RIEC
Amsterdam-Amstelland

Kennisdocument

Cryptobetaalkaarten en criminele geldstromen

Anoniemer dan cash

Samen slimmer tegen ondermijnende criminaliteit

Prepaid betaalkaarten zijn een risicovol fenomeen – ze vormen de brug tussen virtuele valuta en de offline criminaliteit

(TU Delft i.o.v. WODC, 2022)

Inhoud

1 Urgentie

In opsporingsonderzoeken naar ondergronds bankieren en witwassen worden door FinEC Amsterdam-Amstelland twee trends waargenomen: een toenemend gebruik van cryptovaluta (hierna: crypto's) voor het verplaatsen van crimineel vermogen en een toenemend gebruik van prepaid betaalkaarten om dat crimineel vermogen uit te geven. Zo is in 2022 in een opsporingsonderzoek naar ondergronds bankieren een in het buitenland uitgegeven prepaid betaalkaart met een hoog daglimiet in beslag genomen bij een verdachte, die gevoed werd door crypto's.

De opsporing heeft al eerder aandacht gevraagd voor het gebruik van prepaid betaalkaarten bij witwassen. Uit een thematisch onderzoek naar prepaid betaalkaartaanbieders - *card issuers* - bleek dat er veel contante opnames werden gedaan met deze kaarten. Contante opnames met de prepaid betaalkaarten bleken op te lopen tot tonnen per kaarthouder.

De regio Amsterdam-Amstelland vormt daarin een 'hotspot' voor contante opnames met deze betaalkaarten. Daarnaast is uit het onderzoek gebleken dat de prepaid betaalkaarten onder andere zijn gebruikt voor betalingen bij juweliers, luxe warenhuizen en hotels. De belangrijkste conclusie van het onderzoek is dan ook dat de prepaid betaalkaarten hand in hand gaan met witwassen.

Dat prepaid betaalkaarten hand in hand gaan met witwassen wordt mogelijk veroorzaakt door de inrichting van het (gebrek aan) toezicht daarop. Deze betaalkaarten worden nagenoeg altijd uitgegeven in landen waar een lichter toezichtregime geldt dan in Nederland, zoals bijvoorbeeld Guernsey, de Bahama's en de Kaaimaneilanden. Voor het uitgeven van betaalkaarten gelden in dergelijke toezichtregimes buiten de EU ook minder strenge eisen vanuit wet- en regelgeving ter voorkoming van witwassen. Prepaid betaalkaarten kunnen echter overal gebruikt worden: net als in Nederland uitgegeven betaalkaarten zijn deze namelijk aangesloten op het Visa- of Mastercard-betaalnetwerk en kan er dus ook in Nederland mee betaald worden. Het lichte toezichtregime en de mogelijkheid om de betaalkaarten ook in Nederland te gebruiken, waarmee het Europese en nationale antiwitwastoezicht volledig omzeild worden, vergroot het risico op het gebruik van prepaid betaalkaarten bij het verplaatsen of witwassen van crimineel geld. Onderzoekers van de TU Delft wijzen hier ook op in een recent onderzoek in opdracht van WODC en noemen de offline toepassing van deze kaarten zelfs een blinde vlek voor beleidsmakers[1].

Het is de veronderstelling dat prepaid betaalkaarten ook in de regio Amsterdam-Amstelland een blinde vlek voor beleids-makers vormen. De door FinEC Amsterdam-Amstelland waargenomen trends rondom het crimineel gebruik van prepaid betaalkaarten doen vermoeden dat deze een wezenlijk onderdeel uitmaken van de drugseconomie in de regio Amsterdam-Amstelland. Omdat het RIEC Amsterdam-Amstelland zich richt op het verstoren van de drugseconomie en de criminele geldstromen en cruciale schakels daarin, is besloten een aanpak te ontwikkelen op en onderzoek te doen naar het gebruik van prepaid betaalkaarten binnen criminele geldstromen. Het RIEC Amsterdam-Amstelland wil pionieren in deze aanpak: een relatief nieuw en onbekend fenomeen als het verplaatsen van crimineel geld via prepaid betaalkaarten leent zich daar goed voor. Dit kennisdocument heeft tot doel om iedereen in de keten van wetgeving, beleid, uitvoering, toezicht en opsporing van de witwasbestrijding op te roepen tot een gezamenlijke aanpak rondom de ontstane risico's rondom prepaid betaalkaarten. Op papier hebben we alle 'reguliere betaalmiddelen' (i.e. contant en giraal) in het antiwitwasbeleid streng gereguleerd, maar prepaid betaalkaarten brengen nieuwe risico's met zich mee die ook daadwerkelijk worden gebruikt. Witwassers hebben via deze route volledig vrij spel en maken er dankbaar gebruik van. Met gemak kunnen hoge bedragen ongezien worden witgewassen.

Dit kennisdocument is als volgt opgebouwd: de manier waarop we betalen verandert (hoofdstuk 2), hoe werken betaalkaarten? (hoofdstuk 3), monitoring van betaalkaarten (hoofdstuk 4) en crimineel gebruik van prepaid betaalkaarten (hoofdstuk 5).

2 De manier waarop we betalen verandert

Geen enkele sector is in het afgelopen decennium zo sterk veranderd als de financiële sector. Een *perfect storm* van technologische innovatie, veranderingen in wet- en regelgeving, de integratie van de Europese markt en globalisering hebben ervoor gezorgd dat de consument meer betaalmogelijkheden heeft dan ooit tevoren. Op hoofdlijnen zijn er vier grote veranderingen te zien in het betaallandschap:

1 Nieuwe betaalmethoden

Waar de consument voorheen alleen transacties kon verrichten met een betaalkaart met magneetstrip, heeft de introductie van de *NFC-chip* (Near Field Communication) in 2013 het mogelijk gemaakt om met andere middelen te betalen. Van juwelen tot horloge en telefoon: ieder apparaat dat een *NFC-chip* bevat kan anno 2023 gebruikt worden om betalingen mee te verrichten. Daarmee is het uiterlijk van betalen sterk veranderd. Toch is nog altijd een koppeling nodig met een fysieke of virtuele betaalkaart en is de betaalkaart hierdoor niet volledig vervangen door apparaten met een NFC-chip.

2 Fragmentatie

Door wijzigingen in wet- en regelgeving concurreren meer spelers met elkaar in het betaallandschap. Naast de traditionele spelers zoals banken, zorgen nu ook bedrijven die technologie inzetten om financiële diensten mogelijk te maken – *fintech* – voor innovatieve oplossingen op het gebied van betalen. Zo voorzien fintechs tegenwoordig bijvoorbeeld net als reguliere banken in kaartuitgifte *(card issuing)* en kaartacceptatie *(acquiring)*. Het gevolg van de komst van deze nieuwe spelers op de betaalmarkt is een meer gefragmenteerd betaallandschap. Alleen al in Nederland zijn er in de afgelopen vijftien jaar duizenden verschillende betaalkaarten in omloop die worden aangeboden door verschillende betaalkaartaanbieders (card issuers). De lengte van het unieke banknummer op betaalkaarten – *Bank Identification Number* of BIN – moest in 2022 zelfs worden vergroot van 6 naar 8 cijfers[2] om aan de toenemende vraag van card issuers te voldoen. Hoewel het aantal spelers in het betaallandschap sterk is toegenomen, zijn deze spelers toch nog altijd afhankelijk van twee bedrijven die betaalnetwerken onderhouden, namelijk Visa en Mastercard.

3 Bank-klantrelatie is minder persoonlijk

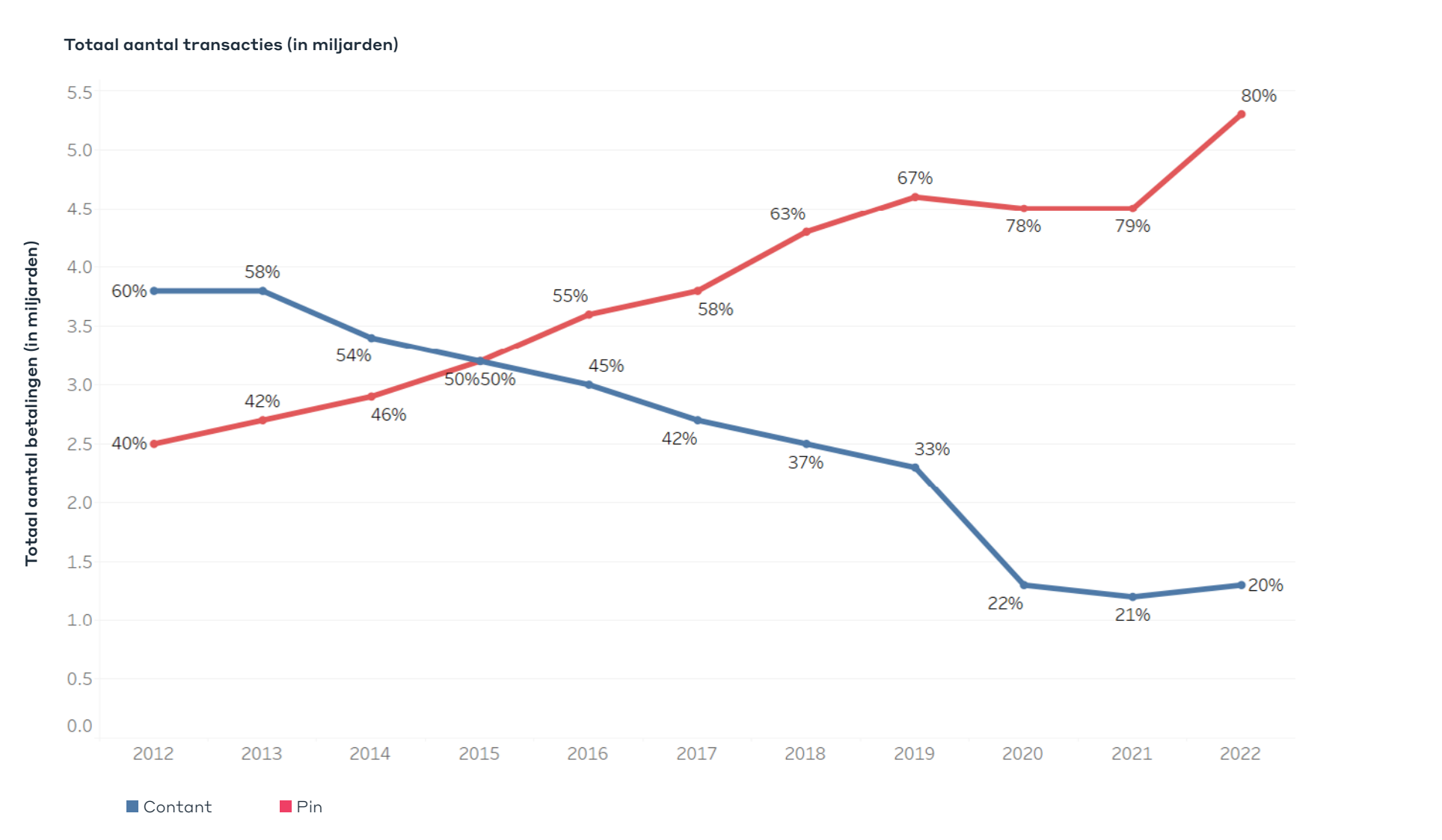
De toegenomen concurrentie en de nieuwe betaalmethoden hebben ook geleid tot een minder persoonlijke bank-klantrelatie. Zo zijn bankkantoren in de afgelopen tien jaar uit het straatbeeld verdwenen. Waar voorheen bij het openen van een nieuwe rekening nog een bezoek aan een bankkantoor nodig was om bijvoorbeeld identiteitsgegevens en NAW-gegevens te controleren, is dit tegenwoordig niet meer nodig. Het *account-opening proces* (AOP) vindt inmiddels volledig digitaal plaats via laptop, telefoon of tablet en duurt slechts enkele minuten. Concurrerende spelers op de betaalmarkt zorgen ervoor dat dit proces zo kort en soepel verloopt, om te voorkomen dat een potentiële klant vroegtijdig afhaakt.

4 Contant geld verdwijnt

Een vierde verandering in het betaallandschap is het verdwijnen van contante betalingen. Hier zijn meerdere redenen voor; de consument vindt kaartbetalingen makkelijk, met name de jongere generaties vinden de portemonnee anno 2024 niet of nauwelijks meer nodig. Vanwege het anonieme karakter van contante betalingen, wordt het door wet- en regelgeving als verhoogd risico gezien, met een afname van contante betalingen als resultaat. Daarnaast doen de betaalkaartmaatschappijen, banken, fintechs en lobbypartijen er alles aan om de betaalkaart te promoten en contante betalingen te ontmoedigen. Aan contante betalingen valt voor deze partijen immers niets te verdienen.

In 2012 wordt nog 60% van de betalingen in contanten afgerekend[3], waarna in 2015 het aandeel contante betaling daalt naar 50%. In 2022 bedraagt het aantal contante betalingen in 2022 nog slechts 20% van het totaal aantal betalingen (zie figuur 1). De verwachting is dat deze trend zich zal voortzetten: klanten kiezen vaker voor het gebruiksgemak van giraal betalen. Giraal betalen wordt ook vanuit de overheid gestimuleerd, vanwege de witwasrisico's rondom contant geld. Door critici wordt dit ook wel de 'war on cash' genoemd. De regering is bijvoorbeeld voornemens om alle contante betalingen boven €3000,- te verbieden.

figuur 1 Aandeel contante- en pinbetalingen van totaal aantal betalingen



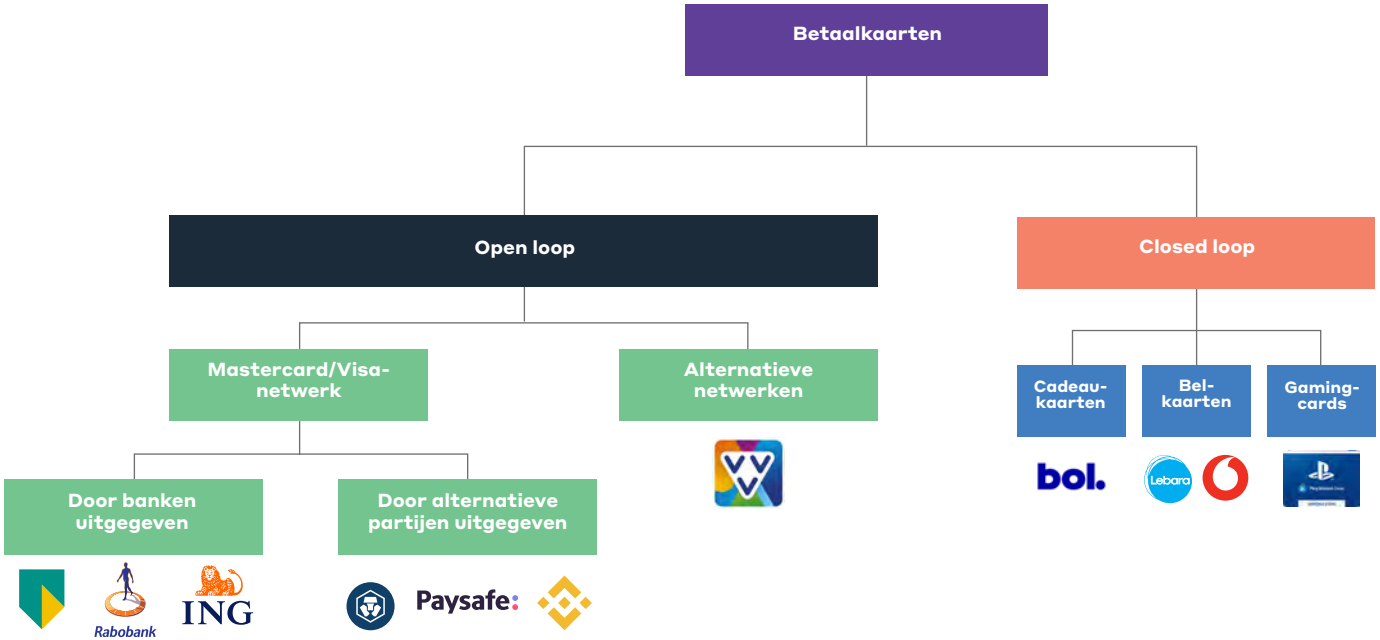
Bron: DNB, 2023-A

3 Hoe werken betaalkaarten?

Het aandeel van betalingen met betaalkaarten heeft sinds de introductie van de betaalkaart op de Nederlandse betaalmarkt in 1988 een vlucht genomen. Contant geld is in de loop der jaren steeds meer naar de achtergrond verdwenen. Anno 2024 wordt het merendeel van de betalingen gedaan met een betaalkaart. Maar waar contante betalingen relatief overzichtelijk zijn – er is een betalende partij en een ontvangende partij – zijn betalingen via betaalkaarten een stuk complexer. In dit hoofdstuk worden daarom de verschillende typen betaalkaarten en de spelers in het betaalkaartlandschap beschreven.

3.1 Type betaalkaarten

Er wordt over het algemeen onderscheid gemaakt tussen twee verschillende typen betaalkaarten: *closed-loop* en *open-loop* betaalkaarten. Closed-loop betaalkaarten kunnen bij één of een beperkt aantal winkels gebruikt worden en bevinden zich dus in een 'gesloten systeem'. Voorbeelden zijn cadeaubonnen (van parfumerie tot online marktplaatsen als Bol.com), belkaarten (Lebara of Vodafone) en gaming kaarten (X-box of Playstation). Deze kaarten zijn anoniem en hebben een lage nominale waarde (van €5 tot €150).



Open-loop betaalkaarten zijn op meer plekken te gebruiken. De open-loop tegenhanger van de eerdergenoemde cadeaubonnen is bijvoorbeeld de VVV-cadeaukaart, die bij ruim 15.000 winkels te besteden is in plaats van bij één specifieke winkel. Deze cadeaukaarten zijn vaak alleen lokaal te besteden; zo kunnen in Nederland uitgegeven kaarten vaak alleen in Nederland besteed worden. Ook open-loop betaalkaarten – zoals de VVV-cadeaukaart – kunnen anoniem zijn, zijn vaak eenmalig te gebruiken en hebben een maximale *load*; het bedrag dat op de kaart gezet kan worden.

Maar de bekendste open-loop betaalkaarten zijn de passen die wij als consumenten op dagelijkse basis gebruiken, zoals een betaalkaart van een bank. Deze kaarten maken over het algemeen gebruik van de infrastructuur van de Amerikaanse betaalnetwerken Visa of Mastercard en zijn nationaal, maar ook internationaal te gebruiken. In het verleden zijn dergelijke betaalkaarten voornamelijk uitgegeven door Wft-plichtige banken (Wet op het financieel toezicht), maar sinds de komst van PSD1 (Payment Service Directive 1), kunnen ook alternatieve partijen deze kaarten uitgeven. Die alternatieve partijen worden elektronischgeldinstellingen of EGI's genoemd. Zij richten zich met name op de uitgifte van 'elektronisch geld'. PayPal en Paysafe zijn voorbeelden van zo'n EGI.

Hoewel er de afgelopen tien jaar veel veranderingen in het betaallandschap hebben plaatsgevonden, zijn de typen betaalkaarten van Visa en Mastercard nog nagenoeg hetzelfde.

1 Debitcards

- Debitcards zijn in Nederland de meest gangbare betaalkaarten
- De klant heeft geen kredietafspraken: transacties met een debitcard worden direct gedebiteerd (afgeschreven) van de betaalrekening van de klant. Er moet dus geld op de bankrekening staan om te kunnen betalen
- Er is geen maximale load; het op te waarderen bedrag. Het bedrag dat kan worden afgeschreven is over het algemeen gelijk aan het saldo op de rekening. Wel kan er een dagelijks of maandelijks bestedingslimiet gelden om misbruik bij fraude of diefstal te voorkomen
- De debitcard en de betaalrekening worden vaak tegelijkertijd uitgegeven en zijn aan elkaar gekoppeld
- Debitcard betalingen zijn relatief goedkoop, want er is geen kredietrisico
- Debitcards zijn in Nederland aangesloten op de betaalnetwerken Debit Mastercard (was tot 2022 Maestro) of Visa Debit (was tot 2022 V PAY). Deze betaalnetwerken zijn kleiner dan de alternatieve betaalnetwerken voor creditcards Mastercard en Visa, waardoor de acceptatie van de kaarten buiten Nederland lager is. Debitcards zijn uitsluitend te gebruiken in winkels (*Point-of-Sale* of POS) en betaalautomaten *(Automated Teller Machine of ATM)*. Voor online betalingen (*e-commerce* of ECOM) zijn debitcards minder geschikt, omdat deze buiten de Europese Unie vaak niet geaccepteerd worden. In Nederland wordt een deel van de ECOM-betalingen daarom verricht met iDeal.

2 Creditcards

- Creditcards zijn in Nederland minder gangbaar dan in andere landen. Zo wordt in de Verenigde Staten voor bijna alle dagelijkse betalingen een creditcard gebruikt
- De klant heeft een kredietafspraak met de card issuer: er wordt bijvoorbeeld een maximaal bestedingstegoed van €2.500 afgesproken. Openstaande transacties worden opgespaard en periodiek gedebiteerd van de betaalrekening van de klant
- Betaalrekening en creditcard zijn in principe gescheiden: voordat een creditcard kan worden aangevraagd, zal er al een betaalrekening moeten zijn. Zo kunnen er meerdere creditcards aan één betaalrekening worden gekoppeld (bijv. zowel een Rabobank-creditcard, een ABN Amro-creditcard als een American Express-creditcard)
- Dit zorgt voor een kredietrisico voor de card issuer. De card issuer moet, ook als de klant verzuimt te betalen, zijn betalingsverplichtingen nakomen. Om deze reden worden creditcardbetalingen

strak gemonitord op misbruik en fraude, om te voorkomen dat de klant het openstaande bedrag niet kan terugbetalen en de card issuer hiervoor opdraait. Dit zorgt ervoor dat creditcardbetalingen in de regel duurder zijn dan debitcardbetalingen; de vergoedingen die hiervoor mogen worden gerekend zijn in de EU wel gemaximeerd

- Creditcards zijn aangesloten op het betaalnetwerk Visa of Mastercard en worden vrijwel overal ter wereld bij POS, ATM en ECOM geaccepteerd.

3 Prepaidcards/prepaid betaalkaarten

- Prepaidcards of prepaid betaalkaarten zijn in Nederland een minder gebruikelijk type betaalkaart, maar zijn inmiddels in opkomst
- Prepaid betaalkaarten worden o.a. gebruikt door mensen die afstand hebben tot de reguliere betaalmarkt. Zo geeft het *Centraal Orgaan Asielzoekers* (COA) al jaren prepaidcards uit aan asielzoekers. Ook de eerdergenoemde EMI's geven prepaid betaalkaarten uit aan bijvoorbeeld cryptogebruikers, die juist zelf afstand willen tot de reguliere betaalmarkt
- De klant heeft een e-*wallet*[1] bij de card issuer, die door de klant zelf moet worden opladen of gevuld. Bij een betaling wordt direct gedebiteerd van de wallet van de klant
- Er is hierdoor geen kredietrisico voor de card issuer waardoor de kosten van transacties met prepaid betaalkaarten relatief laag zijn
- Prepaid betaalkaarten zijn aangesloten op het Visa of Mastercard betaalnetwerk en worden daarom vrijwel overal ter wereld bij POS, ATM en ECOM geaccepteerd

1 Dit hoeft niet perse een crypto-wallet te zijn, maar kan breder geinterpreteerd worden dan een crypto-wallet.

3.2 Betrokken spelers bij kaartbetalingen

Zoals genoemd zijn transacties via betaal-kaarten complexer dan contante betalingen, omdat er meer spelers betrokken zijn die ieder ook een andere rol vervullen. Het meest gebruikelijke model voor kaarbetalingen is het 'vier partijen model' *(four corner model)*:

1 Cardholder / klant

De cardholder, kaarthouder of klant is degene die geld opneemt met een betaalkaart bij een ATM, in de winkel goederen afrekent met een betaalkaart of online goederen of diensten afneemt.

2 Issuing bank

Dit is de instelling die de betaalkaart uitgeeft aan de cardholder of klant

1. Bij debitcards is de issuing bank gelijk aan de bank waar de klant een bankrekening heeft: een ABN Amro-betaalrekening komt met een ABN Amro-debitcard.
2. Bij creditcards kan de issuing bank gelijk zijn aan de bank waar de klant een bankrekening heeft. Een klant heeft dan bijvoorbeeld een ABN Amro-betaalrekening met een ABN Amro-creditcard. De issuing bank en de bank van de klant kunnen echter ook verschillen. De klant heeft dan bijvoorbeeld een ICS-creditcard en een betaalrekening bij Bunq.
3. Bij prepaid betaalkaarten geeft de issuing bank vaak een betaalkaart uit namens een derde partij, bijvoorbeeld een cryptobeurs. De cryptobeurs – bijvoorbeeld Binance, Crypto.com of Coinbase – is hierbij de derde partij *(third party issuer)* omdat het zelf géén licentie heeft om kaarten uit te geven. Dit doen deze partijen vervolgens via een issuing bank. De klant heeft dan een overeenkomst met de derde partij, welke op zijn beurt een overeenkomst heeft met de issuing bank. De issuing bank kent de kaarthouder dus niet. Er zijn echter ook prepaid kaarten die door de issuing bank zélf worden aangeboden.

3 Merchant

De merchant of winkelier is de aanbieder van goederen of diensten die betaald worden met betaalkaarten. Dit kan zowel via POS als ECOM.

4 Acquiring bank

Dit is de partij waar de merchant of winkelier een betaalrekening heeft. Doorgaans is dit een financiële instelling zoals ABN Amro, Rabobank of ING.

Alle acties tussen bovenstaande spelers vinden altijd plaats via een betaalnetwerk, doorgaans Visa of Mastercard[2]. Visa en Mastercard geven de licenties (of lidmaatschappen) uit aan de card issuers en acquiring banks, waardoor deze via hun betaalnetwerken betalingen kunnen verrichten en accepteren. Op hun beurt verrichten card issuers namens cardholders en accepteren acquiring banks namens merchants weer betalingen. Card issuers sluiten daarvoor contracten af met cardholders en acquiring banks met merchants.

2 Hoewel Visa en Mastercard de grootste aanbieders zijn van betaalnetwerken, zijn er ook alternatieven: AliPay, American Express en UnionPay bijvoorbeeld

Naast bovenstaande rollen kunnen er nog twee rollen betrokken zijn bij transacties met betaalkaarten:

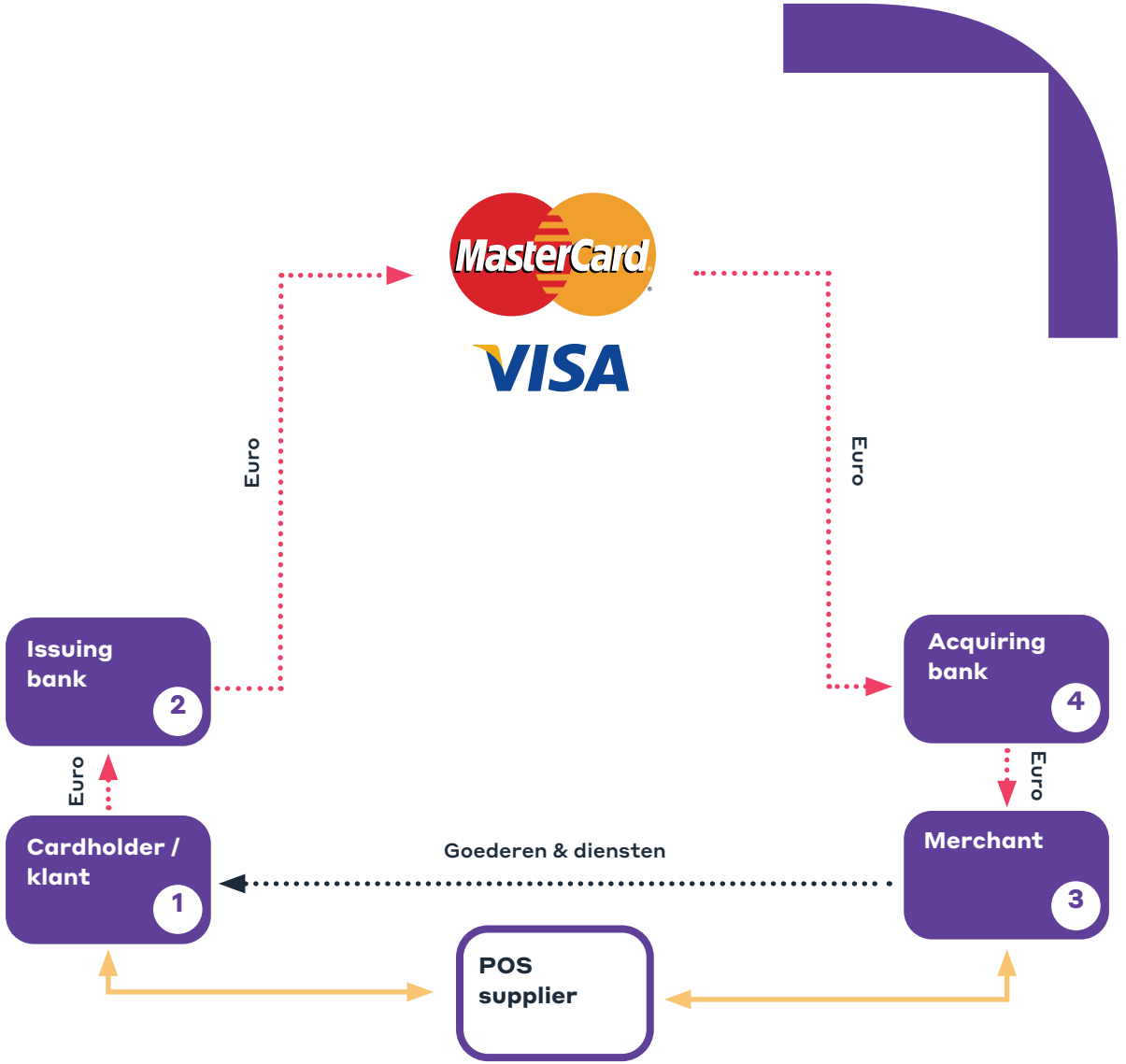
5 Processor

De processor neemt het technische gedeelte van kaartbetalingen voor zijn rekening; het verwerken van de betalingen. EMS is een grote processor.

6 Payment Service Provider

Payment Service Providers of PSP's zorgen ervoor dat online betalingen (ECOM) kunnen worden geaccepteerd door merchants. PSP's zorgen voor een platform waarop meerdere betaaltypes samenkomen: van iDeal tot Visa en van Mastercard tot Paypal. Het Nederlandse Adyen is als PSP gestart maar biedt tegenwoordig ook POS-terminals aan en doet zelfs processing.

Door bovenstaand voorbeeld zien we dat één partij – bijvoorbeeld Adyen – verschillende rollen kan vervullen bij kaartbetalingen: bij de ene betaling is Adyen de PSP, bij een volgende betaling doet het de processing van de transactie.




VISA

4 Monitoring van betaalkaarten

De veranderingen in het betaalkaartlandschap van het afgelopen decennium gingen samen met een groeiende zorg voor witwassen en andere vormen van ondermijnende criminaliteit.

Het toezicht op het betaalkaartlandschap anno 2024 kan worden opgedeeld in drie niveau's:

1 Toezicht op grond van internationale wet- en regelgeving

Op alle in hoofdstuk 3 genoemde partijen in het betaalkaartlandschap is internationale wet- en regelgeving van toepassing. Card issuers dienen hun KYC- en CDD-checks te doen en acquiring banks moeten controleren of de herkomst van de te accepteren transactie legaal is. Visa en Mastercard zelf hebben deze verplichtingen maar beperkt en zijn, omdat ze de infrastructuur aanbieden waarop de transacties worden gedaan, niet aansprakelijk voor de transacties 'zélf' die over de netwerken gaan. Beide partijen hebben 'slechts' een faciliterende rol en bieden 'neutrale infrastructuur'; 'Deze spelers hebben geen boodschap aan de boodschap' omschreef een van onze geinterviewden de rollen van beide spelers. In meerdere interviews werd de vergelijking gemaakt met (social) mediaplatforms als Youtube, Facebook en X (voorheen Twitter); de bedrijven achter deze platforms stelden in beginsel dat zij niet verantwoordelijk waren voor de content op hun platformen omdat zij zelf géén content maakten.

Tot de implementatie van PSD1 in 2009, was de rol van de toezichthouders kleiner dan dat deze nu is; er waren twee typen geld, namelijk contant en giraal. Met de implementatie van PSD1 kwam daar *electronic money* bij: *'een vorm van geld die monetaire waarde heeft en elektronisch of magnetisch bewaard wordt.'* Instanties die zich bezighouden met deze 'nieuwe' vormen van geld noemen we elektronischgeldinstellingen of EGI's. In Nederland is deze verordening – en de opvolger PSD2 – verankerd in de wet op financieel toezicht (Wft) met als Europees toezichthouder de ECB en nationaal DNB.

Zoals eerder genoemd worden veel prepaid betaalkaarten uitgegeven door deze Elektronische Geldinstellingen. Hoewel deze alternatieve partijen ook onder de Wft vallen, is het toezicht dat op hen gehouden wordt minder zwaar dan het toezicht op kredietscheppende banken (vanwege de systeemrelevantie, die de zwaarte van het prudentieel toezicht bepaalt). Bovendien zijn deze instellingen nagenoeg altijd gezeteld buiten Nederland; in de Baltische staten of Gibraltar, Guernsey als de instelling zich binnen de EU bevindt. Via het Europees Paspoort kan vervolgens alsnog de gehele EU bediend worden. Het komt ook vaak voor dat deze kaarten buiten de EU worden uitgegeven. Tot slot geldt het Europees depositogarantiestelsel (DGS) - een verzekering tot €100.000 spaargeld - niet voor de prepaid betaalkaarten.'

2 Toezicht op grond van nationale wet- en regelgeving

De Europese richtlijnen PSD1 en PSD2 hebben weliswaar een Europese reikwijdte – via het Europees paspoort – maar zijn in lokale wetgeving verankerd. De toezichtsrol is bij de lokale toezichthouder ondergebracht. Voor kaartbetalingen is dit in Nederland DNB, specifiek de afdeling Oversight. Omdat het betalingsverkeer tot de kritieke infrastructuur behoort, houdt DNB toezicht op een veilig, stabiel, betrouwbaar, efficiënt en toegankelijk betalingsverkeer. Deze afdeling houdt géén antiwitwastoezicht op grond van de Wwft (uitschrijven) op de kritieke infrastructuur. Het Wwft-toezicht wordt door de afdelingen van de DNB bij integriteitstoezicht uitgevoerd op Wwft-vergunde instellingen, waaronder de card issuers en acquirers.

3 Monitoring vanuit onder toezicht staande instellingen; Visa en Mastercard.

Deelnemende partijen – zoals issuing banks of acuiring banks – gaan een *membership* of lidmaatschap aan bij Visa of Mastercard. Om lid te kunnen worden moeten de deelnemende partijen vooraf door een *due dilligence* heen, waarin onder andere systemen en procedures worden geverifieerd. Na toelating is het mogelijk dat er nog audits volgen om de praktische invulling van de procedures na te lopen.

De invulling van de regelementen voor alle leden van de kaartsystemen worden opgesomd in de regelementen – in jargon *rulebooks* – van Visa en Mastercard. Alles dat met kaartbetalingen te maken heeft, wordt hier beschreven. Van de witwasregelementen waar de leden zich aan moeten houden, de gebieden waarin de leden hun diensten mogen aanbieden en aan de risico-inschattingen die leden moeten maken bij kaartbetalingen tot aan de specifieke plek van het Visa- of Mastercard logo op de betaalkaart en de zichtbaarheid van beide partijen in de winkel van de merchant. Maar hoewel alle regels in beton zijn gegoten, is het onduidelijk of Visa en Mastercard actief toezien op de naleving van de regels, in het bijzonder witwassen en criminele geldstromen. Meerdere geïnterviewde gaven aan dat dit niet het geval is. Beide partijen zijn niet verantwoordelijk voor wat er over het betaalnetwerk gaat, omdat in de wet is vastgelegd dat het een neutrale infrastructuur betreft. Mastercard en Visa verdienen bij iedere transactie op het netwerk, van legitieme transactie tot teruggedraaide transactie *(chargeback)*. Desgevraagd gaven meerdere geïnterviewden aan dat hierdoor een perverse prikkel ontstaat om zóveel mogelijk transacties te verwerken. Zijn de transacties legitiem, dan wordt hier een vergoeding voor gerekend. Blijken transacties niet legitiem te zijn, dan moet deze worden teruggedraaid en wordt opnieuw een vergoeding gerekend.

Voor de verschillende partijen in het vier partijen model geldt de volgende wet- en regelgeving:

1 Cardholder

- Bij debit- en creditcards heeft de kaarthouder in de regel een overeenkomst met de issuing bank. Bij prepaidcards heeft de kaarthouder in de regel een overeenkomst met een third party issuer zoals een cryptobeurs.
- Deze overeenkomst gaat over de productvoorwaarden (o.a. communicatie, kosten en bereikbaarheid), maar ook de Wwft-verplichtingen vanuit de bank: het ken je klant principe (KYC) en doorlopend clientonderzoek (CDD) en het melden van ongebruikelijke transacties (suspicious activity report, SAR).

2 Issuing bank

- De issuing bank heeft een overeenkomst met minimaal twee partijen: de kaarthouder en de netwerkbeheerder. Wanneer de bank betaalkaarten uitgeeft namens een andere partij – zoals bij prepaidkaarten vaak het geval is – is er óók een overeenkomst met deze third party issuer. Voorbeelden zijn de ANWB-creditcard, waarbij ANWB de third party issuer is en ICS de card issuer of de Binance prepaidcard, waarbij cryptobeurs Binance de third party issuer is en Solarisbank de card issuer.
- Om te voldoen aan de wettelijk verplichtingen die voortvloeien uit de Wwft, moet de issuing bank KYC, CDD en SAR doen.
- Aan de kant van de netwerkbeheerder moet de issuing bank zich houden aan de regelementen die door Visa en Mastercard gesteld worden.

3 Merchant

- De verkoper heeft minimaal één overeenkomst, namelijk die met een acquiring bank. In de regel neemt de verkoper bij de acquiring bank ook een pakket voor een betaalautomaat af; een Point of Sale (POS) terminal. Bij grotere concerns voorzien PSP's steeds vaker in deze terminals.
- Deze overeenkomst gaat over de productvoorwaarden (o.a. communicatie, kosten en bereikbaarheid), maar ook de Wwft-verplichtingen vanuit de bank: het ken je klant principe (KYC) en doorlopend clientonderzoek (CDD) en SAR.
- Hoewel de verkoper wél additionele vragen moet stellen wanneer aankopen van méér dan €10.000 worden gedaan met contantgeld, moet dit met kaartbetalingen níet. Voor betaalkaarten geldt het *honor all cards*-principe, waarbij álle betaalkaarten aan elkaar gelijk zijn.

4 Acquiring bank

- De acquiring bank heeft een overeenkomst met minimaal twee partijen: de verkoper en de netwerkbeheerder.
- Om te voldoen aan de wettelijke verplichtingen die voortvloeien uit de Wwft, moet de acquiring bank KYC en CDD en SAR doen. Hiervoor wordt vaak een acquiring processor zoals EquensWorldline ingeschakeld, een partij die voor meerdere instellingen transacties monitort.
- Aan de kant van de netwerkbeheerder moet de acquiring bank zich houden aan de regelementen die door Visa en Mastercard gesteld worden.

Gefragmenteerd zicht en toezicht

Iedere speler in het betaalkaartlandschap heeft zicht op een bepaald gedeelte van alle betalingen die met betaalkaarten worden gedaan. De toegenomen complexiteit van dat betaalkaartlandschap en de toename in de betrokken spelers zorgt er echter voor dat het zicht op betalingen via betaalkaarten versplinterd is. De vraag is dus of het in dit complexe betaalkaartlandschap nog mogelijk is om het totale plaatje te kunnen zien en daar ook effectief toezicht op te houden.

5 Crimineel gebruik van prepaid betaalkaarten

Een ruim aanbod aan betaalkaarten en een versplintering van het toezicht is ook gunstig voor criminelen. 'Cash is King' gold lang voor criminele transacties, maar de 'war on cash' is ook criminelen niet ontgaan. Contant geld wordt op steeds minder plekken geaccepteerd en de coronapandemie (2020 – 2022) heeft ook de acceptatie van contant geld binnen het criminele milieu onder druk gezet: tassen vol geld vielen meer op in een leeg straatbeeld waardoor criminelen moesten uitwijken naar alternatieve betaalmogelijkheden. Een voorbeeld van zo'n alternatieve betaal-mogelijkheid is crypto's; een digitale vorm van waarde die vrij anoniem en binnen korte tijd aan de andere kant van de wereld gebruikt kan worden. Volgens cijfers van Europol is het gebruik van crypto's ook sterk toegenomen sinds de coronapandemie. Hoewel crypto's criminelen veel voorbeelden bieden ten opzichte van contant geld, is er ook een groot nadeel: crypto's worden weinig tot niet geaccepteerd als betaalmiddel in legale systemen. Luxegoederen en dagelijkse aankopen kunnen vaak niet met crypto's betaald worden. Prepaid betaalkaarten die worden gevoed met crypto's worden juist wel overal geaccepteerd en vormen dus weer een alternatief voor crypto's.

Witwasrisico's

Prepaid betaalkaarten kennen een aantal witwasrisico's die het gebruik hiervan binnen criminele geldstromen aantrekkelijk maakt.

1 Brede acceptatie

Veel prepaid betaalkaarten zijn aangesloten op de betaalnetwerken van Visa of Mastercard, waardoor de kaarten nagenoeg overal worden geaccepteerd. Zowel online, bij ATM's als in de winkel (POS) kunnen de kaarten gebruikt worden. Dit in tegenstelling tot contant geld, dat juist op steeds minder plaatsen geaccepteerd wordt. Wordt een prepaid betaalkaart gevoed met crimineel geld, dan kunnen daarmee ook dagelijkse uitgaven worden gedaan of luxegoederen worden aangeschaft.

2 Makkelijk te vervoeren

Anders dan grote hoeveelheden contant geld, zijn betaalkaarten gemakkelijk te vervoeren. Honderduizend euro in briefjes van €50 weegt zo'n 2 kilogram, terwijl een betaalkaart die toegang geeft tot hetzelfde bedrag, enkele grammen weegt. Bovendien kunnen de kaarten makkelijk gedeeld worden met anderen.

3 Makkelijk aan te schaffen

Prepaid betaalkaarten zijn gemakkelijk aan te schaffen doordat het *Account Opening Process* (AOP) inmiddels volledig digitaal en snel doorlopen kan worden. Nieuwe spelers op de betaalmarkt concurreren bovendien met grootbanken, waardoor het AOP nog gemakkelijker gemaakt wordt voor de klant.

En hoewel wel een identiteitscontrole plaatsvindt, is deze vrij eenvoudig te omzeilen. Bijvoorbeeld door een katvangers de kaart aan te laten schaffen. Binnen enkele uren vraag je vrij gemakkelijk tien tot twintig betaalkaarten aan bij verschillende betaaldienstverleners. Hierdoor wordt het vermogen, maar ook het risico verspreid.

4 Lichter toezicht

Er is bij prepaid betaalkaarten vaak sprake van een lichter toezichtsregime ten opzichte van andere betaalkaarten. Allereerst worden prepaid betaalkaarten doorgaans niet uitgegeven door Wft-plichtige partijen zoals een bank, maar door *elektronisch geldinstellingen* (EGI's), die niet onder de Wft vallen. Hoewel deze partijen wel Wwft-verplichtingen hebben, is het toezicht dat zij houden op de naleving van de Wwft lichter. Bovendien vestigen deze EGI's zich ook vaak in zogenaamde toezicht-light regimes, zoals de Baltische staten, Malta, Guernsey of Gibraltar. Middels een Europees paspoort kunnen zij vervolgens de gehele Europese Unie bedienen. Uitgevers van prepaid betaalkaarten bevinden zich echter niet alleen binnen de EU.

In opsporingsonderzoeken worden geregeld betaalkaarten aangetroffen die zijn uitgegeven door card issuers gevestigd op de Bahama's of op de Seychellen. Vanwege de aansluiting op de Visa of Mastercard betaalnetwerken zijn deze betaalkaarten wel te gebruiken binnen de Europese Unie, ondanks het lichtere toezicht hierop.

Daarnaast is het toezicht op prepaid betaalkaarten lichter omdat vaak sprake is van een grotere afstand tussen kaarthouders en issuing banks. Veel prepaid betaalkaarten worden namelijk niet direct door issuing banks aan een kaarthouder uitgegeven, maar namens een derde partij. Deze partij neemt de administratie voor zijn rekening, waardoor de afstand tussen de partij met de vergunning (de issuing bank) die onder toezicht staat en de kaarthouder toeneemt. Er is dan ook geen direct contact tussen de kaarthouder en de card issuer, waardoor het moeilijk is om effectief toezicht te houden op de kaarthouder en diens transacties.

5 Toegang tot alternatieve vormen van geld

Prepaid betaalkaarten worden vaak niet aan een bankrekening gekoppeld maar aan een e-wallet. Zo geven deze betaalkaarten toegang tot alternatieve vormen van geld, zoals crypto's De klant houdt een wallet aan die wordt aangezuiverd met crypto's. Bij een kaartbetaling worden de crypto's uit deze wallet verkocht, zodat de verkoper zijn goederen in euro's US-dollars of Yen's ontvangt.

Conclusie

Het gebruik van prepaid betaalkaarten door criminelen lijkt in opkomst. Die opkomst wordt mogelijk aangewakkerd en versterkt door de teruglopende acceptatie van contant geld vanwege de ingezette *war on cash*. Binnen criminele geldstromen vormen deze betaalkaarten dus een aantrekkelijk betaalmiddel. Prepaid betaalkaarten bieden criminelen, vanwege de genoemde brede acceptatie, gemakkelijke aanschaf, het lichte toezicht en de toegang tot alternatieve betaalmethoden, een alternatief voor contant crimineel geld.

Ook bieden prepaid betaalkaarten voor criminelen een alternatief voor crypto's, omdat crypto's niet overal te besteden zijn. Met prepaid betaalkaarten, die soms ook gevoed kunnen worden met crypto's, kan juist overal betaald worden vanwege de aansluiting van de betaalkaarten op het Visa en Mastercard netwerk. Het *Anti-Money Laundering Centre* (AMLC) benoemt dergelijke betaalkaarten ook als een risicovol fenomeen en als witwasindicator. In het verleden zijn vanwege het overtreden van anti-witwasregelgeving ook licenties van card issuers die betaalkaarten die gevoed worden met crypto's ingetrokken. In 2018 worden bijvoorbeeld de Visa en Mastercard licenties van WaveCrest Holdings, die onder andere een kaart voor BitPay uitgaf, ingetrokken. Volgens het WODC vormen zulke betaalkaarten een brug vormen tussen crypto's en de 'offline criminaliteit'.

Bronvermelding

- *AMLC (2023). Wat is witwassen met cryptovaluta?.* Te benaderen via https://www.amlc.nl/witwassen-via-cryptovaluta/wat-is-witwassen-via-cryptovaluta/#witwassen-met-cryptovaluta-herkennen
- *Cointelegraph (2018). Visa Suspends WaveCrest Status, Stopping Some Crypto Credit Cards.* Te benaderen via https://cointelegraph.com/news/visa-suspends-wavecrest-status-stopping-some-crypto-credit-cards
- *DNB (2023-a). Betalen aan de kassa 2022.* Te benaderen via https://www.dnb.nl/media/e3ucvv4h/betalen-aan-de-kassa.pdf
- *DNB (2023-b). Factsheet Definitie elektronischgeldinstelling.* Te benaderen via https://www.dnb.nl/voor-de-sector/open-boek-toezicht/sectoren/elektronischgeldinstellingen/vergunning-elektronischgeldinstellingen-overzichtspagina/definitie-elektronischgeldinstelling/
- *Mastercard (2023). Marcard Rules.* Te benaderen via https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf
- *TU Delft (2022). Virtuele valuta: Handelingsperspectieven voor data-gedreven opsporing.* Te benaderen via https://repository.wodc.nl/bitstream/handle/20.500.12832/3215/3184-virtuele-valuta-volledige-tekst.pdf
- *Tweede Kamer (2023). Wetsvoorstel Wet plan van aanpakken witwassen.* Te benaderen via https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorstelde-tails&qry=wetsvoorstel%3A36228
- *Visa (2023). Visa Core Rules and Visa Product and Service Rules.* Te benaderen via https://usa.visa.com/content/dam/VCOM/download/about-visa/visa-rules-public.pdf
- *Worldline (2021). Introductie van BIN van 8 cijfers.* Te benaderen via https://www.six-payment-services.com/nl/shared/news/2021/8-digit-bin.html

Colofon

Uitgave	RIEC Amsterdam-Amstelland, februari 2024
Onderzoek en teksten	RIEC & FINEC Amsterdam-Amstelland
Vormgeving	Lassooy Design


BINANCE
Buy Crypto
Markets
Trade
Derivatives
BTC/USDT
49,567.36
Spot
Cross 3x
Isolated 10x
Limit
Market
Stop-limit
Buy BTC
Sell BTC
- USDT
- BTC

RIEC
Amsterdam-Amstelland

Samen slimmer tegen ondermijnende criminaliteit

riecaa@politie.nl

www.riecaa.nl

LAS23457