

# Symposiumverslag 'Cryptogeld'

mr. K.A. Kralj<sup>1</sup>

Op vrijdag 19 januari 2018 vond het door het IvO Center for Financial Law & Governance van de Erasmus School of Law georganiseerde symposium 'Cryptogeld' plaats.<sup>2</sup> Rondom cryptogeld<sup>3</sup> zoals de Bitcoin<sup>4</sup> spelen op dit moment tal van belangrijke vragen, zoals: gaat cryptogeld het geld<sup>5</sup> zoals wij dat nu kennen vervangen en, zo ja, wat zou dit kunnen betekenen voor het klassieke betalingssysteem en de rol van centrale banken? Is cryptogeld veilig en hoe zit het met het investeren in cryptogeld? Is er wellicht sprake van een zogenoemde *bubble*<sup>6</sup> en is cryptogeld kwetsbaar voor witwassen van fiat geld? Deze en andere vragen zijn aan bod gekomen tijdens het symposium met sprekers uit de sector, toezichthouders en wetenschap. De ontwikkelingen rondom crypto's worden kort in paragraaf 8 besproken en in paragraaf 9 is voor de volledigheid een overzicht van begrippen opgenomen.

## 1. Opening – Petra Hielkema

Het symposium ving aan met een welkomstwoord van Hielkema.<sup>7</sup> Samen met Coen Voormeulen

is Hielkema verantwoordelijk voor één van de kerntaken van De Nederlandsche Bank N.V. (hierna: DNB) namelijk een goede werking van betalingsverkeer en dat betekent dat het betalingsverkeer veilig, robuust en betrouwbaar moet zijn. Voormeulen zorgt voor het goud en de bankbiljetten en Hielkema voor de rest. Die zogenoemde 'rest' houdt volgens Hielkema in dat de centrale bank een belangrijke rol in het betalingsverkeer speelt. Iedereen met contant geld, zonder een klant te zijn van een bank, maakt deel uit van het betalingsverkeer in Nederland net als diegenen die een bankrekening aanhouden. Dit laatste geldt ook voor de interbancaire relaties waar DNB eveneens een rol speelt. Het laatste houdt in dat DNB banken 'bedient'<sup>8</sup> maar ook dat DNB controleert of geldstromen tussen banken goed lopen en of het onderpand dat banken aan DNB moeten verstrekken op orde is. Daarnaast houdt DNB ook toezicht op de marktinfrastuur. Tot slot is er een beleidsafdeling die zich met allerhande onderwerpen bezighoudt aan de marktinfrastuur-kant en retail-kant waarbij gedacht kan worden aan instant payments, cybercriminaliteit, interbancaire partijen maar ook aan innovatie, blockchain<sup>9</sup> en crypto's.

1. Katharina Kralj is toezichthouder bij de Autoriteit Financiële Markten en als docent verbonden aan de Erasmus School of Law. Dit artikel is op persoonlijke titel geschreven. De auteur is Adam Pasaribu zeer erkentelijk voor het kritisch nalezen van dit artikel en het geven van nuttige input. De kopij is afgesloten op 20 februari 2018.
2. De presentaties van de sprekers zijn via deze link te benaderen: <https://www.eur.nl/esl/research/institutes/center-financial-law-governance/symposium-cryptogeld> (laatst geraadpleegd op 20 februari 2018).
3. Naast de Bitcoin zijn onder meer de volgende altcoins bekend (geen uitputtelijke opsomming): Bitcoin Cash, Cardano, Dash, Eos, Ethereum, Iota, Litecoin, Monero, Neo, Ripple, en Zcash. Een cryptomunt heeft een public en private key. De private key wordt in een wallet (zie voetnoot 26) bewaard. Een private key kan ook worden geprint. Op die manier kan een cryptomunt fysiek worden bewaard.
4. De Bitcoin is de eerste digitale munt die ontworpen is door Satoshi Nakamoto (zie voetnoot 22). Andere digitale munten of te wel ander cyptovaluta dan de Bitcoin (zie voetnoot 3) worden AltCoins genoemd, waarbij Alt voor alternative staat.
5. Art. 1:1 Wft bepaalt dat onder geldmiddelen moet worden verstaan: chartaal geld (munten en bankbiljetten), giraal geld (bankrekening) en elektronisch geld (cadeaubonnen). Zie ook onder meer de uitspraak van de Rechtbank Overijssel, 14 mei 2014, ECLI:NL:GHARL:2016:4219, waar de rechtbank tot de conclusie is gekomen dat de Bitcoin niet kan worden aangemerkt als geld in de zin van Afdeling 6.1.11 BW, maar dient te worden gezien als ruilmiddel.
6. Een 'bubble' of 'bubbel' kan omschreven worden als bijvoorbeeld een marktprijs ver boven de waarde van een belegging ligt, denk hierbij aan de tulpenbollenmanie en internetbubbel.
7. Drs. Petra Hielkema is divisiedirecteur Betalingsverkeer en Marktinfrastuur bij De Nederlandsche Bank N.V.

8. Denk hierbij onder meer aan dat elke Nederlandse bank een geldrekening bij DNB aanhoudt.
9. Een blockchain is een gedistribueerde database die bestaat uit een keten van datablokken of te wel blocks. Gedistribueerd betekent dat deelnemers de data uitwisselen via een eigen peer-to-peer netwerk. Elke node (een node is bijvoorbeeld een computer of een ASIC-systeem, zoals een 'Antminer S5' die aan het netwerk verbonden is) beschikt over het volledige databasebestand of te wel over alle transacties die in de blockchain zijn gedaan. Bron: tijdschrift: 'Alle geheimen van Bitcoin en blockchain', p. 56 en p. 60, [www.fnl.nl](http://www.fnl.nl).

## 2. Inleiding – Kleis Broekhuizen

De dagvoorzitter, Broekhuizen,<sup>10</sup> nam vervolgens het woord en gaf aan dat het onderwerp van het symposium 'cryptogeld' zeer actueel is. De kranten staan vol met verwijzingen naar cryptogeld en dat is met name vanwege de enorme koersbewegingen van de afgelopen maanden.<sup>11</sup> Als voorbeeld noemt Broekhuizen de Bitcoin die in januari van dit jaar<sup>12</sup> enorm in waarde is gedaald. Broekhuizen vertelt dat hij in de *Financial Times*<sup>13</sup> over een aardige theorie heeft gelezen, namelijk dat die daling te maken zou kunnen hebben met het Chinese nieuw jaar. De gedachte is dat veel Chinezen in Bitcoins hebben belegd en dat met het oog op de feestdagen, ze de Bitcoins massaal hebben verkocht zodat ze over yuan renminbi<sup>14</sup> kunnen beschikken. Het is in China namelijk gebruikelijk om elkaar in het kader van het Chinese nieuw jaar geld te geven in een rood envelopje. Met Bitcoins gaat dat wat moeilijk omdat een Bitcoin niet fysiek is en dus niet in een envelop kan worden gestopt. De theorie is dan ook dat de Bitcoin door de Chinezen op zo'n grote schaal is verkocht met als gevolg een enorme koersdaling van de Bitcoin. In de kranten was verder ook volop te lezen dat vanwege de enorme koersstijging van de Bitcoin van de afgelopen tijd<sup>15</sup> er wellicht sprake is van een bubbel. Broekhuizen geeft aan dat hij het antwoord hierop niet kan geven. Wel is duidelijk dat vele toezichthouders waarschuwen<sup>16</sup> voor verliezen die beleggers kunnen lijden indien zij in cryptogelden beleggen.

In de financiële markten bezigt men vaak jargon en dat is in context van cryptogeld volgens Broekhuizen ook het geval. Er worden technische

termen zoals mining,<sup>17</sup> ICO's,<sup>18</sup> en tokens<sup>19</sup> gebruikt. Broekhuizen geeft aan dat het onderwerp van het symposium hierdoor technisch en complex is. Tot besluit geeft Broekhuizen aan dat gedurende het symposium vragen zoals, wat is cryptogeld, hoe werkt het, gaan cryptomunten het geld zoals wij dat nu kennen wellicht vervangen en hoe zit het bijvoorbeeld met de regulering van cryptogelden, aan bod zullen komen.

## 3. Speelveld, spelers en marktstructuur – Teunis Brosens

Mede naar aanleiding van de financiële crisis in 2008 en zijn rol als econoom bij ING is Brosens,<sup>20</sup> kort gezegd, meer geïnteresseerd geraakt in de rol van de financiële sector in de economie. Voor hem is het met de komst van de Bitcoin dan ook heel natuurlijk om zich af te vragen hoe het systeem van Bitcoin werkt met aanvullend daarop de vragen hoe werkt de rente, het monetair beleid en de kredietverlening bij de Bitcoin. In 2014 (of, zoals Brosens aangeeft, vijf eeuwen geleden in crypto-termen) heeft Brosens een filmpje op Youtube<sup>21</sup> gezet waarin hij heeft aangegeven dat de Bitcoin niet geschikt is als geld, onder meer omdat de hoeveelheid Bitcoins die kunnen worden uitgegeven vastligt en er geen centrale bank is die het monetair beleid kan voeren.

### 3.1. De decentrale belofte van de Bitcoin en blockchain

Brosens gaat in op het decentrale aspect en geldaspect van de Bitcoin. Hij gaat daarvoor terug naar de basis. De belofte van de blockchain is dat er geen tussenpersonen meer zijn. De belofte van blockchain is dat voor eenieder inzichtelijk is

10. Prof. mr. dr. Kleis Broekhuizen is Hoogleraar Recht & Regulering Financiële Markten bij Erasmus School of Law.

11. Zie onder meer *Het Financieele Dagblad*: 'Cryptovaluta's hard onderuit', 17 januari 2018 en 'Bitcoin maakt wilde rit', 2 februari 2018.

12. Zie onder meer *Het Financieele Dagblad*: 'Verlies bitcoin door plan handelsverbod in cryptowalhallen Zuid-Korea', 12 januari 2018.

13. *Financial Times*, 'Authers' Note: Happy Crypto-Chinese New Year', 17 januari 2018, <https://www.ft.com/content/25fbc1e-fb15-11e7-a492-2c9be7f3120a>.

14. De yuan renminbi is het officiële betaalmiddel van China.

15. Zie bijvoorbeeld *Het Financieele Dagblad*: 'Bitcoin is niet de moeder aller bubbels', 11 november 2017 en 'Die bitcoin slijt je wel weer aan een grotere onnozelaar', 23 december 2017.

16. Zie bijvoorbeeld: de AFM via de link: <https://www.afm.nl/nl-nl/professionals/onderwerpen/ico>, DNB via de link: <https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archieef/nieuws-2017/dnb365473.jsp> en European Securities and Markets Authority via de link: <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms> (laatst geraadpleegd op 20 februari 2018).

17. Mining of minen (in het Nederlands: delven) houdt samengevat in dat computers ingewikkelde rekensommen oplossen. Als de oplossing van een som is gevonden dan ontvangt een miner of te wel delver op dit moment 12,5 Bitcoins. Een miner lost niet alleen puzzels op, maar controleert ook de transacties die in een Block zitten waarvoor deze ook een beloning ontvangt.

18. Een ICO is een zogeheten Initial Coin Offering. Een ICO is een uitgifte van digitale tokens dan wel digitale munten die vooral wordt gebruikt door start-ups om projecten te financieren.

19. Zie bijvoorbeeld de link <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/> waar uitgelegd wordt wat het verschil is tussen coin, tokens en altcoins. Samengevat is een token is niets meer dan een nieuwe term om te verwijzen naar een waarde-eenheid die is uitgegeven door een privé-entiteit. Hoewel tokens veel overeenkomsten vertonen met Bitcoins (ze hebben een waarde die aan hen is gekoppeld en die door een community wordt geaccepteerd en op basis van blockchain zijn), hebben tokens een veel breder doel.

20. Drs. Teunis Brosens is senior econoom internationale en monetaire economie bij ING.

21. [https://www.youtube.com/watch?v=79H4CVq\\_\\_NM](https://www.youtube.com/watch?v=79H4CVq__NM).

hoe transacties zijn gedaan. Bij banken werkt dat anders. Banken die bijvoorbeeld onderling geld aan elkaar willen overmaken, doen die betalingen via de centrale bank en die centrale bank houdt in dat kader een database van transacties bij. Die database met transacties wordt door iedereen geaccepteerd. Volgens Satoshi Nakamoto,<sup>22</sup> de bedenker van de Bitcoin en blockchaintechnologie, moet die tussenpersoon zoals de centrale bank ertussen uit worden gehaald. De gedachte achter de blockchaintechnologie is dat partijen onderling zaken met elkaar doen en zelf hun eigen database bijhouden. Al die databases moeten dus synchroon met elkaar zijn, want anders is er een probleem. Brosens lijkt hier te doelen op het probleem dat indien de databases niet synchroon aan elkaar zijn, het niet duidelijk is welke database leidend is; oftewel welke database vervolgens als basis gebruikt dient te worden (toevoeging: KK).

Er zijn volgens Brosens, los van crypto-transacties, allerlei toepassingen van blockchain mogelijk. Het kadaster, waarin is vastgelegd wie welke woning bezit, kan bijvoorbeeld via een blockchain worden bijgehouden net zoals het vastleggen van een medisch dossier op de blockchain mogelijk is. Dit staat nog los van de vraag hoe met privacy moet worden omgegaan. Ook voor voedselveiligheid zou de blockchain kunnen worden gebruikt. Hij geeft het voorbeeld van een ei dat hij in zijn hand houdt dat door een hele keten van schakels is gegaan (van kip naar supermarkt). Via de blockchain kan inzichtelijk worden gemaakt of er in de tussenschakels bijvoorbeeld bestrijdingsmiddelen zijn gebruikt.

De vraag is dan ook: hoe doe je zaken in een wereld waar je niemand kent en hoe kan vertrouwen worden gecreëerd in een wereld waar je niemand kent? In een wereld waar je niemand kent, weet je niets over je tegenpartij, weet je niet of je tegenpartij te goede trouw is, weet je niet of je tegenpartij zijn systemen op orde heeft en hoe kun je zaken doen in een wereld zonder centrale tegenpartij waar je op kunt terugvallen? Brosens verwijst in dit kader naar het Mad Max-probleem.<sup>23</sup> Mad Max leeft in een wereld die zonder overheid opereert. Hij kan niet terugvallen op een centrale partij, zoals DNB, waardoor hij dus niet weet of hij op een tegenpartij waarmee hij zaken doet kan vertrouwen; immers

er wordt geen toezicht gehouden. Mad Max weet bijvoorbeeld niet als hij een transactie in Bitcoins met een tegenpartij doet, of die Bitcoins niet uit een crimineel circuit komen en hij weet ook niet of het geld wel echt is. Dat is het probleem van de blockchain. Satoshi Nakamoto heeft hiervoor twee oplossingen aangegeven, namelijk cryptografie en dat er een openbare transactiehistorie aanwezig moet zijn. Cryptografie in het kader van de Bitcoin houdt samengevat in dat je op de blockchain moet bewijzen dat je zegt wie je bent en dat je over een Bitcoin beschikt waarmee je kunt betalen. Dit moet ook door de anderen in de blockchain worden bevestigd. De openbare transactiehistorie houdt samengevat in dat alle transacties die sinds het allereerste begin van de blockchain, het Genesis block, zijn gedaan, inzichtelijk zijn. Hierdoor kan er geen transactiefraude worden gepleegd omdat iedereen vanaf het begin kan nagaan waar die Bitcoin is geweest. De miners zorgen voor die openbare transactiehistorie. Het toevoegen van transacties die in blocken aan de blockchain worden toegevoegd, kost moeite waardoor het moeilijk is om fraude te plegen maar kost ook heel veel elektriciteit. De beloning voor de miners die de block oplossen bestaat uit een blockreward,<sup>24</sup> op dit moment 12,5 Bitcoin, en daarnaast de transactiekosten die betaald worden door degenen die een transactie in Bitcoins doen.<sup>25</sup> Met betrekking tot de governance van de blockchain geeft Brosens aan dat de programmacode openbaar is of te wel iedereen kan bijdragen aan transparantie en dit leidt er toe dat er geen rare dingen in de Bitcoin zitten. In de praktijk blijkt de Bitcoin niet zo decentraal te zijn als werd beoogd omdat de individuele miners zich zijn gaan bundelen in coöperaties waardoor er meer kans is om een block te minen. Op dit moment controleren de drie grootste miners meer dan 50% van het netwerk. In theorie zouden zij de programmacode van de block kunnen wijzigen zodat er bijvoorbeeld dat er meer Bitcoins als blockreward worden uitgekeerd. Met betrekking tot de programmacode zijn er slechts 3 programmeurs die de sleutel hebben die de voorgestelde wijzigingen van andere programmeurs kunnen autoriseren oftewel die de broncode kunnen wijzigen. Met betrekking tot de handel in cryptogeld vindt 70% van de handel op een beurs plaats. Er is dan sprake van één wallet<sup>26</sup>

22. Satoshi Nakamoto, waarschijnlijk een pseudoniem en het is onduidelijk of het één persoon is of meerdere personen zijn, is of zijn de ontwerper(s) van de virtuele munt de Bitcoin en de blockchain technologie die daar achterligt. In 2008 heeft hij een paper gepubliceerd: 'Bitcoin: A Peer-to-Peer Electronic Cash System'. De paper is via deze link te raadplegen (laatst geraadpleegd op 18 februari 2018): <https://Bitcoin.org/Bitcoin.pdf>.

23. Mad Max is een Australisch sciencefictionfilm uit 1979, met als hoofdrolspeler Mel Gibson die de rol van Mad Max vertolkt. De film gaat over een post-apocalyptisch Australië, waar de macht van politie en overheid langzaam afbreekt en motorbendes de straten van de steden overnemen.

24. Een blockreward is een beloning die een miner ontvangt voor het succesvol oplossen van de rekensom die aan een block is verbonden, zie onder meer deze link: <https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/> (laatst geraadpleegd op 20 februari 2018). Bij de Bitcoin was de blockreward in het begin 50 Bitcoins. Als er 210.000 blocken zijn oplost, wordt de blockreward gehalveerd. De blockreward staat nu op 12,5 Bitcoin.

25. Zie deze link waarom er transactiekosten moeten worden betaald: <https://bitcoin.nl/nieuws/waarom-betalen-we-fees-99>.

26. Een wallet is een digitale portemonnee waarin cryptomunten kunnen worden bewaard. Om een wallet

die door de beurs wordt gehouden en transacties verlopen daarbij niet via een blockchain waardoor het decentrale aspect ook verdwijnt. Indien via een beurs in Bitcoins wordt gehandeld, is er dus sprake van een tussenpersoon namelijk de beurs en een eventuele claim in Bitcoins die op die beurs verloren raken ligt dan ook bij die beurs.<sup>27</sup> Binnen die beurzen waar de handel in Bitcoin plaatsvindt, is er ook sprake van centralisatie, de 4 grootste Bitcoin-beurzen nemen drie kwart van de handel voor hun rekening. Bitfinex heeft bijvoorbeeld 35% van het marktaandeel, Coinbase heeft een marktaandeel van 17%, Bitflyer 12% en Bitstamp 11%.<sup>28</sup>

### 3.2. Kwalificeert een Bitcoin of cryptogeld als geld?<sup>29</sup>

Brosens gaat vervolgens in op de vraag of een Bitcoin en (ander) cryptogeld als een rekeneenheid, ruilmiddel of opotmiddel kan kwalificeren. Volgens Brosens kan een Bitcoin niet als rekeneenheid kwalificeren. De waarde van de Bitcoin is namelijk extreem volatiel waardoor de Bitcoin niet als rekeneenheid kan worden gebruikt. Als voorbeeld geeft Brosens dat indien op een menu de prijzen in Bitcoin zouden worden weergegeven, de prijzen elke 5 minuten moeten worden aangepast. Of cryptogeld in theorie als rekeneenheid kan fungeren betwijfelt Brosens. Het probleem is daarbij dat de instabiliteit in de cryptovaluta zit ingebakken omdat het geldaanbod vastligt. Het geldaanbod van bijvoorbeeld Bitcoins groeit via een vaste formule en ligt vast op 21 miljoen. Brosens geeft aan dat

---

te creëren kan software op een computer worden gedownload. Maar ook via een mobiele app kan een wallet worden aangehouden of via een online dienst. Ook zijn er hardware wallets, die ook wel 'kluisen' of 'lockers' worden genoemd, en is een apparaat dat bijvoorbeeld via een USB stick op een computer kan worden aangesloten. Bekende hardware wallets zijn onder meer de Ledger Nano S, KeepKey en Trezor.

27. Denk hierbij aan Mt. Gox, een beurs in Tokio waar Bitcoins werden verhandeld, en in februari 2014 failliet is gegaan. Mt. Gox was gehackt en het gerucht gaat dat er tijdens de hack ook 850.000 Bitcoins zijn gestolen. Zie onder meer *Het Financieele Dagblad*: 'Mijn bitcoins brand ik op een dvd en die gaat in de kluis', 9 september 2017 en 'Schuldeisers proberen faillissement Mt. Gox ongedaan te maken', 13 december 2017 en <https://www.nu.nl/internet/3714876/mt-gox-honderden-miljoenen-bitcoins-verloor.html>. Zie ook de Bitcoinbeurs Coincheck in Tokio waar 523 miljoen Bitcoins met een waarde van bijna 500 USD zijn gestolen, *Het Financieele Dagblad*: 'Discussie over cryptovaluta's laait op na diefstal ter waarde van honderden miljoenen', 29 januari 2018.
28. Brosens verwijst in zijn presentatie naar de site van [bitcoinity.org](http://bitcoinity.org) en zijn overzicht is exclusief Koreaanse beurzen.
29. Zie bijvoorbeeld ook de uitspraak van Rechtbank Midden-Nederland van 7 december 2017, ECLI:NL:RB-MNE:2017:6646, waar voorzieningenrechter er vanuit gaat dat Ethereum een goed is en geen geld, vgl. HvJ EU 22 oktober 2015 C-264/15 (Hedqvist).

wat je eigenlijk wil is dat het geldaanbod actief beheerd wordt door een centrale bank indien vraag en aanbod fluctueert. Dit verhoudt zich slecht met het decentrale karakter van cryptogeld waar geen centrale bank aanwezig is en een algoritme het aanbod beheert. Een endogeen geldaanbod op basis van een algoritme is ingewikkeld maar is volgens Brosens in theorie niet onmogelijk. Als voorbeeld wordt de Tether genoemd die gekoppeld aan de USD is, maar dat komt omdat er iemand achter zit die de koppeling met de USD actief beheert en is daardoor geen zuivere cryptomunt.

De tweede vraag die Brosens behandelt, is of een Bitcoin als een ruilmiddel kwalificeert. Hij geeft aan dat de Bitcoin niet meer overal geaccepteerd wordt,<sup>30</sup> omdat het te duur is vanwege de hoge transactiekosten die per transactie ten tijde van het symposium zo rond de 30 USD ligt en de bevestiging van een transactie te lang duurt. Voor andere cryptomunten kan dit wellicht anders liggen. De oplossing voor deze problematiek voor de Bitcoin kan het lightning netwerk<sup>31</sup> zijn waar een aantal gebruikers van de Bitcoin een betalingskanaal openen en dus niet via de blockchain onderling transacties doen. Een nadeel hiervan kan zijn dat het minder veilig is en dat het gebruikersgemak afneemt. Brosens denkt dat het voor alle cryptocurrencies moeilijk is om het criterium van ruilmiddel te vervullen.

Met betrekking tot de vraag of een Bitcoin als opotmiddel kan worden gebruikt, verwijst Brosens naar de paper uit 2008 van Nakamoto<sup>32</sup> waarin een peer-to-peer electronic cash system wordt beschreven. Nakamoto wilde een systeem van elektronisch geld creëren zonder financiële instituties te betalen, zonder snel rijk te worden. Tien jaar later, in 2018, twittert John McAfee<sup>33</sup> onder

---

30. Zie bijvoorbeeld *Het Financieele Dagblad*: 'Gameswebshop Steam stopt met bitcoin-betalingen', 8 december 2017. Samengevat is de webwinkel voor computerspellen Steam gestopt met het accepteren van betalingen in bitcoins. Volgens het bedrijf zijn betalingen in bitcoins zo onbetrouwbaar en duur geworden, dat de cryptovaluta als betaalmiddel buitengewoon onpraktisch is.

31. Het lightning netwerk is een 'tweede laag' van een betalingsprotocol dat werkt bovenop een blockchain (meestal Bitcoin). Het maakt directe transacties mogelijk tussen deelnemende nodes en wordt aangeprezen als een oplossing voor het probleem van de schaalbaarheid van Bitcoins. Het beschikt over een peer-to-peer-systeem voor het maken van microbetalingen van digitale cryptocurrency via een netwerk van bidirectionele (beweging of actie is in twee richtingen mogelijk) betaalkanalen zonder de bewaring van gelden of vertrouwen aan derden te delegeren. Zie: J. Poon en T. Dryja, 'The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments', 14 januari 2016, <https://lightning.network/lightning-network-paper.pdf> (laatst geraadpleegd op 18 februari 2018).

32. Zie voetnoot 22.

33. John McAfee is de oprichter van het computer- en netwerkbeveiligingsbedrijf McAfee en is nu fulltime bezig met cryptocurrencies. Zie voor zijn twitterber-

meer over de Bitcoin, vanwege de laatste dip: *'The dip will drive sellers into fiat – because all crypto is affected. If you don't see that fiat is the walking dead, then you've missed the power of crypto'* en *'No matter where crypto settles, it's value will increase.'* Maar met betrekking tot Bitconnect,<sup>34</sup> dat recent ontmanteld is, worden op de website van reddit<sup>35</sup> berichten gepubliceerd als: *'Lost my savings in Bitconnect.'*<sup>36</sup> Reacties die op dit soort berichten volgen zijn of de Securities and Exchange Commission (hierna: SEC) niet zou moeten worden ingelicht zodat de SEC hier iets aan kan doen. Uit deze reacties blijkt volgens Brosens dat de cryptogemeenschap opnieuw het wiel aan het uitvinden is en dat ze dit heel snel doen. Hij denkt dat, gezien de ontwikkeling van het financiële stelsel van de afgelopen 200 jaar zoals freebanking in de VS in 1900 en het stelsel dat we nu kennen, crypto's diezelfde ontwikkeling doorgaan naar een gereguleerd en ordelijk stelsel. Of crypto's als oppotmiddel kunnen fungeren, daarvan zegt Brosens dat: *'the jury is still out'*.

### 3.3. Cryptovaluta, blockchain en ICO's: hype of revolutie?

Brosens rondt zijn betoog af met de vraag of er sprake is van een hype of revolutie. De sceptische conclusies die hij hierbij trekt, zijn onder meer dat de huidige generatie cryptovaluta onvolwassen is, gezien de schaalbaarheid, energieverbruik, volatiliteit, en governance. Een ander punt is de tot nu toe twee bewezen 'use cases' van cryptovaluta en ICO's namelijk criminaliteit en speculatie. Volgens Brosens blijft er behoefte aan dienstverlening waarbij een tussenpersoon betrokken is.

De positieve conclusies die Brosens noemt zijn onder meer dat de blockchain-beloofte, namelijk in een decentrale context, zonder vertrouwen en op een veilige manier handelen, wordt waargemaakt. Hij geeft daarbij aan dat de meeste problemen veelal praktisch van aard zijn en dus opgelost kunnen worden. Cryptovaluta en blockchain doorlopen, wat betreft innovatie, governance en regulering, in 20 jaar tijd een ontwikkeling door waar de traditionele financiële markten 200 jaar over hebben gedaan. Brosens rondt zijn betoog af met het volgende. ICO's kunnen een nuttige aanvulling zijn op het palet aan financieringsinstrumenten die voor bedrijven, en voor start-ups in het bijzonder,

beschikbaar zijn. Start-ups kunnen naar een bank stappen, of naar een venture capitalist of angel investor, maar ze kunnen ook proberen een ICO te doen. Een ICO is een aanvulling op het 'oude' palet, een vorm van crowdfunding, waaraan in principe iedereen kan meedoen, ook met kleine bedragen. Dat is volgens Brosens echt nieuw ten opzichte van andere financieringsinstrumenten. Daarbij noemt Brosens een ander positief punt, namelijk dat bij een ICO een aanvullend financieringsdocument zelf door de sector wordt geïnitieerd.

## 4. Emissie, handel en belegging – Leonard Franken

Franken<sup>37</sup> begint zijn voordracht met de vraag hoe een instelling een blockchain zou kunnen auditen. Er zit namelijk niemand achter een blockchain. Tijdens zijn voordracht zal hij daar tot zekere hoogte de aandacht op vestigen. De eerste blockchain is volgens Franken in 1453 ontstaan, namelijk door middel van een feoffment<sup>38</sup> van grondoverdracht in Schotland Tamper-proof te bewerkstelligen. Het Tamper-proof maken, of te wel het fraudebestendig maken van een document, houdt kort gezegd in dat het gebruik van grond door middel van handtekeningen en zegels over en weer werd vastgelegd. Een soort van eerste blockchain waarmee overdracht kon plaatsvinden.

### 4.1. Het creëren van een crypto

De term cryptogeld vermijdt Franken, hij spreekt liever over crypto's. Volgens Franken kan iedereen met behulp van de blockchaintechnologie een crypto creëren om daarmee geld te verdienen. Om dat laatste te verwezenlijken dienen er drie stappen te worden ondernomen. Als eerste moeten er een paar miljoen volgers worden gevonden die in het idee geloven dat ten grondslag ligt aan de uitgegeven crypto. Stap twee is dat je een crypto niet meer dan 1 keer kunt uitgeven. Als je het geld dat je bij een bank hebt staan meer dan 1 keer uitgeeft, dan sta je gewoon rood en dat is wat bijvoorbeeld de Bitcoin wil voorkomen (voorkomen van het double spending probleem of creëren van geld wat er niet is). De derde stap is dat degene die een crypto creëert er voor moet zorgen dat er niet te veel crypto's gecreëerd worden, of te wel volgens Franken moet je voor schaarste in de uitgegeven crypto zorgen, net zoals bij de Bitcoin waar slechts

richt de link: <https://www.trendsmat.com/twitter/tweet/953674427044069381> (laatst geraadpleegd op 18 februari 2018).

34. Bitconnect is/of was, dat is nog steeds niet duidelijk, een platform waaraan je bitcoins kon uitlenen. Zie verder deze link: <http://www.quotenet.nl/Nieuws/Ondergang-Bitconnect-sleept-Cryptogirl-mee-en-oud-Ajacië-Derk-Boerrigter-een-absurd-verhaal-209918> (laatst geraadpleegd op 18 februari 2018).

35. <https://www.reddit.com> (laatst geraadpleegd op 18 februari 2018).

36. [https://www.reddit.com/r/Bitconnect/comments/7qkgr/lost\\_my\\_life\\_savings\\_in\\_bitconnect/](https://www.reddit.com/r/Bitconnect/comments/7qkgr/lost_my_life_savings_in_bitconnect/) (laatst geraadpleegd op 18 februari 2018).

37. Dr. ir. Leonard Franken is senior toezichthouder Innovatie en Fintech bij Autoriteit Financiële Markten.

38. In de Middeleeuwen en met name onder het Europese feodale systeem, was de 'feoffment' of 'enfeoffment' een document waarmee een persoon land kreeg in ruil voor een onderpand van dienstbetoon. Dit mechanisme werd later gebruikt om beperkingen op het eigendomsrecht in het land te voorkomen door een systeem waarin een grondbezitter land zou geven aan één persoon voor het gebruik van een ander.

21 miljoen van kunnen worden uitgegeven. De garantie en daarmee de grote belofte van de blockchain is dat een crypto niet meer dan 1 keer kan worden uitgegeven, net als de schaarste van de crypto's. Als je die volgers hebt gevonden dan is er een stelsel van vertrouwen gecreëerd. Indien een uitgever van een crypto deze drie stappen volgt dan kan er in principe geld worden verdiend.

#### 4.2. Het huidige systeem vs het systeem van crypto's

Het huidige systeem van emissie, handel en belegging zoals dat nu bestaat, bestaat uit een centraal systeem met beurzen, handelaren, banken, clearing en settlementsystemen, custodians en consumenten. Hierbij is een stelsel van vertrouwen over een periode van 200 jaar gecreëerd door middel van regels, toezicht, organisaties en spelers op de financiële markten. Daarnaast is er sprake van een infrastructuur die evolueert, waarbij Franken de punten legacy, vernieuwing en innovatie benoemt die langzaam doorgroeien. Het huidige systeem zorgt volgens Franken voor emissie waarbij gedacht kan worden aan het uitgeven van aandelen door een onderneming, correcte transacties in geval van handelen, betalen en beleggen, en de rol hierbij van de banken en de toezichhouders. Daarnaast bestaat er een consensus tussen alle marktpartijen over toestand van het systeem, zoals bijvoorbeeld wie wat bezit.

Het huidige systeem is anders dan bij crypto's. De blockchain is decentraal terwijl het huidige systeem centraal is. Ook het vertrouwen in crypto's is anders geregeld dan in het huidige systeem doordat het gebaseerd is op software en algoritmes die aan een crypto ten grondslag ligt. De algoritmes dwingen namelijk de werking van de blockchain en crypto's af. De nieuwe infrastructuur van crypto's is verder niet gebaseerd op enige legacy, maar op internet en de blockchain die daarop ligt. Wat wel blijft gelden voor de blockchain is de noodzaak voor emissie, correcte transacties, geen double spending en consensus. In de regel is het mechanisme om de transacties in de verschillende crypto's te bewerkstellingen redelijk generiek. De transacties worden zonder tussenkomst van een derde partij bewerkstelligd en vindt plaats tussen twee adressen of wallets. Vanuit Wallet A kan een waarde, zoals een coin, crypto of token overgedragen worden naar wallet B. De transactie wordt vervolgens 'getekend' met een digitale handtekening waardoor de transactie vastligt en iedereen kan zien dat vanuit wallet A een waarde is overgedragen naar wallet B. Per crypto kan er een andere digitale handtekening nodig zijn omdat er veel verschillende algoritmes zijn waarmee een digitale handtekening gezet kan worden. Franken geeft aan dat hij over wallets spreekt omdat je de persoon die achter een transactie zit, niet kunt zien. Die anonimiteit is volgens Franken een groot goed in het netwerk.

Om een transactie te bewerkstelligen is er uiteindelijk toch een derde partij of te wel een

miner nodig. De miner kijkt naar de correctheid van een transactie: klopt het wat diegene die achter wallet A zit heeft gedaan, bezat de eigenaar van wallet A hetgeen dat aan wallet B is overgedragen en klopt de handtekening? Daarnaast is consensus belangrijk. Er moet consensus bestaan over de nieuwe toestand en of een coin of token niet twee of meerdere keren door de eigenaar van wallet A is uitgegeven, oftewel het double spending issue. De miner controleert iedere transactie en vult de block met die gecontroleerde transacties die vervolgens verzegeld wordt en daarmee is afgesloten. De vraag hierbij is welke miner het volgende nieuwe block mag gaan bepalen, want die bepaalt wat de volgende toestand van het netwerk is. In de normale wereld gebeurt dit door een bank, maar niet bij crypto's. In het decentrale systeem waar een heleboel miners over die toestand kunnen beslissen, moeten zij het met elkaar eens worden. Je wilt voorkomen dat dezelfde miner de nieuwe toestand bepaalt. Dit omdat er dan mogelijkheden voor fraude ontstaan. Bij de Bitcoin is dit opgelost door een complexe rekensom aan het block te koppelen. Wie die rekensom als eerste oplost mag, nadat 51% van de andere miners het eens zijn met de oplossing, bepalen wat het volgende block wordt. De miner krijgt hiervoor een beloning namelijk de transactiefee en een beloning voor het oplossen van de rekensom.

In een decentraal systeem waar je niet op elkaar kunt vertrouwen, kan op verschillende wijzen worden vastgelegd hoe die consensus bereikt kan worden. Hoe die consensus bereikt kan worden hebben ze volgens Franken al heel vroeg bij Byzantium ontdekt en daar komt het probleem ook vandaan, ook bekend als het Byzantijns generaals probleem.<sup>39</sup> Er waren 13 generaals met legers die met elkaar een gemeenschappelijk doel hadden namelijk de hoofdstad van Byzantium belegeren, maar ze vertrouwden elkaar niet en de berichtgeving kon mank zijn. Alleen een gelijktijdige aanval kon tot verovering van de stad leiden. Doordat er zich mogelijk verraders onder de generaals bevonden, wist men niet welke berichtgeving over het tijdstip van aanval te vertrouwen was. Het betrouwbaar overeenstemmen over het tijdstip van de aanval was alleen mogelijk als minder dan een derde van de generaals de berichten saboteerde.<sup>40</sup> Om dit probleem tussen de miners bij de Bitcoin op te lossen, moet daarom een rekensom worden opgelost en degene die de rekensom als eerste oplost, heeft het dus voor het zeggen. Een klein aantal 'corrupte miners' (minder dan 49%) kan er niet toe leiden dat er een verkeerde nieuwe toestand geaccepteerd

39. L. Lamport, R. Shostak, M. Pease, 'The Byzantine Generals Problem', *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, juli 1982, p. 382-401, te benaderen via deze link: <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf> (laatst geraadpleegd op 20 februari 2018).

40. Bron: tijdschrift *Alle geheimen van Bitcoin en blockchain*, p. 59, [www.fn1.nl](http://www.fn1.nl).

wordt. Het is hierdoor wel een soort van loterij geworden wie op welk moment wat mag zeggen.

Met betrekking tot de emissie geeft Franken aan dat het niet uitmaakt wat er op een blockchain zit. Er kunnen bijvoorbeeld huizen, goederen, auto's, coins, crypto's, smart contracts en tokens opzitten. Iedere blockchain heeft zijn eigen kenmerken waar die beter of minder goed in is en dat is volgens Franken bijzonder. Franken geeft aan dat men zegt dat ze crypto's kopen en in de blockchain beleggen, maar volgens Franken koopt men crypto's waarvan men hoopt dat die in waarde stijgen omdat niemand, behalve wellicht de miners, in de achterliggende technologie of te wel de blockchain belegt. Ook geeft Franken aan dat iedereen een token of crypto kan creëren. Hij verwijst onder meer naar de Ripple, waarvan de tokens XRP initieel in het bezit van de bedenkers van deze crypto waren die ze nu langzaam aan het verkopen zijn. De Bitcoin is hier volgens Franken iets democratischer in want bij Bitcoin wordt er bij ieder block die gecreëerd wordt, een aantal nieuwe Bitcoins gecreëerd wat de emissie binnen het systeem is.

In de cryptomarkt heeft iedere coin zijn eigen blockchain. Er zijn meer soorten coins, meer dan 1300, dus meer dan het aantal landen dat de wereld kent en Franken vraagt zich af of het aanbod van het aantal coins wel reëel is. Het verschil tussen bijvoorbeeld een Bitcoin en een ICO en token is dat op de ethereum blockchain iedereen een token kan aanmaken die je kunt verkopen. Een token kan kwalificeren als een schuldbewijs, of een token kan worden uitgegeven in het kader van crowdfunding, maar kan ook een bioscoopkaartje zijn. Het verhaal dat achter een uitgegeven token ligt is erg belangrijk en als je een token koopt dan hoop je dat diegene die de token heeft uitgegeven eventuele winsten met je deelt. Een krachtig maar ook een riskant instrument.

Het ecosysteem van crypto's staat volledig buiten het financiële systeem. Cryptobeurzen vallen niet onder toezicht.<sup>41</sup> Op het darkweb zijn communities waar strategieën worden besproken om koersen te beïnvloeden. De blockchains waar je tokens en crypto's op kunt maken zijn complete ecosystemen en als deze ecosystemen circulaire economieën worden dan kunnen ze niet meer genegeerd worden volgens Franken. De crypto ecosystemen raken de huidige economie bij de handelaren. Handelaren in crypto's zitten op dit moment op het interface vlak waar fiatgeld gewisseld wordt voor cryptovaluta. Het groeien van dit ecosysteem is een uitdagend verhaal ook voor de auditor van dat systeem, want de vraag die daarbij rijst is hoe een auditor daar

toezicht op kan houden. Het decentrale systeem past niet binnen de huidige gedachte om één legal entity te kunnen aanspreken op de beheerste bedrijfsvoering, die legal entity is er gewoon niet.

### 4.3. Afsluiting

Franken rondt af met de opmerking dat het decentrale systeem niet binnen het huidige denkpatroon of wetgevingskader valt. Onder meer zijn de miners onbekend. Volgens Franken zijn er op dit moment 12.000 Bitcoin miners op de wereld, de clusters daarbij in geteld, en Nederland staat wereldwijd op vijfde plaats qua hoeveelheid miners, na de Verenigde Staten, Duitsland, China en Frankrijk. Er is een verandering in het traditionele bankieren door een switch in vertrouwen in techniek en algoritmes. Governance is wel een onderdeel van dit vertrouwen, waaronder wie de besluitvorming neemt en hoe dit in elkaar zit. Dit governance model wijkt sterk af van hetgeen we kennen vanuit de traditionele financiële sector. Een interessant onderwerp naar de mening van Franken om verder naar te kijken mede gezien hoe hier toezicht op moet worden gehouden.

## 5. Geld, betaalsysteem en toezicht – Kirsten van Driel

Van Driel<sup>42</sup> is binnen DNB betrokken bij blockchain experimenten en begint haar betoog met dat technische innovatie niet alleen van buiten af moet worden bekeken maar ook dat je het moet snappen en doorgronden. Ze haakt hiermee in op de voordrachten van Brosens en Franken. Haar voordracht is technisch en bondig. Een aantal vragen dat bij de Bitcoin speelt, is volgens Van Driel of de Bitcoin voor een breder publiek geschikt is als betaalmiddel en of de Bitcoin gezien moet worden als een speculatiemiddel dan wel belegging. Oorspronkelijk is de Bitcoin bedoeld als betaalmiddel, maar als zodanig wordt de Bitcoin relatief weinig gebruikt. De indruk van Van Driel is daardoor dat de Bitcoin zich nog in een onvolwassen fase bevindt en daarom dit moment niet geschikt is als betaalmiddel en dus ook niet geschikt voor een breder publiek.

### 5.1. Knowhow, schaalbaarheid en milieubelasting

Volgens Van Driel vereist de Bitcoin technische knowhow waardoor de Bitcoin niet geschikt is voor een breder publiek. Als voorbeeld geeft Van Driel het aanmaken van een wallet waar je een Bitcoin in bewaart. Dit kan op verschillende manieren, bijvoorbeeld op een PC, mobiele telefoon of USB stick. Daarnaast betaal je niet aan een persoon

41. De herziene vierde anti-witwasrichtlijn brengt hier verandering in, Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering en tot wijziging van Richtlijn 2009/101/EG, COM (2016) 450, zie hierover meer in paragraaf 6.

42. Drs. Kirsten van Driel is beleidsmedewerker betalingsverkeer bij DNB.

maar aan een Bitcoin-adres en zijn termen zoals een private key<sup>43</sup> niet bij het breder publiek algemeen bekend. Hierdoor is een breed gemak nog niet aan de orde en op dit moment nog niet haalbaar.

Daarnaast geeft Van Driel aan dat de technologie achter de Bitcoin nog niet schaalbaar is. Gemiddeld worden 2200 transacties in Bitcoin in een block gestopt en dat is weinig, temeer omdat er doorgaans 160.000 tot 200.000 transacties staan te wachten om opgenomen te worden in een block. Het vormen van een block kan van een minuut tot een uur duren, waarbij Van Driel aangeeft dat het gemiddeld 10 minuten duurt om een block te vormen, oftewel dat een transactie wordt afgewikkeld. De duur van het afwikkelen van een transactie en de hoeveelheid van transacties die in een block kunnen worden afgewikkeld is volgens Van Driel in de software vastgelegd, maar ondanks die software is het niet bekend wanneer een transactie in een block wordt opgenomen en kan zo een uur duren. Daarbij komt dat de transactiekosten erg hoog zijn, met name als je een transactie snel wil laten doorvoeren. Afhankelijk waarvoor gekozen wordt, kan een transactie binnen 2 blokken worden opgenomen en dat kost op het moment van het symposium ongeveer 19 USD<sup>44</sup> aan transactiekosten waardoor het betalen met een Bitcoin voor kleine aankopen niet geschikt is. De miners bepalen welke transacties in een block worden opgenomen en bepalen de transactiefees. Van Driel geeft aan, zoals ook eerder werd aangegeven door de andere sprekers, dat je als miner voor het oplossen van de rekensom die aan een block verbonden is 12,5 Bitcoin ontvangt alsmede een transactiefee, wat op ongeveer 15 tot 16 Bitcoins neerkomt en dat is een bedrag van ongeveer 180.000 USD. Omdat er zoveel geld mee kan worden verdiend, is minen zeer populair en een keerzijde daarvan is dat dit tot milieubelasting leidt. Het minen van een block kost namelijk erg veel elektriciteit. Van Driel geeft aan dat de Bitcoin hiermee een 'vies product' is.

## 5.2. Volatiliteit, governance, anonimiteit en finaliteit

Net als de vorige sprekers geeft Van Driel aan dat de waarde van de Bitcoin een enorme volatiliteit kent en daardoor niet geschikt is als betaalmiddel. Ook het beleggen in Bitcoin is door de enorme schommeling in waarde zeer risicovol. Met betrekking tot governance geeft Van Driel aan dat er bij de Bitcoin sprake is van een peer-to-peer netwerk.<sup>45</sup> Dit houdt in dat indien een transactie

in Bitcoin wordt gedaan er geen centrale partij die je kunt aanspreken. Ook is er geen garantiestelsel en met betrekking tot de aansprakelijkheid is er niets geregeld. Daarnaast is het doorvoeren van wijzigingen in het systeem door de 'gemeenschap' niet flexibel waardoor veranderingen moeilijk kunnen worden doorgevoerd. De pseudoanonimiteit van de Bitcoin is eveneens een grote zorg van DNB. Omdat betalingen van een Bitcoinadres worden gedaan kun je niet zien wie er achter een transactie in Bitcoins zit. Hierdoor is de Bitcoin volgens Van Driel niet geschikt als betaalmiddel voor een breder publiek. Tot slot gaat Van Driel in op hoe het met de finaliteit zit. Als je met cash of met je pinpas betaalt, dan weet je zeker dat de transactie wordt bevestigd en is er sprake van finaliteit. Bij crypto's is dat niet het geval omdat niet duidelijk is of, en zo ja wanneer, een transactie wordt afgewikkeld, zelfs niet indien de transactie in een block is opgenomen. Het kan namelijk zo zijn dat er een fork<sup>46</sup> in de blockchain ontstaat. Een fork ontstaat als volgt. Mensen schieten vanuit de hele wereld blokken in en die blokken worden in de blockchain opgehangen. Het kan zo zijn dat blokken tegelijkertijd aan de blockchain gehangen worden, en dat zijn dan niet dezelfde blokken. Pas op het moment één streng van de blockchain langer is dan wordt dat de leidende blockchain. Indien een transactie in een block zit, die niet in de leidende vertakking van de blockchain zit, dan kan het zijn dat de transactie niet wordt afgewikkeld. Volgens Van Driel wordt een fork doorgaans na 2 of 3 blokken opgelost<sup>47</sup> en moet je volgens Van Driel 6 blokken wachten voordat je zeker weet dat een transactie definitief is. Het kan ook nog zo zijn, en volgens Van Driel wordt dit de fifty-one percent attack genoemd, dat een groep van miners zich gaat verenigen die samen heel veel rekencapaciteit hebben en daardoor een transactie kunnen manipuleren. Door die grote rekencapaciteit kunnen die miners een transactie wijzigen die vervolgens in een block wordt gezet en door de grote rekenkracht kunnen zij ervoor zorgen dat alle blokken die daarna komen door die groep miners gemined zijn waarmee de betreffende transactie gemanipuleerd is. Volgens Van Driel is dit op dit moment nog een theoretisch

---

lijst (de blockchain) met alle transacties, zodat door middel van synchronisatie gecontroleerd kan worden of toekomstige transacties geldig zijn en dubbele transacties voor komen worden, zie hierover meer het tijdschrift *Alles geheimen van Bitcoin en blockchain*, p. 7.

43. Zie voetnoot 3.

44. Vermoedelijk ligt het verschil in de door Brosens genoemde transactiekosten van USD 30 en van Van Driel in het feit dat de transactie van Van Driel in het tweede block wordt opgenomen en de transactie van Brosens in het eerste block, zie bijvoorbeeld: <https://charts.bitcoin.com>.

45. Een peer-to-peer netwerk is een gedecentraliseerd digitaal systeem. Elke peer in het netwerk heeft een

46. Een fork is simpel gezegd een vertakking van de blockchain. In een blockchain worden nieuwe blokken tegelijkertijd door alle miners berekend. Als meerdere miners op hetzelfde moment de oplossing van een Block vinden kan een fork ontstaan, waardoor de blockchain meerder vertakkingen krijgt. Alleen de langste tak wordt gehandhaafd. Bron: tijdschrift *Alle geheimen van Bitcoin en blockchain*, p. 59, [www.fnl.nl](http://www.fnl.nl).

47. Zie bijvoorbeeld: <https://bitcoin.nl/nieuws/in-het-kort-hard-fork-vs-soft-fork-150>.

verhaal, maar ze geeft daarbij mee dat je daarom sowieso 6 blocken moet wachten voordat zeker is dat een transactie definitief is. Zij eindigt haar voordracht met de opmerking dat er ook andere blockchains zijn, dan de Bitcoin blockchain die nog in een experimentele fase zitten, zoals een blockchain voor de voedselindustrie, vastgoed of diamanten en zij verwacht dat over een paar jaar deze blockchains in productie zullen zijn.

## 6. Cryptogeld en cybercrime – Rutger de Doelder

De Doelder<sup>48</sup> wil de cryptocurrencies vanuit het witwasperspectief bekijken en volgens De Doelder is er bij cryptocurrencies vaak sprake van een moderne variant van hawala bankieren,<sup>49</sup> ook bekend als ondergronds bankieren. Tijdens zijn voordracht laat hij een foto zien van een winkel in Rotterdam-west, waar ondergronds bankieren plaatsvond door het internationaal overmaken van geld waarop geen toezicht stond en waar de politie een inval heeft gedaan.<sup>50</sup> Juridisch gezien zou je tegen hawala bankiers kunnen optreden omdat zij zonder vergunning opereren. Bij de Bitcoin loopt dit volgens De Doelder juridisch spaak omdat er bijvoorbeeld geen sprake is van centrale partij die een vergunning zou moeten aanvragen. De Doelder geeft aan dat hij blij is dat er Kamervragen<sup>51</sup> over het witwassen van virtuele valuta zijn gesteld en of dit niet gereguleerd zou moeten worden om het criminelere wat lastiger te maken, waarbij hij ook naar het sentiment in Frankrijk en Zuid-Korea verwijst die bezig zijn om extra regels opstellen. De vraag die De Doelder daarbij stelt is of het überhaupt nodig is om regels te maken en zo ja, wat voor effectieve regels er dan gemaakt moeten worden.

### 6.1. Anonimiteit en witwasrisico's

Er is op dit moment volgens De Doelder een redelijk goed systeem om witwasrisico's met

48. Mr. Rutger de Doelder is als wetenschappelijk docent en onderzoeker verbonden aan de Erasmus School of Law.

49. Zie bijvoorbeeld M.R. J. Soudijn en E.M. de Groen, 'De criminele levensloop van hawaladars. Een verkennend onderzoek', *Justitiële verkenningen*, 2015, p. 66, waar zij aangeven dat hawala systemen zijn, waarbij geld wordt overgemaakt via niet-reguliere financiële instellingen, ook wel *informal value transfer systems* genoemd. De term hawala wordt met name gebruikt in relatie tot de Indiase, Afghaanse en Pakistaanse gemeenschap.

50. Zie *Het Algemeen Dagblad*, 'Rotterdamse sigarenzaak is de bank van de onderwereld', 6 januari 2015, en 'Primera haalt naam weg van 'bank van de onderwereld'', 22 januari 2015.

51. Antwoorden op vragen van het lid Van der Linde (VVD) over het bericht 'Maatregelen tegen witwassen weinig effectief' van 3 januari 2018 (2018Z00025), 16 februari 2018.

betrekking tot Bitcoins, maar ook vanuit een breder perspectief, vanuit de overheid te mitigeren. Vanuit het perspectief witwasbestrijding is De Doelder niet ongelukkig over de ontwikkelingen die nu gaande zijn en dat komt met name omdat de grote cryptovaluta al heel transparant zijn, waarbij hij verwijst naar de voordracht van Brosens over de openbare transactie historie. Die openbare transactie historie biedt mogelijkheden om te onderzoeken wat er met bepaalde Bitcoins is gebeurd. Bitcoins die worden verhandeld zitten in een wallet waaraan een code, oftewel het Bitcoin-adres, is gekoppeld en dat Bitcoin-adres kan gezien worden als een bankrekeningnummer en is openbaar. Met het Bitcoin-adres kun je naast de transactiehistorie zien hoeveel geld iemand op zijn rekening heeft staan, oftewel in zijn wallet heeft. Bij het idee dat cryptocurrencies anoniem zijn, geeft De Doelder aan dat door de openbare blockchain de cryptocurrencies als pseudoanoniem moeten worden gezien oftewel zoals De Doelder het noemt 'pseudoniem'. De witwasgevoeligheden van die cryptocurrencies worden hierdoor minder. Met cryptomunten die zich richten op niet-openbare blockchains moet wel voorzichtig worden omgegaan.

Volgens De Doelder is men niet zo succesvol om crimineel geld op te sporen aangezien er op dit moment volgens hem ongeveer 1% zicht is op het crimineel vermogen waar beslag op zou kunnen worden gelegd. Het is dus niet zo dat door de opkomst van de cryptocurrencies het witwassen veel makkelijker gaat worden. Het feit dat criminelen op dit moment 99% van het criminele vermogen verborgen weet te houden, geeft aan dat het nu ook niet moeilijk is om geld wit te wassen omdat er al criminele infrastructures voor ontwikkeld zijn, zoals bijvoorbeeld het hawala bankieren.

### 6.2. De herziene vierde anti-witwasrichtlijn en overige regulering

De Doelder vindt het gunstig dat er een update van de vierde anti-witwasrichtlijn heeft plaatsgevonden, mede in het licht van de cryptocurrencies, en wordt ook wel de vijfde anti-witwasrichtlijn<sup>52</sup> genoemd. Op grond van de vierde anti-witwasrichtlijn<sup>53</sup> moet

52. Voorstel voor een Richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering en tot wijziging van Richtlijn 2009/101/EG, COM (2016) 450.

53. Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, *PbEU* 2015, L 141.

er een UBO-register<sup>54</sup> komen dat inzichtelijk maakt wie de uiteindelijke belanghebbende van een rechtspersoon is. In het kader van transparantie vindt De Doelder dit een goede ontwikkeling maar in de vierde anti-witwasrichtlijn<sup>55</sup> die in 2015 was aangenomen, is de Europese wetgever de cryptocurrencies vergeten. De Europese Commissie heeft daarom in juni 2016 een voorstel ingediend om de vierde anti-witwasrichtlijn te updaten om de cryptocurrencies te reguleren en afgelopen december 2017<sup>56</sup> is het akkoord in Brussel bereikt. De implementatie van deze update dient volgens De Doelder in Nederland over anderhalf jaar plaats te vinden maar hij ziet mogelijkheden om het aan de implementatiewet van de vierde anti-witwasrichtlijn toe te voegen. De Doelder gaat kort in op wat de Wet ter voorkoming van witwassen en financieren van terrorisme<sup>57</sup> regelt en geeft daarbij aan dat het een preventieve wet is die witwassen en financieren van terrorisme moet tegengaan. In die wet zijn een hoop poortwachters aangewezen die moeten helpen om het financieel stelsel 'schoon' te houden waarmee hij bedoelt dat er geen crimineel geld door het stelsel mag stromen. Als voorbeeld noemt De Doelder banken, betaalinstanties en makelaars die een rol als poortwachter hebben. Zij moeten klanten identificeren en hebben een meldplicht indien er ongebruikelijke transacties plaatsvinden.

De reikwijdte van de richtlijn wordt verruimd naar platforms of wisselkantoren die wisseldiensten voor fiatgeld en cryptogeld aanbieden, waardoor zij die poortwachterfunctie ook krijgen. Ze moeten klanten identificeren, hebben een meldplicht indien er ongebruikelijke transacties plaatsvinden en criminele activiteiten tegenhouden. Dit geldt ook voor de 'custodian wallet provider' waarbij hij verwijst naar de definitie van 'virtual currencies' die als volgt luidt: *'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically'*.<sup>58</sup>

54. De afkorting UBO staat voor Ultimate Beneficial Owner, oftewel de uiteindelijke belanghebbende, zie art. 1, eerste lid, onder f, Wwft. Zie art. 30 Richtlijn (EU) 2015/849 voor het UBO-register.

55. De vierde anti-witwasrichtlijn diende uiterlijk op 26 juni 2017 in Nederlandse wetgeving te zijn geïmplementeerd (zie art. 67 Richtlijn (EU) 2015/849), maar die deadline is niet gehaald.

56. Zie 2016/0208 (COD): te raadplegen via [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST\\_15849\\_2017\\_INIT&from=NL](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15849_2017_INIT&from=NL) (laatst geraadpleegd op 18 februari 2018).

57. *Sib.* 2008, 303, zoals laatstelijk gewijzigd op 19 november 2014, *Sib.* 2014, 472. De implementatiedatum van 26 juni 2017 heeft Nederland niet gehaald. Zie hierover meer: J.M. van Poelgeest, 'De implementatie van de vierde en vijfde anti-witwasrichtlijn', *OeF* 2017, p. 46 e.v.

58. Art. 1, tweede lid, onder c 2016/0208 (COD).

De definitie van 'custodian wallet provider' gaat als volgt luiden: *'an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies'*.<sup>59</sup>

De open norm met betrekking tot criminaliteit staat in het Wetboek van Strafrecht en kort gezegd houdt die open norm het volgende in. Indien er een redelijk vermoeden is van criminaliteit dan moet je daar je handen van aftrekken en mag je er niets mee doen. Als voorbeeld geeft De Doelder een gestolen fiets die te koop wordt aangeboden. Met de Bitcoin is dit niet anders; als daar criminele activiteiten aan verbonden zijn dan mag je daar niets mee doen. Het Openbaar Ministerie en het Financial Intelligence Unit Nederland hebben witwastypologieën met betrekking tot virtueel betaalmiddelen ontwikkeld die op 15 augustus 2017 zijn vastgesteld.<sup>60</sup> Ze geven daarbij aan dat als er criminele activiteiten aan een Bitcoin vastzitten, dan mag die Bitcoin niet geaccepteerd worden.<sup>61</sup> Deze witwastypologieën, die vastgesteld zijn naar aanleiding van een onderzoek naar aan- en verkopen van virtuele betaalmiddelen, kunnen wat De Doelder betreft wellicht een tandje strenger. De Doelder geeft aan dat het hem niet vreemd naar voren komt dat als iemand een grote som in Bitcoins accepteert die mogelijk afkomstig zijn uit het criminele circuit en die door een 'mixer' zijn gehaald waar fiat geld voor betaald is, zich voor de strafrechter moet verantwoorden. Ook voor chartaal geld zijn typologieën ontwikkeld. Indien je een bankbiljet van 500 euro ontvangt, dan zou je je moeten afvragen waar dat biljet vandaan komt omdat het algemeen bekend is dat deze biljetten met name in het criminele circuit worden gebruikt. Op een bepaald moment geldt er voor de ontvanger een onderzoeksplicht bijvoorbeeld indien een Bitcoin door een mixer is gegaan of zoals bij het voorbeeld van de gestolen fiets. Pas als je alle onderzoek hebt gedaan om vast te stellen dat het niet om een crimineel object gaat zou je het object kunnen accepteren.

De Doelder geeft aan dat ook in de praktijk wordt nagedacht wat er verwacht wordt met betrekking tot het voorkomen van witwassen. Hij verwijst hierbij naar het stoplichtconvenant tussen de Makelaarsvereniging Amsterdam, de politie Amsterdam-Amstelland en de Dienst Basisinformatie Amsterdam die voor verhuurders van onder meer woningen is opgesteld.<sup>62</sup> Indien een verhuurder van een appartement het vermoeden

59. Art. 1, tweede lid, onder d, 2016/0208 (COD).

60. <https://www.fiu-nederland.nl/nl/witwas-typologieen-0>, onder punt 2.2 (laatst geraadpleegd op 20 februari 2018).

61. Zie hierover ook: S. Visser, 'Nieuwe witwastypologieën in de strijd tegen witwassen met virtuele betaalmiddelen', *TBSøH*, december 2017, nr. 4, p. 217-223.

62. Het stoplichtconvenant is te benaderen via: <https://www.mva.nl/pdf/flyer%20stoplicht%20convenant%20tbv%20makelaars%20def.pdf>.

heeft dat er sprake is van criminaliteit, bijvoorbeeld indien huurder elke maand zijn huur van 3.000 euro in cash betaalt, dan moet je als verhuurder onderzoek doen. Je ziet in gebieden die gevoelig zijn voor criminaliteit convenanten worden ontwikkeld en dat puur vanwege de open normen in het strafrecht. Met betrekking tot Bitonic geeft De Doelder aan dat dit platform waar cryptogelden worden verhandeld inmiddels met justitie in overleg is om te bekijken hoe criminele transacties voorkomen kunnen worden.<sup>63</sup> De Doelder ziet dit als een gunstige ontwikkeling.

### 6.3. Cryptovaluta: kans of bedreiging?

De Doelder geeft tot slot aan dat hij dacht dat het moeilijk zou zijn om te kunnen zien of een virtuele munt door een mixer is geweest en dat je technisch onderlegd zou moeten zijn om de blockchain helemaal te kunnen analyseren. Maar zelfs juristen zouden dit volgens de technische collega's van De Doelder moeten kunnen zien. Hij verwijst hierbij naar een tool Etherscan dat voor en door ethereum is ontwikkeld. Als een nummer van een wallet in Etherscan wordt ingevuld, dan wordt een lijst met transacties getoond maar waar ook zichtbaar is van wie betalingen afkomstig zijn en aan wie betalingen in ethereum zijn gedaan.

De boodschap die De Doelder wil meegeven is dat extra regulering voor cryptogeld volgens hem niet nodig is. Het maken van convenanten is zeker nuttig net als het aansporen van wisselkantoren van cryptogeld om standaard onderzoek te doen in geval van een grote of verdachte transactie. De Doelder komt hiermee tot de conclusie dat cryptovaluta met betrekking tot de opsporing van criminele activiteiten meer een kans dan bedreiging is.

## 7. Enkele vragen vanuit het publiek

Voordat de dagvoorzitter het symposium afsluit, is het publiek in de gelegenheid gesteld vragen te stellen aan de sprekers. Een aantal vragen met antwoorden van de sprekers<sup>64</sup> wordt hieronder uitgelicht.

Van Driel had het over de beperkte schaalbaarheid van de Bitcoin, en de vraag is of DNB zich bewust is van het feit dat dit alleen voor de Bitcoin geldt en niet voor de andere cryptomunten. Van Driel geeft aan dat de beperkte schaalbaarheid inderdaad alleen voor de Bitcoin blockchain geldt, maar zij denkt dat het voor andere blockchains mogelijk ook zou kunnen gelden omdat volgens haar de block-grootte bij andere cryptomunten ook beperkt kan zijn.

63. <https://bitonic.nl/safety>.

64. Brosens moet het symposium vanwege andere verplichting voortijdig verlaten. De antwoorden zijn van de overige sprekers.

Een andere vraagsteller verwijst onder meer naar de website van de AFM waar de AFM voor ICO's waarschuwt. De website van de AFM geeft volgens de vraagsteller aan dat 99% van die ICO's niet gereguleerd is, waarbij zij zich afvraagt of de AFM en DNB zich bewust zijn van het feit dat regulering van de uitgegeven tokens afhankelijk is van wat een token vertegenwoordigt. Het antwoord van Franken is een bondige 'ja'. Volgens Franken is de structuur van een token zeker belangrijk voor de vraag of een token binnen de reikwijdte van het toezichtrecht komt; een token kan bijvoorbeeld ook een bioscoopkaartje zijn waarvan je verwacht dat het toegang geeft tot een film in een bioscoop. In het kader van ICO's dient door de initiatiefnemer duidelijk te worden gemaakt dat er bijvoorbeeld sprake is van het ophalen van seed capital<sup>65</sup> of te wel dat het een zeer hoog risicoproject betreft dat binnen het domein van venture capitalists past. Franken geeft daarbij aan als het ophalen van seed capital zo gestructureerd wordt dat er sprake is van equity based crowd funding dit onder regulering valt. Als een ICO op een wijze gestructureerd wordt zodat het niet onder regulering valt, dan is Franken van mening dat er informatie aan het publiek moet worden verstrekt zodat duidelijk is wat het publiek koopt. Er zijn volgens Franken veel misstanden met tokens die worden aangemaakt. Een klein percentage van de tokens kwalificeert als effect en valt onder de prospectusplicht en het is volgens Franken daarom makkelijker om een token zo te structuren dat het niet onder wet- en regelgeving valt. Broekhuizen verwijst in dit kader naar een paper van ESMA<sup>66</sup> waarin beschreven wordt wat passende wetgeving zou kunnen zijn om deze discussie af te ronden.

In Amerika zijn er binnen de SEC bepaalde ontwikkelingen gaande waardoor er volgens een andere vraagsteller met betrekking tot crypto's en ICO's sneller sprake is van een effect.<sup>67</sup> Franken verwijst hier kort naar de Howey-test.<sup>68</sup> De vraag

65. Seed capital is, samengevat, het verkrijgen van risicokapitaal door innovatieve ondernemingen op technologisch en creatief gebied. Zie onder meer deze link met betrekking tot de initiatieven van de Nederlandse overheid: <https://www.rvo.nl/subsidies-regelingen/seed-capital> (laatst geraadpleegd op 20 februari 2018).

66. Vermoedelijk doelt Broekhuizen hier op de Call for evidence van ESMA, 'Potential product intervention measures on contracts for differences, and binary options to retail clients', 18 januari 2018, ref.: ESMA35-43-904.

67. Zie bijvoorbeeld de Staff Letter van de SEC: Engaging on Fund Innovation and Cryptocurrency-related Holdings, 18 januari, 2018, <https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm> (laatst geraadpleegd op 20 februari 2018).

68. De 'Howey-test' is een test die is opgesteld door de Supreme Court in Amerika om te bepalen of bepaalde transacties kwalificeren als een zogenoemde 'investment contract'. Als dat het geval is, worden die contracten volgens de Securities Act van 1933 en de Secu-

is of de AFM ook naar Amerika dan wel de rest van Europa kijkt en of er vanuit Europa ook een verbreding van het begrip 'effect' aanstaande is. Franken geeft aan dat ESMA, zoals Broekhuizen reeds aangaf, haar gedachten hierover heeft laten gaan. De toezichthouders kijken naar die ontwikkelingen maar volgens Franken is het ook belangrijk dat er goed nagedacht moet worden over het oprekken van definities omdat anders mogelijk alle ICO's onder toezicht komen te staan waarbij de vraag kan worden gesteld of dit wenselijk dan wel passend is. Er kan ook worden nagedacht of er een heel nieuw kader voor ICO's zou moeten worden opgesteld. Het oprekken van definities waardoor een token onder regulering komt te vallen brengt wellicht mee dat onder meer de cryptoplatforms waarop die tokens worden verhandeld onder toezicht komen te staan. Op dit moment is volgens Franken het oprekken van definities nog niet aan de orde, maar dit onderwerp staat zeker op de agenda van de toezichthouders en er is met de SEC over gesproken. Of het Amerikaanse model, waar de SEC heel nauw samenwerkt met de FBI om tegen tokens die niet 'goed' zijn oftewel de uitgever van een token haalt fiat geld op met slechte bedoelingen, op te treden één op één gekopieerd kan worden naar Europa, is volgens Franken een grote vraag. Broekhuizen verwijst in dit kader naar de voordracht van De Doelder waar ingegaan is op de open normen van het strafrecht die er toe nopen dat je een bepaalde onderzoeksplicht hebt naar herkomst of identiteit van de klant. Broekhuizen vult hierbij aan dat er vanuit het burgerlijk recht zorgvuldig gedrag wordt vereist waarbij het informeren over het product een onderdeel is van dit zorgvuldige gedrag.

Een andere vraag die gesteld wordt is of de beurzen waar crypto's op verhandeld worden onder toezicht staan, met name omdat je doorgaans geld overmaakt naar een buitenlandse rekening. Volgens De Doelder vallen beurzen op dit moment nog niet onder toezicht, maar als gevolg van de herziene vierde anti-witwasrichtlijn komt er toezicht op wisselkantoren dan wel wisselplatforms binnen de Europese Unie. Als er sprake is van een anoniem platform of wisselkantoor dan wordt het moeilijker om dergelijke partijen aan te pakken. De Doelder geeft verder aan dat ondanks hij geen voorstander is van extra regulering het wel tijd wordt dat de overheid gaat optreden mede omdat er nu geen verbod is en het brede publiek niet kan overzien waar die handel in crypto's nu precies op ziet. Een mediacampagne opzetten is volgens De Doelder een goed idee omdat de waarschuwingen van de AFM en DNB waarschijnlijk weinig gelezen worden.

---

rities Exchange Act van 1934 als effecten beschouwd en zijn daarom onderworpen aan bepaalde openbaarmakings- en registratievereisten. Zie: SEC v. W.J. Howey Co., 328 U.S. 293 (1946), <https://supreme.justia.com/cases/federal/us/328/293/case.html> (laatst geraadpleegd op 20 februari 2018).

## 8. Ontwikkelingen

In mei 2010 werd de eerste officiële Bitcoin transactie voltooid: het kopen van 2 pizza's voor 10.000 Bitcoins.<sup>69</sup> De beginwaarde van een Bitcoin was nihil (ongeveer €0,001).<sup>70</sup> De Bitcoin werd in haar jonge jaren met name gebruikt in het illegale circuit via het dark web. Een bekend voorbeeld is de in 2011 gelanceerde en inmiddels verdwenen website Silk Road. Dit was een online zwarte markt, waar onder meer drugs en wapens gekocht konden worden met Bitcoins. Silk Road is in oktober 2013 door de FBI opgerold.<sup>71</sup> De Bitcoin en daarmee ook andere cryptomunten zijn wellicht, door het illegale gebruik van de Bitcoin, onder een vergrootglas gelegd.

Gelet op de recent gestelde Kamervragen,<sup>72</sup> waarschuwingen vanuit de AFM, DNB, ESMA maar ook de roep van de Europese Centrale Bank om de Bitcoin te reguleren,<sup>73</sup> kan wellicht de vraag worden gesteld of de ontwikkeling van de crypto's een belofte dan wel bedreiging is. De achterliggende techniek, zoals de blockchain, kan een belofte zijn om transacties zonder derden te bewerkstelligen. Denk aan het overdragen van vastgoed, maar ook het vervangen van het custody netwerk van banken en central securities depositaries zoals Euroclear, waar de bewaring van financiële instrumenten plaatsvindt. De cryptomunten, tokens of tokens die middels ICO's worden uitgegeven waarbij gebruik wordt gemaakt van blockchaintechnologie, kunnen een bedreiging vormen omdat het kopen van een cryptomunt of token door het publiek mogelijk als een belegging wordt gezien. Dit staat nog los van het feit dat een crypto of token als een recht van deelneming of effect kan worden gestructureerd, waarbij mogelijk een illegale aanbidding plaatsvindt indien niet aan de regels van de Wet op het financieel toezicht wordt voldaan.<sup>74</sup>

---

69. *FD.Outlook*, nr. 1, maart 2014, p. 60.

70. Zie bijvoorbeeld; <https://allesovercrypto.nl/article/tijdlijn-bitcoin> (laatst geraadpleegd op 20 februari 2018).

71. <https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#161251685b4f>.

72. *Kamerstukken II* 2017/18, vraagnummer 2018Z00025, 3 januari 2018. Zie voetnoot 51 voor de antwoorden op deze Kamervragen.

73. *Het Financieele Dagblad*, 'ECB roept op tot reguleren bitcoin', 9 februari 2018.

74. Zie bijvoorbeeld Position paper AFM, Hoorzitting cryptocurrencies, 24 januari 2018 en het ronde tafelgesprek in de Tweede Kamer dat op 24 januari 2018 plaatsvond, [https://www.tweedekamer.nl/debat\\_en\\_vergadering/commissievergaderingen/details?id=2017A04360](https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2017A04360).

## 9. Overzicht van enkele begrippen<sup>75</sup>

Achterwaartse compatibiliteitOndersteuning voor bijvoorbeeld een ouder computersysteem wanneer een nieuw computersysteem de plaats van een oudere versie inneemt of overneemt.

**AltCoin** Alt staat voor alternative. Het gaat hier om andere coins dan de Bitcoin, zoals Ethereum, Ripple en Dash.

**Bitcoin** De digitale/virtuele munt ontworpen door Satoshi Nakamoto.

**Bitcoincash** Fork van de Bitcoin. Gelanceerd op 1 augustus 2017. Eveneens een AltCoin. Deze variant van de Bitcoin heeft grotere blocken in de blockchain, waardoor er meer transacties per block verwerkt kunnen worden.

**Block** Block met transacties.

**Blockchain** Een blockchain is een gedistribueerde database die bestaat uit een keten van datablokken of te wel blocken. Gedistribueerd betekent dat deelnemers de data uitwisselen via een eigen peer-to-peer netwerk.

**Blockreward** Beloning die een miner ontvangt voor het succesvol oplossen van de rekensom die aan een block is verbonden.

**Bubble** Kan bijvoorbeeld omschreven worden als een marktprijs ver boven de waarde van een belegging ligt.

**Chartaal geld** Fysiek geld: **1) munten** (zie Wet van 29 november 2001 tot vaststelling van het Nederlandse muntstelsel in verband met de invoering van de chartale euro (Muntwet 2002)<sup>76</sup> waar de Euromunt in art. 2 van deze wet door de Staat der Nederlanden kan worden uitgegeven als wettig betaalmiddel) en **2) bankbiljetten** (zie Wet van 26 maart 1998, houdende nieuwe bepalingen inzake De Nederlandsche Bank N.V. in verband met het Verdrag tot oprichting van de Europese Gemeenschap (Bankwet 1998)<sup>77</sup> waar in art. 6 wordt bepaald dat DNB bevoegd is tot het uitgeven van bankbiljetten.)

75. Niet alle begrippen komen in dit artikel terug, maar is wellicht interessant voor de geïnteresseerden in deze materie.

76. *Stb.* 2001, 631.

77. *Stb.* 1998, 200.

**Cold storage** Hard wallet, maar kan ook een paper wallet zijn. Met dat laatste wordt zowel de private key als public key geprint en fysiek bewaard.

**Elektronisch geld** Art. 1:1 Wft: geldswaarde die elektronisch of magnetisch is opgeslagen die een vordering op de uitgever vertegenwoordigt, die is uitgegeven in ruil voor ontvangen geld om betalingstransacties te verrichten als bedoeld in art. 4, punt 5, van de richtlijn betaaldiensten,<sup>78</sup> en waarmee betalingen kunnen worden verricht aan een andere persoon dan de uitgever.

**Fork** Vertakking van de blockchain. In een blockchain worden nieuwe blocken tegelijkertijd door alle miners berekend. Als meerdere miners op hetzelfde moment de oplossing van een block vinden kan een fork ontstaan, waardoor de blockchain een vertakkingen krijgt. Alleen de langste tak wordt gehandhaafd.

**Geldmiddelen** Art. 1:1 Wft bepaalt dat onder geldmiddelen moet worden verstaan: chartaal geld, giraal geld, en elektronisch geld.

**Giraal geld** Opeisbare tegoeden, die niet fysiek zijn en die bij een bank worden aangehouden.

**Hard Fork** Een permanente afwijking van de vorige versie van de blockchain en nodes die met oudere versie van het software protocol werken, worden niet langer geaccepteerd door de nieuwste versie. Dit vereist dat alle nodes in het blockchainnetwerk een upgrade moeten uitvoeren en ook consensus moeten bereiken over de nieuwe regels voor het aanbrengen van een verandering. Hierbij

78. Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betaaldiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG, *PbEU* L 319, 2007. In deze richtlijn wordt onder betalingstransactie verstaan: een door de betaler of de begunstigde geïnitieerde handeling waarbij geldmiddelen worden gedeponneerd, overgemaakt of opgenomen, ongeacht of er onderliggende verplichtingen tussen de betaler en de begunstigde zijn.

	is geen sprake achterwaartse compatibiliteit. <sup>79</sup>		
Hard wallet	Een middel om cryptogeld te bewaren, ook wel kluis genoemd, middels een USB-stick of bluetooth. Een hardware wallet is een vorm van cold storage. Cold storage houdt in dat de private key van een cryptomunt offline wordt bewaard.	Satoshi Nakamoto	Waarschijnlijk een pseudoniem en ontwerper (onduidelijk is of het één persoon is of meerdere personen zijn) van de virtuele munt Bitcoin en de blockchain technologie die daar achterligt. Zie verder voetnoot 22.
Hawala-bankieren	Systemen waarbij geld wordt overgemaakt via niet-reguliere financiële instellingen. Hawala-bankieren wordt wel aangeduid als ondergronds bankieren. De gebruikte systemen worden ook wel <i>informal value transfer systems</i> genoemd. De term hawala wordt met name gebruikt in relatie tot de Indiase, Afghaanse en Pakistaanse gemeenschap.	Soft Fork	Verandering in de regels van het software protocol waarbij de oude blokken dan wel transacties ongeldig worden verklaard waardoor er sprake is van achterwaartse compatibiliteit omdat de oude nodes de nieuwe blokken als geldig beschouwen. Slecht een meerderheid van de miners dient hiervoor een upgrade te doen om de nieuwe regels van het software af te dwingen. <sup>80</sup>
ICO	Initial Coin Offering. Een ICO is een uitgifte van digitale tokens dan wel digitale munten die vooral wordt gebruikt om start-ups of projecten te financieren.	Tamper-proof	Fraudebestendig maken van een document.
Lightning netwerk	Een 'tweede laag' van een betalingsprotocol dat bovenop een blockchain werkt.	Token	Geen digitale valuta, er kan geen betaling mee worden gedaan. Tokens zijn wel inwisselbaar tegen coins. Een token heeft geen eigen blockchain maar maakt gebruik van de blockchain van een andere digitale valuta zoals ethereum. Een token wordt dus boven op een bestaande blockchain gebouwd.
Minen/mining	Mining of minen (in het Nederlands: delven) houdt samengevat in dat computers ingewikkelde rekensommen oplossen. Als de oplossing van een som is gevonden dan ontvangt een miner of te wel delver een Bitcoin. Een miner lost niet alleen puzzels op, maar controleert ook de transacties die in een block zitten waarvoor deze ook een beloning ontvangt.	Wallet	Digitale portemonnee waarin crypto's kunnen worden bewaard. Dit kan onder meer via een hard wallet, of soft wallets zoals smart phone en computer.
Node	Een node is bijvoorbeeld een computer of een ASIC-systeem, zoals een 'Antminer S5' die aan het netwerk verbonden is en beschikt over het volledige databasebestand of te wel over alle transacties die in de blockchain zijn gedaan.		
Private key	Een cryptomunt heeft een public en private key. De private key wordt in een wallet bewaard. Een private key kan ook worden geprint. Op die manier kan een cryptomunt fysiek worden bewaard.		
Public key	De public key wordt gebruikt om ervoor te zorgen dat je eigenaar		

79. <https://www.investopedia.com/terms/h/hard-fork.asp>.

80. <https://www.investopedia.com/terms/s/soft-fork.asp>.