Betreft: internet consultatie "Implementatiewet wijziging vierde anti-witwasrichtlijn"[1], versie 1 van Concept Regeling en Ontwerp Toelichting.

Utrecht, 14 januari 2019

Geachte minister Hoekstra,

Met deze brief wil ik graag een bijdrage leveren vanuit het oogpunt van een software-ontwikkelaar en vooral ook van een Bitcoin gebruiker.

Ik ben pakweg vijf jaar actief als Bitcoin gebruiker, enthousiasteling, software ontwikkelaar en als iemand die actief deelneemt aan discussies binnen de community en met toezichthouders, zie voor mijn bona fides aan het einde van deze brief. De Bitcoin-gerelateerde aspecten van dit wetsvoorstel zullen daardoor van belang zijn voor mijn werk en het in euro's omzetten van mijn inkomsten. Hoewel per definitie niemand namens Bitcoin kan spreken en ik dat ook niet pretendeer, kan ik door mijn lange aanwezigheid en betrokkenheid bij diverse (technische) ontwikkelingen naar ik denk een uniek perspectief geven vanuit een community die doorgaans niet veel met wetgevers spreekt.

In deze brief ga ik op meerdere zaken in, maar mijn drie belangrijkste zorgen over deze wet zijn:

1. Er wordt veel te weinig aandacht aan het grondrecht privacy geschonken; GDPR wordt met een enkel zinnetje aan de kant geschoven en maakt plaats voor m.i. niet proportionele financiële surveillance.
2. Het kan een drastische afname in concurrentie veroorzaken, omdat de wetgeving geen rekening houdt met kleine ondernemingen, met als gevolg hogere tarieven en minder gebruiksvriendelijkheid voor de consument. De voorgenomen snelle invoer is daarnaast ongunstig voor buitenlandse ondernemingen die actief willen zijn in Nederland en nog niet aan de vereiste "vergelijkbare" vergunning kunnen komen.
3. Het is zorgwekkend dat DNB over de vergunningen gaat, gezien deze instantie feitelijk een concurrent is van Bitcoin en zij en de ECB zich regelmatig negatief uitlaten.

Ik behandel eerst de definities van virtuele valuta en bewaarportemonnees en ga daarna in op bovenstaande drie bezwaren.

Relevante artikelen

Mijn reactie concentreert zich op de volgende artikelen:

Artikel 1a

> In artikel 1, eerste lid, worden in alfabetische volgorde ingevoegd:
> *aanbieder van een bewaarportemonnee:* entiteit die diensten aanbiedt om namens haar cliënten cryptografische privésleutels te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen;
> [...]
> *virtuele valuta:* een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, maar die door natuurlijke personen of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld;

[1] https://www.internetconsultatie.nl/wijzigingamld4

Artikel 23c

1. Het is een ieder verboden zonder een daartoe door de Nederlandsche Bank verleende vergunning beroeps- of bedrijfsmatig in of vanuit Nederland diensten aan te bieden voor het wisselen tussen virtuele valuta en fiduciaire valuta.
2. Het is een ieder verboden zonder een daartoe door de Nederlandsche Bank N.V. verleende vergunning beroeps- of bedrijfsmatig in of vanuit Nederland bewaarportemonnees aan te bieden.
3. Het eerste en tweede lid zijn niet van toepassing op een aanbieder als bedoeld in het eerste of tweede lid die beschikt over een vergelijkbare vergunning in een andere lidstaat en waarop toezicht wordt uitgeoefend dat in voldoende mate waarborgen biedt ten aanzien van de belangen die deze wet beoogt te beschermen.

Definities

Virtuele valuta

In deze brief ga ik alleen in op Bitcoin. Soms is wat ik zeg ook van toepassing op andere virtuele valuta, maar lang niet altijd.

Virtuele valuta zoals gebruikt in het spraakgebruik is een zeer brede term. Omdat Bitcoin al ingewikkeld genoeg is om te begrijpen wordt vaak aangenomen dat alle virtuele valuta "ook zoiets" zijn. Er zijn echter grote onderlinge verschillen die van belang zouden kunnen zijn voor wetgeving. Ik geef hieronder een aantal voorbeelden. Idealiter zou per cryptomunt bekeken moeten worden hoe deze zich verhoudt tot de wet. Het is uiteraard begrijpelijk dat de wetgever daar niet aan toe komt, maar daardoor kan onverstandig beleid ontstaan.

Wat betreft de Wwft, zou ik de voorvraag willen stellen om te overwegen geen definitie te hanteren, doch i.i.g. nog eens goed naar die definitie te kijken. Ik weet zelf niet wat precies een betere definitie zou zijn, maar ik kan wel een aantal aandachtspunten benoemen.

Aan de ene kant kan het hanteren van een definitie het risico met zich meebrengen dat bepaalde zaken er tegen de bedoeling in niet onder vallen.

Als voorbeeld, de Kansspelautoriteit heeft de m.i. ongelukkige keuze gemaakt om te stellen dat *geen enkele* cryptomunt een piramidespel kan zijn.[2] Waarschijnlijk heeft men eerst Bitcoin bestudeerd, daarbij uit de decentrale aard geconcludeerd dat het geen piramidespel kan zijn, en vervolgens maar aangenomen dat dit voor alle andere cryptovaluta geldt. Dit is echter a priori onmogelijk om vast te stellen, want er is geen zinnige definitie van cryptovaluta. Of een bepaalde cryptomunt een piramidespel vormt zoals bedoeld in artikel 1a van de Wet op de kansspelen, kan m.i. alleen van geval tot geval bepaald worden aan de hand van de feiten (zoals de mate van centrale aansturing, de rol van verschillende promotors, de geldstroom van het brede publiek richting de oprichters, etc). Een concreet voorbeeld is dat eind vorig jaar in Japan bijvoorbeeld mensen zijn opgepakt op verdenking van een cryptovaluta piramidespel, waarin een hoog rendement beloofd werd.[3]

[2] https://kansspelautoriteit.nl/nieuws/nieuwsberichten/2018/januari/kansspelautoriteit-1/
[3] https://www.newsbtc.com/2018/11/14/tokyo-police-crackdown-on-alleged-crypto-pyramid-scheme-arrest-eight/

Hierdoor geeft de wetgever, potentieel, ruimte aan oprichters van een cryptovaluta om onder artikel 1a van de Wet op de kansspelen[4] uit te komen. Ze laat weliswaar de mogelijkheid open dat er piramidespelen *rondom* een cryptomunt plaatsvinden, wat zeker ook voorkomt,[5] vaak zonder medeplichtigheid van de oprichters van de munt. Dit lijkt mij echter een onnodige handicap; de wetgever heeft juist de definitie van piramidespel bewust vaag gehouden.

Aan de andere kant kan het goed zijn dat vele, maar niet alle, bestaande virtuele valuta die regulering behoeven reeds onder de Wwft vallen via bestaande wetgeving, waardoor een aparte definitie niet nodig is. Denk bijvoorbeeld aan:

* stablecoins: hierbij is de waarde gekoppeld aan de euro of dollar en staat één specifiek bedrijf garant voor die waarde. Dat lijkt op een obligatie.[6] Voorziet de huidige Wwft niet reeds in wetgeving over de handel in obligaties? Zo nee, is er niet reeds andere wetgeving die voorkomt dat obligaties voor witwassenen en terrorismefinanciering gebruikt worden, zoals de Wft? In dat geval kan die bestaande wetgeving wellicht aangescherpt worden om rekening te houden met de mogelijkheden van cryptovaluta;
* de virtuele valuta die tijdens Initial Coin Offerings (“ICO's”) zijn uitgegeven. Deze lijken weer meer op aandelen, waar binnen de Wwft danwel Wft al regels voor voor bestaan;
* virtuele valuta die slechts in hun marketing beweren decentraal en vergelijkbaar met Bitcoin te zijn, maar feitelijk volledig onder controle staan van één bedrijf of nauw samenwerkingsverband. Zo'n bedrijf kan ten alle tijden tegoeden bevriezen en eisen stellen aan transacties. Zij zijn dan wellicht het beste te vergelijken met PayPal of het ter ziele bedrijf Liberty Reserve.[7] Denk hierbij ook aan bestaande regelgeving over elektronisch geld. Wederom zou die bestaande regelgeving aangepast kunnen worden, om beter rekening te houden met de aard van deze nieuwe technologie.

Mocht u toch vasthouden aan de wenselijkheid van een definitie, dan is de vraag of de nu gekozen definitie de gewenste lading dekt. Er zijn veel dingen die "elektronisch [...] worden overgedragen, opgeslagen en verhandeld". Denk bijvoorbeeld aan domeinnamen, websites, game items en zelfs game valuta (in grote online-multiplayer spellen zoals World of Warcraft goud werd goud al verhandeld voordat Bitcoin bestond). Daar tegenover staat dat er virtuele valuta zijn die niet tot nauwelijks als “ruilmiddel” gebruikt worden, maar meer als postzegels verhandeld worden, zoals Rare Pepe[8] en Crypto Kitties.[9] Deze worden soms via dezelfde platformen verhandeld als andere cryptovaluta.

Bewaarportemonnee

[4] https://wetten.overheid.nl/BWBR0002469/2018-07-28#TiteldeelI_Artikel1
[5] https://arxiv.org/abs/1811.10109
[6] Een obligatie zonder rente weliswaar, maar wie weet of in de toekomst stablecoins rente gaan betalen. Een andere mogelijke interpretatie is elektronisch geld.
[7] https://en.wikipedia.org/wiki/Liberty_Reserve
[8] http://rarepepedirectory.com
[9] https://hackernoon.com/how-to-buy-a-cryptokitty-the-complete-guide-dna-sequencing-26e14596a9cf

De definitie (aanbieder van) "bewaarportemonnee" is taalkundig verwarrend,[10] terwijl de oorspronkelijke Engelstalige terminologie wel duidelijk is. Artikel 1a definieert het als volgt:

> "[...] entiteit die diensten aanbiedt om namens haar cliënten cryptografische privésleutels te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen;"

In de Engelstalige versie van de richtlijn wordt gesproken over "custodial wallets" en "non-custodial wallets". Een custodial wallet is een soort bank waarbij iemand anders de Bitcoin namens de eigenaar beheert. Bij een non-custodial wallet heeft de eigenaar zelf de private keys.

De gehanteerde definitie"bewaarportemonnee" verwijst enkel naar de "custodial wallet" en geeft vervolgens geen definitie voor een "non-custodial wallet".

Een oplossing kan gevonden worden in het onderscheid tussen het bijvoeglijk naamwoord custodia**l** (custodial wallet) en het zelfstandig naamwoord custodia**n** (beheerder).[11] De vergunningsplicht rust tenslotte op de custodian, (rechts)persoon die andermans coins beheert, niet op de custodial wallet (software) zelf.

Mijn voorstel voor de vertaling van "custodial wallet [beheerder]" is dan ook "virtuele valuta beheerder". In het dagelijks spraakgebruik kunnen "wallet" en "portefeuille" dan gewoon blijven verwijzen naar zowel custodial als niet-custodial oplossingen.

De term "beheerder" (custodia**n**) kan daarnaast ook verwijzen naar exchanges, die vaak[12] ook (tijdelijk) coins bewaren van klanten. Dat ze daarbij een wallet gebruiken is daarbij secundair. Dit voorkomt wederom spraakverwarring, omdat "wallets" meestal als iets anders gezien worden dan "exchanges", maar beide dus "bewaarportemonnees" kunnen zijn.

In de toelichting 2.1.1. "Reikwijdte aanbieders" staat wat gezien wordt als custodial wallet:

> "Aanbieders van bewaarportemonnees (in het Engels custiodial [sic] wallet providers) dienen te worden onderscheiden van aanbieders van 'software' portemonnees. De eerste zijn in het bezit van de privésleutel van hun gebruikers en kunnen daarmee ook beschikken over hun virtuele valuta."

> "In tegenstelling tot aanbieders van bewaarportemonnees zijn deze aanbieders niet in het bezit van de privésleutel, en hebben zij op geen enkele manier toegang tot de virtuele valuta van hun gebruikers. Daardoor zijn zij niet of nauwelijks in staat om te voldoen aan de verplichtingen van de vierde anti-witwasrichtlijn, zoals het monitoren van transacties. Om die reden zijn deze aanbieders (vooralsnog) niet onder de reikwijdte van de richtlijn gebracht."

Dit onderscheid kan scherper worden gedefinieerd.

In de meest eenvoudige situatie van een custodial wallet, heeft de aanbieder de privésleutel die nodig is om Bitcoins te kunnen verplaatsen, dan wel te bevriezen, bv. in afwachting van

---

[10] en voor taalkundigen en programmeurs tenenkrommend, omdat een portemonnee per definitie dingen bewaart. De letterlijke vertaling van 'custodian' is een 'bewaarder', een term met een bredere betekenis dan enkel bewaren an sich.

[11] https://wikidiff.com/custodial/custodian

[12] Er zijn diverse projecten die proberen exchanges zodanig te ontwerpen dat ze, in het belang van de veiligheid, nooit controle over de coins van een klant hebben. Dit zouden dan dus geen bewaarportemonnees zijn, maar wellicht nog wel als wisseldienst onder de vergunningplicht vallen.

cliëntenonderzoek. De klant heeft, vanuit de techniek gezien, geen enkele controle over haar coins. Dit heeft in het verleden nog wel eens tot rampzalige verliezen geleden, het bankroet van MtGox[13] is het meest bekende voorbeeld, waarbij ook Nederlanders veel Bitcoin zijn kwijtgeraakt.[14]

In de meest eenvoudige situatie van een niet-custodial wallet, zoals de Bitcoin Core software waar ik aan bijdraag, heeft de gebruiker zelf ten alle tijden volledige controle over haar coins. De software wordt gedownload op de eigen computer, Ook dit leidt echter tot problemen, zoals hacks en zelfs gewapende overvallen.[15]

Er is daardoor vanuit de markt vraag naar hybride oplossingen. Daar lijkt de toelichting van de wet ook naar te verwijzen, maar ik denk deze onterecht als custodian worden aangemerkt. Dit hangt m.i. sterk van de situatie af. Neem het volgende voorbeeld:

Er zijn wallets waarbij, voor de veiligheid, de wallet aanbieder mee moet tekenen bij iedere transactie. De aanbieder en de eigenaar hebben dan ieder één privésleutel. Dit geeft de aanbieder dus een veto over alle transacties, maar niet de mogelijkheid de coins tegen de wil van de eigenaar te verplaatsen. Om te voorkomen dat de aanbieder de coins onbeperkt kan blokkeren, is er meestal een derde sleutel, bv. in een kluis van de eigenaar of bij een notaris. Of er is een afkoelperiode waarna de klant volledige controle krijgt. Dit alles is dus met computer code vastgelegd.

Dit is niet mogelijk bij traditionele banken, waarbij de eigenaar hooguit juridisch controle blijft houden over zijn of haar geld, en inbeslagname regelmatig voorkomt. Faillisementen en bail-ins[16] worden ook technisch uitgesloten.

Of de wallet aanbieder mee kan kijken in (een deel van) de wallet hangt van de implementatie af.

Bovenstaand voorbeeld is m.i. niet een custodial wallet, ondanks de aanwezigheid van privé sleutels bij de aanbieder, omdat het belangrijkste verschil m.i. tussen een custodial wallet en een niet-custodial wallet is dat de aanbieder van een custodial wallet op elk moment beslag kan leggen op de coins van hun klant, en dat ze coins van de klant kwijt kunnen raken. Dit is de enige manier waarop een aanbieder überhaupt druk uit kan oefenen op hun klant om informatie aan te leveren; zonder die mogelijkheid kan de klant gewoon de coins naar andere aanbieder verplaatsen of volledig zelf beheren.

In de toelichting staat echter:

> “Onder deze categorie [custodial wallet] vallen ook portemonnees waarbij de privésleutel, naast de aanbieder, wordt gedeeld met meer dan één gebruiker.”

Deze zin klopt sowieso niet, want een privésleutel wordt om veiligheidsredenen nooit gedeeld. In plaats daarvan is er sprake van meerdere privésleutels (of andere cryptographische mechanismes), met daaraan gekoppelde voorwaarden, zoals in het voorbeeld hierboven.

> “Het aanbieden van bewaarportemonnee waar de virtuele valuta gestald kunnen worden, en waarbij de aanbieder kan beschikken over de virtuele valuta, is een soortgelijke dienst

[13] https://en.wikipedia.org/wiki/Mt._Gox
[14] https://www.bright.nl/nieuws/artikel/3926331/groep-nederlanders-wil-843-bitcoins-3-miljoen-euro-terug
[15] https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md
[16] https://www.volkskrant.nl/nieuws-achtergrond/wat-zei-dijsselbloem-letterlijk-financial-times-publiceert-transcript-interview~becd4f7d/

> als het aanbieden van een betaalrekening door een bank. Aanbieders van bewaarportemonnees zouden, net als banken, in staat moeten zijn om onderzoek te doen naar hun cliënten en transacties te monitoren. Zij worden om die reden onder de reikwijdte van de vierde anti-witwasrichtlijn gebracht."

Hier worden twee dingen door elkaar gehaald, namelijk de controle hebben over coins van een klant en de mogelijkheid een klant te observeren. Wie op welk moment daadwerkelijk controle heeft over coins is redelijk objectief vast te stellen. Echter, indien slechts de mogelijkheid om te observeren al voldoende zou zijn om de "bewaarportemonnee" te moeten monitoren, dan wordt het volstrekt onduidelijk hoe groot de reikwijdte is. De wetgever lijkt met dit idee te spelen:

> "Daardoor zijn zij niet of nauwelijks in staat om te voldoen aan de verplichtingen van de vierde anti-witwasrichtlijn, zoals het monitoren van transacties. Om die reden zijn deze aanbieders **(vooralsnog)** niet onder de reikwijdte van de richtlijn gebracht."

Deels door het openbare karakter van de blockchain zijn er veel partijen die in staat zijn tot het "monitoren van transacties", niet alleen de in het wetsvoorstel bedoelde partijen. Neem bijvoorbeeld een applicatie die investeerders helpt om hun boekhouding op orde te krijgen. Zo'n applicatie kan transacties importeren uit een (bewaar)portemonnee. Vallen aanbieders van dergelijke SAAS (Software As A Service) applicaties dan ook onder deze wet?

Maar ook winkeliers, van juwelierszaken tot de ijscowagen, die Bitcoin accepteren kunnen via de blockchain deels inzicht krijgen in de coins van hun klanten. Werkgevers die personeel uitbetalen in Bitcoin kunnen dit ook (tenzij de werknemer zeer bekwaam is in het beschermen van de eigen privacy). Het lijkt mij onwenselijk en ook niet de bedoeling om eenieder die transacties op de blockchain kan monitoren onder deze wet te laten vallen.

Tot slot zou het zorgwekkend zijn voor de veiligheid van Bitcoin gebruikers als hybride oplossingen verdwijnen vanwege de regeldruk. Enerzijds zullen gebruikers dan meer volledig custodial wallets gaan gebruiken, met MtGox achtige scenario's in het verschiet. Anderzijds zullen gebruikers dan, zonder voldoende technische kennis, hun coins in eigen beheer nemen, met als gevolg een toename van berovingen en hacks (wat ironisch genoeg weer leidt tot meer witwassen).

Privacy, proportionaliteit en subsidiariteit

De toelichting van de richtlijn noemt in haar 40 pagina's nul keer het woord "privacy". De gehele tekst heeft een vrij negatieve ondertoon als het gaat om zowel privacy als cryptovaluta. Wellicht omdat het vanuit de handhavende hoek geschreven is en zij beroepsmatig nou eenmaal alleen met de duistere aspecten te maken krijgen, en niet de positieve. Deze negatieve houding blijkt nog het meest uit de volgende zin:

> "De richtlijn beoogt dan ook de anonimiteit die is verbonden aan transacties in virtuele valuta, en het verhullen van dergelijke transacties, zoveel mogelijk tegen te gaan."

Dit staat in schril contrast met Artikel 8 van het Europees Verder voor de Rechten van de Mens:

> "Recht op eerbiediging van privé familie- en gezinsleven
>
> 1. Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie."

Er vindt mijns inziens te weinig maatschappelijke discussie plaats over privacy in het financiële systeem in het algemeen. Hoewel ik begrijp dat er niet zomaar voor Bitcoin een uitzondering gemaakt kan worden, vind ik het toch noodzakelijk om hier iets over te zeggen.

Witwaswetgeving lijkt over het algemeen slechts een hamerstuk. Logisch, want "Wet ter voorkoming van witwassen en financieren van terrorisme" klinkt nou eenmaal niet heel spannend en de meeste mensen zijn het eens dat witwassen en terrorisme slecht zijn. Maar daardoor ziet men niet de consequenties, en die zijn op privacy gebied zeer ernstig.

Inbreuk op een grondrecht als privacy mag alleen indien dit noodzakelijk is, en binnen de grenzen van proportionaliteit en subsidiariteit.[17] De noodzaak staat met onderwerpen als witwassen en terrorismefinanciering niet ter discussie. De beginselen van proportionaliteit en subsidiariteit echter des te meer, gezien de digitale (bewaar)mogelijkheden die er ondertussen zijn. Ik geef een voorbeeld.

Als ik een openbaar toilet bezoek op Utrecht Centraal, ga ik eerst door een OV poortje, loop dan langs pakweg 100 camera's naar de ingang van het toilet, alwaar ik mijn contactloze pinpas gebruik. De cameragegevens worden binnen enkele dagen verwijderd. Het inchecken en annuleren van dat inchecken met mijn OV chip kaart wordt binnen 18 maanden verwijderd.[18] De pintransactie wordt echter afhankelijk van de bank soms meer dan 10 jaar bewaard.[19]

Ik zie niet hoe mijn WC bezoek tien jaar geleden van belang is voor het voorkomen van terrorisme. Dit is een probleem met subsidiariteit en proportionaliteit waar de wet m.i. te weinig nuance in toont.

De barre toestand en achteruitgang van privacy in het financiële systeem is voor veel cryptovaluta enthousiastelingen een belangrijke drijfveer om een alternatief te bouwen. Peter Van Valkenburgh van het Amerikaanse Coin Center gebruikt vaak de term Financiële Surveillance:[20] het volgen van mensen middels de bankrekening in plaats van met camera's of schaduwen.

Gezien het bovenstaande, is wellicht is volgende formulering beter:

> De richtlijn beoogt dan ook de anonimiteit die is verbonden aan transacties in virtuele valuta, en het verhullen van dergelijke transacties, zo veel mogelijk te beschermen in lijn met Artikel 8 van het Europees Verder voor de Rechten van de Mens, en slechts gericht en proportioneel de anonimiteit te doorbreken waar er een zwaarwegend belang is in het voorkomen van witwassen en terrorismefinanciering.

Vanuit een nieuwe doelstelling die privacy een gelijkwaardige prioriteit geeft, kunnen we dan vervolgens proportionaliteit aanbrengen in de uitvoering door te waken dat de inbreuk niet verder gaat dan nodig en subsidiariteit door de inbreuk te beperken tot de lichtste middelen.

In de toelichting onder §7.1 "Persoonsgegevens in het kader van het cliëntenonderzoek" staat:

> "Er geldt een bewaartermijn van vijf jaar vanaf het moment dat een zakelijke relatie is beëindigd of een transactie is verricht, voor de persoonsgegevens die uit hoofde van het cliëntenonderzoek worden verzameld.

---

[17] Arrest Sunday Times EHRM 26 april 1979, NJ 1980/146

[18] https://www.ov-chipkaart.nl/privacy.htm

[19] https://www.consumentenbond.nl/betaalrekening/meerderheid-bewaart-rekeningafschriften-ten-minste-5-jaar

[20] https://www.youtube.com/watch?v=MdU4PL6ZeB0

> Zonder het verrichten van cliëntenonderzoek zou een effectieve bestrijding van witwassen en financieren van terrorisme niet mogelijk zijn. Ten einde signalen die duiden op onder meer witwassen of terrorismefinanciering te kunnen herkennen, is het verwerven van kennis en informatie over de identiteit van een cliënt onmisbaar. Ook voor het functioneren van de (Nederlandse) opsporingsautoriteiten is deze informatie essentieel."

Hier wordt een valse tegenstelling gecreëerd. Aan de ene kant is er de GDPR die het mensenrecht op privacy probeert waar te borgen. Aan de andere is er de noodzaak om witwassen te bestrijden. Er wordt gedaan alsof het volledig opheffen van het recht op privacy de enige optie is.

Het is belangrijk om het contrast goed in beeld te krijgen. Als alléén het recht op privacy van belang zou zijn, dan moet iedere wisseldienst van cryptovaluta alle gegevens van hun klanten verwijderen zodra een transactie compleet is. Ze moeten dus vrijwel onmiddellijk het rekeningnummer waar vandaan betaald is verwijderen, het bitcoin adres waar de coins naar verzonden zijn vergeten, de naam en adresgegevens van de klant wissen, etc, etc. Die gegevens hebben namelijk totaal geen bedrijfsmatig nut. Daarnaast zou het absoluut verboden zijn om de bitcoins van een klant na aankoop te volgen.

Als alléén het bestrijden van witwassen van belang is, dan mogen gegevens nooit gewist worden en moet iedere klant maximaal bespioneerd worden, vooral ook na de aankoop.

Het enige compromis wat de wet hier doet is de termijn op 5 jaar na beëindiging van de relatie zetten. Dit werkt misschien bij bankrekeningen waarbij men jaarlijks voor de service moet betalen, maar sluit niet aan bij de praktijk rond cryptovaluta. Mensen sluiten vrijwel nooit online accounts en dus eindigt de relatie feitelijk nooit. In de praktijk zouden deze gegevens daardoor onbeperkt bewaard moeten worden.

Daarnaast is de blockchain voor iedereen in te zien, waardoor de gevolgen van een eventueel datalek veel ingrijpender zijn. Kwaadwillenden kunnen dan zien welke personen veel Bitcoin bezitten. Dit leidt nu soms al tot berovingen en ontvoeringen.[21]

Waarom kan de wet hier geen subsidiariteit en proportionaliteit toepassen? Moet iedere Nederlander in al zijn financiële doen en laten dag en nacht bespioneerd worden voor het geval dat? Moet elk met de pin betaalde WC bezoek tot het einde der tijden digitaal bewaard worden? Als er X dagen na een transactie geen grond van verdenking is, waarom moeten transactiegegevens dan niet verwijderd worden?

Voor zover het verwijderen van transactiegegevens wel degelijk verplicht is, kan de wet dit wellicht expliciet vermelden. Denk daarbij ook aan het verwijderen van het Bitcoin adres waar de klant op betaald is. Dit verwijderen is mogelijk technisch ingewikkeld, maar bij cryptovaluta van extra belang vanwege o.a. het bovengenoemde verhoogde risico op beroving.

Daarnaast dient opgemerkt te worden dat wisseldiensten en bewaarportemonnees vaak gebruik maken van zogenaamde cluster analyse, waarmee ze inzicht krijgen in de transacties van hun klanten en bv. de herkomst van coins kunnen natrekken. De aanbieders deze diensten zijn vaak buiten Nederland en zelfs buiten de EU gevestigd. Dit kan ertoe lijden dat gevoelige informatie van *alle* klanten buiten de landsgrenzen terecht komt, en mogelijk in handen valt van buitenlandse inlichtingendiensten die daar weer hun voordeel mee kunnen doen.

---

[21] https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md

Onschuldpresumptie

Tevens wordt in dit wetsvoorstel m.i. de onschuldpresumptie in gevaar gebracht. Dit gezien de deels omgekeerde bewijslast in witwaszaken. Uiteraard zijn daar in de jurisprudentie beperkingen in aangebracht ter bescherming van een verdachte. Echter op het gebied van cryptovaluta bestaat momenteel zo bar weinig kennis en expertise binnen de rechterlijke macht en de advocatuur, dat een situatie ontstaan is waarin ik sterk vermoed dat sommige verdachten geen eerlijk proces krijgen.[22]

Met name het gebruik van voor de verdediging oncontroleerbare clusteranalyse als black box bewijsmateriaal is zeer zorgwekkend. Als aanbieders van wisseldiensten en bewaar portefeuilles door deze wet ook (meer) clusteranalyse gaan toepassen en die vervolgens delen met handhavers, wordt dit probleem verergerd.

Benadeling kleine en buitenlandse concurrentie

Ik ga hier in op de toelichting 4.1.1 "Nieuwe instellingen binnen de reikwijdte van de Wwft", waar een schatting gemaakt wordt van het aantal bedrijven dat met deze regelgeving te maken krijgt en van de kosten die zij gaat maken.

Het aantal wisseldiensten wordt ingeschat op 27 en het aantal bewaarportemonnees op 3. Ik begrijp niet waar deze getallen op gebaseerd zijn. Alleen al het aantal LocalBitcoins[23] en Bisq[24] aanbieders in Nederland is hoger; dit zijn bedrijven en individuen die over the counter Bitcoins verhandelen tegen contant of giraal geld. Bij gebrek aan nadere specificatie van “bedrijfsmatig” is het niet duidelijk welk deel van deze aanbieders onder de vergunningplicht valt.

Belangrijker nog is dat dit vergunningstelsel effect heeft op aanbieders uit de hele wereld die momenteel de Nederlandse markt bedienen en/of dat in toekomst willen doen.

In een snelgroeiende markt is een groot risico om te onderschatten om hoeveel bedrijven het echt gaat straks en wat voor kosten ze maken. De Amerikaanse beurs Kraken gaf bijvoorbeeld laatst aan dat hun compliance kosten exponentieel stijgen en een serieus probleem beginnen te worden.[25] Bedrijven in de cryptocurrency wereld moeten het vaak doen met aanzienlijk minder budget per klant dan traditionele banken.

Tegelijkertijd de aard van nieuwe technologie het meer werk om aan alle regelgeving te voldoen. Een vertegenwoordiger van de Amerikaanse beurs Kraken verklaarde recentelijk dat hun medewerkers onevenredig veel tijd moeten besteden aan het uitleg geven aan handhavers, die vaak totaal verkeerde vragen stellen en om de verkeerde gegevens vragen.[26]

Het voorstel maakt geen onderscheid wat betreft het handelsvolume van wisseldiensten. Moet een ZZP'er die Bitcoins wil verhandelen tussen enkele tientallen klanten straks dezelfde compliance machine optuigen als Coinbase, een Amerikaans handelsplatform wat inmiddels meer dan $300 miljoen bij investeerders heeft opgehaald? Niet iedere ondernemer kan zo even de in

---

[22] https://medium.com/provoost-on-crypto/van-wie-is-deze-bitcoin-e455bcd73dd7

[23] https://localbitcoins.com/country/NL

[24] https://bisq.network/

[25] https://www.coindesk.com/crypto-exchange-kraken-says-us-subpoenas-becoming-barrier-to-entry en https://www.coindesk.com/shapeshift-cuts-staff-by-a-third-in-latest-industry-layoffs

[26] https://twitter.com/krakenfx/status/1081716123383418880

toelichting geschatte €4,320 ophoesten voordat ze überhaupt hun zaak kunnen openen, en ze moeten vele miljoenen verhandelen om dat terug te verdienen. Voor startups die beginnen met een paar duizend euro per maand verhandelen, om zo ervaring op te doen en later uit te breiden, lijkt dus onmogelijk.

Een mogelijke oplossing kan zijn om, tot een bepaalde totaal omzet en omzet per klant, een duidelijke maar voor kleine ondernemers realistisch te hanteren lijst van vereisten op te stellen, zoals bijvoorbeeld wanneer identificatie gevraagd moet worden, en wat er in de administratie moet staan. Vanaf een bepaalde omzet zou er dan een meldplicht kunnen zijn, en pas op weer een niveau daarboven een vergunningplicht.

Artikel 23c lid 3 maakt een uitzondering voor buitenlandse aanbieders:

> 3. Het eerste en tweede lid zijn niet van toepassing op een aanbieder als bedoeld in het eerste of tweede lid die beschikt over een vergelijkbare vergunning in een andere lidstaat en waarop toezicht wordt uitgeoefend dat in voldoende mate waarborgen biedt ten aanzien van de belangen die deze wet beoogt te beschermen.

Ik vrees alleen dat deze uitzondering weinig soelaas biedt voor buitenlandse concurrenten. Het probleem is dat, als Nederland vooruit loopt op andere EU landen met het vergunningenstelsel, Europese concurrenten niet aan de vereiste "vergelijkbare" vergunning komen kunnen. Zij moeten dan eerst hun eigen regering afwachten. Dit is een snel bewegende markt waarin een paar maanden vertraging al het verschil kan maken tussen faillissement en dominantie.

Daarom vermoed ik dat zij massaal Nederlandse klanten zullen gaan weren. Daardoor ondervinden Nederlandse aanbieders minder concurrentie, wat voor consument uiteindelijk hogere tarieven kan betekenen. Zelfs nu zijn de tarieven van Nederlandse aanbieders vrijwel altijd minder gunstig dan die van buitenlandse aanbieders. Dit komt bv. doordat buitenlandse aanbieders veel meer volume hebben.

Daarnaast is het waarschijnlijk niet de moeite waard voor ze om in Nederland een vergunning aan te vragen, zeker zolang hun eigen land en het grootste deel van de wereld nog geen vergunningplicht heeft.

Uiteindelijk is het de bedoeling van de richtlijn dat in heel Europa vergelijkbare vergunningstelsels worden opgetuigd. Echter niet elk land zal dit op hetzelfde tempo doen, en de vraag is of ieder land de richtlijn op dezelfde wijze uit zal leggen. Hierdoor kan dus i.i.g. een tijdelijk de situatie ontstaan die ik hierboven beschrijf waarin Nederlandse consumenten geweerd worden. Dit zou goed te voorkomen moeten zijn door Europees de timing goed af te stemmen.

Afstemming binnen Europa helpt niet met de situatie daarbuiten, terwijl juist veel grote aanbieders van diensten in cryptovaluta wereld buiten Europa gevestigd zijn. Vrijwel geen enkel land heeft een vergunningstelsel. Het is ook volstrekt onduidelijk wat met “vergelijkbaar” bedoeld wordt. De meeste internationale bedrijven zullen eieren voor hun geld kiezen en Nederlandse klanten weren, wat slecht is voor de Nederlandse consument. Deze dynamiek is reeds te zien in een aantal cryptovaluta bedrijven wat gebruikers in de staat New York blokkeert, omdat de vergunning voor hen onbetaalbaar is[27]. Omgekeerd zullen sommige aanbieders wellicht denken aan de handhaving te kunnen ontsnappen, waardoor oneerlijke concurrentie ontstaat die ongunstig is voor Nederlandse aanbieders.

[27] https://blog.kraken.com/post/253/farewell-new-york/

Sommige van die diensten hebben een Europese bankrekening, wat wellicht - afhankelijk van de voorwaarden - voldoende is om aan een vergunning te kunnen komen. Dat geldt echter niet voor alle bedrijven. Aanbieders van een pure bewaarportemonnee, zonder wisseldienst, hebben bv. geen reden om een bankrekening te hebben.

Het is dus belangrijk om de uitrol van dit vergunningstelsel wereldwijd, doch i.i.g. Europees, te coördineren, zodat consumenten niet (enkele jaren) de dupe worden.

Een bijkomend probleem van de "vergelijkbare vergunning" regel, is dat er landen zijn met extreem dure vergunningen. Neem bijvoorbeeld BitLicense in New York, die tonnen of zelfs een miljoen dollar kost. Bedrijven die dat kunnen betalen, zoals bijvoorbeeld Coinbase, zijn aanmerkelijk duurder dan hun concurrenten.

Een oplossing voor buitenlandse aanbieders die moeilijk aan een "vergelijkbare" vergunning kunnen komen, is om het zo laagdrempelig mogelijk te maken om in Nederland zo'n vergunning aan te vragen, die dan ook gelijk voor heel Europa geldt. Dit vereist echter wel het nodige enthousiasme vanuit de vergunningverlener om Nederland op de kaart te zetten op dit vlak. Enthousiasme is niet via de wet te regelen, zie daarom het volgende hoofdstuk.

DNB als vergunningverlener

Ik vind het zorgwekkend dat de Nederlandsche Bank over deze vergunningen gaat. Zowel DNB als ECB laten zich regelmatig in de media negatief uit over Bitcoin; zo noemde Coeure Bitcoin de “evil spawn of the [2008] financial crisis". Ze zijn weliswaar enthousiast over "distributed ledger technology" danwel "blockchain technologie" (wat daar ook van zij), maar niet over cryptovaluta en dat is waar deze wet over gaat.

Wellicht is dat enthousiasme te repareren, maar dan blijft alsnog het probleem dat Bitcoin bedoeld is als alternatief voor het huidige geldsysteem, waar de ECB en de DNB een centrale rol in spelen. Het is een beetje vergelijkbaar met Holland Casino over kansspelvergunningen laten gaan.

Het zou goed kunnen dat Bitcoin en de Euro vredig langs elkaar blijven bestaan, maar als puntje bij paaltje komt, als ze bijvoorbeeld Bitcoin zien als een serieuze bedreiging voor de financiële stabiliteit, kan DNB de macht over vergunningen gebruiken in het nadeel van Bitcoin.

Het doel van deze wet is echter niet het waarborgen van de euro, maar het voorkomen van witwassen en terrorismefinanciering.Het lijkt mij beter om een neutraal overheidsorgaan op te zetten voor deze vergunningen, dan wel het mandaat van DNB uit te breiden om niet alleen de euro maar ook privaat geld te ondersteunen.

Mijn vrees is concreet dat DNB terughoudend zal zijn in het uitgeven van vergunningen. Het jarenlange traject dat Bunq moest doorlopen in het aanvragen van een vergunning,[28] en het gebrek aan daadkracht in het Deposito Bank initiatief,[29] maken mij niet heel erg hoopvol.

---

[28] https://www.bol.com/nl/f/breken-met-banken/9200000057850318/

[29] https://www.ftm.nl/artikelen/de-echte-reden-dat-de-saaiste-bank-van-nederland-er-niet-mag-komen?share=1

Als we perse een vergunningstelsel moeten krijgen, dan zou ik graag zien dat Nederland voorop loopt en de beste vestigingsplaats wordt voor Bitcoin bedrijven. Daarvoor is het noodzakelijk dat de vergunningverlener het enthousiasme deelt en proactief met bedrijven in binnen- en buitenland werkt om ze snel mogelijk aan de slag te kunnen.

Bedankt voor uw aandacht,

Met vriendelijke groet,

Sjors Provoost

Over de auteur

Ik, Sjors Provoost,[30] ben sinds 2013 als software ontwikkelaar actief bezig met Bitcoin. In eerste instantie puur uit interesse,[31] maar later full-time zowel in loondienst als op freelance basis. Ik word vrijwel volledig in Bitcoin uitbetaald, dus ik gebruik het regelmatig en kom ook in aanraking met de te reguleren wisseldiensten.

Van eind 2014 tot medio 2017 werkte ik voor blockchain.info, bekend van de gelijknamige block explorer. Een explorer (verkenner) is een website waarop eenieder kan zien wat er op de Bitcoin blockchain gebeurt, zonder daarvoor aparte software te hoeven downloaden. De naam blockchain.info is gebaseerd op de technische term “blockchain”, maar dient daarmee niet verward te worden. Het bedrijf was toentertijd, mogelijk nog steeds, de grootste bitcoin wallet[32] aanbieder ter wereld. Ik heb indertijd geholpen hun niet-custodial wallet van de grond af aan opnieuw te programmeren.[33] Daarnaast was ik betrokken bij het mogelijk maken van het kopen en verkopen van Bitcoin rechtstreeks vanuit hunde wallet via hun Deense partner Coinify.[34]

Sinds 2017 werk ik aan Bitcoin Core,[35] de originele software achter Bitcoin. Daarbij concentreer ik me vooral op de wallet functionaliteit. Ik gaf eind 2018 een presentatie[36] in Londen over een deel van mijn werkzaamheden, en was in januari 2019 te gast bij BNR.[37]

De code die ik bijdraag is open source en terug te vinden op Github.[38] Daarnaast help ik ook met het controleren en testen van open source software bijdragen van andere vrijwilligers.[39] Bitcoin is van niemand, dus heeft ook geen baas die me kan betalen voor mijn open source software bijdragen. Gelukkig sponsort blockchain.info mijn open source werk sinds eind 2017.[40] Voor alle duidelijkheid: ik spreek volledig namens mezelf in deze brief.

Ik heb in 2013 een presentatie over Bitcoin gegeven bij het Landelijk Platform Officieren van Justitie Cybercrime bij het Openbaar Ministerie Parket Rotterdam. In februari 2018 gaf ik een demonstratie en technische uitleg bij De Nederlandsche Bank van het Lightning netwerk (een laag bovenop Bitcoin voor snellere transacties). Komende maand geef ik een keynote bij Odyssey[41], o.a. partners met het Ministerie van BZK, DNB en AFM, over de laatste technische ontwikkelingen binnen Bitcoin.

Met dank aan mr.drs. A.G. Haasnoot en enkele Twitter gebruikers voor feedback op de conceptversie.

[30] https://nl.linkedin.com/in/provoost
[31] https://www.slideshare.net/Provoost/bitcoin-transaction-in-ruby
[32] Blockchain is een niet-custodial wallet, dus geen "bewaarportomonnee" volgens het huidige voorstel
[33] https://blog.blockchain.com/2015/07/24/exclusive-sneak-peek-sign-up-now/
[34] https://coinify.com/news/blockchain-coinify-integration/
[35] https://bitcoincore.org/en/download/
[36] https://www.youtube.com/watch?v=SUDkYbkcTsQ
[37] https://www.bnr.nl/podcast/cryptocast/10366604/cryptocast-48-bitcoin-developer-sjors-provoost
[38] https://github.com/bitcoin/bitcoin/commits?author=Sjors
[39] https://bitcoinacks.com/?search=sjors
[40] https://blog.blockchain.com/2017/12/21/first-open-source-developer/
[41] https://www.odyssey.org/technical-deep-dive/