

FINNIUS

MEMORANDUM

Aan **Coöperatie Greenhood U.A.** | Jeroen Slaman

Van **Finnius** | Daniëlle van de Vijver en Tim de Wit

Datum 17 december 2025

Onderwerp Reikwijdteadvies Greenhood App

SAMENVATTING

Greenhood verleent naar ons oordeel geen gereguleerde diensten in Nederland onder de Wft of MiCAR op basis van de feiten zoals door Greenhood geschetst. Dit kan als volgt worden samengevat:

Cryptoactivadienst (g) - Het ontvangen en doorgeven van cryptoactivaorders namens cliënten	Greenhood ontvangt en geeft naar ons oordeel geen cryptoactivaorders door namens cliënten. De Gebruiker gebruikt de Greenhood App immers als instrument om zelf, rechtstreeks op de blockchain, transacties uit te voeren. Greenhood fungeert hierbij niet als tussenpersoon maar als softwareleverancier van een technische interface. Greenhood heeft geen kennis van de door de Gebruiker ingeleigde order.
Cryptoactivadienst (h) - Het verlenen van advies over cryptoactiva	Greenhood geeft geen advies over cryptoactiva of cryptoactivadiensten. Wel geven wij Greenhood mee dat zij ervoor moet waken dat dit in de toekomst ook niet gebeurt.
Cryptoactivadienst (j) - het verlenen van cryptoactivaoverdrachtdiensten namens cliënten	Greenhood verleent naar ons oordeel geen cryptoactivaoverdrachtdiensten. De Gebruiker initieert en signeert transacties vanuit de Greenhood App immers zelf zonder dat Greenhood in de cryptoactivastroom betrokken is. Daarna moet de Gebruiker een transactie zelf publiceren op de blockchain. Greenhood initieert de transactie ook niet, dat doet de Gebruiker zelf. Als ondersteunend argument geldt dat de SAFE Wallet kwalificeert als een non-custodial wallet, welke type wallet zijn uitgezonderd van de scope van MiCAR.
Bemiddelen (Wft)	
Bemiddelen in betaalrekeningen	Greenhood bemiddelt naar ons oordeel niet in de betaalrekeningen zoals aangeboden via Monerium. Greenhood is immers niet inhoudelijk betrokken bij de totstandkoming van de overeenkomst tussen de Gebruiker en Monerium. De Gebruiker levert zelf direct de voor de overeenkomst relevante gegevens aan bij de aanbieder en bovendien ontvangt Greenhood geen vergoeding van de aanbieder.
Bemiddelen in elektronisch geld	Greenhood bemiddelt niet in elektronisch geld. Greenhood is immers niet inhoudelijk betrokken bij de totstandkoming van de overeenkomst tussen de Gebruiker en de aanbieder van elektronisch geld. De Gebruiker levert zelf direct de voor de overeenkomst relevante gegevens aan bij de aanbieder en bovendien ontvangt Greenhood geen vergoeding van de aanbieder.

Aanbevelingen

Wel merken wij op dat het van belang is dat Greenhood nooit de indruk wekt dat zij de aanbieder is van een bepaalde dienst die door een derde wordt aangeboden. Denk hierbij aan de IBAN die wordt aangeboden via Monerium, maar waar door Greenhood naar wordt verwezen als de Greenhood IBAN. Dergelijke uitspraken wekken immers de impressie dat Greenhood de aanbieder is van een dergelijk product, wat niet het geval is. Een ander voorbeeld is de in-app browser om een account aan te maken bij Monerium. In deze in-app browser is het logo van Greenhood zichtbaar, maar het logo van Monerium niet. In dat geval is het belangrijk om duidelijk aan te geven dat Monerium de exclusieve aanbieder is van deze diensten samen met het logo van Monerium. Dit is wat ons betreft een zeer belangrijk aandachtspunt, nu de dienstverlening van Greenhood veel gelijkenis toont met gereguleerde dienstverlening.

In dat kader is het van belang dat Greenhood aan goede informatieverstrekking doet en duidelijk maakt wat de rol is van iedere betrokken partij met wie relaties worden aangegaan en welke bescherming daarbij hoort voor de Gebruiker.

1. INTRODUCTIE

- 1.1 Coöperatie Greenhood U.A. (**Greenhood**) biedt de infrastructuur voor een betaaloplossing aan op basis waarvan gebruikers (**Gebruikers**) zelfstandig hun vermogen kunnen beheren gebruikmakend van de blockchain technologie via de app van Greenhood (**Greenhood App**). Op dit moment is dit slechts mogelijk in verband met cryptoactiva. Greenhood is voornemens om dit in de toekomst uit te breiden met andere producten, waaronder met geldmiddelen, financiële instrumenten, verzekeringen, eigendomsbewijzen, abonnementen of andere producten van waarde (**Aanvullende Producten**).
- 1.2 In dit advies wordt geanalyseerd of de diensten die Greenhood verleent in verband met de Greenhood App mogelijk gereguleerd zijn onder het financieel toezichtrecht dat van toepassing is in Nederland, op basis van de Wet op het financieel toezicht (**Wft**), Richtlijn (EU) 2015/2366 betreffende betalingsdiensten in de interne markt (**PSD2**), Richtlijn 2009/110/EG betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld (**EMD2**) en de Verordening (EU) 2023/1114 betreffende cryptoactivamarkten (**MiCAR**). Dit advies heeft geen betrekking op andere financieel toezichtraamwerken, waaronder Richtlijn 2014/65/EU betreffende markten voor financiële instrumenten (**MiFID II**).
- 1.3 Dit advies is uitsluitend opgesteld ten behoeve van Greenhood en beperkt zich tot een analyse van het toezichtrecht dat van toepassing is in Nederland voor zover de diensten betrekking hebben op cryptoactiva. De Aanvullende Producten die Greenhood in de toekomst zal betrekken in de Greenhood App blijven voor dit advies dus buiten beschouwing. Verder ziet dit advies slechts op de diensten die volgen uit de Greenhood App. Let op: op voorhand is zeker niet uitgesloten dat het aanbieden van de Greenhood App ten aanzien van de Aanvullende Producten leidt tot toepasselijkheid van regelgeving, zoals MiFID II. Wij begrijpen verder dat het ook mogelijk is om lid te worden van de Greenhood coöperatie door via een dApp (hierna gedefinieerd) te investeren in Greenhood certificaten. Deze constructie valt echter buiten de scope van dit advies. Daarnaast laten wij ons niet uit over de kwalificatie van diensten die door partners van Greenhood worden verleend, zoals Monerium en Gnosispay, noch de toelaatbaarheid van de diensten die zij verlenen.
- 1.4 Dit advies is gebaseerd op de relevante wet- en regelgeving en interpretaties van de relevante financiële toezichthouder(s) zoals van toepassing in Nederland op de datum van

dit advies. Dit advies heeft geen betrekking op andere juridische of fiscale aspecten, zoals aspecten met betrekking tot contract-, goederen-/eigendoms- en/of privacyrecht. Dit advies geeft evenmin een oordeel over wetgeving van andere lidstaten van de Europese Unie (**EU**) of niet-EU-rechtsgebieden.

1.5 Tegen deze achtergrond, heeft dit advies de volgende structuur:

- de informatie waarop dit advies is gebaseerd, met inbegrip van een beschrijving van de relevante feiten met betrekking tot de Greenhood App (paragraaf 2);
- het relevante juridisch kader voor de kwalificatie van de diensten verbonden aan de Greenhood App (paragraaf 3); en
- een analyse van de diensten verbonden aan de Greenhood App (paragraaf 4).

2. FEITEN

2.1 Via de Greenhood App kunnen Gebruikers cryptoactiva bewaren, aankopen, versturen en ontvangen. De Greenhood App fungeert in feite als een portaal. Hiervoor wordt gebruikt gemaakt van andere partijen, *decentralized exchanges* (**DEX**) en gedecentraliseerde applicaties van derden.

2.2 Gebruikers kunnen gratis van de Greenhood App gebruik maken. In de toekomst gaat dit veranderen en zal de Greenhood App naast de gratis variant ook beschikbaar zijn tegen maandelijkse betaling in de vorm van een abonnement. Daarbij geldt dat Greenhood geen persoonlijke gegevens (zoals naam, e-mailadres of geboortedatum) van de Gebruiker verzamelt wanneer de Greenhood App wordt gedownload.

2.3 Hieronder bespreken we de verschillende functionaliteiten van de Greenhood App, namelijk i) het creëren van een seed en een SAFE Wallet, ii) het uitvoeren van betaaltransacties en iii) het gebruik van dApps.

i) Het creëren van een seed en een SAFE Wallet

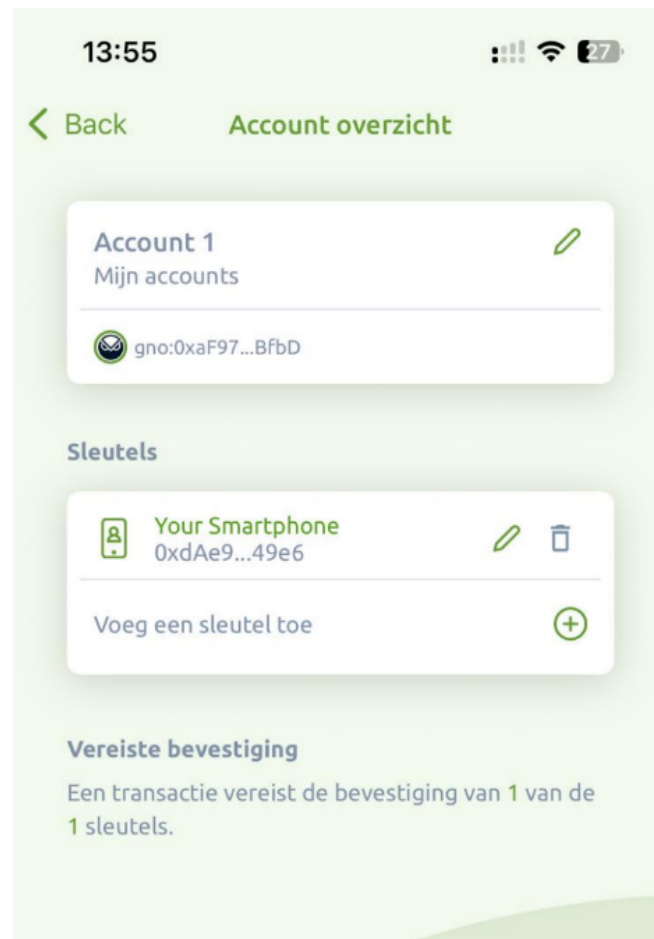
2.4 Via Greenhood kan een Gebruiker zelf zijn cryptoactiva beheren en transacties uitvoeren. Hiervoor wordt er voor de Gebruiker een wallet aangemaakt bij SAFE (zoals hieronder uitgewerkt) en kan de Gebruiker andere SAFE wallets koppelen.

2.5 Greenhood maakt voor iedere Gebruiker een smart-contract wallet (SAFE Wallet) aan. Hiervoor maakt Greenhood gebruik van 'SAFE'¹, een *decentralized autonomous organization* die een smartcontractoplossing aanbiedt op basis waarvan Gebruikers hun cryptoactiva kunnen beheren. Een SAFE Wallet is geen traditionele wallet waarbij het walletadres rechtstreeks wordt gecontroleerd door een private key. In plaats daarvan is een SAFE Wallet een smart contract dat op de blockchain is gepubliceerd. Het SAFE smart contract houdt een lijst bij van geautoriseerde *owners* (Ethereum-adressen) die transacties mogen ondertekenen. Transacties vanuit een SAFE Wallet vereisen een geldige handtekening van een of meer van deze geautoriseerde owners. In dit geval is dat de Gebruiker.

¹ Zie ook: <https://safe.global/wallet>.

FINNIUS

- 2.6 Het adres behorende bij de SAFE Wallet en de bijbehorende sleutels (i.e. ondertekeningsmethode) zijn zichtbaar in de Greenhood App. Deze sleutel kan worden gebruikt om transacties te verrichten met een SAFE Wallet vanuit de Greenhood App. In de Greenhood App kan de Gebruiker bijvoorbeeld gebruik maken van een pincode. Overigens wordt het in de toekomst mogelijk om ook andere sleutels toe te voegen aan de SAFE Wallet, waardoor het een *multisignature* account wordt of waardoor het mogelijk wordt om een transactie middels een andere private key te signeren. Ook over deze aanvullende sleutels heeft Greenhood geen beschikking. Dit wordt als volgt weergegeven in de Greenhood App:



FINNIUS

- 2.7 Bij het installeren van de Greenhood App wordt er op het apparaat van de Gebruiker een seed gegenereerd bestaande uit twaalf Engelstalige woorden. Deze seed wordt uitsluitend op het apparaat van de Gebruiker gegenereerd en moet worden opgeslagen door de Gebruiker. Deze seed verlaat nooit de telefoon van de Gebruiker en wordt dus ook niet naar of over de server van Greenhood gestuurd. Een Gebruiker heeft deze seed nodig als hij met de ingestelde verificatiemethoden niet meer bij zijn SAFE Wallet kan via de Greenhood App (bijvoorbeeld omdat hij zijn telefoon is verloren) en dus zijn SAFE Wallet moet herstellen. Voor de rest van dit advies gaan wij ook van deze assumptie uit. Hierdoor geldt dat de Gebruiker zijn private key *self-hosted* beheert (Greenhood heeft hier geen toegang tot), terwijl de SAFE Wallet zelf een smart contract is dat on-chain wordt beheerd. In de Greenhood App zelf hoeft de Gebruiker overigens geen gebruik te maken van zijn seed. De seed wordt als volgt weergegeven in de Greenhood App:



- 2.8 Gebruikers die al over een SAFE Wallet beschikken, kunnen hun seed inladen in de Greenhood App. Hiervoor vult de Gebruiker de twaalf woorden van de seed in de Greenhood App. De Greenhood App genereert het publieke adres dat hoort bij de seed van de gebruiker. Dit publieke adres wordt via de Greenhood Wallet naar SAFE gestuurd. Op basis van dit publieke adres, dat fungeert als sleutel van de Gebruikers SAFE Wallet, wordt de bijbehorende SAFE Wallet van de gebruiker gevonden en geactiveerd in de Greenhood App. De seed blijft echter ten alle tijden enkel beschikbaar voor de Gebruiker en wij nemen dus aan dat Greenhood hier geen toegang tot heeft. Gebruikers kunnen daarbij meerdere SAFE Wallets koppelen aan de Greenhood App, waardoor iedere SAFE Wallet voor een andere functionaliteit gebruikt kan worden.
- 2.9 Zodra de Gebruiker cryptoactiva opslaat in de SAFE Wallet worden deze cryptoactiva ook zichtbaar in de Greenhood App. De Greenhood Wallet heeft immers het publieke SAFE adres van de gebruiker en leest hiermee de informatie (bv EURE coin en aantallen) van de blockchain. Greenhood zelf heeft echter geen inzicht in de gebruikersdata omtrent het saldo en transacties van de Gebruiker.
- ii) Het uitvoeren van betaaltransacties
- 2.10 Gebruikers kunnen cryptoactiva versturen en ontvangen naar respectievelijk van andere Gebruikers met wallets die ondersteuning bieden voor Ethereum en EVM-compatibele blockchains. Dit kan onder meer door een QR code te scannen van een andere Gebruiker. De transactie wordt vervolgens gesigneerd door de Gebruiker via de Greenhood app, waarna de cryptoactiva worden verstuurd via de blockchain.
- 2.11 De Gebruiker kan deze transactie op drie verschillende mogelijkheden publiceren op de blockchain afhankelijk van het abonnement van de Gebruiker (Greenhood heeft geen invloed op deze keuze en heeft hier ook geen kennis van):
- 1) De transactie wordt afgehandeld door een 'Relayer' van Gelato. Dit is een Zwitsers bedrijf dat een non-custodial service aanbiedt om de transactie voor de Gebruiker op de blockchain te publiceren. Greenhood betaalt hierbij (voorlopig) de transactiekosten door middel van een prepaid tegoed per maand.
 - 2) De Gebruiker betaalt de transactie zelf door native cryptoactiva aan te houden in de wallet voor de betreffende blockchain (e.g. Ether voor de Ethereum blockchain).
 - 3) De Gebruiker kan via de Greenhood App zijn SAFE Wallet verbinden met elke relayer service en de transactie publiceren op de blockchain door gebruik te maken van de externe aanbieder Wallet Connect.

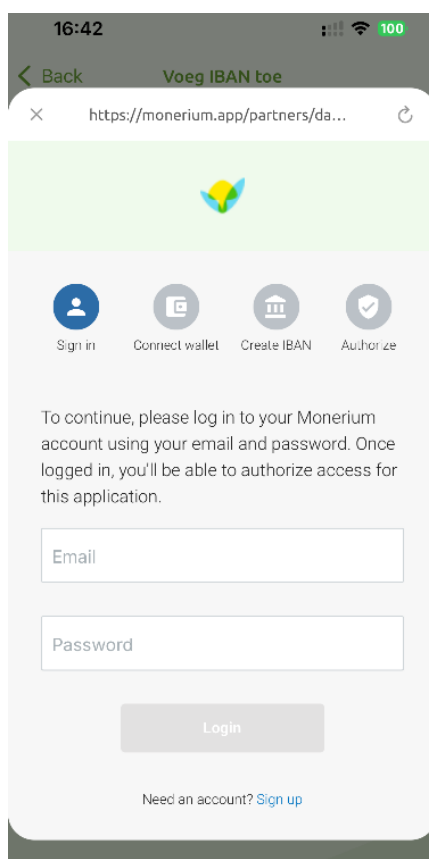
Samenwerking met derde partijen

- 2.12 Voordat een Gebruiker gebruik kan maken van Greenhood is het vereist dat de Gebruiker een betaalrekening met IBAN koppelt aan zijn SAFE Wallet. Daarnaast kan een Gebruiker ook een betaalinstrument koppelen aan zijn SAFE Wallet. Hiervoor maakt Greenhood gebruik van Monerium ehf. (**Monerium**) en Gnosispay (**Dienstverleners**) (dit wordt in de toekomst mogelijk uitgebreid met andere partijen). De Gebruiker gaat daarvoor een directe contractuele relatie aan met de Dienstverlener. Vervolgens kan de Gebruiker de diensten van de Dienstverlener koppelen aan zijn SAFE Wallet in de Greenhood App via een API door middel van de inloggegevens van de Gebruiker. Hiervoor is Greenhood een zogenoemde partner van de Dienstverlener.
- 2.13 Greenhood faciliteert enkel dat de Gebruiker een dienst van Dienstverlener kan afnemen in de Greenhood App. Greenhood is verder echter niet betrokken bij deze overeenkomst. Greenhood heeft ook geen inzicht wie van haar Gebruikers gebruikt maakt van de Dienstverlener en speelt daarbij ook geen rol in de customer due diligence die door de Dienstverlener wordt uitgevoerd.

- 2.14 De gebruikersinformatie wordt voor de Gebruiker inzichtelijk gemaakt in de Greenhood App op basis van een API key die de Gebruiker ontvangt van de Dienstverlener en die door de Greenhood App wordt gebruikt om transacties mogelijk te maken. Ook deze gebruikersinformatie wordt niet geaggregeerd weergegeven. Dit betekent dat Greenhood de data niet ontvangt via de Greenhoodserver en deze data ook niet verwerkt voordat de data wordt getoond aan de Gebruiker. De Gebruiker hoeft dus niet per se gebruik te maken van Greenhood om zijn gegevens in te zien, maar kan hiervoor ook een andere applicatie gebruiken.

Samenwerking met Monerium

- 2.15 Zoals aangegeven kan een Gebruiker pas gebruik maken van de SAFE Wallet, nadat de Gebruiker een IBAN koppelt aan zijn SAFE Wallet via de Greenhood App. Hiervoor maakt de Gebruiker een account aan bij Monerium. Dit gaat in principe helemaal buiten Greenhood om. De Gebruiker kan dit namelijk doen via de website van Monerium of via een webpagina van Monerium in de Greenhood App. Dit kan het beste worden geïllustreerd aan de hand van de volgende afbeelding:



- 2.16 Greenhood krijgt daarbij geen fee voor ieder aangebrachte Gebruiker bij Monerium.
- 2.17 Monerium geeft de e-money token (**EMT**) "EURE" uit en beschikt daarvoor over een vergunning als elektronischgeldinstelling (**EGI**). Monerium geeft Gebruikers de mogelijkheid om – uiteindelijk - betalingen in EUR te doen of te ontvangen. Daarvoor is het vereist dat de Gebruiker zijn SAFE Wallet koppelt aan de IBAN service die wordt aangeboden door Monerium.² Monerium biedt deze dienst overigens niet zelf aan, maar maakt hiervoor gebruik van AS LHV Pank (**LHV**) een geregeleerde bank door de Estonian Finantsinspeksioon.³

² Zie ook: <https://www.greenhoodwallet.com/how-to/apply-for-a-greenhood-iban>.

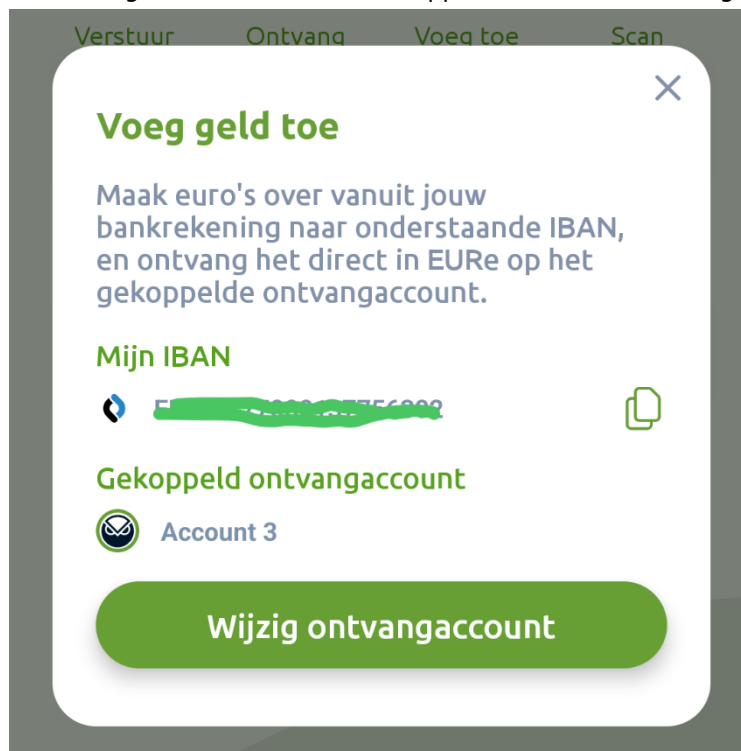
³ Zie Monerium's Business terms of service ([link](#)).

FINNIUS

2.18 Zodra een Gebruiker EUR overmaakt naar zijn IBAN zal Monerium dit bedrag omzetten naar EURE en versturen naar de gekoppelde SAFE Wallet. Dat gaat dus volledig buiten de Greenhood App om. De gebruiker zal immers vanuit zijn gebruikelijke bankierenapplicatie een fiat transactie versturen van zijn ene IBAN naar de IBAN zoals aangehouden via LHV via Monerium. Daarbij geldt dat het saldo op deze IBAN niet zichtbaar is in de Greenhood App (en daarbij is dit bedrag natuurlijk altijd 0).

2.19 Vervolgens kan een Gebruiker vanuit de SAFE Wallet transacties met EURE versturen. Dit werkt als volgt (deze informatie is overigens niet inzichtelijk voor Greenhood zelf):

- 1) De Gebruiker geeft in de Greenhood App aan voor welk bedrag en naar welke IBAN



de Gebruiker een transactie wil versturen.

- 2) De Gebruiker signeert deze transactie met zijn sleutel (zoals zijn pincode op zijn telefoon) in de Greenhood App en de transactie wordt gepubliceerd op de blockchain op een van de manieren zoals beschreven in paragraaf 2.11.
- 3) Het bedrag aan EURE wordt op de blockchain geburned (vernietigd), wordt afgeschreven van de SAFE Wallet van de Gebruiker en bijgeschreven bij de Gebruikers IBAN.
- 4) LHV (via Monerium) draagt het bedrag in EUR over naar de ontvangende partij via de IBAN zoals aangehouden bij LHV naar de ontvangende IBAN.

2.20 Een Gebruiker kan ook EURE ontvangen, die zichtbaar zijn in de Greenhood App (maar niet voor Greenhood zelf). Dit werkt als volgt:

- 1) De Gebruiker ontvangt een bedrag in EUR op zijn IBAN die via Monerium wordt aangehouden bij LHV.
- 2) Monerium krijgt een melding van LHV dat er een bedrag in EUR voor een Gebruiker is ontvangen.
- 3) Monerium mint hetzelfde bedrag in EURE op de blockchain waarna de EURE worden bijgeschreven op de SAFE Wallet en voegt het bedrag in EUR toe aan Monerium's reserves (waarvan een deel wordt geïnvesteerd in kortlopende staatsobligaties).
- 4) Het bedrag in EURE wordt zichtbaar in de Greenhood App.

2.21 Overigens is het geen vereiste om een IBAN via Monerium aan te houden om EURE te ontvangen. Het is namelijk ook mogelijk om EURE te ontvangen van een andere self-hosted wallet.

Samenwerking Gnosispay service

2.22 Greenhood werkt samen met Gnosispay zodat Gebruikers met een (virtuele) "**Gnosispay Debit Card**" betalingen kunnen verrichten. Deze kaart wordt uitgegeven door UAB Monavate.⁴ Zodra de Gebruiker de Gnosispay Debit Card heeft ontvangen en geactiveerd, kan de Gebruiker hier overal mee betalen. Deze kaart kan worden gekoppeld zodra de Gebruiker een account heeft aanmaakt bij Gnosispay.⁵

2.23 Een betaling met de Gnosispay Debit Card werkt als volgt:

- 1) De Gebruiker gebruikt de Gnosispay Debit Card om bij een pinterminal te betalen in EUR.
- 2) Er wordt via Visa een melding verstuurd naar Gnosispay dat de Gebruiker een transactie wil verrichten. Visa checkt of er voldoende saldo op de SAFE Wallet staat.
- 3) Gnosispay schrijft EURE af van de, zoals door Greenhood omschreven, gezamenlijke SAFE Wallet die de Gebruiker met Gnosispay heeft, nu de betreffende SAFE Wallet werkt als tegenrekening van de Gnosispay Debit Card.
- 4) Het bedrag aan EURE wordt op de blockchain geburned (vernietigd) en wordt afgeschreven van de SAFE Wallet van de Gebruiker.
- 5) Monerium zorgt ervoor dat er een bedrag in EUR wordt overgeschreven naar de begunstigde namens de Gebruiker.

iii) Het gebruik van dApps

2.24 Daarnaast heeft Greenhood een interne dApp browser zodat een Gebruiker zijn publieke sleutels kan verbinden met de decentrale applicatie van derden. Greenhood verwijst hiernaar als "**dApps**" (een *decentralized application*). Hiervoor maakt Greenhood gebruik van de diensten van Wallet Connect. Een dergelijke koppeling werkt als volgt:

- De Gebruiker initieert via de Greenhood App een verbinding met een externe dApp door middel van het scannen van een QR-code of link;
- WalletConnect faciliteert een beveiligde end-to-end encrypted sessie tussen de Greenhood App en de dApp;
- Na succesvolle koppeling kan de dApp transactievoorstellingen versturen naar de Greenhood App;
- De Gebruiker behoudt te allen tijde volledige controle: elke transactie vereist expliciete goedkeuring binnen de Greenhood App middels ondertekening van een transactie (bijvoorbeeld via de pincode van de Gebruiker) lokaal op het apparaat van de Gebruiker;

⁴ Dit is een EGI met een vergunning van de Bank of Lithuania.

⁵ Zie ook: <https://www.greenhoodwallet.com/how-to/apply-for-a-gnosis-pay-payment-card>.

- De ondertekende transactie wordt vervolgens via de Greenhood App naar het relevante blockchain-netwerk verstuurd.

2.25 Deze functionaliteit zal onder andere gebruikt worden om cryptoactiva te wisselen voor andere cryptoactiva. Hierdoor kan de Gebruiker zijn SAFE Wallet direct verbinden met een DEX en EURE of andere cryptoactiva ruilen voor andere cryptoactiva. Denk hierbij aan exchanges zoals Uniswap of Cowswap.

3. JURIDISCH KADER

3.1 Door het aanbieden van de Greenhood App loopt Greenhood mogelijk tegen verschillende juridische raamwerken aan, namelijk: i) het verlenen van betaaldiensten, ii) het verlenen van cryptoactivadiensten en iii) het bemiddelen in betaalrekeningen en/of elektronisch geld.

Het verlenen van betaaldiensten

3.2 Het is ieder met een zetel in Nederland verboden om zonder een vergunning van de Nederlandsche Bank (**DNB**) het bedrijf van betaaldienstverlener uit te oefenen.⁶ Betaaldiensten zijn gereguleerd op basis van PSD2 zoals geïmplementeerd in de Wft. Op basis van PSD2 worden er acht betaaldiensten gereguleerd.

EMTs als elektronisch geld onder PSD2

3.3 Het verlenen van betaaldiensten speelt voor Greenhood mogelijk een rol, omdat EMT ook binnen het PSD2 raamwerk vallen. Dat werkt als volgt. Een EMT wordt gezien als een type 'cryptoactivum' onder MiCAR.⁷ Daarmee vallen EMTs en diensten met EMTs binnen de reikwijdte van MiCAR. MiCAR bepaalt echter ook dat EMTs ook geacht worden elektronisch geld te zijn.⁸ PSD2 is van toepassing op diensten omtrent geldmiddelen. Onder geldmiddelen wordt onder meer elektronisch geld verstaan. Dit betekent dus dat EMTs een zogenaamde *dual natura* hebben en daarom zowel binnen het PSD2 als het MiCAR raamwerk vallen. Nu de Greenhood App betrekking heeft op EMTs (namelijk EURE), kan Greenhood mogelijk te maken krijgen met PSD2.

Relevante betaaldiensten

3.4 In het kader van de Greenhood App zijn de volgende betaaldiensten van belang:

- "Uitvoering van betalingstransacties, met inbegrip van geldovermakingen, op een betaalrekening bij de betalingsdienstaanbieder van de gebruiker of bij een andere betalingsdienstaanbieder" (**Betaaldienst 3**).
- "Betaalinitiatiedienst" (**Betaaldienst 7** of **PIS**) wat ziet op een dienst voor het initiëren van een betaalopdracht op verzoek van de betaaldienstgebruiker, met betrekking tot een betaalrekening die bij een andere betaaldienstverlener wordt aangehouden (betaaldienst 7).
- "Rekeninginformatiedienst" (**Betaaldienst 8** of **AIS**) wat ziet op een online dienst voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betaaldienstgebruiker bij een andere betaaldienstverlener of bij meer dan één betaaldienstverlener aanhoudt (betaaldienst 8).

Relevante definities

3.5 Daarbij zijn de volgende definities onder meer van belang:

⁶ Artikel 2:3a (1) Wft.

⁷ Artikel 3 (7) MiCAR.

⁸ Artikel 48 (2) MiCAR.

- Een betaalrekening wordt gedefinieerd als “een op naam van een of meer betaaldienstgebruikers aangehouden rekening die voor de uitvoering van betalingstransacties wordt gebruikt”.⁹
- Een betalingstransactie wordt gedefinieerd als “een door of voor rekening van de betaler of door de betalingsbegunstigde geïnitieerde handeling waarbij geldmiddelen worden gedeponneerd, overgemaakt of opgenomen, ongeacht of er onderliggende verplichtingen tussen de betaler en de betalingsbegunstigde zijn”.¹⁰
- Een betaaldienstgebruiker wordt gedefinieerd “als een natuurlijke persoon of rechtspersoon die in de hoedanigheid van betaler, begunstigde of beide van een betalingsdienst gebruik maakt”.¹¹
- Een rekeninghoudende betalingsdienstaanbieder (**ASPSP**) wordt gedefinieerd als “een betalingsdienstaanbieder die ten behoeve van een betaler een betaalrekening aanbiedt en beheert”.¹²

Betaaldienst 3 – uitvoering van betalingstransacties

- 3.6 Een van de gereuleerde betaaldiensten is de uitvoering van Betaaldienst 3. DNB geeft nauwelijks toelichting over de precieze reikwijdte van Betaaldienst 3 en geeft hiervan geen concrete voorbeelden. Op haar website beperkt DNB zich tot de volgende omschrijving van Betaaldienst 3: “Deze dienst betreft het verrichten van betalingstransacties op betaalrekeningen van de betaaldienstgebruikers, bedoeld in de omschrijving van de diensten 1 en 2, of op betaalrekening van betaaldienstgebruikers bij een andere betaaldienstverlener.”
- 3.7 Onder de oude richtlijn betaaldiensten¹³ (**PSD**), de voorganger van PSD2, werd Betaaldienst 3 door DNB ruim uitgelegd. DNB heeft lange tijd op haar website aangegeven dat als een onderneming een dienst verleent die meebrengt dat zij in opdracht van een ander geld overmaakt tussen betaalrekeningen, hiermee sprake is van Betaaldienst 3. Hoe die opdracht er precies uitziet en in welke vorm die wordt gegeven is daarbij dan niet van belang. Onder deze oude uitleg leek het ook irrelevant of de onderneming feitelijk de onderliggende betalingstransactie zelf uitvoerde. Het leek al voldoende om als Betaaldienst 3 te kwalificeren op het moment dat de onderneming haar bank de instructie gaf de betaling vanaf haar rekening uit te voeren, ondanks dat de daadwerkelijke uitvoering van de betalingstransactie werd uitgevoerd door de bank van deze onderneming.
- 3.8 Door het ontbreken van verdere uitleg van DNB op dit moment, is het niet helemaal duidelijk of Betaaldienst 3 nog steeds ruim moet worden uitgelegd. Op basis van onze praktijkervaring kunnen wij wel concluderen dat er geen redenen zijn om aan te nemen dat Betaaldienst 3 door DNB minder ruim wordt uitgelegd dan onder het PSD-regime.
- 3.9 Daarbij geldt wel dat diverse diensten met betrekking tot betalingsverkeer niet worden gezien als betaaldiensten en vereisen daarom geen vergunning als betaalinstelling. Dit ziet onder meer op diensten die worden verleend door ‘technische dienstverleners’, ter ondersteuning van het aanbieden van betaaldiensten, zonder dat deze technische dienstverlener op enig moment in het bezit komt van de over te maken geldmiddelen.¹⁴ Deze technische dienstverleners kunnen onder meer betrokken zijn bij het verwerken en opslaan van gegevens, diensten ter bescherming van het vertrouwen en het privéleven, authenticatie van gegevens en entiteiten, het aanbieden van informatie- en communicatietechnologie en van communicatienetwerken, en het aanbieden en onderhouden van voor betaaldiensten gebruikte automaten en instrumenten (met

⁹ Artikel 4 (12) PSD2.

¹⁰ Artikel 4 (5) PSD2.

¹¹ Artikel 4 (10) PSD2.

¹² Artikel 4 (17) PSD2.

¹³ Richtlijn 2007/64/EG.

¹⁴ Artikel 1:5a lid 2 sub j Wft.

uitzondering van betaalinitiatiediensten en rekeninginformatiediensten). En dergelijke technische dienstverlening verleent dus ook geen Betaaldienst 3.

Betaaldiensten 7 en 8 – AIS en PIS

- 3.10 Er kan pas sprake zijn van een AIS of PIS indien er een betaalrekening bij de dienst wordt betrokken. Daarbij is het recht om gebruik te maken van een AISP en/of PISP onder PSD2 uitsluitend een recht van de betaaldienstgebruiker op basis van *open banking*.¹⁵ Een ASPSP kan het verzoek van de betaaldienstgebruiker niet weigeren als dit betrekking heeft op AIS of PIS. Als de betaaldienstgebruiker een ASPSP echter verzoekt om rekeninginformatie te delen met een derde partij of een derde partij mandateert om betalingen te verrichten zonder de betrokkenheid van een AISP of PISP, is PSD2 niet van toepassing en kan de ASPSP een dergelijk verzoek weigeren.¹⁶ De ASPSP heeft in dat geval de controle over de relatie en kan bijvoorbeeld eisen stellen aan de manier waarop toegang wordt verkregen

Het verlenen van cryptoactivadiensten

- 3.11 Op basis van MiCAR worden partijen die cryptoactiva uitgeven en partijen die cryptoactivadiensten verlenen gereguleerd binnen de EU. Voor dit advies gaan we enkel in op de regulering van cryptoactivadiensten.
- 3.12 Op grond van MiCAR is het verboden om als persoon binnen de EU cryptoactivadiensten aan te bieden zonder daarvoor over de juiste vergunning te beschikken.¹⁷ Een rechtspersoon of andere onderneming waarvan de activiteit of het bedrijf bestaat in het beroepsmatig aanbieden van één of meer cryptoactivadiensten aan cliënten en die dit ook is toegestaan, wordt aangeduid als "**CASP**".¹⁸ Een CASP kan vervolgens een EER-paspoort aanvragen om ook in andere EER-landen cryptoactivadiensten te kunnen verlenen.¹⁹
- 3.13 MiCAR introduceert tien gereguleerde cryptoactivadiensten. Deze cryptoactivadiensten zijn van toepassing op cryptoactiva, waaronder EMTs. De opzet van deze diensten is sterk geïnspireerd op het MiFID II-kader.
- 3.14 Voor Greenhood zijn de volgende cryptoactivadiensten relevant:
- Het bewaren en beheren van cryptoactiva namens cliënten (cryptoactivadienst (a)).
 - Het uitvoeren van ccryptoactivaorders namens cliënten (cryptoactivadienst (e)).
 - Het verlenen van advies over cryptoactiva (cryptoactivadienst (h)).
 - Het ontvangen en doorgeven van cryptoactivaorders namens cliënten (cryptoactivadienst (g)).
 - Het verlenen van cryptoactivaoverdrachtdiensten namens cliënten (cryptoactivadienst (j)).
- 3.15 Elke cryptoactivadienst wordt afzonderlijk gedefinieerd in MiCAR. De voor dit memorandum relevante cryptoactivadiensten worden hieronder kort toegelicht. Daarbij moet worden opgemerkt dat er onder MiCAR nog weinig aanvullende richtsnoeren bestaan over de interpretatie van deze diensten. Aangezien deze cryptoactivadiensten zijn geïnspireerd op het MiFID II-kader kan aansluiting worden gezocht bij de uitleg van beleggingsdiensten onder MiFID II, waarbij uiteraard rekening wordt gehouden met de specifieke kenmerken van de betrokken cryptoactiva en cryptodienstverleners.

¹⁵ Artikel 66 (1) en 67 (1) PSD2.

¹⁶ Zie onder meer DNB 'Q&A Boekhoudkoppelingen' ([link](#)).

¹⁷ Artikel 59 (1) MiCAR.

¹⁸ Artikel 3 (15) MiCAR.

¹⁹ Artikel 65 MiCAR.

(a) - Het bewaren en beheren van cryptoactiva namens cliënten

- 3.16 Het bewaren en beheren van cryptoactiva namens cliënten ziet op het bewaren of beheren van cryptoactiva of van de toegangsmiddelen tot dergelijke cryptoactiva, in voorkomend geval in de vorm van geheime cryptografische sleutels.²⁰ Daarbij wordt in de overwegingen van MiCAR aangegeven dat hardware- of softwareaanbieders van non-custodial portemonnees niet binnen het toepassingsgebied van MiCAR vallen.²¹

(g) - Het ontvangen en doorgeven van cryptoactivaorders namens cliënten

- 3.17 Deze dienst ziet op het namens een persoon ontvangen van een order om één of meer cryptoactiva te kopen of te verkopen dan wel in te schrijven op één of meer cryptoactiva en het doorgeven van dat order aan een derde partij voor uitvoering.²²
- 3.18 Deze cryptoactivadiens is duidelijk geïnspireerd op MiFID II en wordt gelijkwaardig geacht aan de beleggingsdienst 'het ontvangen en doorgeven van orders met betrekking tot een of meer financiële instrumenten'.²³ Onder MiFID II omvat deze dienst eveneens ook het met elkaar in contact brengen van twee of meer beleggers waardoor tussen deze beleggers een transactie tot stand kan komen.²⁴ Hoewel deze overweging in MiCAR ontbreekt, is het wat ons betreft het meest veilig om deze toevoeging ook voor MiCAR in acht te nemen.

(h) - Het verlenen van advies over cryptoactiva

- 3.19 Het verlenen van advies over cryptoactiva ziet op het op verzoek van de cliënt of op initiatief van de CASP, geven van gepersonaliseerde aanbevelingen aan een cliënt over cryptoactivatransacties of het gebruik van cryptoactivadiens.²⁵ Deze dienst komt overeen met de beleggingsdienst beleggingsadvies onder MiFID II.²⁶
- 3.20 Wat er precies wordt verstaan onder gepersonaliseerde aanbevelingen wordt niet gedefinieerd in MiCAR. Voor de definitie kan echter worden gekeken naar MiFID II. Van een gepersonaliseerde aanbeveling is sprake indien het gaat om een aanbeveling die geschikt is voor de betrokken persoon, of berust op een afweging van diens persoonlijke omstandigheden. Een aanbeveling wordt niet als een gepersonaliseerde aanbeveling beschouwd als deze uitsluitend aan het publiek wordt gedaan.²⁷

(j) - Het verlenen van cryptoactivaoverdrachtdiensten

- 3.21 MiCAR definieert het verlenen van cryptoactivaoverdrachtdiensten als het verlenen, namens een natuurlijke of rechtspersoon, van diensten van overdracht van cryptoactiva van één distributed-ledgeradres of -rekening naar een andere.²⁸ Daarbij sluit MiCAR de volgende partijen expliciet uit van de definitie van cryptoactivaoverdrachtdiensten:

*"Een dergelijke overdrachtdienst mag geen validators, knooppunten of miners omvatten die een rol spelen bij de bevestiging van een transactie en het bijwerken van de toestand van de onderliggende distributed ledger."*²⁹

²⁰ Artikel 3 (17) MiCAR.

²¹ Overweging 83 MiCAR.

²² Artikel 3 (23) MiCAR.

²³ Artikel 60 (3) (f) MiCAR.

²⁴ Overweging 44 MiFID II.

²⁵ Artikel 3 (24) MiCAR.

²⁶ Artikel 60 (3) (g) MiCAR.

²⁷ Artikel 9 Gedelegeerde Verordening (EU) 2017/565.

²⁸ Artikel 3 (26) MiCAR.

²⁹ Overweging 93 MiCAR.

- 3.22 Wel wordt er in MiCAR aangegeven dat veel CASPs waarschijnlijk cryptoactivadiensten verlenen als onderdeel van een andere cryptoactivadienst.³⁰
- 3.23 Hoewel de definitie van deze cryptoactivadienst niet geheel duidelijk is, volgt uit de doorlopende vereisten die van toepassing zijn op cryptoactivaoverdrachtdiensten dat een cliënt altijd een instructie geeft aan een CASP om cryptoactiva over te dragen naar een ander.³¹ Daarnaast moet de CASP bijvoorbeeld een uitvoeringstermijn vaststellen en kunnen bepaalde instructies worden geweigerd. Dit veronderstelt dat de CASP zich in de cryptoactivastroom bevindt.
- 3.24 Aanverwante regelgeving die ziet op de zogenaamde *travel rule* geeft ook aan in welke gevallen er sprake is van een overdracht van cryptoactiva, op basis waarvan vereist is dat er een CASP betrokken is bij een overdracht van cryptoactiva voordat de travel rule zoals volgt uit Verordening (EU) 2023/1113 (**TFR**) van toepassing is:

"een transactie met als doel cryptoactiva van één distributed-ledger-adres, cryptoactivarekening of ander hulpmiddel voor de opslag van cryptoactiva naar een ander te verplaatsen, uitgevoerd door ten minste één aanbieder van cryptoactivadiensten die optreedt namens een initiator of een begunstigde (...)"

- 3.25 TFR is dan ook niet van toepassing op cryptoactivaoverdrachten tussen personen waarbij geen aanbieder van cryptoactivadiensten betrokken is.³² Hoewel de definitie van een overdracht van cryptoactiva in TFR meer overdrachten omvat dan de transferdiensten in MiCAR, veronderstelt TFR wel dat er altijd een derde (i.e. de CASP) betrokken is bij een overdracht van cryptoactiva. Hieruit kan worden afgeleid dat dat onder MiCAR ook het geval zou moeten zijn.

Bemiddelen in betaalrekening en/of elektronisch geld

- 3.26 Het is verboden om zonder vergunning van de Autoriteit Financiële Markten (**AFM**) in Nederland te bemiddelen. Bemiddelen heeft betrekking op alle werkzaamheden in de uitoefening van een beroep of bedrijf gericht op het als tussenpersoon tot stand brengen van een overeenkomst inzake een financieel product³³, waaronder elektronisch geld en een betaalrekening, tussen een consument en een aanbieder.³⁴ Let er ook op dat onderbemiddelaars, bemiddelaars die bemiddelen voor een andere bemiddelaar, onder de Wft vallen.³⁵
- 3.27 Met betrekking tot de term 'bemiddelen' zijn de definities van 'consument' en 'aanbieder' van belang. Een consument is een niet in de uitoefening van zijn bedrijf of beroep handelende natuurlijk persoon aan wie een financiële instelling een financiële dienst verleent.³⁶ Voorts is een 'aanbieder' gedefinieerd als een entiteit die diensten aanbiedt en derhalve in de uitoefening van een beroep of bedrijf direct of indirect een voldoende bepaald voorstel doet om een overeenkomst aan te gaan met een consument als wederpartij met betrekking tot een financieel product, waaronder elektronisch geld, of een dergelijke overeenkomst in de uitoefening van een beroep of bedrijf aangaat, beheert of uitvoert.³⁷

³⁰ Idem.

³¹ Richtsnoeren betreffende de procedures en beleidslijnen inzake beleggersbescherming, met inbegrip van de rechten van cliënten, in het kader van cryptoactivaoverdrachtdiensten overeenkomstig de verordening betreffende cryptoactivamarkten (MiCA) (ESMA35-1872330276-2032).

³² Artikel 2 (4) (b) TFR.

³³ Artikel 1:1 met betrekking tot "financiële producten".

³⁴ Artikel 1:1 Wft met betrekking tot "bemiddelen" onder (a).

³⁵ Artikel 1:1 Wft met betrekking tot "onderbemiddelaar".

³⁶ Artikel 1:1 Wft met betrekking tot "consument".

³⁷ Artikel 1:1 Wft met betrekking tot "aanbieden" onder (a).

3.28 'Bemiddelen' wordt in het Nederlandse toezichtrecht zeer ruim uitgelegd en daarom kwalificeren veel diensten en activiteiten als zodanig, hetgeen ook heeft geleid tot de ontwikkeling van richtsnoeren van de AFM en jurisprudentie. Om als bemiddeling te kwalificeren, is 'inhoudelijke betrokkenheid' bij het tot stand brengen van een overeenkomst tussen de consument en aanbieder vereist.³⁸ De interpretatie van wat 'inhoudelijke betrokkenheid' vormt is echter contra-intuïtief. Volgens de AFM is aan de eis van inhoudelijke betrokkenheid reeds voldaan indien een persoon:

- (i) meer informatie van de consument verkrijgt dan alleen contactgegevens (naam, adres, woonplaats, telefoonnummer en e-mailadres (**NAWTE-gegevens**)), die hij doorgeeft aan de aanbieder of een andere tussenpersoon (**Toets 1**). Denk daarbij bijvoorbeeld aan de hoeveelheid elektronisch geld dat een consument wil aankopen of een IBAN als zijnde 'meer dan NAWTE-gegevens'; of
- (ii) de voornoemde informatie van de consument verkrijgt en deze niet zelf doorgeeft aan de aanbieder of een andere tussenpersoon, maar in plaats van het doorgeven van deze gegevens de consument op basis van de verkregen informatie doorverwijst naar de aanbieder/andere tussenpersoon met wie een overeenkomst bestaat die erop gericht is consumenten in contact te brengen met die aanbieder/tussenpersoon. Een dergelijke overeenkomst hoeft niet schriftelijk te zijn. Ook betalingsstromen tussen twee partijen kunnen duidelijk maken dat er een feitelijke overeenkomst bestaat voor deze vorm van 'lead generation' (**Toets 2**).

4. ANALYSE

4.1 In deze paragraaf analyseren wij of er Greenhood mogelijk één van de volgende gereguleerde diensten verleent: het verlenen van betaaldiensten, ii) het verlenen van cryptoactivadiensten en iii) het bemiddelen in betaalrekeningen en/of elektronisch geld.

4.2 In dit hoofdstuk wordt de Greenhood App in het licht van deze raamwerken geanalyseerd. Daarbij merken wij op dat dit geen eenvoudige analyse is. Het business model van Greenhood is complex en schuurt dicht tegen deze diverse raamwerken aan. Daarbij zijn de details uiteindelijk bepalend of er wel of niet sprake is van een gereguleerde dienst. Voor deze analyse zijn we uitgegaan van de feiten zoals ons door Greenhood gepresenteerd. Indien Greenhood wijzigingen aanbrengt in het feitencomplex of haar diensten uitbreidt, kunnen de analyses in dit hoofdstuk daardoor worden beïnvloed.

Het verlenen van betaaldiensten

4.3 Zoals aangegeven in paragraaf 3.3 kan Greenhood mogelijk te maken krijgen met PSD2. Dit is het geval omdat de Greenhood App Gebruikers in staat stelt om EURE op te slaan in de SAFE Wallet en transacties te verrichten met EURE vanuit de SAFE Wallet. Dit zijn EMTs die, nu deze naast als cryptoactivum ook kwalificeren als elektronisch geld, ook als geldmiddelen onder PSD2 kwalificeren. Dit maakt dat op diensten met EMTs zowel MiCAR als PSD2 van toepassing is. In dat kader wordt in dit hoofdstuk geanalyseerd of Greenhood mogelijk betaaldiensten en meer specifiek Betaaldienst 3 en/of Betaaldiensten 7 en 8 verleent.

Betaaldienst 3 – uitvoeren van betalingstransacties

4.4 Vanuit de Greenhood App is het mogelijk om transacties in EMTs te verrichten. Indien Greenhood betrokken is in deze betaalstroom, verleent Greenhood mogelijk Betaaldienst 3. Dit veronderstelt dat Greenhood zich als derde opwerpt in de betaalstroom tussen de betaler en begunstigde.

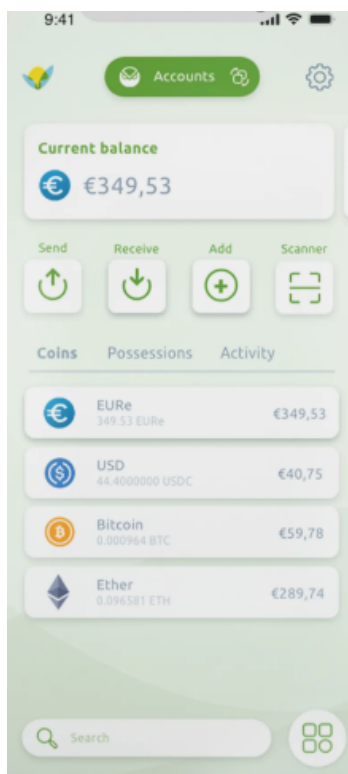
³⁸ Zie bijvoorbeeld *Kamerstukken II* 2003/04, 29 507, nr. 9, blz. 60, maar ook AFM, 'Publicatie bemiddelen', september 2014, blz. 1.

- 4.5 Dit is echter niet het geval. Greenhood is naar onze mening immers niet betrokken in de betaalstroom en verleent daarom geen betaaldienst. Een transactie wordt namelijk volledig uitgevoerd door de Gebruiker zelf. Een Gebruiker initieert een transactie in de Greenhood App en ondertekent deze transactie door middel van de door de Gebruiker gekozen authenticatiemethode. Daarna moet de Gebruiker een transactie zelf publiceren op de blockchain (zoals beschreven in paragraaf 2.11) en daar is Greenhood dus niet actief bij betrokken. De Greenhood App fungeert hierbij slechts als een interface, maar Greenhood heeft zelf nooit beschikking over de EMTs van de Gebruiker en kan dus ook niet namens een Gebruiker transacties initiëren of uitvoeren of EMTs overdragen.
- 4.6 Deze conclusie wordt ondersteund door het feit dat diensten van technische dienstverleners die andere betaaldienstverleners ondersteunen ook niet kwalificeren als betaaldiensten, nu het essentieel is voor betaaldienstverlening (behalve voor Betaaldiensten 7 en 8) dat een dienstverlening op enig moment in bezig komt van de over te maken geldmiddelen.
- 4.7 Greenhood verleent Betaaldienst 3 dus niet.

FINNIUS

Betaaldiensten 7 en 8 – AIS en PIS

- 4.8 Wij begrijpen dat een Gebruiker via de Greenhood App inzicht verkrijgt in het saldo dat wordt aangehouden op de SAFE Wallet. Dit ziet onder meer op de waarde aan EURE zoals uitgegeven door Monerium. Het saldo op de IBAN zoals aangehouden via Monerium is niet zichtbaar in de Greenhood App (dit saldo zal overigens in principe altijd 0 zijn). Welke informatie zichtbaar is in de Greenhood App kan het beste worden geïllustreerd aan de hand van de volgende afbeelding:



- 4.9 Daarnaast is het middels de Greenhood App mogelijk om transacties vanuit een SAFE Wallet te verrichten.
- 4.10 De diensten die Greenhood in dit kader verricht hebben kenmerken van AIS en PIS. Zoals uitgelegd in paragraaf 3.10 is hiervoor echter vereist dat deze diensten betrekking hebben op betaalrekeningen en moeten deze diensten worden verricht in het kader van open banking. Nu hier allebei geen sprake van lijkt te zijn, verleent Greenhood naar onze mening geen Betaaldienst 7 of 8. Dit lichten wij hieronder verder toe.
- 4.11 De diensten van Greenhood hebben enkel betrekking op de SAFE Wallet (smart contract accounts), die dezelfde werking hebben als self-hosted wallets. Er hoeft namelijk geen custodian aan te pas te komen die de cryptoactiva namens een cliënt bewaart en beheert. Nu er op de SAFE Wallets EMTs kunnen worden aangehouden, zou de SAFE Wallet kunnen kwalificeren als betaalrekening.
- 4.12 Wij achten dit echter onwaarschijnlijk. Een SAFE Wallet is naar ons oordeel immers vergelijkbaar met een fysieke portemonnee waarin contant geld wordt bewaard. Op betaaltransacties in contanten is PSD2 namelijk niet van toepassing en (fysieke) portemonnees worden niet als betaalrekening worden gezien. Dat is het geval omdat hier

geen tussenpersoon aan te pas komt.³⁹ In de laatste concept versie van de Payment Services Regulation (**PSR**), onderdeel van het nieuwe PSD raamwerk, wordt gezien deze werking van self-hosted adressen eenzelfde uitzondering voorgesteld voor selfhosted adressen.⁴⁰ Hoewel dit hier niet met zoveel woorden wordt gezegd, leiden wij hieruit ook af dat een self-hosted adres niet zou moeten kwalificeren als betaalrekening, mits de wallet zuiver 'self-hosted' is en er dus geen tussenpersoon bij betrokken is.

4.13 Deze lezing wordt ondersteund door het feit dat een self-hosted wallet niet gebruikt kan worden om betaaltransacties uit te voeren (i.e. Betaaldienst 3). Vanuit een self-hosted wallet kan een houder uiteraard wel transacties verrichten, maar er komt geen derde partij aan te pas die op een zeker moment in de geldstroom in het bezit komt van de EMTs (buiten uiteraard de betaler en de begunstigde) om deze EMTs vervolgens van de betaler over te dragen naar de begunstigde. Om te kunnen spreken van het uitvoeren van betaaltransacties moet er echter een derde partij betrokken zijn die deze dienst namens betaler of begunstigde uitoefent. Daar is bij een self-hosted wallet geen sprake van. Dit betekent dat een self-hosted adres, en daarmee ook de SAFE Wallets, naar ons oordeel niet zouden moeten kwalificeren als betaalrekening.

4.14 Omdat enkel inzicht wordt verkregen in de SAFE Wallet en transacties worden verricht vanuit de SAFE Wallet (en dus niet vanuit de gekoppelde IBAN), volgt dat de functionaliteiten van de Greenhood App buiten de scope van AIS en PIS vallen. Daarom komen we niet toe aan de vraag of Greenhood mogelijk Betaaldiensten 7 en 8 verleent, nu de diensten van Greenhood geen betrekking hebben op betaalrekeningen. Zelfs als het wel zou kwalificeren als betaalrekening, geldt dat Greenhood heeft daarnaast zelf geen toegang tot de betaalrekening van de Gebruiker zoals aangehouden via Monerium. Greenhood verleent dus geen Betaaldienst 7 of 8.

Tussenconclusie

4.15 Concreet betekent dit dat Greenhood geen betaaldiensten verleent middels de Greenhood App en dus niet over een vergunning als betaalinstelling hoeft te beschikken.

Het verlenen van cryptoactivadiensten

4.16 Daarnaast hebben wij geanalyseerd of Greenhood met de Greenhood App mogelijk cryptoactivadiensten verleent.

(a) - Het bewaren en beheren van cryptoactiva namens cliënten

4.17 Cryptoactiva worden enkel namens cliënten bewaard en beheerd indien de betreffende instelling beschikking over de cryptoactiva heeft, bijvoorbeeld omdat de instelling toegang heeft tot de "geheime cryptografische sleutels". Een CASP die deze cryptoactivadienst verleent, moet dus in staat zijn om de cryptoactiva aan te houden, op te slaan of over te dragen. Deze uitleg is ook in lijn met de doorlopende verplichtingen waar een CASP die cryptoactiva bewaart en beheert aan moet voldoen:

"Aanbieders van cryptoactivadiensten die namens cliënten bewarings- en beheerdiensten voor cryptoactiva aanbieden, moeten met hun cliënten een overeenkomst met bepaalde bindende bepalingen sluiten en moeten een bewaringsbeleid vaststellen en ten uitvoer leggen dat op verzoek aan cliënten in een elektronisch formaat beschikbaar moet worden gesteld. In een dergelijke

³⁹ Artikel 3 (a) PSD2.

⁴⁰ Zie overweging 29b van <https://data.consilium.europa.eu/doc/document/ST-10268-2025-INIT/en/pdf>.

*overeenkomst moet onder meer de aard van de verleende dienst worden gespecificeerd, waaronder het aanhouden van cryptoactiva die aan cliënten toebehoren of de middelen om toegang te krijgen tot dergelijke cryptoactiva, in welk geval de cliënt de controle over de cryptoactiva kan houden. Als alternatief kunnen de cryptoactiva of de toegangsmiddelen onder de volledige controle van de aanbieder van cryptoactivadiensten komen.*⁴¹

- 4.18 Greenhood is naar wij begrijpen niet in staat om cryptoactiva van Gebruikers aan te houden, op te slaan of over te dragen namens een Gebruiker. Daarnaast kan Greenhood ook niets voor de Gebruiker betekenen in het kader van recovery van de SAFE Wallet. Greenhood bewaart of beheert dus geen cryptoactiva of de toegangsmiddelen daartoe namens cliënten. In dat kader kwalificeert de SAFE Wallet als een non-custodial wallet. Dit type wallets zijn in de overwegingen van MiCAR uitgezonderd van de scope. Greenhood verleent cryptoactivadienst (a) naar onze mening dus niet.

(g) - Het ontvangen en doorgeven van cryptoactivaorders namens cliënten

- 4.19 Daarnaast hebben wij geanalyseerd of Greenhood mogelijk betrokken is bij het ontvangen en doorgeven van cryptoactivaorders namens cliënten. Deze dienst veronderstelt dat een aanbieder (i) orders ontvangt van cliënten, en (ii) deze orders doorgeeft aan een derde partij (zoals een handelsplatform of exchange) voor uitvoering. De aanbieder fungeert hierbij als tussenpersoon die de order van de cliënt naar de uitvoerende partij leidt.
- 4.20 Naar onze mening verleent Greenhood deze dienst niet. De Greenhood App functioneert als een technische interface waarmee de Gebruiker zelfstandig zijn SAFE Wallet bedient. De Gebruiker geeft geen opdracht aan Greenhood om namens hem een transactie uit te voeren of door te geven aan een derde. In plaats daarvan gebruikt de Gebruiker de Greenhood App als instrument om zelf, rechtstreeks op de blockchain en zonder tussenkomst van Greenhood, transacties uit te voeren. Greenhood fungeert hierbij niet als tussenpersoon maar als softwareleverancier van een technische interface. Greenhood is niet bekend met de (omvang van) de transacties.
- 4.21 Voor zover de Gebruiker via de Greenhood Wallet gebruik maakt van gedecentraliseerde exchanges (DEX) of andere dApps, geldt dat de Gebruiker rechtstreeks interacteert met deze protocollen via zijn SAFE Wallet. Greenhood ontvangt en geeft in dat geval geen orders door; de Gebruiker verbindt zijn wallet direct met de DEX en autoriseert transacties zelf. Greenhood is niet bekend met de (omvang van) de transacties.
- 4.22 Concluderend is Greenhood naar onze mening niet betrokken bij het ontvangen en doorgeven van cryptoactivaorders namens cliënten onder MiCAR.

(h) - Het verlenen van advies over cryptoactiva

Daarnaast geven wij Greenhood voor de volledigheid mee dat zij geen advies mag geven over cryptoactivatransacties of cryptoactivadiensten zonder vergunning. Voor zover Greenhood namelijk gepersonaliseerde aanbevelingen zou doen aan een cliënt over cryptoactivatransacties of het gebruik van cryptoactivadiensten, verleent Greenhood cryptoactivadienst (h) waarvoor een CASP vergunning vereist is. Op basis van de verstrekte informatie lijkt daar geen sprake van te zijn, nu enkel het verwijzen naar bijvoorbeeld een bepaalde CASP (zoals een handelsplatform) niet kwalificeert als advies over cryptoactivatransacties of cryptoactivadiensten.

- 4.23 Wel geven wij Greenhood mee dat zij ervoor moet waken dat dit in de toekomst ook niet gebeurt. Denk bijvoorbeeld aan de situatie waarbij Greenhood voor een specifieke Gebruiker

⁴¹ Overweging 83 MiCAR.

een bepaalde afweging meegeeft om te kiezen tussen verschillende dienstverleners en kenmerken van de aangeboden diensten, gelet op de persoonlijke omstandigheden van de gebruiker.

(j) - het verlenen van cryptoactivaoverdrachtdiensten namens cliënten

4.24 Daarnaast hebben wij geanalyseerd of Greenhood mogelijk betrokken is bij het verlenen van cryptoactivaoverdrachtdiensten. Dat is naar onze mening ook niet het geval. Om te kunnen spreken van een overdrachtdienst moet Greenhood namens een cliënt cryptoactiva overdragen van één distributed-ledgeradres of -rekening naar een andere. Hier is in het geval van de Greenhood App geen sprake van. De Gebruiker initieert en signeert transacties vanuit de Greenhood App immers zelf zonder dat Greenhood in de cryptoactivastroom betrokken is. Daarna moet de Gebruiker een transactie zelf publiceren op de blockchain (zoals beschreven in paragraaf 2.11) en daar is Greenhood dus niet actief bij betrokken. Een cryptoactivatransactie wordt daarmee rechtstreeks van de SAFE Wallet van de Gebruiker naar de ontvanger uitgevoerd zonder dat Greenhood op enig moment controle krijgt over de cryptoactiva. Daarom verleent Greenhood wat ons betreft geen cryptoactivadienst (j).

4.25 Als ondersteunend argument geldt dat de SAFE Wallet kwalificeert als een non-custodial wallet, welke type wallet is uitgezonderd van de scope van MiCAR. Het ligt daarom voor de hand dat transacties die worden verricht vanuit een non-custodial wallet ook niet worden gezien als een 'dienst' onder MiCAR nu een non-custodial wallet veronderstelt dat er geen derde te pas komt bij dergelijke activiteiten.

Tussenconclusie

4.26 Concreet betekent dit dat Greenhood naar onze mening geen cryptoactivadiensten verleent middels de Greenhood App en dus niet over een vergunning als CASP hoeft te beschikken.

Bemiddelen in een betaalrekening en/of elektronisch geld

4.27 Tot slot hebben wij beoordeeld of Greenhood mogelijk bemiddelt in betaalrekeningen en/of elektronisch geld.

Bemiddelen in een betaalrekening

4.28 Monerium biedt betaalrekeningen aan aan de Gebruikers. Afhankelijk van de rol van Greenhood kan Greenhood hierbij betrokken zijn als bemiddelaar door het als tussenpersoon tot stand brengen van de overeenkomst tussen Monerium en de Gebruiker. Om te kijken of daar sprake van is, moet gekeken worden naar het moment van totstandkoming van de overeenkomst tussen de Gebruiker en Monerium:

- (i) **Toets 1:** Om gebruik te kunnen maken van de Greenhood App moet de Greenhood App worden gekoppeld aan een IBAN van de Gebruiker via Monerium. Daarvoor wordt de Gebruiker direct doorverwezen naar Monerium (via een browser van Monerium in de Greenhood App). Omdat de Gebruiker NAWTE-gegevens verstrekt aan Monerium via de browser van Monerium, zonder tussenkomst van Greenhood, verkrijgt Greenhood dus geen gegevens – en dus ook geen NAWTE-gegevens of aanvullende gegevens – die worden doorgegeven aan Monerium. Aan Toets 1 is dus niet voldaan.
- (ii) **Toets 2:** Greenhood verkrijgt geen contactgegevens of aanvullende gegevens van de Gebruiker voordat de Gebruiker een overeenkomst sluit met Monerium, waardoor betoogd kan worden dat Greenhood geen inhoudelijke betrokkenheid heeft bij de totstandkoming van de overeenkomst in het kader van de betaalrekening. Het

openen van een IBAN via Monerium verloopt immers volledig via de server van Monerium. Aan Toets 2 is dus ook niet voldaan. Daarbij merken wij voor de volledigheid op dat Greenhood ook niet nadat Gebruiker en Monerium een overeenkomst hebben gesloten gegevens van de Gebruiker verkrijgt.

- 4.29 Nu er niet wordt voldaan aan Toets 1 of 2 is er naar ons oordeel geen sprake van het bemiddelen in betaalrekeningen door Greenhood. We merken daarbij op dat de AFM veel aandacht heeft voor 'embedded' dienstverlening en snel de conclusie trekt dat sprake is van bemiddeling. Het is daarbij niet geheel duidelijk welke definitie de AFM hanteert voor 'embedded' dienstverlening. De kans bestaat dat met verdere guidance van de AFM, de wijze waarop de dienst door Greenhood is ingericht, op enig moment toch als bemiddeling moet worden gezien.

Bemiddelen in elektronisch geld

- 4.30 EMTs kwalificeren ook als elektronisch geld. Dit is onder meer beschreven in paragraaf 4.4. Dit maakt dat het verbod op het bemiddelen in elektronisch geld mogelijk van toepassing is op Greenhood.
- 4.31 Gebruikers kopen elektronisch geld aan via Monerium, namelijk EURE. Daarnaast kunnen Gebruikers EMTs aankopen via gedecentraliseerde exchanges (DEX) of andere dApps. Afhankelijk van de rol van Greenhood kan Greenhood hierbij betrokken zijn als bemiddelaar door als tussenpersoon een overeenkomst tot stand te brengen in het kader van elektronisch geld. Om te kijken of daar sprake van is, moet gekeken worden naar het moment van totstandkoming van de overeenkomst van de aankoop van het elektronisch geld.
- 4.32 Wat betreft de aankoop van EURE door een Gebruiker bij Monerium geldt het volgende:
- **Toets 1:** De Gebruiker koopt geen EURE via de Greenhood App. Om EURE aan te kopen maakt de Gebruiker fiat gelden over naar zijn IBAN bij LHV. Vervolgens zal Monerium dit bedrag in EUR omzetten van EURE. Dat gaat dus volledig buiten de Greenhood App om. Greenhood geeft dus geen informatie (en zeker niet meer dan NAWTE-gegevens) door aan Monerium in het kader van de aankoop van EURE door de Gebruiker. Aan Toets 1 is dus niet voldaan.
 - **Toets 2:** Greenhood verkrijgt geen contactgegevens of aanvullende gegevens van de Gebruiker voordat de Gebruiker een overeenkomst sluit met Monerium, waardoor betoogd kan worden dat Greenhood geen inhoudelijke betrokkenheid heeft bij de totstandkoming van de overeenkomst in het kader van de EURE. De aankoop van EURE via Monerium verloopt immers volledig via Monerium. Aan Toets 2 is dus ook niet voldaan. Daarbij merken wij voor de volledigheid op dat Greenhood ook niet nadat Gebruiker en Monerium een overeenkomst hebben gesloten gegevens van de Gebruiker verkrijgt.
- 4.33 Nu naar ons oordeel er niet wordt voldaan aan Toets 1 of 2 is er geen sprake van het bemiddelen in EURE via Monerium door Greenhood.
- 4.34 Daarnaast kan een Gebruiker ook elektronisch geld aankopen via gedecentraliseerde exchanges (DEX) of andere dApps. In dat geval acteert de Gebruiker rechtstreeks met deze protocollen via de SAFE Wallet. Ook in dat geval kan goed betoogd worden dat Greenhood niet bemiddelt in elektronisch geld. Greenhood ontvangt immers geen NAWTE-gegevens die hij doorgeeft aan de DEX/dApp. Daarnaast heeft Greenhood zelf ook geen overeenkomst met de DEX/dApp. Er is dus geen inhoudelijke betrokkenheid van Greenhood bij de aankoop van elektronisch geld door Gebruikers via DEX/dApps.

Tussenconclusie

- 4.35 Concreet betekent dit dat Greenhood niet bemiddelt in betaalrekeningen of elektronisch geld en dus niet over een vergunning als bemiddelaar hoeft te beschikken.

Conclusie

- 4.36 Gebaseerd op de bovenstaande analyse komen wij dus tot de conclusie dat Greenhood geen gereguleerde diensten verleent op basis van de feiten zoals ons door Greenhood voorgesteld. Zoals aangegeven is het business model van Greenhood complex en schuurt het tegen diverse raamwerken, zoals MiCAR, aan. Zeker omtrent MiCAR bestaat nog veel onduidelijkheid, met name over de uitleg van de diverse cryptoactivadiensten. Wij kunnen daarom niet uitsluiten dat onze conclusies in de toekomst wijzigen vanwege nieuwe regelgeving of nieuwe interpretaties van toezichthouders.
- 4.37 Daarbij merken we ook op dat Greenhood samenwerkt met diverse Dienstverleners in EER-landen met minder strenge toezichthouders dan de AFM en DNB. Deze samenwerking kan een verhoogd toezichtrisico met zich meebrengen. Dat betekent ook dat mocht Greenhood meer zichtbaarheid krijgt in de markt en daarmee op de radar van de AFM en/of DNB komt, het belangrijk is dat Greenhood kan aantonen dat er geen gereguleerde diensten verleend worden. In dat geval verwachten wij namelijk veel kritische vragen van de AFM en/of DNB. Greenhood zal in dat geval dus met een sterke onderbouwing van de kwalificatie van de Greenhood App moeten komen.
- 4.38 Daarnaast is het van belang dat Greenhood zich realiseert dat haar dienstverlening wel kwetsbaar kan zijn voor misbruik ten behoeve van witwassen. Hoewel uit onze analyse volgt dat Greenhood geen gereguleerde diensten verleent en daarom niet onder de reikwijdte van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) valt, betekent dit niet dat er geen risico's bestaan. Toezichtrechtelijk levert dit geen directe verplichtingen of overtredingen op, maar strafrechtelijk kan betrokkenheid bij witwashandelingen mogelijk gevolgen hebben.
- 4.39 Tot slot merken wij op Greenhood dat het van belang is dat Greenhood nooit de indruk wekt dat zij de aanbieder is van een bepaalde dienst die door een derde wordt aangeboden. Denk hierbij aan de IBAN die wordt aangeboden via Monerium, maar waar door Greenhood naar wordt verwezen als de Greenhood IBAN. Dergelijke uitspraken wekken immers de impressie dat Greenhood de aanbieder is van een dergelijk product, wat niet het geval is. Een ander voorbeeld is de in-app browser om een account aan te maken bij Monerium. In deze in-app browser is het logo van Greenhood zichtbaar, maar het logo van Monerium niet. In dit geval is het belangrijk om duidelijk aan te geven dat Monerium de exclusieve aanbieder is van deze diensten samen met het logo van Monerium. In dat kader is het van belang dat Greenhood aan goede informatieverstrekking doet en duidelijk maakt wat de rol is van iedere betrokken partij met wie relaties worden aangegaan en welke bescherming daarbij hoort voor de Gebruiker.
