Digitale anonimiteit is ook bij gebruik van de bitcoin een gevaarlijke illusie

Subtielere consequentie van cryptogeld is versterking machtsconcentratie internetgiganten

Axel Arnbak

ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIEELE DAGBLAD

Naast het weer en de staat van het Nederlandse voetbal zijn de spectaculaire pieken en dalen van cryptomunt bitcoin een populair gespreksonderwerp bij de koffieautomaat. De krankzinnige waarderingen van cryptomunten steunen vooral op de belofte van anonimiteit en veiligheid van betalingen. Maar behendige wetenschappers ontdekken steeds meer manieren om die anonimiteit te doorbreken. Onlangs publiceerden onderzoekers van Princeton een succesvolle hack die de identiteit achter een bitcoin prijsgeeft, door bitcointransacties te combineren met onlinesurfgedrag, opgeslagen in internetcookies. Via het openbaar toegankelijke transactieregister blockchain linkten zij de identiteit vervolgens aan alle cryptotransacties uit het verleden. In plaats van veronderstelde anonimiteit, ligt zo ineens je gehele betaalgeschiedenis op straat. Niet alleen wat je speculeert op de koers, maar ook wat je in de winkel of een restaurant afrekent met de bitcoin. Bij iedere volgende hack zal de bredere samenleving zich stilaan realiseren dat het fundament van cryptomunten, anonimiteit, wankelt. En dat anonimiteit op internet een gevaarlijke illusie is.

Sinds de jaarwisseling is de bitcoin vier of zes keer zoveel waard geworden, afhankelijk van de dag waarop je meet. Natuurlijk wordt er veel gespeculeerd. Maar de bitcoin wordt ook steeds breder geaccepteerd als betaalmiddel. De belofte van anonimiteit en veiligheid speelt daarin een cruciale rol. Anders dan je pinpas en creditcard zouden je bitcointransacties nooit meer en door niemand tot jou te herleiden zijn.

Een onderzoeksteam uit Princeton toont in een reeks onderzoeken aan dat je niet op die anonimiteit kunt vertrouwen. In hun nieuwste onderzoek van drie weken terug — 'When the cookie meets the blockchain' — kraken zij niet zozeer de briljante versleuteling van het protocol, maar liften zij mee op cookies, stukjes spionagesoftware die vrijwel alle populaire websites op onze computers en smartphones installeren. Cookies dienen vooral om onlinegedrag in kaart te brengen, zodat websites gepersonaliseerde advertenties kunnen tonen. Maar cookies zijn meestal zo slecht beveiligd en in ieder geval zo talrijk op het web, dat het de onderzoekers vrijwel steeds lukt de ware identiteit achter een bitcointransactie te ontmaskeren. Door vervolgens het openbare transactieregister blockchain te analyseren, stellen zij dat juist de beheerders van cookies in staat zijn de betaalgeschiedenis achter een bitcoinaccount bloot te leggen.

De inventiviteit en creativiteit van de wetenschappers is uniek, maar hun tools zijn gratis en hun methoden, sinds kort, online gepubliceerd. En die naïeve en privacyminnende webshopper maar denken dat bitcoinbetalingen anoniem waren. De Princeton-onderzoekers trekken het bovendien breder. Anonimiteit is juist bij cryptomunten vrijwel onhaalbaar. Vanwege de technische noodzaak van het openbare transactieregister blockchain om transacties te valideren. En vanwege de maatschappelijk noodzakelijk interactie van cryptogeld met hun eigenaren en de reële economie — anders heb je niets aan je centen. De bedoelingen achter de bitcoin zijn revolutionair, maar de belofte van anonimiteit was altijd al naïef.

We moeten ons realiseren dat onfeilbare technologie onhaalbaar is

De illusie van anonimiteit is natuurlijk slecht nieuws voor de bitcoin en andere cryptomunten. Allereerst is ongerechtvaardigd vertrouwen op lange termijn funest voor de stabiliteit van een munt. De illusie is bovendien gevaarlijk: iedere shopper dacht een veilig betaalmiddel te hebben gevonden, maar met terugwerkende kracht is in één klap je gehele betaalgeschiedenis bekend. Een subtielere consequentie van cryptogeld is de versterking van de machtsconcentratie van internetgiganten. Omdat de cookies van giganten als Google Analytics op zoveel websites meekijken, kunnen juist zij de beste verbanden leggen tussen je surfgedrag en je cryptotransacties — en advertenties nog dieper toesnijden op je persoon. Hun netwerkeffecten blijven zich maar versterken, hun informatiemacht blijft maar groeien.

De bitcoin is natuurlijk meer dan alleen een anoniem betaalmiddel en de echte innovatie, het blockchainprotocol, zal in de toekomst tot veel spannender innovatie leiden dan geld. Maar een flinke dosis nuchterheid en besef van het gevaar van veronderstelde anonimiteit van het betaalmiddel zijn op hun plaats. We moeten ons realiseren dat onfeilbare technologie, ook bij cryptomunten, onhaalbaar is. En dat de koers van cryptomunten, net als het Nederlandse voetbal, overgewaardeerd is.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Voor reacties: @axelarnbak