ONDERNEMERSCHAP & INNOVATIE

Bitcoin reguleren: een huzarenstukje

De bitcoin is sinds zijn inceptie paradoxaal genoeg zowel besmet als aansprekend geweest. De aanhangers ervan menen dat de bitcoin in een eerlijker, meer gedecentraliseerde vorm van financiering zal gaan voorzien. Tegenstanders wijzen er daarentegen op dat dubieuze klanten veel gebruik maken van bitcoin-betalingen. De traditionele regels voor klantidentificatie werken echter niet goed voor deze bedrijfstak. Het gebruik van financiële prikkels kan wel leiden om tot een identificatiesysteem te komen dat het nationale niveau overstijgt.

HANNA DELEANU
Postdoctoraal onderzoeker aan de Universiteit Utrecht

Bitcoin is een online-communicatieprotocol dat elektronische betalingen mogelijk maakt. Het is ontworpen door IT'ers en voorziet in een alternatief voor de gevestigde betaalsystemen (Böhme et al., 2015). De regels zouden moeten leiden tot een systeem dat minder vatbaar is voor reguleringsmissers, en minder gevoelig voor misbruik vanuit centrale banken. Het protocol stelt iedereen in staat om een rekening te openen tegen minimale kosten en zonder identiteitscheck. Het protocol is ingericht met waarborgen tegen machtsconcentraties, en op een manier dat er een vaste hoeveelheid geldcreatie en een publieke transactiegeschiedenis is (Nakamoto, 2008). Na de wereldwijde financiële crisis floreerde de bitcoin, vooral dankzij zijn decentrale karakter. Door decentralisatie kon een *single point of failure* vermeden worden en kregen de gebruikers – in ieder geval tijdelijk – een grotere financiële privacy. Voorheen faalden gecentraliseerde initiatieven: het cryptografische geld (Chaum, 1983) en virtuele valuta, zoals E-gold en Liberty Reserve (Foley, 2013; Lee, 2016). In navolging van de bitcoin kwamen er andere virtuele valuta (VV), zoals bytecoin en zerocoin, die nog meer privacy boden (Miers et al., 2013; Patterson, 2017).

In vergelijking tot gangbare betaalsystemen bestaat de hele bitcoin-beheerstructuur alleen uit het onderliggende protocol. Dit protocol vereist geen verificatie van de gebruikersidentiteit, wat de verdenking voedt dat de bitcoin een witwasmiddel zou zijn. In het algemeen is deze aantijging gebaseerd op drie veronderstellingen: bitcoins zijn waarschijnlijk niet onderhevig aan regulerend toezicht, ze zijn minder gevoelig voor blokkering of inbeslagname, en ze zijn makkelijker anoniem te verhandelen (Grinberg, 2011; FATF, 2015).

Als transacties anoniem zijn, kan de financiële sector geen onderscheid maken tussen klanten die te goeder trouw transacties uitvoeren en klanten die criminele opbrengsten overmaken. Om de identiteit te kunnen vaststellen van de uiteindelijk begunstigde eigenaar, is de financiële gemeenschap in 2003 een reeks KYC-protocollen *(know-your-customer)* overeengekomen die financiële entiteiten moeten uitvoeren wanneer ze met hun klanten in zee gaan (FATF, 2016a). Onder toenemende druk van berichtgeving over gebrek aan supervisie legden de regulatoren de traditionele KYC-protocollen op bij VV-overmakingen naar fiat geld (VV-naar-fiat) (OESO, 2015) (zie kader 1). Hoewel een protocolverandering ook denkbaar is in VV-naar-VV-overmakingen, is om bitcoin-gebrui-

Dit artikel is gebaseerd op Deleanu en Rose-Ackerman (2017)

kers te kunnen identificeren algehele consensus van de bitcoingemeenschap vereist. Dit zou het aanstellen van centrale arbiters met zich mee kunnen brengen en daarmee het gedecentraliseerde uitgangspunt van de bitcoin onderuit kunnen halen. Vanwege deze complicatie is hiervoor niet gekozen.

Van oudsher is het een huzarenstukje om het betalingsverkeer zo te reguleren dat er een adequate klantidentificatie mogelijk is zonder dat het systeem overbelast raakt. VV is de laatste in een lange reeks van betaalsystemen die gebruikt kunnen worden om over de grenzen heen anoniem geld over te maken en daarop geen uitzondering.

Om te onderzoeken in hoeverre VV-naar-fiat-betaaldienstverleners de facto de noodzakelijke KYC-protocollen naleven, heb ik een veldexperiment opgezet. In navolging van het onderzoek van Findley et al. (2014) naar lege vennootschappen, heb ik onder pseudoniem e-mails gestuurd naar 234 VV-naar-fiat-betaaldienstverleners waarin ik hun vroeg of ze bereid waren om op basis van anonimiteit een zakelijke relatie aan te gaan. De ontvangen reacties suggereren dat er diverse maatregelen zijn die zouden kunnen nemen om de blootstelling van hun bedrijfstak aan criminaliteit te beperken en het algemene vertrouwen in VV te versterken.

METHODE

In de studie is gekeken naar alle bedrijven die VV-naar-fiat-diensten aanboden tegen een vast tarief tussen mei 2016 en januari 2017. Deze definitie sluit VV-gebruikers, *miners* en *peer-to-peer*-platforms uit, maar omvat wel wallets en betaaldiensten die valuta wisselden. Verder regelden alle bedrijven in feite de geldstromen tussen kopers en verkopers of vormden ze zelf een van de transactiepartijen, en waren ze te identificeren met behulp van traditionele zoekopdrachten aan zoekmachines, zoals Google Search.

In navolging van Gerber en Green (2012) zijn de VV-naar-fiat-dienstverleners gegroepeerd in gestratificeerde blokken naar de nationale wet- en regelgeving en hun verplichting om KYC-protocollen uit te voeren die op hen van toepassing is. Ook is gekeken naar of ze KYC-protocollen op hun website vermelden.

Wat zou het effect van de prikkels van de Financial Action Task Force kunnen zijn?

KADER 1

Door het classificeren van VV-naar-fiat-betaaldiensten als betaaldienstverleners zet de Financial Action Task Force (FATF) aan tot consolidatie- of vluchtgedrag van de betaaldienstverleners. Consolidatie haalt de decentralisatie-inspanning onderuit, terwijl vluchtgedrag naar minder strikte rechtsgebieden de doelstelling om tot een eerlijkere maatschappij te komen frustreert. Beide reacties worden gedreven doordat men aan de kosten van de KYC-protocollen moet voldoen. Terwijl de technische belemmeringen om zulke VV-naar-fiat-betaaldiensten op te zetten minimaal zijn, kan een bedrijfsregistratie als betaaldienst hoge vergunningskosten en borgsommen met zich meebrengen (Bitstamp, 2017; Buenaventura, 2017). Recent onderzoek toont aan dat, in alle sectoren van het bedrijfsleven, de handhaving van KYC-protocollen beschouwd wordt als een van de belangrijkste bedrijfsrisico's en kostenposten, en dat *wallet*- en betaalsystemen vaak samengaan met VV-naar-fiat-betaaldiensten, om zo gemakkelijker klanten te trekken en vast te houden en hun operationele kosten te reduceren (Hileman en Rauchs, 2017).

Daarbij komt ook nog dat er grote verschillen zijn tussen de diverse rechtsgebieden qua effectiviteit van het toezicht, waar VV-naar-fiat-betaaldienstverleners hun voordeel mee kunnen doen. Het is lastig om de uiteindelijke begunstigde te kunnen identificeren en de grondigheid waarmee verplichte financiële entiteiten de KYC-protocollen uitvoeren, wordt gemonitord door nationale toezichthouders en afgedwongen via financiële sancties. In wat soepeler rechtsgebieden zijn financiële entiteiten wellicht in staat om zich zonder repercussies aan hun KYC-verplichtingen te onttrekken (FATF, 2016a).

Er is een grote verscheidenheid aan rechtsgebieden waar bedrijven gevestigd zijn, en een recente enquête uitgevoerd door Cambridge University toont aan dat er sprake is van incidenten bij regelgeving. De 51 betaaldienstverleners uit de enquête bevinden zich in 27 landen, en slechts 52 procent van de kleine kantoren en 35 procent van de grote had een overheidslicentie of -vergunning. Verder beschouwen de grote dienstverleners regelgeving als de factor met het hoogste bedrijfsrisico, gevolgd door het hacken van beveiliging en het handhaven van KYC-protocollen, terwijl kleine kantoren regelgeving en handhaving van KYC-protocollen tot de minst verontrustende operationele risico's rekenen (Hileman en Rauchs, 2017). Ondanks deze statistieken wil het feit dat men geen officiële vergunning heeft nog niet zeggen dat de betaaldiensten zich *niet* aan internationale wet- en regelgeving houden.

Tabel 1 laat zien dat de meeste VV-naar-fiat-kantoren het rechtsgebied van hun vestiging noemden – minder dan tien procent van de steekproef zei *'geen bedrijfsregistratie'* te hebben –, dat vele in rechtsgebieden waren gevestigd waar geen specifieke maatregelen golden om ze te reguleren, en dat de meeste van hen verwezen naar de protocollen om klanten op hun website te identificeren.

E-MAILVIGNETTEN

VV zijn producten met een hoog risico omdat ze de anonimiteit prefereren, makkelijk internationale grenzen kunnen overschrijden en geen transactielimiet kennen (FATF, 2016b). Toch zou het toegeven aan een anoniem verzoek zowel kunnen wijzen op betrokkenheid bij de bitcoin-principes als op onbekendheid met witwasrisico's. Om die twee uit elkaar te houden, zijn er e-mailvignetten gebruikt die land- en klantenrisico combineerden. De FATF meent dat landspecifieke risicofactoren onder meer landen omvatten waarvan men vermoedt dat ze terroristische activiteiten financieren of faciliteren, landen die geteisterd worden door georganiseerde misdaad of corruptie, en landen met een zwakke wetshandhaving.

Klantspecifieke risicofactoren bestaan wanneer een klant bereid is om niet-toegelichte afstanden te reizen om een transactie te regelen, die steekpenningen aanbiedt om de transactie uitgevoerd te krijgen, die gerelateerd is aan of handelt namens een politiek prominent persoon (PEP; *politically exposed person*), die de anonimiteit van de begunstigde niet wil prijsgeven, die een band met een criminele activiteit lijkt te hebben, of geassocieerd wordt met andere waarschuwingssignalen die door de FATF zijn afgegeven (Deleanu en Rose-Ackerman, 2017).

Land- en klantspecifieke risico's werden gevarieerd om drie identiteiten te creëren. Allereerst bevatte een *controlegroep* e-mails, ondertekend door een pseudoniem uit een land zonder risico voor terrorisme-financiering of corruptie, die als reden voor zijn anonimiteit ongewenste belangstelling of belastingontduiking noemde.

De *Behandelgroep Corruptie* bevatte e-mails, ondertekend door een pseudoniem uit een land met een groot corruptierisico, die als reden gaf om anoniem te blijven dat hij de financiële belangen van 'politiek prominente personen' behartigde. En de *Behandelgroep Terrorismefinanciering* bevatte e-mails die ondertekend waren door een pseudoniem uit een land met bekende terroristische groeperingen, die als reden gaf om anoniem te blijven omdat hij een soort liefdadigheidsinstelling runde – een bekende dekmantel voor de financiering van terrorisme.

Om de authenticiteit van de e-mails te vergroten, werden de pseudoniemen gekozen uit de meest algemene jongensnamen in het land van herkomst, werden inhoud en vorm van de e-mails willekeurig gevarieerd, en werden er willekeurig taal- en spelfouten toegevoegd. Afgezien van de inhoud waren de e-mails van de controle- en behandelgroepen op gelijke wijze van spelfouten voorzien, volgden ze dezelfde structuur en waren ze alle even lang.

Een aantal observaties zijn buiten de eindresultaten gehouden, bijvoorbeeld omdat subjecten met hun zakelijke activiteiten waren gestopt voordat het experiment was beëindigd of omdat ze op een niet te coderen manier antwoordden, zoals respondenten die niet in het Engels konden communiceren. De uiteindelijke steekproef bestond uit 384 responsen van 198 VV-naar-fiat-betaaldienstverleners. Het verschil in antwoorden tussen de groepen werd gemeten aan de

De steekproef van VV-naar-fiat-platforms, met gestratificeerde blokken

TABEL 1

	Landen	KYC-protocollen op de website vermeld	Geen verwijzing naar KYC-protocollen
Nationale wet- en regelgeving	Canada, China (incl. Hongkong), Frankrijk, Duitsland, Luxemburg, Zwitserland, VS	54	9
Voorstel voor nationale regulering	VK, Singapore, overige EU-lidstaten, Japan, Australië	60	21
Verboden	Thailand, Rusland, Bangladesh, Bolivia, Ecuador, Kirgizië, IJsland	3	6
Geen specifieke nationale regulering		45	21
Geen bedrijfsregistratie		3	12
Totaal		165	69

De steekproef is gerandomiseerd binnen de gestratificeerde blokken, en controles op randomiseringsgevoeligheid hebben bevestigd dat de steekproef goed gerandomiseerd is. Aan elk subject werden twee verschillende e-mailvignetten toegekend en men ontving twee e-mailberichten met een interval van minstens een maand, tussen september 2016 en januari 2017.

Bron: Deleanu en Rose-Ackerman (2017)

hand van een *difference-in-proportions*-test en een *multinomial-logarithmic*-regressie (tabel 2). Alle antwoorden werden blind gecodeerd door drie onafhankelijke codeerders.

RESULTATEN

Er was weinig significant verschil tussen de reacties op de behandelingen en de placebo-e-mails, en meer dan één op de tien betaaldienstverleners verlangden geen enkele vorm van identificatie van hun klanten, ongeacht welk ander land het was en de klantrisico's die deze klanten opleverden. Wat betreft de *'dodgy shopping count'* – de poging van een crimineel om verschillende ingangen tot het financiële systeem uit te proberen, totdat er eentje open gaat – zijn VV-naar-fiat-dienstverleners aantrekkelijk. Het kostte gemiddeld vijf tot tien e-mails om een bedrijf te vinden dat geen enkele vorm van identificatie vroeg of bereid was om de regels opzij te zetten teneinde klandizie binnen te halen.

We nemen aan dat de getoonde bereidheid van VV-naar-fiat-dienstverleners oprecht is, en niet bijvoorbeeld een gevolg van misleiding of een undercoveractie van de politie. De Internal Review Board van Yale University stemde met deze misleidingsstudie in onder voorwaarde dat er geen zakelijke relatie zou worden aangegaan tussen onderzoekers en subjecten.

VV-naar-fiat-dienstverleners kwamen de regels zelfs nog minder na dan partijen die anonieme lege vennootschappen oprichten (Findley et al., 2014). Additionele land- en klantspecifieke risico's maakten de waarschijnlijkheid alleen maar geringer dat bedrijven hun KYC-protocollen deels zouden nakomen. De totale of gedeeltelijke naleving van de KYC-protocollen was groter als de VV-naar-fiat-betaaldiensten specifiek genoemd werden in de nationale wet- en regelgeving, maar niet-nakoming kwam in alle jurisdicties voor, en was ook sterker in landen waar er discussies waren over voorstellen om transacties te reguleren (figuur 1).

LESSEN EN LANGETERMIJNOPLOSSINGEN

Regulering van de bitcoin-branche is noodzakelijk om de kans op crimineel misbruik te verminderen en om het vertrouwen in de bedrijfstak te vergroten. Het toepassen van oude regulerende praktijken brengt echter het risico met zich mee dat er situaties ontstaan die de bitcoin juist wilde verbeteren. Zo kunnen bijvoorbeeld de kosten die

Responsen van VV-naar-fiat-betaaldiensten, per behandelingstype

TABEL 2

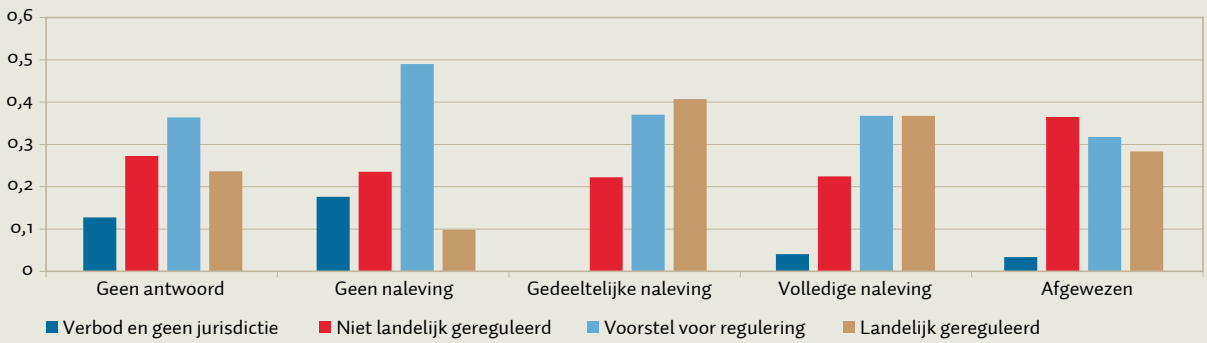
In procenten	N	Geen antwoord	Overeenstemming met KYC-protocollen			Afgewezen
			Niet	Gedeeltelijk	Volledig	
Ref.: Controlegroep	125	37	16	12	13	22
Groep Corruptie	133	45	14	3***	14	24
Groep Terrorismefinanciering	126	44	10	6*	11	29

*/*** *Significant in difference tests vergeleken met de placebo-conditie op respectievelijk tien- en eenprocentsniveau.*

Bron: Deleanu en Rose-Ackerman (2017)

Gemiddelde mate van naleving, per type rechtsgebied van de vestiging

FIGUUR 1



Bron: Deleanu en Rose-Ackerman (2017)

LITERATUUR

Arner, D.W., J. Barberis en R.P. Buckley (2017) FinTech and RegTech in a nutshell, and the future in a sandbox. *Research Foundation Briefs*, 3(4), 1–20.

Bitstamp (2017) *Payment institution license*. Te vinden op www.bitstamp.net.

Böhme, R., N. Christin, B. Edelman en T. Moore (2015) Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238.

Buenaventura, L. (2017) *The Philippines has decided to regulate bitcoin exchanges as remittance companies*. Te vinden op medium.com.

Chaum, D. (1983) Blind signatures for untraceable payments. In: D. Chaum, R.L. Rivest en A.T. Sherman (red.), *Advances in Cryptology*. New York: Springer, 199–203.

Deleanu, I.S. en S. Rose-Ackerman (2017) *Are Bitoins a Safe Haven for Money Launderers? Evidence from a Field Experiment*. Working Paper, te verschijnen.

FATF (2015) *Guidance for a risk-based approach: virtual currencies*. Parijs: FATF-GAFI/OESO. Te vinden op www.fatf-gafi.org.

FATF (2016a) *FATF Report to the G20: beneficial ownership*. Parijs: FATF-GAFI/OESO. Te vinden op www.fatf-gafi.org.

FATF (2016b) *Guidance for a risk-based approach: money or value transfer services*. Parijs: FATF-GAFI/OESO. Te vinden op www.fatf-gafi.org.

Findley, M.G., D.L. Nielson en J. Sharman (2014) *Global shell games: experiments in transnational relations, crime, and terrorism*. Cambridge: Cambridge University Press.

Foley, S. (2013) E-gold founder backs new Bitcoin rival. *Financial Times*, 28 november.

Gerber, A.S. en D.P. Green (2012) *Field experiments: design, analysis, and interpretation*. New York: W.W. Norton & Company.

Grinberg, R. (2011) BitCoin: an innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4, 159–208.

Hileman, G. en M. Rauchs (2017) *Global cryptocurrency benchmarking study*. Cambridge Centre for Alternative Finance. Te vinden op www.jbs.cam.ac.uk.

Lee, D. (2016) *Liberty Reserve digital cash chief jailed for 20 years*. BBC News, 9 mei. Te vinden op www.bbc.com.

Miers, I., C. Garman, M. Green en A.D. Rubin (2013) *Zerocoin: anonymous distributed e-cash from Bitcoin*. Te vinden op zerocoin.org.

Nakamoto, S. (2008) *Bitcoin: a peer-to-peer electronic cash system*. Paper te vinden op bitcoin.org.

Patterson, R. (2017) *Alternatives for proof of work, Part 1: Proof of stake*. Bytecoin Blog. Te vinden op bytecoin.org.

Vega-Serrano, J.M. (2017) *FATF FinTech and RegTech Forum 2017*. Te vinden op www.fatf-gafi.org.

men moet maken om traditionele KYC-protocollen uit te voeren, ertoe leiden dat VV-naar-fiat-dienstverleners zich vestigen in of verhuizen naar soepeler rechtsgebieden om zo hun KYC-verplichtingen geheel te ontlopen. Dit kan zonder enige repercussie.

Aan de andere kant kunnen big data en kunstmatige intelligentie de wijze veranderen waarop KYC-protocollen afgedwongen worden (Arner et al., 2017). Hoewel de bitcoin-gemeenschap geen wijziging van het bitcoinprotocol zal willen accepteren die iedere bitcoingebruiker tot identificatie verplicht, kunnen wereldwijde *compliance tools* toegepast op toezichtsplichtige entiteiten in de bitcoin-branche op meer steun rekenen. Dit was het onderwerp van de FATF-forumdiscussies in 2017 (Vega-Serrano, 2017).

In een sector waar KYC-protocollen minder worden toegepast dan door bedrijven die anonieme lege vennootschappen maken, waar 49 procent van de betaaldienstverleners tussen de één en tien werknemers heeft (Hileman en Rauchs, 2017), en waar 83 procent van de *wallets* die VV-naar-fiat-diensten aanbieden hun KYC-checks intern uitvoeren (Hileman en Rauchs, 2017) is er ruimte zijn om de identificatie van de uiteindelijke begunstigde te outsourcen. Als VV-naar-fiat-diensten verplicht worden om hun klanten te laten toetsen door een supranationale of nationale derde partij neemt dat de verleiding om met de KYC-protocollen te frauderen weg. Dan zou 'dodgy shopping' kunnen worden vermeden en zouden sommige *agency*-problemen waarmee de FATF zich geconfronteerd ziet, aangepakt kunnen worden. Als men deze service aan de VV-naar-fiat-dienstverleners gratis aanbiedt, zouden ze eerder geneigd zijn om dit te accepteren, omdat het dan zowel hun totale bedrijfskosten als hun risico's beperkt.

In het kort

- Het is van oudsher een lastige taak om betaalsystemen te isoleren van criminele activiteiten.
- Veel VV-naar-fiat-betaaldienstverleners spelen in op risicovolle klanten.
- KYC-protocollen worden makkelijker geaccepteerd als ze de nalevingskosten en blootstelling aan risico verminderen.