggegeven.
5. Als Bob beweert dat hij de website heeft voltooid, maar Alice is het daar niet mee eens, kan na een wachttijd van 7 dagen een rechter worden ingeschakeld om een uitspraak te doen ten gunste van Alice of Bob. (Buterin, 2014)

Voordelen van slimme contracten

Slimme contracten bieden veel voordelen. Chaintrade (2017) heeft de volgende elf opgesomd:

1. *Nauwkeurigheid:* Alle voorwaarden moeten in detail worden vastgelegd in een smart contract. Het weglaten van bepaalde voorwaarden kan leiden tot ongewenst gedrag van het smart contract.
2. *Transparantie:* alle voorwaarden zijn volledig zichtbaar en toegankelijk voor alle betrokken partijen. Zodra het contract definitief is, kunt u het niet meer betwisten.
3. *Duidelijke communicatie:* de noodzaak van nauwkeurig gedefinieerde slimme contracten zorgt ervoor dat de communicatie in het contract duidelijk wordt vastgelegd, zodat er geen ruimte is voor miscommunicatie en verkeerde interpretaties.
4. *Snelheid:* smart contracts kunnen traditionele bedrijfsprocessen automatiseren en aanzienlijk versnellen. Er hoeven geen aanvragen ter goedkeuring te worden ingediend en geen documenten te worden verwerkt of goedgekeurd door individuen.
5. *Veiligheid:* smart contracts draaien op Blockchain-platforms en maken gebruik van data-encryptie.
6. *Efficiëntie:* Door de nauwkeurigheid en snelheid voeren slimme contracten bedrijfsprocessen efficiënter uit of elimineren deze zelfs volledig.
7. *Papiervrij: er is* geen papierwerk nodig voor de uitvoering van slimme contracten.
8. *Opslag en back-up:* slimme contracten en hun gegevens worden permanent opgeslagen op de Blockchain. Daardoor kunnen ze niet verloren gaan en zijn ze gemakkelijk terug te vinden.
9. *Kostenbesparing:* slimme contracten kunnen veel kosten besparen, omdat er minder tussenpersonen zoals advocaten, getuigen en banken nodig zijn om de contracten te interpreteren en af te dwingen.
10. *Vertrouwen:* betrokken partijen kunnen erop vertrouwen dat slimme contracten - als ze

2.2.6 Gedecentraliseerde toepassingen

Wij definiëren een ***gedecentraliseerde toepassing*** (dApp) als een toepassing die gebruik maakt van de gedecentraliseerde gegevensopslag van een Blockchain. De toepassing wordt niet uitgevoerd via een centrale server, maar via een gedecentraliseerd netwerk van knooppunten. Net als een normale applicatie heeft zij vaak een front-end en een gebruikersinterface. De interface biedt de gebruiker een gemakkelijkere interactie met smart contracts en de Blockchain. Door de smart contracts die de kerncode van een dApp vormen decentraal op te slaan en uit te voeren, is er geen Single Point of Failure. De werking van de applicatie en de gegevens van de applicatie kunnen niet zomaar gecensureerd of verwijderd worden.

2.2.7 Gedecentraliseerde autonome organisatie (DAO)

Gedecentraliseerde autonome organisaties (DAO's) kunnen worden gedefinieerd als een niet-hiërarchische organisatie die routinetaken uitvoert en registreert op een Blockchain. De regels waaraan de DAO zich houdt, worden ook op de Blockchain vastgelegd. Daarnaast is de

DAO afhankelijk van vrijwillige bijdragen van interne belanghebbenden om de organisatie te sturen via een democratisch overlegproces. (Hsieh et al., 2018, p. 2)

Wat een DAO fundamenteel onderscheidt van een gecentraliseerde organisatie is dat zij geen topmanagementteam of CEO heeft. Zij heeft ook geen filialen, werknemers of dochterondernemingen. In plaats daarvan bestaat een DAO op een gedecentraliseerd netwerk van gebruikers en knooppunten die transacties op een Blockchain verzamelen, verifiëren en bijwerken. Beslissingen over wijzigingen in de code worden genomen via democratische stemprocedures. Het is een radicaal andere manier om een bedrijfsorganisatie op te zetten. Vanwege het autonome karakter - het is immers een zelfvoorzienend en zelforganiserend systeem - kan Bitcoin worden gekarakteriseerd als een DAO, omdat het (a) een betalingssysteem runt, (b) onderaannemers in dienst heeft die werken als miners en (c) deze onderaannemers betaalt met nieuw gedistribueerde bitcoins (Vigna & Casey, 2015, p. 229). Daarnaast kunnen miners door middel van hun rekenkracht stemmen op voorstellen ter verbetering van het protocol. DAO's worden gecontroleerd door een collectief besluitvormingsproces van belanghebbenden via een gedecentraliseerd protocol en worden niet beïnvloed door een centraal bestuursorgaan.

Slotopmerkingen

- Met Blockchain 2.0 kan een overvloed aan nieuwe soorten toepassingen worden ontwikkeld.
- Je kunt smart contracts ontwikkelen op Ethereum waarbij de voorwaarden zo duidelijk zijn vastgelegd dat bij contractbreuk interpretatie van derden niet meer nodig is.
- Bitcoin is een first-to-file systeem.
- Bitcoin is de eerste gedecentraliseerde autonome organisatie (DAO).

3 Soorten Blockchain

In dit hoofdstuk zullen wij Blockchain onderverdelen in typen vanuit drie invalshoeken: consensusprotocol, governance en typen samenwerking tussen Blockchain-systemen.

3.1 Soorten Blockchain volgens het consensusprotocol

Consensusprotocollen zijn essentieel om het vertrouwen tussen de verschillende deelnemers binnen een gedistribueerd netwerk te waarborgen. Er moet vertrouwen zijn dat de deelnemers niet corrupt zijn en dat de onderling gedeelde gegevens niet corrupt zijn. Om dit vertrouwen te waarborgen moeten de deelnemende knooppunten berichten of transacties op juistheid controleren en andere deelnemers die corrupt en misleidend zijn neutraliseren: de oplossing voor het Byzantijnse Generaliteitsprobleem zoals besproken in het vorige hoofdstuk.

Aangezien een consensusprotocol dus de essentie van een Blockchain-systeem raakt, wordt het hier gebruikt als een manier om Blockchain-types te onderscheiden.
In het vorige hoofdstuk is het eerste consensusprotocol, **Proof-of-Work**, geïntroduceerd met de Bitcoin als voorbeeld. Volgens dit protocol mag een gegevensblok alleen aan de Blockchain worden toegevoegd als er een geldige hash van het blok is gevonden. Aangezien Bitcoin-miners een hevige competitie in rekenkracht zijn aangegaan om als eerste een geldige hash te vinden, heeft het elektriciteitsverbruik van het Bitcoin-netwerk geleid tot bezorgdheid over de negatieve effecten van Blockchain op het milieu. De daaruit voortvloeiende zoektocht naar duurzamere oplossingen voor het Byzantijnse Generaalsprobleem heeft geleid tot alternatieve consensusprotocollen.
Een van de belangrijkste alternatieven voor Proof-of-Work is Proof-of-Stake, dat nu in verschillende Blockchain-projecten is geïmplementeerd, met als opmerkelijk voorbeeld Ethereum, dat in 2022 overgaat op Proof-of-Stake.

Terwijl miners bij Proof-of-Work nieuwe blokken mogen produceren wanneer zij een geldige hash kunnen vinden, wordt een blokproducent bij Proof-of-Stake gekozen op basis van (a) een willekeurig selectieproces en (b) een **'inzet'** zoals het aantal munten dat hij heeft. Bijgevolg heb je geen rekenkracht nodig om deel te nemen. Alles wat nodig is, is een standaardcomputer, een internetverbinding en het hebben van een munt. De blokproducent bij Proof-of-Stake wordt daarom geen miner genoemd, maar een ***forger***. Omdat de **vervalser** ook een beloning krijgt bij het produceren van een nieuw blok, kunt u Proof-of-Stake ook zien als een methode waarbij u een passief inkomen verdient op uw munten. Hoe meer inzet u heeft, hoe groter de kans dat u het volgende blok produceert. Naast het produceren van blokken, valideren vervalsers ook transacties, en helpen zo het netwerk te beveiligen.

Naast energie-efficiëntie zijn de voordelen van Proof-of-Stake van Proof-of-Work dat het gemak van staking een betere distributie van de Blockchain mogelijk maakt en dat het uitvoeren van een 51%-aanval minder aantrekkelijk is.

Er zijn verschillende varianten binnen Proof-of-Stake die hun eigen unieke eigenschappen hebben. Ten eerste kan in de **gedelegeerde Proof-of-Stake** iedereen die een munt heeft, stemmen op getuigen en gedelegeerden. De getuigen valideren transacties en produceren nieuwe blokken waarvoor zij een beloning ontvangen. De gedelegeerden houden toezicht op

de bestuursstructuur van het Blockchain-protocol. Daardoor kan gedelegeerde Proof-of-Stake meer transacties per seconde verwerken dan Blockchains die meer gedecentraliseerd zijn.
Ten tweede kan in een **geleased Proof-of-Stake** iedereen zijn munten leasen aan stake nodes, waardoor de kans voor stake nodes om een blok te produceren toeneemt. Stake nodes verdelen hun beloning evenredig tussen henzelf en de lessees. Bijgevolg moedigt dit protocol mensen aan om deel te nemen aan het stakingproces.

Ten derde, met **Proof-of-Stake Velocity worden** gebruikers beloond voor (a) het aantal munten dat zij bezitten en (b) hoe actief zij hun munten gebruiken. De gemeenschap wordt dus aangemoedigd om de munten niet alleen te houden, maar ook daadwerkelijk te gebruiken voor transacties.

Ten vierde, met **Proof-of-Authority worden** blokproducenten (authority nodes) geverifieerd en goedgekeurd op basis van hun identiteit en reputatie. Door de reputatie te koppelen aan de identiteit worden authority nodes extra gestimuleerd om goed gedrag te vertonen en geen kwaadaardige transacties in de Blockchain op te nemen. Doen zij dat toch, dan zal dat reputatieschade veroorzaken. Proof-of-Authority is een voorbeeld van het creëren van een Proof-of-Stake variant waarbij de kans op het creëren van een nieuw blok niet geheel afhankelijk is van het aantal munten dat je inzet.
Het is twijfelachtig of Proof-of-Authority onder Proof-of-Stake valt. Het wordt soms beschouwd als een vorm van gedelegeerde Proof-of-Stake en wordt vaker gebruikt in gesloten Blockchains met toestemming.

Een voordeel van het typeren van de Blockchain aan de hand van consensusprotocollen is dat het helpt de verschillen in **schaalbaarheid van Blockchains te verklaren**. Dit omdat schaalbaarheid in het algemeen afhangt van de invloed van de consensusprotocollen op de bloktijd, de blokgrootte, het distributie- of decentralisatieniveau van de Blockchain en de manier waarop blokken worden geproduceerd, transacties naar de Blockchain worden gestuurd en transacties worden geverifieerd. Om deze schaling te verbeteren worden verschillende oplossingen getest, zoals het off-chain halen van transacties. Bekende voorbeelden hiervan zijn het lightning netwerk, plasma (beide zogenaamde 'Layer 2' oplossingen) en sharding.

3.2 Blockchaingovernance en wie met welke rol kan deelnemen

Een Blockchain, zoals elk samenwerkingsverband, moet worden beheerd en gecontroleerd. De daaruit voortvloeiende Blockchain-governancestructuur biedt een tweede manier om Blockchain-types te onderscheiden die hier zal worden besproken.

Opmerkelijke bestuurselementen zijn:

1. **Rechten** op het indienen, uitvoeren en controleren van beslissingsvoorstellen door een groep of aan allen.
2. **Verantwoordingsplicht** en het recht om beslissingen en gedragingen te controleren en verantwoording af te leggen voor uw verantwoordelijkheden.
3. **Prikkels** en het aanmoedigen van deelnemers om de Blockchain te onderhouden.

Hoe deze elementen worden geïnterpreteerd hangt af van de doelstellingen die het partnerschap nastreeft en dus van het soort bestuur dat het nodig heeft.

Een van de bestuursbehoeften kan zijn dat een centrale groep mensen controle uitoefent en de voorwaarden dicteert (**centrale** controlementaliteit**)**, tegenover de behoeften van een grotere groep om op voet van gelijkheid samen te werken zonder hiërarchie of centrale controle (**gedecentraliseerde** controlementaliteit).

Het type controle dat wordt uitgeoefend, wordt gebruikt om te beslissen wie al dan niet toestemming krijgt om deel te nemen aan een Blockchain. Als centrale autoriteiten de toegang verlenen, is de Blockchain van het type **private** Blockchain. Als de toegang voor iedereen wordt geregeld, wordt de Blockchain een **publieke** Blockchain genoemd. De publieke en private Blockchain types worden gecombineerd in het **consortium** Blockchain type, een tussenvorm die meer gecentraliseerd is dan een publieke Blockchain en meer gedecentraliseerd dan een private Blockchain.

In een consortium werken meerdere organisaties samen om een Blockchain op te zetten en wordt de consensus beheerd door een selectie van knooppunten. Het consortium bepaalt voor het hele netwerk wie met welke rol kan deelnemen, welke transacties openlijk te zien zijn of afgeschermd kunnen worden van andere deelnemers en hoe de governance gestructureerd moet worden.

Je gebruikt vooral een **publieke Blockchain**, waar iedereen gelijk wordt behandeld, als je wilt dat een groep gelijkgestemden samenwerkt. Samenwerking wordt hier gegarandeerd door het consensusmechanisme dat werkt als een 'vertrouwensmachine'. 'Toegang voor iedereen' leidt tot een groter aantal knooppunten die vertrouwen opbouwen in het Blockchain-systeem. Bij een openbare Blockchain is er minder vertrouwen in autoriteiten die de Blockchain in naam van anderen besturen. Deze houding ten aanzien van vertrouwen bevordert de keuze voor consensusprotocollen met een meer gedecentraliseerd karakter, vertrouwen in het open source karakter van de Blockchain en de wens tot volledige transparantie van de besluitvorming. Deze houding leidt dus tot een groter vertrouwen in de toetreding en deelname van vreemden. Het vertrouwen ligt immers in het systeem en niet in de gebruiker.

In het algemeen zal een bedrijf dat neigt naar een **private Blockchain**, willen weten wie er in het Blockchain systeem zit. Denk aan een intranet waarin je de nodes, data en broncode controleert. Je kent iedereen en alle transacties zijn in te zien als dat nodig is, maar je schermt mensen ook af van het verifiëren of zien van bepaalde transacties. Dit is handig als de gegevens bedrijfsgevoelig zijn. In een openbaar systeem is het ook mogelijk om dit technisch in te bouwen, maar vooralsnog blijkt dit in de praktijk een uitdaging.

Daarom is het in een private Blockchain relevant om op de hoogte te zijn van alle rollen die u toekent aan de deelnemers aan wie u toegang hebt verleend. Een belangrijke rol is de mogelijkheid om **het consensusmechanisme in stand te houden**. Moet deze mogelijkheid worden gegeven aan alle deelnemers aan de Blockchain of alleen aan een selecte groep?

Het antwoord op deze vraag leidt tot de types Blockchain **zonder toestemming** en Blockchain **met toestemming**.

Als iedere toetreder tot de Blockchain het consensusmechanisme mag onderhouden, gaat het om een **permissionless** Blockchain type. Als de rol om het consensusmechanisme te onderhouden is voorbehouden aan een selecte groep, gaat het om een **permissioned** Blockchain type.

Naast het handhaven van consensus zijn er rollen waarmee u transacties in de Blockchain kunt uitvoeren, bekijken en aanpassen, de Blockchain technisch kunt onderhouden, of kunt deelnemen aan het stemmen over ideeën. Deze rollen zijn niet relevant voor de keuze tussen een permissionless of permissioned systeem. Deze rollen zijn echter wel relevant voor de aard van de partnerschappen. Dit is relevant omdat als de overheid het niet erg vindt wie toegang heeft tot het systeem, en vertrouwen stelt in het systeem zelf, zij eerder geneigd zal zijn anonimiteit te verlenen aan de deelnemers. Momenteel zouden bedrijven die classis beheerscontrolesystemen gebruiken er echter voor kiezen de mensen te kennen aan wie zij toegang verlenen, alsook te weten welke rollen er zijn en aan welke deelnemer zij welke rol kunnen toekennen.

Door de rollen te scheiden, kunnen deze bedrijven gebruik blijven maken van hun onderliggende organisatiestructuur. Zo kunnen zij hun bedrijfsidentiteit afdwingen binnen hun Blockchain, aangezien zij het profiel van de personen en hun rollen controleren. Naast het gedeeltelijk overdragen van vertrouwen aan het systeem, kunnen zij hun organisatie blijven beheren, hun eigen beheerscontrolesysteem zoals specifiek personeelsbeheer.

Dit verklaart waarom binnen een toestemmingsvrij systeem cryptomunten beschikbaar worden gesteld om samenwerking aan te moedigen.

De verschillende soorten Blockchain worden in de huidige Blockchains in combinatie gebruikt:

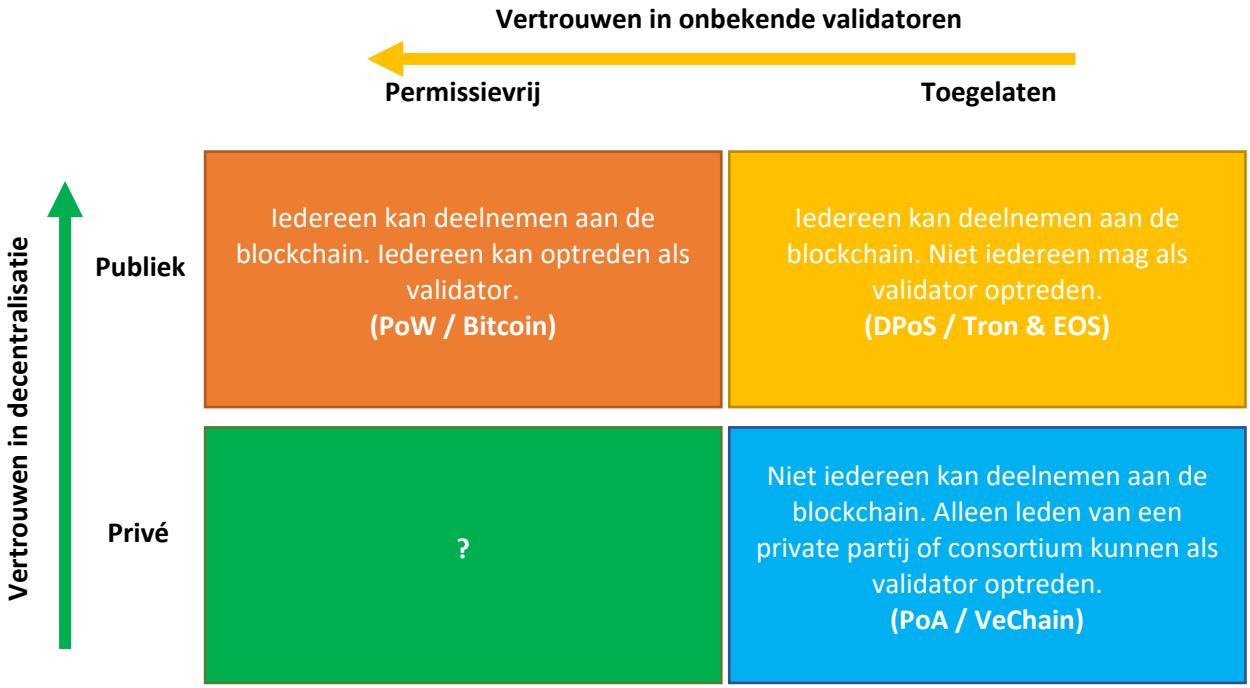


Figure 8: Een overzicht van verschillende Blockchain types, uitgedrukt in permissionless, permissioned, private en public (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 9).

Nu het vertrouwen in het systeem met publieke Blockchains ligt, wordt het 'wie schrijft gegevens naar de Blockchain', 'wie leest gegevens van de Blockchain' en 'wie mag de Blockchain onderhouden' van minder belang geacht. Dit leidt er dan weer toe dat de meeste publieke Blockchains permissievrij zijn. Door de lage drempel om toe te treden tot het netwerk zijn dergelijke Blockchains het meest gedecentraliseerd.

De deelnemers bepalen de werking van de Blockchain volgens groepsmotieven als openheid, neutraliteit en vrijheid. Binnen de publieke Blockchain kan iedereen ook deelnemen aan de besluitvorming over alle bestuurlijke kwesties.

Een **publieke** Blockchain is niet altijd wenselijk voor bedrijven, vooral in een meer gereguleerde omgeving waarin onder meer wordt verwacht dat zij de identiteit kennen van alle partijen die gegevens naar de Blockchain schrijven.

Deze centrale partij heeft vaak een aantal knooppunten opgezet die zichzelf beheren en die samen de Blockchain draaiende houden. In het meest extreme geval heeft de partij een enkele node waarop de Blockchain draait. Dit biedt echter geen voordelen ten opzichte van een gecentraliseerd netwerk dat ook een SPOF is.

Keuzes tussen de verschillende soorten Blockchains zijn van invloed op de controle van de organisatie. Hoe meer vertrouwen er is in het gedecentraliseerde karakter van de Blockchain, hoe gemakkelijker het is om deel te nemen. Hoe meer vertrouwen er is dat validators als onbekenden kunnen deelnemen aan de consensusvorming, hoe transparanter het systeem. Iedereen kan dan immers een volledig knooppunt draaien en alle gegevens helpen valideren. Door het decentrale karakter hebben dergelijke systemen vaak veel validators en mede daardoor nog steeds schaalbaarheidsproblemen. Ook zijn dergelijke Blockchains relatief duurder dan de minder gedecentraliseerde en permissioned varianten.

De verwachting is echter dat op termijn een permissievrije publieke Blockchain steeds efficiënter wordt, zodat meer professionele partijen voor dergelijke Blockchains zullen kiezen. Deze Blockchains moeten dan zo worden ingericht dat de rollen die deelnemers kunnen innemen voor zakelijke toepassingen goed zijn gedefinieerd en voldoen aan zakelijke eisen. Zo kunnen bedrijven op permissionless public Blockchains gegevens anonimiseren via Zero-Knowledge Proofs en kunnen deelnemers op applicatieniveau gevraagd worden hun identiteit aan te tonen.

3.3 Platforms en consortia

Een Blockchain waarbij verschillende bedrijven en derden samenwerken zonder dat een centrale gebruiker deze Blockchain controleert, wordt een Enterprise Blockchain genoemd. Om zo'n Enterprise Blockchain te bouwen, gebruiken bedrijven Blockchain-platforms. Deze **platforms maken** het mogelijk om applicaties te schrijven met behulp van bepaalde technologieën. Rond deze platforms zijn verschillende samenwerkingsverbanden georganiseerd. Platformen zijn de derde en laatste manier waarop we hier naar verschillende soorten Blockchains kijken.

Met blockchainplatforms kan uw toepassing samenwerken met andere toepassingen, bijvoorbeeld in een eigen of gedeelde programmeertaal, worden documenten opgeslagen of gedeeld en wordt toegang verkregen tot een bepaald netwerk. De twee meest prominente platforms zijn momenteel Ethereum en Hyperledger, met Corda als derde meest prominente.

Elk platform heeft zijn eigen unieke kenmerken. Ethereum is, over het algemeen, een publieke Blockchain, Hyperledger biedt plug-and-play modules met verschillende technologieën, en Corda is Decentralized Ledger Technology die meer gespecialiseerd is in financiële diensten. Leden die zich hebben aangesloten bij een partnerschap rond één platform zijn vaak ook lid van partnerschappen rond de andere platforms. De platformen zelf zijn open source.

Ethereum en Hyperledger streven de laatste jaren naar meer onderlinge integratie in hun gezamenlijk streven om Blockchain-systemen overal bij bedrijven te implementeren.

Wanneer partnerschappen een vorm van samenwerking van Blockchains betreffen waarbij de nieuwe toetreders bekend zijn en specifieke rollen krijgen toebedeeld, werken zij in structuren die verwarrend genoeg ook consortia worden genoemd (zie punt 3.2. hierboven), maar vanuit een ander perspectief dan het mengen van kenmerken van alleen publieke en private Blockchains. De samenwerkende partijen kunnen variëren van overheidsinstanties, belangengroepen en onbekenden, tot leveranciers, klanten en directe concurrenten.

Daarnaast helpen consortia hier partijen bij het overwinnen van vier belangrijke uitdagingen die organisaties tegenkomen bij de implementatie van Blockchain. Ten eerste delen consortia kennis over en onderhouden actief contact met (boven)nationale toezichthoudende instanties. Consortia helpen dan onder meer bij het verduidelijken van wet- en regelgeving.

Ten tweede helpen consortia organisaties om de risico's te spreiden over verschillende partijen door middelen te delen om Blockchain-systemen te ontwikkelen.

Ten derde zorgen consortia door samenwerking voor een kritische massa om een stabiel presterend systeem aan te nemen.

En ten vierde bieden consortia de mogelijkheid om nieuwe gedecentraliseerde partnerschappen aan te gaan met vertrouwde en niet-vertrouwde partijen, zonder dat de deelnemende organisaties al te veel van hun autonomie verliezen. Dit biedt concurrenten bijvoorbeeld standaardprocedures om gegevens met elkaar te creëren en uit te wisselen, of samen te werken met elkaars klanten en leveranciers. Maar aangezien de deelnemende partijen elkaar moeten vertrouwen om te kunnen samenwerken, dwingen zij hun vertrouwen gewoonlijk af met contracten over gedeelde middelen, besluitvorming, sancties, gevoelige informatie en het wederzijds delen van gegevens. Deze contracten verhogen zowel de drempel om tot een consortium toe te treden als de drempel om een consortium te verlaten. Verschillende consortia zullen waarschijnlijk naast elkaar bestaan. Interoperabiliteit binnen en tussen consortia speelt hierbij een belangrijke rol.

4 Cryptocurrencies en tokens

Een van de grote uitvindingen van Satoshi Nakamoto is de combinatie van reeds bestaande technologieën met een beloningssysteem dat een gedecentraliseerd netwerk draaiende houdt. Zoals gezegd wordt de beloning in Bitcoins betaald aan de miner die een blok produceert.

In onze huidige samenleving zijn **tokens** bekend als vouchers en munten - bijvoorbeeld loyaliteitspunten, casinomunten en cadeaukaarten. We kennen ook tokens in de IT die toegangsrechten geven tot een netwerk om een taak uit te voeren of als representatie van rechten op onderliggende activa. Een Bitcoin, die je ook zou kunnen zien als een cryptografisch token, verschilt van de bovengenoemde tokens in die zin dat het waarde vertegenwoordigt. Cryptografische tokens kunnen om vele redenen worden gebruikt. In het Blockchain landschap dienen ze vooral een **Internet of Value** waar waarden op een vertrouwde manier kunnen worden uitgewisseld via een gedecentraliseerd internet.

Met cryptografische tokens zoals Bitcoin kun je betalen of sparen, maar je kunt ook een stap verder gaan. Bitcoin kan bijvoorbeeld worden verdiend door computerkracht te leveren om nieuwe blokken te produceren. Zo ontstaat een economie waarin verschillende deelnemers worden aangemoedigd om het netwerk te helpen beveiligen in ruil voor crypto. Het gebruik van cryptomunten om bepaald gedrag van deelnemers te stimuleren en verkeerd gedrag te bestraffen via een consensusprotocol is onderdeel van **crypto-economie**.

In dit hoofdstuk beschrijft 4.1 eerst **crypto-economie** als basisconcept waarin tokens een nuttige rol blijken te spelen. Vervolgens beschrijft 4.2 **wat tokens** zijn en **classificeert** ze. Deze indeling omvat dApp-tokens en cryptocurrency, maar ook het verschil tussen fungibele en niet-fungibele tokens en hoe deze de crypto-economie ondersteunen. Het hoofdstuk wordt vervolgd in paragraaf 4.3 met een overzicht van hoe tokens kunnen worden gebruikt voor fondsenwerving door een Initial Coin Offering, Security Token Offering en Initial Exchange Offering.

4.1 Crypto-economie

Cryptografische tokens dienen verschillende doeleinden, zoals toegang tot een systeem of het weergeven van informatie van een fysiek object. Hierdoor krijgen de tokens **waarde** die kan worden uitgewisseld tussen verschillende partijen binnen een Blockchain. Deze nieuwe discipline die de overdracht van rijkdom via computernetwerken, cryptografie, speltheorie en softwareontwikkeling bestudeert, samen met het creëren en consumeren van rijkdom, wordt **crypto-economie** genoemd**.**

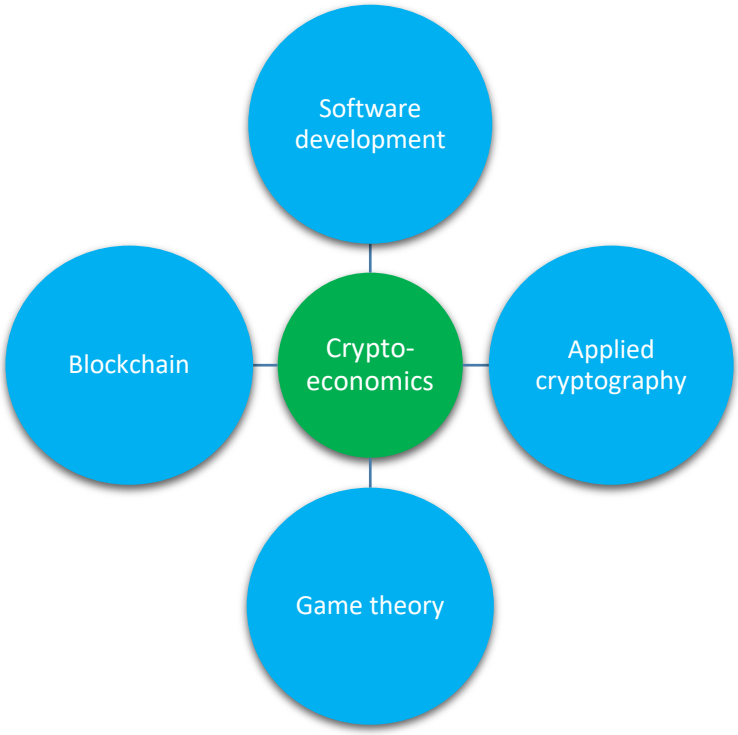


Figure 9:Multidisciplinaire aspecten van cryptoeconomie. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 10).

Computernetwerken zijn ontworpen met bepaalde regels die fungeren als een soort wet voor iedereen die eraan deelneemt. Deze wetten worden echter ontworpen door private partijen/gemeenschappen en deels afgedwongen door software in plaats van door overheden. Binnen deze wetten worden dus veronderstellingen gemaakt over hoe deelnemers zich kunnen gedragen en misdragen binnen het netwerk.

Het centrale idee achter crypto-economie binnen **Blockchain** is dat er protocollen worden ontwikkeld die mensen aanmoedigen om op zo'n manier aan het netwerk deel te nemen dat de **waarde** van het netwerk voor de deelnemers wordt **gemaximaliseerd**. De waarde van het netwerk kan alleen worden gemaximaliseerd als het netwerk en de transacties die daarin plaatsvinden ook **beveiligd zijn**. Om dit te bereiken wordt **cryptografie** gebruikt om transacties binnen het netwerk te beveiligen via **software** zoals hashfuncties en digitale handtekeningen. Daarnaast worden beloningen betaald aan deelnemers die het netwerk helpen beveiligen via bijvoorbeeld mining of staking. De combinatie van dit denken wordt geïllustreerd door de rol van Bitcoin als een token dat mensen stimuleert om samen te werken en zo een zelforganiserend crypto-economisch systeem in stand te houden. Crypto-economie is een belangrijke premisse ter ondersteuning van het idee van een duurzaam en bij voorkeur zelforganiserend systeem, zonder centrale partijen die mensen aansporen op een bepaalde manier te handelen. Van belang voor dit uitgangspunt is **de speltheorie,** een studie naar hoe in een concurrerende omgeving optimale voorwaarden worden geschapen om deelnemers altijd te laten kiezen voor goed gedrag in hun keuzes, omdat dit tot meer winst leidt dan slecht gedrag. Een manier om deelnemers tot goed gedrag aan te zetten is door beloningen met cryptotekens.

4.2 Classificatie van Blockchain-tokens

Het internet is oorspronkelijk opgezet om informatie met elkaar uit te wisselen. Dit wordt ook wel een **internet van informatie genoemd**. Daarbinnen is het moeilijk om waarde op te slaan en te verplaatsen zonder een vertrouwde tussenpersoon (Tapscott, 2016) die vooral controleert of een waarde, zoals euro, niet dubbel wordt uitgegeven (Satoshi, 2008, p. 2). Met de komst van Blockchain kun je de noodzaak van tussenpersonen omzeilen en direct peer-to-peer waarde verhandelen. Dit wordt ook wel het **internet van waarde genoemd**. Cryptomunten spelen een centrale rol in dit crypto-economische systeem. Een crypto-token kan worden gecreëerd op een Blockchain en ook een verhandelbaar activum vertegenwoordigen. Soms worden tokens gecreëerd in een ICO of een STO om een project te financieren. Het proces van tokencreatie wordt **tokenisatie genoemd**. Door deze tokens te verhandelen, kunt u het eigendom van de onderliggende activa overdragen.

Er zijn verschillende perspectieven om naar cryptomunten te kijken. De volgende indeling vat alle verschillende tokens samen, met als bijkomend voordeel dat de toekomstige rol van tokens in een Internet van Waarde aan bod komt:

Toepassing	Token ten voordele van de toepassing	Token als activa
Fungible Tokens	Netwerk: Ether dApp: Augur	Activa: goud Beveiliging: deel Shell Cryptovaluta: Bitcoin
Niet-funguleerbare penningen		Activa: geboorteakte Zekerheid: persoonlijke lening

Figure 10: Dubbel formaat van tokens. Aan de ene kant, om tokens te onderscheiden die worden gebruikt om Blockchain-netwerk te onderhouden vs om eigendom aan te tonen en over te dragen. Anderzijds, om onderscheid te maken tussen tokens die inwisselbaar vs niet inwisselbaar zijn. (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021, hoofdstuk 10).

Denk eraan dat tokens een dubbele tokenstructuur kunnen hebben, waarbij ze meerdere doelen tegelijk dienen. Bitcoin wordt bijvoorbeeld gebruikt als netwerk- of applicatietoken en als activa.

Tokens ten bate van de toepassing worden op het meest basale niveau gebruikt om mensen aan te moedigen deel te nemen aan een Blockchain-toepassing en dit netwerk draaiende te houden. Dit netwerk kan dienen als een platform waarop gedecentraliseerde applicaties, dApps, draaien. Hier worden **netwerktokens** gebruikt om deelnemers te **belonen** voor het werk dat zij doen om het netwerk te helpen onderhouden. Deze tokens nemen een centrale plaats in binnen een Blockchain, omdat zij als organisatiegedachte een gedistribueerd vertrouwd netwerk ondersteunen en daarmee het crypto-economische systeem van een

Blockchain vormgeven. Naast een toepassing kan een netwerk ook een **platform** zijn waarop toepassingen draaien zoals op Ethereum of Cardano met hun ETH- en ADA-tokens om consensus te bereiken en het transactiesysteem te belonen. Een stap verder denkend zie je dat er binnen een Blockchain de keuze is om een token te gebruiken, of om helemaal geen tokens te gebruiken.

dApp tokens , of **utility tokens**, zijn alleen nuttig binnen hun eigen applicatie en worden gebruikt om toegang te krijgen tot deze utility. Ze hebben geen nut buiten die applicatie. U kunt ze nog steeds buiten de applicatie verhandelen. Ze zijn echter niet altijd geprogrammeerd als valuta of aandeel in een netwerk. Bijvoorbeeld Siacoin (SC) waar mensen SC kunnen verdienen als ze hun vrije schijfruimte beschikbaar stellen aan anderen in het netwerk.

dApp tokens op Ethereum worden gemaakt volgens het **Ethereum Request For Comments 20** (ERC-20) protocol. Het protocol definieert bepaalde regels en normen met betrekking tot de uitgifte van tokens op het Ethereum-netwerk. Alle volgens ERC-20 gemaakte dApp-tokens zijn uniek voor hun toepassing en kunnen binnen het Ethereum-netwerk worden verhandeld.

Tokens ten behoeve van toepassingen verschillen van tokens die draaien om het vastleggen en uitwisselen van waarde binnen de Blockchain-toepassingen waarmee zij het bezit van deze waarde aantonen en de overdracht van het recht op deze waarde mogelijk maken, **tokens als activa**. Dit kan worden onderverdeeld in Asset tokens, Security tokens en cryptomunten.

Asset Tokens vertegenwoordigen registraties van rechten en verplichtingen op de onderliggende waarde, zoals op goud of olie, maar ook op een huis, een paperclip of crypto-verzamelobjecten zoals spelavatars of digitale kunstwerken. Deze tokens kunnen verwaarloosbare tot zeer grote onderliggende waarden vertegenwoordigen. Een belangrijke voorwaarde voor asset tokens is dat de identiteit van de eigenaar kan worden vastgesteld. Asset-cryptokaarten bieden potentieel voordelen door de mogelijkheid ze te programmeren (**smart tokens**) en te verhandelen met weinig wrijving en hoge veiligheid:

1. U kunt de bezittingen gemakkelijk opdelen en beschikbaar maken in kleine eenheden. Een voorbeeld van deze **fractionering** is het eigendom van de Mona Lisa weergeven in 1.000 tokens om te verkopen/leasen.
2. U kunt rechten programmeren op het cryptografische token en deze afdwingen via slimme contracten. Stel bijvoorbeeld in dat uw Mona Lisa-token alleen mag worden verkocht aan non-profitorganisaties, of programmeer dat een doorverkoop automatisch een commissie van 2% omvat voor de oorspronkelijke verkoper.
3. Je vermindert de frictie van het kopen en verkopen, mede door de snelle en goedkope microtransacties. Een slimme koelkast scant bijvoorbeeld de goedkoopste elektriciteit voor bepaalde tijdsintervallen.
4. U kunt alle relevante informatie voor de onderliggende activa vastleggen in het token. Controleer bijvoorbeeld de vorige eigenaars van uw tweedehands machine en verbeter zo de sharing economy.
5. U kunt gemakkelijk zelf een goed maken, zoals een toegangskaart voor een huisconcert.

Kortom, slimme tokens dragen gemakkelijk waarde, informatie, ideeën, rechten en verplichtingen over via slimme contracten.

Security tokens vertegenwoordigen obligaties, aandelen, leningen, futures, opties en andere verhandelbare financiële activa. Hoewel zij tot de activa-tokens behoren, worden zij apart vermeld. Aan security tokens kunnen allerlei rechten worden toegekend. Bijvoorbeeld het recht om het effect niet aan iedereen door te verkopen, of om uw stemrecht over de koers van het bedrijf tijdelijk aan iemand uit te kunnen lenen.

Cryptocurrency-tokens behoren ook tot de activa-tokens en worden apart behandeld gezien hun grote verwachte financieel-economische impact. Bitcoin is het bekendste voorbeeld van een cryptocurrency. In dit geval is het token bedoeld om als geld te fungeren. Langzaam maar zeker komen **stabiele munten in** de belangstelling omdat zij mogelijke manieren laten zien om de waarde van cryptomunten te stabiliseren en daardoor onder meer kunnen dienen als gedecentraliseerde alternatieven voor of representaties van fiatmunten. Stabiele munten kunnen worden afgedekt met verschillende activa zoals fiatvaluta, goud of cryptomunten, of helemaal niet worden afgedekt.

Een aantal centrale banken test stabiele munten in wat een **Central Bank Digital Currency** (CBDC) wordt genoemd. Hoewel de CBDC elementen van Blockchain kan gebruiken, is het niet noodzakelijkerwijs een Blockchain-toepassing. CBDC's staan haaks op de gedecentraliseerde oorsprong van Bitcoin, omdat een CBDC een centraal gereguleerde valuta is.

De vraag is hoe cryptomunten kunnen worden toegepast in een economisch systeem waar uitwisseling plaatsvindt. Een manier om dit te doen is te kijken naar **de fungibiliteit van tokens**. Sommige tokens kunnen gemakkelijker worden geruild voor een andere. Bijvoorbeeld een pak meel van 1 kg kan worden geruild voor een ander pak meel van 1 kg. Een bankbiljet van 10 euro kan ook worden ingewisseld voor twee bankbiljetten van 5 euro. Hetzelfde geldt voor **vervangbare penningen**: de afzonderlijke eenheden zijn niet van elkaar te onderscheiden en kunnen met elkaar worden geruild. Een voorbeeld is Polkadot: 1 Polkadot-penning kan worden ingewisseld voor een andere en twee halve Polkadot-penningen kunnen worden ingewisseld voor 1 hele Polkadot.

Daartegenover staan de **niet-vervalsbare tokens**, waarbij de tokens op zichzelf uniek en dus schaars zijn. Denk bijvoorbeeld aan personen, landen en geboorteakten die niet kunnen worden geruild tegen andere personen, landen en geboorteakten.

Met name blockchain is zeer geschikt om deze tokens efficiënt vast te leggen en te verhandelen, zelfs als de tokens slechts een minuscule waarde vertegenwoordigen en/of uniek zijn in hun soort. Dit is belangrijk omdat het in een digitale wereld gemakkelijk is een kopie van een digitaal goed te maken. Met een token als representatie is er dus niet alleen een mogelijkheid om gemakkelijk goederen uit de echte wereld te verhandelen. Het biedt ook de mogelijkheid om elk fysiek goed een authentieke digitale representatie te geven, hoe klein of onnozel dat goed ook is, en het te verhandelen. Bovendien is het creëren van een schaars token economisch interessant als je de prijs hoog wilt houden gezien het adagium: "hoe lager het aanbod van een token, hoe groter de schaarste en dus de kans op een hogere prijs".
Een aantal van de eerder genoemde voordelen voor asset crypto tokens, zoals fractionering en het creëren van smart tokens, ondersteunen de user case voor non-fungible tokens in die zin dat zij zeer individuele representaties kunnen worden van elk (te digitaliseren) object dat wordt gecreëerd en verhandeld via een laagdrempelig (iedereen kan binnenkomen, iedereen kan deelnemen) veilig netwerk, het Internet of Value. Een internet dat kan worden gebruikt om op transparante wijze uw impact op het milieu te meten en u ertoe aanzet de

doelstellingen van een grotere gemeenschap te ondersteunen. Uw rol is die van eigenaar van zonnepanelen, gebruiker van elektriciteit of investeerder in het netwerk.

In de toekomst kunt u in theorie elk goed dat u bezit, tokenen en deze tokens fractioneel of anderszins gebruiken als betaal- of financieringsmiddel.

4.3 Fondsverwerving tokens

Al deze afzonderlijke tokens kunnen vervolgens op verschillende manieren worden gebruikt om fondsen te verwerven: van Initial Coin Offerings (ICO), via Security Token Offerings (STO) en Initial Exchange Offerings (IEO) tot Initial DEX offerings (IDO).

De **Initial Coin Offering** (ICO) werd in het verleden vooral gebruikt om op internet geld in te zamelen voor Blockchain-projecten. Vooral Ethereum was de primaire Blockchain om tokens te creëren en te verkopen. In het begin van de ICO-trend ontstond een aanzienlijk aantal gevallen van misbruik, ook omdat ICO's plaatsvonden buiten de bescherming van nationale wet- en regelgeving. Als gevolg daarvan heeft de **Security**

Token Offering (STO) werd opgezet met hetzelfde doel als een ICO, maar nu met betrekking tot een token als een effect met standaardprotocollen, stemrechten en meer in overeenstemming, hoewel niet volledig, met verschillende nationale wetten en voorschriften inzake effecten en beurzen. De STO is tot dusver niet bijzonder succesvol gebleken in de openbare ruimte. Ook als nieuwe meer gereguleerde, maar nog steeds "open" alternatieven werden bedacht, zoals de **Initial Exchange Offering** (IEO) en **Initial DEX Offering** (IDO). Hier bieden gecentraliseerde of gedecentraliseerde beurzen zoals Binance of Uniswap start-ups een kans om crowdfunding te verkrijgen via hun bemiddelingsplatform, dat gewoonlijk KYC- en AML-controles uitvoert.

De ontwikkeling van een decentraal Internet van Waarde door de gemeenschap lijkt zich voort te zetten in een wervelwind van botsende idealen, ideeën, technische mogelijkheden, fouten, wonderlijke ongelukken en doorzettingsvermogen.

5 Gebruik en toepassingen van Blockchain

In dit hoofdstuk worden drie voorbeelden gegeven van het gebruik en de toepassingen van Blockchain. Voorafgaand wordt een inleiding gegeven over hoe organisaties strategisch kunnen nadenken over relevante elementen van hun businessmodel en de kansen die Blockchain biedt. Het hoofdstuk eindigt met specifieke punten waar een bedrijf op let zodra het Blockchain implementeert.

5.1 Bedrijfsmodellen

Blockchain levert typisch waarde binnen bedrijfsmodellen en bedrijfsecosystemen waar digitale gegevens en technologie worden/kan worden gecreëerd en gedeeld tussen partners. Dit omdat Blockchain een digitale technologie is die past bij deze digitale datagedreven bedrijfsmodellen en partners in staat stelt samen te werken waar dat voorheen niet kon. Deze partners kunnen nu hun vertrouwen 'in het systeem' stellen waar ze voor Blockchain elkaar niet vanaf het begin vertrouwden om samen te werken. In die zin is Blockchain vooral een kans om ecosystemen die gebruik maken van **digitale datagedreven bedrijfsmodellen te laten** groeien en digitaliseren.

Wat bedrijfsmodellen betreft, is het **gedecentraliseerde Business Model Canvas**[6][7] relevant, aangezien decentralisatie centraal staat in de publieke permissionless Blockchain-aanpassingen. In dit specifieke canvas hebben tokenhouders een centrale positie aangezien zij meerdere rollen hebben zoals zowel gebruiker, validator, werknemer en/of eigenaar. Dit soort "nieuw" denken geeft een idee van de potentiële nieuwe mogelijkheden die publieke permissionless Blockchain biedt, aangezien partijen die elkaar niet kennen een alternatief hebben om een relatief laagdrempelig systeem op te zetten en te gebruiken om samen gegevens te delen en te verifiëren terwijl zij elkaar niet kennen.

Het bestuur wordt dan op een decentrale manier door het publiek opgezet, gegevens worden decentraal opgeslagen en de communicatie tussen de verschillende partijen vindt peer-to-peer plaats. Dit is de meest open vorm van een Blockchain. Een bedrijf is vrij om de bouwstenen van Blockchain zelf aan te passen. Bij een gecentraliseerd systeem neemt een centrale organisatie de beslissingen.

In een gedecentraliseerd bedrijfsmodel wordt de omzet vaak verdeeld onder degenen die het meest bijdragen aan het netwerk en zijn de kosten voor het gebruik van het platform zeer laag - bijvoorbeeld bij het sociale blogging Blockchain-platform Steemit.

5.2 Blockchaintoepassingen voor ondernemingen

Deze paragraaf schetst drie ingezette toepassingen binnen vier verschillende industrieën, en vergelijkt ze aan de hand van de comparatieve voordelen die Blockchain in deze toepassingen bood. De vier toepassingen zijn:

1. Overheid en publieke goederen door Lantmäteriet.
2. Vervaardiging door BMW.

[6] https://canvanizer.com/new/decentralized-business-model-canvas
[7] https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

3. Digitale portemonnee van Singapore Airlines.

Een nuttig overzicht hier om u te helpen begrijpen waar veel Blockchain sectoren Blockchain implementeren komt uit onderstaand onderzoek onder 67 enterprise Blockchain netwerken en de sectoren waarin deze implementaties vallen (Rauchs, Blandin, Bear, McKeon, 2019).

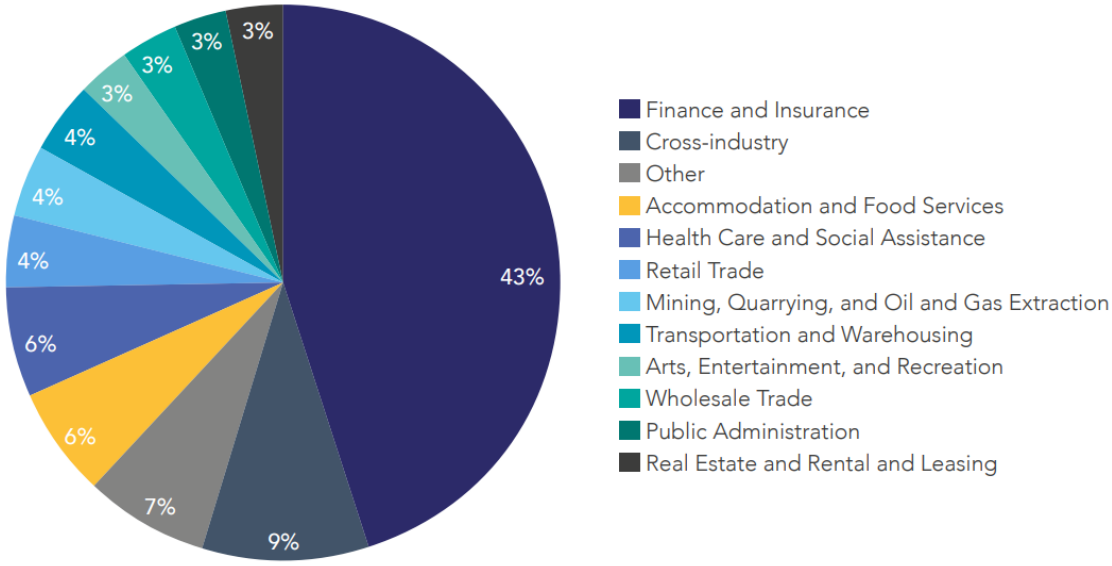


Figure 11: Overzicht van 67 live enterprise Blockchain netwerken en in welke sectoren ze vallen (Bron: Rauchs, Blandin, Bear, McKeon, 2019).

Het eerste voorbeeld betreft de **sector overheid en collectieve goederen**. De Zweedse **Lantmäteriet heeft** als taak het kadastrale systeem te onderhouden, geodata te verstrekken en landregistratie te verrichten. Er is behoefte aan meer transparantie en meer efficiëntie van het project, aangezien verschillende partners samenwerken en handmatige processen gebruiken die inefficiënt en foutgevoelig lijken.

Lantmäteriet testte daarom een oplossing om te zien hoe actoren zoals kopers, verkopers, makelaars, financiële diensten, advocaten, pensioenfondsen en de Lantmäteriet kunnen samenwerken op een efficiënt online platform dat onmiddellijke transparantie van een aanvraag via digitale apparaten biedt. Het project werd opgezet als een incrementeel project (2015-2019) in een gecontroleerde boxsituatie met vertrouwde partners, maar zonder al te ambitieus te streven naar decentralisatie op korte termijn. Er was een duidelijke focus op het plukken van laaghangend fruit met het kadaster en het creëren van een basis voor toekomstige diensten.

Tijdens het project dienden zich juridische kwesties aan die moesten worden opgelost. Zo moest Lantmäteriet nadenken over hoe om te gaan met het recht van individuen om hun eigen gegevens te controleren (EU General Data Protection Regulation - GDPR) inclusief het kunnen beschermen en verwijderen ervan waar gewenst en mogelijk. Evenals over hoe digitale handtekeningen kunnen worden gebruikt als juridisch bindende handtekeningen binnen de EU (eIDAS-richtlijn) of de status van digitaal ondertekende (e-)contracten op basis van Blockchain.

De verkoop van grondbewijzen was ambitieus omdat verschillende partijen een nieuw proces en spel creëerden met een nieuwe technologische oplossing. De Blockchain-oplossingen omvatten zowel private, gesloten Blockchain-systemen met toestemming als een gedistribueerd publiek netwerk. De private Blockchain is eigendom van de overheid, wordt gerund door een beperkt aantal knooppunten van vertrouwde tussenpersonen en staat onder toezicht van de Zweedse overheid. Dit systeem werkt samen met ChromaWay en het particuliere netwerk van belanghebbenden. Het maakt gebruik van smart contracts, de Practical Byzantine Fault Tolerance en Proof-of-Work consensusmechanismen, off en on chain digitale identiteiten via een mobiele telefoon app en geen tokens.

De akte blijft geregistreerd bij Lantmäteriet en wordt niet overgebracht naar een publieke Blockchain gezien de eerdere problemen met GDPR. Contracten worden handmatig ondertekend en via hashes op de Blockchain geplaatst. De originele contracten staan op de server bij andere partijen, deze informatie heeft back-ups. Telia biedt een mobiele app ID oplossing waarmee mensen zich kunnen registreren zonder hun Zweedse Burgerservicenummer te publiceren. Deze registraties worden via een hash op de Bitcoin Blockchain opgeslagen en geverifieerd. Digitale persoonlijke informatie kan worden verwijderd als een individu dat wenst en het is niet wettelijk verplicht om openbare informatie te zijn.

De belangrijkste voordelen waren de veiligheid van het gebruik van Blockchain-technologie en de operationele voordelen. Wat dit laatste betreft, is de termijn voor de registratie van een landtitel van 4 tot 6 maanden verschoven naar enkele dagen. Ook werd 100 miljoen euro per jaar bespaard door minder fouten en onderhoud (Kairos Future, 2017). Dit vermindert vervolgens de risico's van contracten met dubbelzinnige kenmerken, frauduleuze gegevens of kansen om eigendom te stelen. Ook het controlespoor naar zowel opdrachtgever, controleur als wetgever werd transparant. Ook versterkte het ecosysteem zijn onderlinge processen en gegevensuitwisseling zonder al te veel opschudding van zijn centrale dienst en bedrijfsmodel. En, last but not least, verhoogde de publieke toegankelijkheid het vertrouwen in het proces en de partijen. Na de test kon het systeem worden uitgebreid met partijen als verzekeraars, notarissen en andere lokale overheden.

Het project werd in 2019 afgerond en de architectuur van het platform bleek te werken, maar volgens Mats Snäll, chief innovation officer bij Lantmäteriet, "werd het nooit geïntegreerd in het productiesysteem van het kadaster," omdat een wetswijziging nodig zou zijn voordat het systeem in de toekomst zou kunnen worden opgeschaald. (Baraniuk, 2020). Waarschijnlijk wijst dit op de uitdaging van het publiceren van identiteitsgegevens van gebruikers op de openbare Blockchain.

Ook ander onderzoek wijst in de richting van een "fundamentele verandering in de bestuursstructuur, zoals de rol van de Lantmäteriet", die specifiek voor de vastgoedecosystemen een onderliggende drijfveer zou kunnen zijn geweest om verdere voortgang van het project te bevriezen (Schnuer, 2020).

Maar ondertussen gebruikt Lantmäteriet zijn lessen om verder te experimenteren met Bockchain. Bijvoorbeeld de gezamenlijke overheidsopdracht met DIGG om "een model of conceptuele oplossing te vinden voor het opbouwen van vertrouwen in automatisering met AI en met andere nieuwe technologie zoals Blockchain-technologie". (AI Zweden, Lantmäteriet, 2020).

Het tweede Blockchain toepassingsvoorbeeld betreft BMW binnen de **Manufacturing sector. De automotive business modellen hebben te maken met** 4th industriële revolutie technologieën zoals elektrificatie en autonome systemen onder steeds meer milieubewuste omstandigheden.

BMW probeert in dit voorbeeld te begrijpen hoe een digitale identiteit voor auto's kan worden gebruikt om het gebruik van andere technologieën en concepten van de 4e industriële revolutie mogelijk te maken. Met name de privacy/veiligheidsproblemen van een constante internetverbinding van de auto en de gebruiker, alsmede de noodzaak om deze gegevens veilig op te slaan. Deze veilige gegevensuitwisseling tussen apparaten, die veilige digitale identiteiten garandeert, is wat Blockchain potentieel ter tafel brengt en zo BMW een toegang biedt tot de markt van de autodeeleconomie.

BMW heeft een aantal car sharing apps getest zoals Share Now waarbij de digitale identiteit van zowel auto als gebruiker kan worden betrokken. Deze automotive gecombineerde digitale identiteiten kunnen bijvoorbeeld registreren wanneer er benzine is getankt of waar de auto is geparkeerd. Dit soort informatie kan vervolgens worden gebruikt in bedrijfsmodellen waarbij de autofabrikanten, al dan niet samen met tussenpersonen, gepersonaliseerde diensten aanbieden zoals schadeverzekeringen, autonome autoritten of het verbeteren van de auto-ervaring in het algemeen.

In dit specifieke voorbeeld experimenteerde BMW echter met een eenvoudiger project met uitsluitend aandacht voor de ID van de auto en de opgeslagen gegevens, dus geen aandacht voor de gebruiker. Het idee is dat mogelijke kopers van gebruikte BMW's geïnteresseerd zouden zijn in vertrouwde gegevens over de kilometerstand, de ongevalhistorie, de onderhoudsgeschiedenis en andere info van de auto. Een potentiële verkoper zou deze gegevens kunnen delen met een potentiële verkoper of zijn verzekeraar, BMW zou de info kunnen gebruiken om zijn bedrijfsmodel te verbeteren, bijvoorbeeld om zijn klanten beter van dienst te zijn.

Om deze oplossing te creëren werkte BMW's Startup garage samen met Blockchain start-ups, in dit geval VeChain. Ook gebruikt BMW de resultaten om de ID van een auto te ontwikkelen, een eerste stap naar een Vehicle Identity (VID) die de leden van het Mobility Open Blockchain Initiative (MOBI) samen kunnen gebruiken. MOBI is een Blockchain-consortium dat samen Blockchain-standaarden ontwikkelt.

De samenwerking met VeChain resulteerde in de **VerifyCar** app. VeChain is een Decentrale Autonome Organisatie met een centraal bestuursorgaan dat gebruik maakt van de Proof-of-Authority consensusmethode en verschillende tokens op haar publieke VeChain Blockchain.

De VID heeft een unieke ID op deze Blockchain. Periodiek legt de app data vast (via in-car simkaarten en Machine-to-Machine communicatie), die geverifieerd wordt op de VeChain Blockchain: VeChain slaat alleen de verwijzing naar de data op, de data blijft op het voertuig zelf. De vastgelegde autodata bevat zowel statische informatie zoals type en productiedatum van de auto als dynamische informatie zoals het aantal gereden kilometers. Wanneer een auto-eigenaar gegevens wil delen met een andere partij, gebruikt hij de VerifyCar app om de gegevens inclusief de referenties op de Blockchain te laten zien dat dit de werkelijke gegevens zijn die op het voertuig zijn opgeslagen.

Het is BMW's bedoeling om geen controle te hebben over het VeChain bestuur of de code. Begin 2022 heeft de app geen productie gezien.

Door deze oplossing te testen zet BMW een gecontroleerde eerste stap naar een stapsgewijze integratie van gedecentraliseerde Blockchain-technologie. Bovendien, als VerifyCar kan worden gebruikt voor auto's, waarom dan niet een VID-achtige digitale identiteitskaart om er zeker van te zijn dat auto-onderdelen niet worden nagemaakt, op welke locatie gekochte grondstoffen in de productielijn te vinden zijn of inzicht in de productie- of transportomstandigheden van bepaalde productiemachines die je hebt besteld? In lijn met dat denken experimenteert BMW met Blockchain om ook een **transparante toeleveringsketen ten** goede te komen.

Zo werd in 2019 de PartChain-pilot voor de inkoop van voorlichten met behulp van Amazon Web Services, Microsoft Azure en Hyperledger Fabric Blockchain (Ledger Insights (2020, 31 maart) uitgebreid naar andere leveranciers. Hierdoor kon BWM haar onderdelen en op lange termijn kritische grondstoffen 'van mijn tot smelterij' traceren. (BMW Pressclub Global, 2020). En bovendien te zorgen voor 'eenvoudigere certificering en kortere douaneprocedures' (BMW, 2019).

Een **laatste voorbeeld is de digitale portemonnee van Singapore Airlines, KrisPay**. Singapore Airlines wilde de loyaliteit van haar klanten verder vergroten door het gebruik van Blockchain. Dit resulteerde in het versterken van haar frequent flyer programma KrisFlyer met de KrisPay digitale Blockchain wallet in 2018.

Met KrisPay kunnen klanten hun KrisFlyer airmiles inwisselen voor KrisPay miles, cryptocurrency tokens. Deze KrisPay tokens kunnen worden gespaard bij / uitgegeven bij verschillende handelaren zoals banken, tankstations en winkels. Ook kan de klant andere beloningen sparen en inwisselen zoals met de creditcard van DBS (Development Bank of Singapore Limited), of Singapore Airlines miles verdienen, kopen of uitgeven zoals voor vluchtupgrades. De geldwaarde van de KrisPay-token zelf wordt bepaald door Singapore Airlines. Dus de oplossing die KrisPay hier biedt is om klanten een gemakkelijke manier te geven om hun beloningen in te wisselen om te voorkomen dat mijlen verloren gaan naast het sparen van deze tokens in het merchant netwerk. In zekere zin krijgen klanten een digitale aanvulling / alternatief voor fiatmunten.

De functionaliteit van KrisPay is eenvoudig te gebruiken via een app op uw mobiele apparaat en directe point-of-sale transacties. Voor nog meer gebruiksgemak kunnen de KrisFlyer miles worden overgedragen binnen de familie of geautoriseerde nominees.

Door Blockchain wallets en cryptocurrencies te combineren, maakt KrisPay gebruik van Blockchain sterke punten zoals veiligheid voor alle gebruikers omdat de registratie van de transacties fraudebestendig is. Merchants hebben onmiddellijk hun transacties goedgekeurd en inzichtelijk gemaakt, zonder het gebruik van een langzamere en duurdere tussenpersoon. Dit ondersteunt de reconciliatie van tokenbetalingen tussen de handelaren (en hun financiële administraties) en geeft hen actuele klanteninformatie.

KrisPay is ontwikkeld met KPMG Digital Village en Microsoft. KrisPay is een private onderneming die eigendom is van Singapore Airlines en werkt op een combinatie van Microsoft Azure (oorspronkelijk gebaseerd op het Ethereum protocol) met Azure app en

database functies. Verschillende partners onderhouden en verifiëren de Blockchain-database, zodat iedereen tegelijkertijd over de klant/transactie-informatie beschikt.

Microsoft heeft aangekondigd zijn Azure Blockchain in 2021 met pensioen te sturen en klanten te ondersteunen bij de migratie naar de Quorum Blockchain Service, een andere variant van het Ethereum-protocol (Microsoft, 2021).

De KrisPay tokens en portemonnee werden gecombineerd in een nieuwe app in 2020, Kris+. Deze app gebruikt verder klantgegevens zodat Singapore Airlines haar klanten beter kan bedienen en gepersonaliseerde deals kan aanbieden, zelfs op basis van de geolocatie van de mobiele telefoon.

In potentie kan de KrisPay-portemonnee worden gebruikt voor het kopen van tickets, als bewijs van uw digitale identiteit of als een ander algemeen token dat kan worden gebruikt om in te wisselen tegen fiatmunten of andere loyaliteitspunten.

Concluderend zijn **al deze toepassingen** beheersbare, goed gedefinieerde Blockchain-cases die zorgvuldig worden geïmplementeerd als onderdeel van een grotere visie binnen een omgeving die de initiatiefnemers vertrouwen en controleren. De cases tonen duidelijkheid over de elementen die zij zien als een kans of geen kans, en gebruiken een incrementeel veranderingsproces waarin zij de inspanning opvoeren van voorzichtige eerste stappen naar volledige implementatie.

Hun omgeving bestaat uit stabiele processen, een bekend bedrijfsmodel en vertrouwde partners om te experimenteren met de meer beproefde aspecten van de technologie en de gedecentraliseerde zakelijke implicaties ervan.

Er was geen ruimte om de toepassing van een volledig gedecentraliseerd bedrijfsmodel te tonen, als u een voorbeeld wilt, lees dan zeker het voorbeeld van de Augur Predicatiemarkt in hoofdstuk 16.5. (Lin Lim, Janse, 2021).

5.3 Wanneer heeft welke Blockchain implementatie zin?

Uit de voorgaande voorbeelden blijkt duidelijk dat er bepaalde voorwaarden moeten bestaan om Blockchain met succes te implementeren.

Er zijn een aantal criteria waar u naar kunt kijken om te beslissen of Blockchain een zinvolle zaak is voor uw bedrijf. Deze criteria hebben tot doel fricties met data of dataverkeer weg te nemen, of kansen te creëren met data en dataverkeer tussen partijen. Als vuistregel kunnen de criteria als volgt worden samengevat:

1. **Digitale innovatie maakt** deel uit van de strategie.
2. Verschillende partijen **delen gegevens**.
3. Deze gegevens en hun transacties hebben **een monetaire waarde**.
4. De gegevens zijn **vertrouwelijk**.
5. Verschillende partijen bewerken gegevens.
6. De gegevens moeten worden geverifieerd.
7. Er is een **duidelijk en voldoende rendement op de investering te** berekenen.
8. Verificatie is **complex en kost en/of kost veel tijd**.

9. De oplossing om te kiezen voor Blockchain is de **eenvoudigste oplossing** om het probleem te overwinnen.
10. De oplossing beïnvloedt de bestaande organisatiestructuur.
11. De oplossing beïnvloedt de bestaande workflow.
12. De oplossing beïnvloedt het bestaande ecosysteem.
13. De technische oplossing ligt dicht bij of kan worden geïntegreerd in bestaande systemen.
14. De oplossing is gegevensintensief maar schaalbaar. Denk in verschillen van 1k, 10k, 100k, 1 miljoen of> 10 miljoen transacties per uur.

Zodra u de kans ziet om Blockchain te implementeren op basis van deze criteria, kunt u verdergaan met het begrijpen van de onderliggende gebruikershulpprogramma's die nodig zijn, evenals de bouwstenen waaruit deze hulpprogramma's bestaan. De bouwsteen "betalingstoken" heeft bijvoorbeeld invloed op het gemak, de snelheid en de transparantie van betalingstransacties. Andere voorbeelden van bouwstenen zijn wallets, smart contracts, dApps, tokensoorten, oracles, enzovoort.

Momenteel is de impact van Blockchain in bedrijven vooral gericht op efficiëntie, disintermediatie en registratie. En de impact is daar het grootst waar samenwerkende partijen nieuwe gegevens ontsluiten en creëren. In de toekomst worden echter complexe Blockchain implementaties verwacht die decentralisatie en integratie van ecosystemen aansturen.

U kunt de volgende vereenvoudigde beslisboom gebruiken om het gebruik van een Blockchain-project in te schatten:

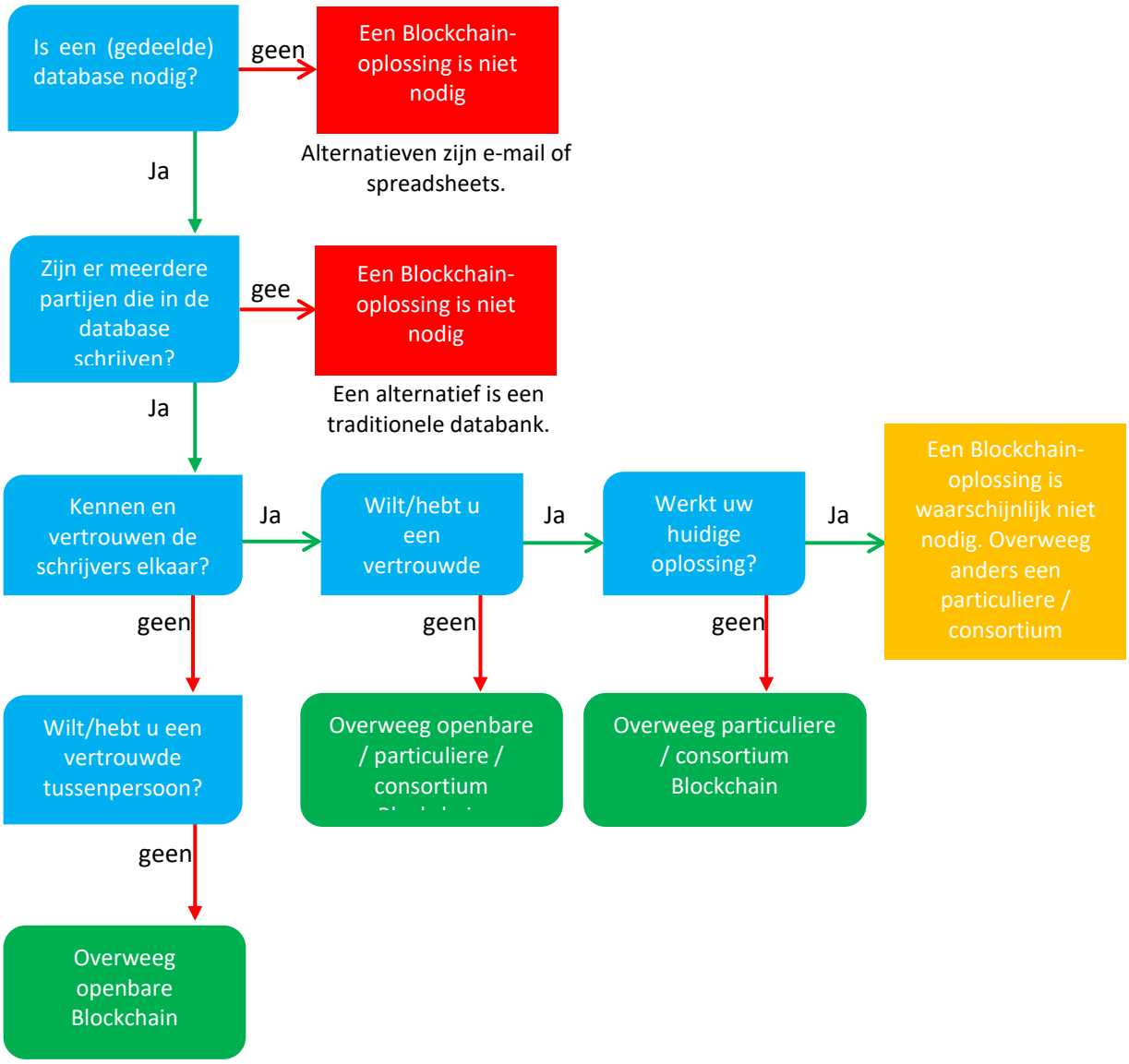


Figure 12: Vereenvoudigde beslisboom om al dan niet Blockchain te gebruiken (Bron: Lin Lim, C., Janse, A., Blockchain Basics, 2021).

6 Referenties en bronnen voor verdere lezing

Ackermann, J. & Meier, M. (2018). *Blockchain 3.0: De volgende generatie Blockchain-systemen*.

Advanced Seminar Blockchain Technologies, Summer Term 2018, Technische Universiteit Munch.

AI Zweden, Lantmäteriet (2020, november). *Bouwen aan een AI-vertrouwensmodel voor de publieke sector,*

Geraadpleegd van https://www.ai.se/en/node/85154

Antonopoulos, A. M. (2016). *Het internet van geld: lezingen door*. Merkle Bloom Llc.

Augur. (n.d.). *Overzicht*. Geraadpleegd op 23 december 2019, van https://docs.augur.net/#overview

Augur (2018, juli 9). *Augur Stichting OU Privacybeleid*. Geraadpleegd op 23 december 2019, van Augur.net website: https://www.augur.net/privacy-policy/

Baraniuk, C. (2020, februari 11). *Blockchain: De revolutie die nog niet helemaal heeft plaatsgevonden*. Geraadpleegd van https://www.bbc.com/news/business-51281233

Bitcoin Block Reward Halving Countdown. (2019). Geraadpleegd op 23 december 2019, van

Bitcoinblockhalf.com website: http://www.bitcoinblockhalf.com

BMW, (2019, 14 oktober). Hoe Blockchain-oplossingen de bestuurder kunnen helpen. Geraadpleegd van https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW Pressclub Global (2020, 31 maart). *BMW Group gebruikt Blockchain om supply chain transparantie te stimuleren.* Geraadpleegd van https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency.

Buterin, V. (2013). *Ethereum white paper: een volgende generatie smart contract en gedecentraliseerd applicatieplatform* [White paper]. Geraadpleegd op 27 december 2019, van Blockchainlab: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, mei 6). *DAO's, DAC's, DA's en meer: Een onvolledige terminologiegids*.

Geraadpleegd op 27 december 2019, van de Ethereum.org website: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

ChainTrade. (2017, 27 december*). 10 Voordelen van het gebruik van Smart Contracts*. Geraadpleegd op

27 december 2019, van website Medium: https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin en de opkomst

van gedecentraliseerde autonome organisaties. Journal of Organization Design, 7(1).

https://doi.org/10.1186/s41469-018-0038-1

Kaoris Future. (2017) *Het Kadaster in de blockchain - proeftuin*. Geraadpleegd van https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *Het Kadaster in de blockchain.* Geraadpleegd van http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights (2020, 31 maart). *BMW breidt supply chain blockchain uit voor traceerbaarheid van onderdelen.* Geraadpleegd van https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, 15 oktober), *Singapore Airlines breidt zijn op blockchain gebaseerde belonings digitale portemonnee uit*. Geraadpleegd op https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook*, september 2021, hoofdstuk 10. Uitgever: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

Microsoft, 2021, 14 mei). *Actie vereist: Migreer uw Azure Blockchain Service gegevens voor 10 september 2021*. Geraadpleegd op https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, 2 mei), *Singapore Airlines transformeert klantentrouw met blockchain op Azure*. Geraadpleegd op 4

MOBI. (2019). *Standaard voor voertuigidentiteit*. Geraadpleegd van https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Nakamoto, S. (2008). *Bitcoin P2P e-cash paper.* Geraadpleegd op 23 december 2019, van Metzdowd.com website: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, 30 september). *Re: Ik heb mijn portemonnee gebroken, zendingen bevestigen nu nooit meer.* [Online [forum commentaar]. Bericht geplaatst op https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, november 1). *PayPal's recente stroomstoring stimuleert bitcoin-adoptie*. Geraadpleegd op 23 december 2019, van Bravenewcoin.com website: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Beer, K., McKeon, S. (2019). 2e *Global Enterprise Blockchain benchmarking study*. Geraadpleegd van https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, 7 december). *Verandering van de vastgoedmarkt door blockchain*. Geraadpleegd van https://delano.lu/article/delano_changing-property-market-through-blockchain

Strategyzer. (n.d.) *Business Model Canvas*. Geraadpleegd op 23 december 2019, van https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U., & Lakhani, R. (2018). *Conceptualiseren van Blockchains: Kenmerken & Toepassingen.* 11e IADIS Internationale Conferentie Informatiesystemen 2018, 49-57.

Vigna, P., & Casey, M. (2015). *Het tijdperk van de cryptocurrency: hoe bitcoin en de blockchain zijn De wereldwijde economische orde op de proef stellen*. New York, N.Y.: Picador/St. Martin's Press.

Young, S. (2018). *Handhaving van grondwettelijke rechten via computercode.* Geraadpleegd van CUA Law Scholarship Repository website: https://scholarship.law.edu/jlt/vol26/iss1/5/

Bijlage I - Begrippenlijst

51% aanval: Een aanval op de Blockchain die wordt uitgevoerd door meer dan 51% van alle rekenkracht van het netwerk te bemachtigen.

Client-server model: Het model waarbij clients (gebruiker) verbonden zijn met een server. De server bevat gegevens die relevant zijn voor de clients. De clients maken verbinding met de server om toegang te krijgen tot deze gegevens. Dit maakt de clients afhankelijk van de server.

Distributed Ledger Technology (DLT): Distributed ledger technology.

Dubbele uitgaven: Een Bitcoin twee keer uitgeven. Bijvoorbeeld dat u 1 Bitcoin hebt, maar daarmee 1 Bitcoin naar persoon A stuurt en 1 Bitcoin naar persoon B.

Volledig knooppunt: Een knooppunt dat een volledige kopie van de Blockchain heeft.

Miner: Een computer die rekenkracht levert om een geldig blok te produceren. Een blok is alleen geldig als het een nonce vindt die leidt tot een geldige hashwaarde.

Knooppunt: Apparaat dat is aangesloten op een computernetwerk.

P2P: Zie peer-to-peer.

Peer-to-peer: Een computernetwerk waar computers gelijk zijn aan elkaar en elkaar diensten kunnen aanbieden.

Proof-of-Work: Een consensusmechanisme waarbij miners computerkracht moeten gebruiken om de juiste hashwaarde voor een nieuw blok te vinden. Door de juiste hashwaarde te vinden, mogen zij het blok aan de Blockchain toevoegen en ontvangen zij een beloning.

Single Point of Failure (SPOF): Het deel van een netwerk dat bij een storing de werking van het hele netwerk stopt.

SPOF: Zie Single Point of Failure.

Trusted Third Party (TTP): Vertrouwde tussenpersoon.

TTP: Zie vertrouwde derde partij.

Witboek: Een document dat beschrijft hoe een specifiek probleem wordt opgelost. Satoshi Nakamoto heeft in het Bitcoin-witboek geschreven hoe Bitcoin het probleem van dubbele uitgaven in een gedistribueerd netwerk oplost.

Blockchain 1.0: De eerste generatie Blockchains die voornamelijk zijn gebruikt om de opslag en overdracht van cryptocurrencies te vergemakkelijken.

Blockchain 2.0: De tweede generatie Blockchains die meer gericht zijn op het mogelijk maken van smart contracts, dApps en DAO's.

Blockchain 3.0: De derde generatie Blockchains die een cluster van problemen heeft opgelost waar blockchain 2.0 nog mee te maken heeft. Voorbeelden van dergelijke kwesties zijn schaalbaarheid, interoperabiliteit, privacy, duurzaamheid en governance.

Gas: Transactiekosten voor het uitvoeren van een transactie op de Ethereum Blockchain.

Gedecentraliseerde Applicatie (dApp): Een toepassing die gebruik maakt van de gedecentraliseerde gegevensopslag van een Blockchain. De applicatie wordt niet uitgevoerd

via een centrale server, maar via een gedecentraliseerd netwerk van nodes. Net als een normale applicatie heeft deze vaak een front-end en een gebruikersinterface.

Gedecentraliseerde Autonome Organisatie (DAO): Een autonome entiteit die ook afhankelijk is van het inhuren van individuen. Deze individuen kunnen bepaalde noodzakelijke taken uitvoeren die de entiteit niet kan uitvoeren. De DAO beschikt hiervoor over intern kapitaal, waarmee bepaalde activiteiten van deze individuen kunnen worden beloond. Wat een DAO fundamenteel anders maakt dan een gecentraliseerde organisatie, is dat zij geen topmanagementteam of CEO heeft. Het is een niet-hiërarchische organisatie.

Smart contract: Een contract met bepaalde voorwaarden die in code zijn vastgelegd. Het contract is zelfuitvoerend, aangezien het zelf de juiste overeenkomstige handelingen verricht wanneer aan de voorwaarden is voldaan. Het contract moet echter voldoende informatie bevatten van elke bij het contract betrokken partij om partijen de mogelijkheid te ontnemen het contract te beëindigen. Er zijn twee soorten slimme contracten: deterministische en niet-deterministische.

Solidity: De programmeertaal speciaal ontwikkeld voor Ethereum om slimme contracten te schrijven.