

Szymon Ciach^{*}

ORCID: 0000-0002-2240-7640

szymon.ciach@osborneclarke.com

Kamil Prokopowicz^{**}

ORCID: 0000-0002-1519-2733

kamil.prokopowicz@osborneclarke.com

Wybrane problemy usługi przechowywania kryptoaktywów w świetle MiCAR

Streszczenie

Jedną z usług w zakresie kryptoaktywów, której świadczenie zostało uregulowane przepisami unijnego rozporządzenia 2023/1114 w sprawie rynków kryptoaktywów (MiCAR), jest usługa zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów. Celem artykułu jest omówienie najważniejszych problemów związanych ze świadczeniem wskazanej usługi, ze szczególnym uwzględnieniem wymogów regulacyjnych, które prawodawca unijny nałożył na dostawców usług w zakresie kryptoaktywów (CASP) w celu zapewnienia wysokiego poziomu ochrony klientów, a także stabilności i integralności rynków kryptoaktywów. W ocenie autorów pomimo tego, że rozwiązania unijne przyjęte w MiCAR, charakteryzują się niedoskonałościami, kierunek regulacyjny przyjęty przez prawodawcę unijnego należy ocenić za słuszny. Ostateczna ocena spełnienia celów stojących za ustanowieniem przepisów MiCAR w omawianym zakresie będzie zależała jednak od kształtujących się w przyszłości tendencji rynkowych, nadzorczych oraz aktywności krajowych organów ustawodawczych państw członkowskich UE.

Słowa kluczowe: przechowywanie kryptoaktywów, blockchain, DLT, CASP, MiCAR

Kody JEL: K22, K23, K24

^{*} Szymon Ciach – radca prawny, Counsel w kancelarii Osborne Clarke.

^{**} Kamil Prokopowicz – aplikant radcowski, Associate w kancelarii Osborne Clarke.

Selected issues related to crypto-asset custody services in light of MiCAR

Abstract

One of the crypto-assets services that has been regulated by the European Union Regulation 2023/1114 on markets in crypto-assets (MiCAR) is the service of providing custody and administration of crypto-assets on behalf of clients. The aim of the article is to discuss the key issues related to the provision of this service, with particular emphasis on the regulatory requirements that the EU legislator has imposed on crypto-asset service providers (CASPs) to ensure a high level of client protection, as well as the stability and integrity of crypto-asset markets. According to the authors, despite the shortcomings of the EU solutions adopted in MiCAR, the regulatory direction taken by the EU legislator should be considered appropriate. The final assessment of the achievement of the objectives behind the establishment of MiCAR regulations in this area will, however, depend on future market trends, supervisory activities, and the actions of national legislative bodies of EU member states.

Keywords: crypto-asset custody, blockchain, DLT, CASP, MiCAR

JEL Codes: K22, K23, K24

Wstęp

Wprowadzenie do MiCAR. Jednym z dwóch głównych przedmiotów uregulowania rozporządzenia Unii Europejskiej (dalej: „UE”) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów (dalej: „MiCAR”, od ang. *Market in Crypto-Assets Regulation*)¹, obok wymogów dotyczących oferty publicznej i dopuszczania do obrotu na platformie obrotu kryptoaktywów, są wymogi w odniesieniu do dostawców usług w zakresie kryptoaktywów (dalej: „CASP”, od ang. *Crypto-Asset Service Provider*).

Wymogi w odniesieniu do CASP zostały zawarte w szczególności w przepisach tytułu V MiCAR, zatytułowanego: *zezwolenie na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów oraz warunki prowadzenia działalności przez tych dostawców*. W art. 3 ust. 1 pkt 16 MiCAR prawodawca unijny zdefiniował „usługi w zakresie kryptoaktywów” poprzez przytoczenie zamkniętego katalogu takich usług. W pierwszej kolejności (w art. 3 ust. 1 pkt 16 lit. a MiCAR) wskazał w tym zakresie na usługę zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów (ang. *providing custody and administration of crypto-assets on behalf of clients*). Odpowiednikami tej usługi w ramach obszaru tradycyjnych finansów (tzw. TradFi) są chociażby: usługa sprawowania pieczy nad instrumentami finansowymi oraz administrowania nimi na rachunek klientów, któ-

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937, Dz.U. L 150 z 9.6.2023, s. 40–205.

ra stanowi bankową usługę pomocniczą w ramach MiFID², a także usługa przechowywania i administrowania w odniesieniu do udziałów lub jednostek uczestnictwa przedsiębiorstw zbiorowego inwestowania, która stanowi usługę poboczną w ramach UCITS³ oraz AIFMD⁴.

Wcześniejsze regulacje. Poszukując źródeł wyodrębnienia i uregulowania w prawie unijnym usługi zapewniania przechowywania kryptoaktywów, należy zwrócić uwagę, że MiCAR jest historycznie pierwszą kompleksową regulacją dotyczącą świadczenia usług w zakresie kryptoaktywów, uchwaloną na poziomie UE. Przed 30 grudnia 2024 r., tj. dniem rozpoczęcia stosowania przepisów MiCAR w zakresie wymogów dotyczących świadczenia tego typu usług przez CASP, wykonywanie opisywanej działalności było zasadniczo regulowane wyłącznie przez wybranych prawodawców państw członkowskich UE. Prawodawca unijny przed 30 grudnia 2024 r. jedynie szczątkowo regulował świadczenie usług w zakresie kryptoaktywów (w dodatku stanowiących wyłącznie waluty wirtualne) za pośrednictwem przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Do 10 stycznia 2020 r. państwa członkowskie UE musiały bowiem wdrożyć do swoich krajowych porządków prawnych przepisy tzw. V Dyrektywy AML⁵ uchwalonej 30 maja 2018 r., która włączyła w katalog tzw. instytucji obowiązanych: 1) podmioty zajmujące się świadczeniem usług wymiany walut pomiędzy walutami wirtualnymi a walutami fiducjarnymi, a także 2) dostawców kont walut wirtualnych (ang. *custodian wallet providers*).

Charakterystyka usługi. Umieszczenie przez prawodawcę unijnego usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów na pierwszym miejscu w katalogu usług w zakresie kryptoaktywów zawartym w art. 3 ust. 1 pkt 16 MiCAR wydaje się nieprzypadkowe. W praktyce rynkowej świadczenie omawianej usługi wiąże się zasadniczo z zapewnieniem, że kryptoaktywa przechowywane w imieniu klienta będą dla niego dostępne, w tym nie staną się przedmiotem kradzieży lub nie zostaną utracone z jakiegokolwiek innego powodu. Niewywiązanie się z tego zapewnienia najczęściej będzie skutkowało znacznym naruszeniem interesów użytkownika, biorąc pod uwagę fakt, że wykonanie transakcji z wykorzystaniem środka dostępowego do kryptoaktywa jest trudne do śle-

² Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz.U. L 173 z 12.6.2014, s. 349–496.

³ Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS), Dz.U. L 302 z 17.11.2009, s. 32–96.

⁴ Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010, Dz.U. L 174 z 1.7.2011, s. 1–73.

⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE, Dz.U. L 156 z 19.6.2018.

dzenia i jest zwykle nieodwracalne, podobnie jak nieodwracalne jest również utracenie tego środka. Użytkownik powierzający dostawcy kontrolę nad posiadanym przez siebie kryptoaktywem musi zatem działać na podstawie silnej więzi zaufania łączącej go z dostawcą, której naruszenie może z kolei podważyć zaufanie do całego rynku kryptoaktywów. W przeszłości takie osłabienie zaufania materializowało się na dużą skalę chociażby w wypadku upadku takich giełd, jak FTX, które sprawowały aktywną kontrolę nad kryptoaktywami swoich klientów (Arner, Zetzsche, Buckley, Kirkwood 2023).

Cele artykułu. Celem niniejszego opracowania jest opisanie uregulowania MiCAR w zakresie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, ze wskazaniem potencjalnych problemów interpretacyjnych oraz słabych stron tej regulacji z punktu widzenia wypełniania celu ochrony interesów majątkowych użytkownika. Dalsze rozważania zostały przeprowadzane w odniesieniu do trzech szczegółowych zagadnień, do których należą: 1) zakres usługi zapewniania przechowywania kryptoaktywów, a także 2) publicznoprawne oraz 3) prywatnoprawne wymogi związane z jej świadczeniem zawarte w MiCAR. Przyporządkowanie określonych czynności usługodawcy do omawianej usługi w ramach pierwszego zagadnienia stanowi istotne zagadnienie praktyczne, od którego zależy zidentyfikowanie zakresu podmiotów zobowiązanych do wypełnienia wybranych wymogów MiCAR, a także zakresu dopuszczalnego nadzoru publicznoprawnego sprawowanego przez właściwe organy nadzoru. Jednak to właśnie od skuteczności określonych wymogów o charakterze publiczno- i prywatnoprawnym zależy to, czy regulacja przewidziana w MiCAR faktycznie będzie spełniała swoje cele, chroniąc użytkownika od otaczających go ryzyk oraz zwiększając tym samym bezpieczeństwo i stabilność rynków kryptoaktywów.

1. Zakres usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów

Definicja usługi. Zgodnie z art. 3 ust. 1 pkt 17 MiCAR zapewnianie przechowywania kryptoaktywów i administrowania nimi w imieniu klientów oznacza *sprawowanie pieczy nad kryptoaktywami lub środkami dostępu do takich kryptoaktywów, w stosownych przypadkach w postaci prywatnych kluczy kryptograficznych, lub sprawowanie nad nimi kontroli w imieniu klientów*. Zgodnie z tą definicją usługa ta będzie zatem świadczona w sytuacji, w której CASP sprawuje: 1) pieczę (ang. *safeguarding*) lub 2) kontrolę (ang. *controlling*) w stosunku do: a) kryptoaktywa lub b) środka dostępu do kryptoaktywa. W motywie 83 MiCAR prawodawca unijny określił natomiast, że omawiana usługa może obejmować: *przechowywanie kryptoaktywów należących do klientów lub dysponowanie środkami dostępu do takich kryptoaktywów*. W anglojęzycznej wersji MiCAR w tym kontekście nie rozróżniono jednak pojęć „przechowywania” i „dysponowania”, posługując się jednolicie wyrazem *holding* (a nie *custody*).

Definicja kryptoaktywa. Dla zdefiniowania zakresu usługi przechowywania kryptoaktywów i administrowania nimi w imieniu klientów istotna jest definicja „kryptoaktywa” zawarta w art. 3 ust. 1 pkt 5 MiCAR. Zgodnie z tym przepisem „kryptoaktywo” oznacza: *cyfrowe odzwierciedlenie wartości lub prawa, które da się przenosić (ang. *transferred*) i przechowywać (ang. *stored*) w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru (dalej: „DLT” od ang. *distributed ledger technology*) lub podobnej technologii.*

Definicja „kryptoaktywa” składa się z dwóch zasadniczych elementów, tj. wskazania ekonomiczno-prawnej natury kryptoaktywa, jako cyfrowego zapisu odzwierciedlającego wartość lub prawo oraz wskazania jego technologicznej natury, zawężającego to pojęcie do cyfrowych zapisów istniejących w DLT lub podobnej technologii. W tym kontekście odwołanie do „odzwierciedlenia” (ang. *representation*) wartości, należy rozumieć jako zdolność aktywa do bycia przedmiotem obrotu w wyniku zaistnienia popytu na takie aktywo (Völkel 2023). Pozwala to ująć w zakresie definicji kryptoaktywa te tokeny, których wartość wynika *stricte* ze stosunku popytu do podaży, a ich emisja nie odbywa się w związku z jakimikolwiek zapewnieniami podmiotu wprowadzającego te tokeny do obiegu. Przykładem tego typu kryptoaktywa jest Bitcoin, którego posiadanie nie wiąże się z jakimikolwiek umownie określonymi zobowiązaniami wobec jego twórców. Z drugiej strony, tokeny mogą być wykorzystywane jako nośnik oświadczeń woli, związanych np. z przyznaniem każdorazowemu posiadaczowi tokena określonych umownie uprawnień. Przykładem tego typu kryptoaktywów są tokeny użytkowe, których posiadanie zwykle uprawnia do korzystania z funkcjonalności usług cyfrowych⁶. Usługa zapewnienia przechowywania i administrowania kryptoaktywami w imieniu klienta może się odnosić zarówno do pierwszego, jak i drugiego typu kryptoaktywa opisanego powyżej, do których odnosi się definicja zawarta w MiCAR.

Wobec szerokiej definicji „kryptoaktywa” świadczenie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów zasadniczo nie jest zależne zatem od rodzaju kryptoaktywa i może obejmować wszystkie rodzaje kryptoaktywów, w tym zarówno tokeny powiązane z aktywami (dalej: „ART”), tokeny będące e-pieniędzem (dalej: „EMT”), jak również inne kryptoaktywa, w tym tokeny użytkowe. Może obejmować także zarówno kryptoaktywa reprezentujące wartość (np. Bitcoin), jak i kryptoaktywa reprezentujące prawa (np. tokeny ART, tokeny EMT lub tokeny użytkowe). Ponadto, usługa zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów może dotyczyć także kryptoaktywów, które nie będą podlegały przepisom MiCAR dotyczącym oferty publicznej z uwagi na fakt, że nie mają możliwości do zidentyfikowania emitenta. Motyw 22 do MiCAR wspominający o takich kryptoaktywach nie wyłącza bowiem stosowania do nich przepisów tytułu V MiCAR. Wymogi MiCAR dotyczące przechowywania kryptoaktywów nie znajdują natomiast zastosowania w stosunku do kryptoaktywów, które są unikalne i nie są zamienne z innymi kryptoaktywami (NFT – od ang. *Non-Fungible Tokens*). Takie kryptoaktywa zostały bowiem w sposób generalny wyłączone z zakre-

⁶ Zob. tokeny reprezentujące wirtualne nieruchomości w platformie Decentraland.

su stosowania MiCAR (art. 2 ust. 3 MiCAR). Omawiane wymogi nie znajdują ponadto zastosowania w wypadku pozostałych grup kryptoaktywów wymienionych w art. 2 ust. 4 MiCAR (m.in. instrumenty finansowe, depozyty, ubezpieczenia).

Przechowywanie danych w DLT. Od strony technologicznej należy zaznaczyć, że zasadniczą cechą DLT jest rozproszenie przetwarzania danych. Oznacza to, że kopie baz danych zawierające zapisy cyfrowe stanowiące kryptoaktywa są powielone i zlokalizowane w pamięci komputerów tworzących DLT (węzły). W przypadku publicznych, otwartych i globalnie rozproszonych DLT nie da się wskazać jednego konkretnego podmiotu przechowującego dane ani jednej konkretnej lokalizacji. Wskazanie takich podmiotów i lokalizacji jest możliwe w przypadku prywatnych, zamkniętych DLT, które są utrzymywane przez określoną grupę podmiotów. W obu wypadkach jest to jednakże irrelevantne dla usług zapewnienia przechowywania i administrowania kryptoaktywami w imieniu klientów, których nie należy odnosić do faktycznego procesu przetwarzania danych (ich przechowywania) w ramach DLT, lecz do ekonomicznego aspektu tej usługi, związanego z pieczę lub kontrolą w stosunku do kryptoaktywa lub środka dostępu do kryptoaktywa.

Pieczę lub kontrola. W praktyce rynkowej usługa zapewnienia przechowywania i administrowania kryptoaktywami odbywa się w dwóch wiodących modelach, które znajdują odzwierciedlenie w definicji omawianej usługi. Po pierwsze, pieczę lub kontrola nad kryptoaktywami może odbywać się poprzez transfer kryptoaktywa z adresu lub rachunku rozproszonego rejestru posiadacza (lub innej osoby) do adresu lub rachunku rozproszonego rejestru CASP. W takiej sytuacji, kryptoaktywo trafia pod bezpośrednie władanie CASP, który sprawuje nad nim całkowitą kontrolę. Szczególnego znaczenia praktycznego nabiera wtedy obowiązek CASP do prowadzenia rejestru pozycji odpowiadających prawom każdego klienta do kryptoaktywów (zob. art. 75 ust. 2 MiCAR). Kryptoaktywa klientów mogą bowiem znajdować się na jednym lub więcej adresach lub rachunkach rozproszonego rejestru, kontrolowanych przez CASP, a CASP musi być w stanie określić wysokość pozycji swoich klientów. Po drugie, sprawowanie pieczy lub kontroli może odbywać się nad środkami dostępu do kryptoaktywów. W tym przypadku kryptoaktywa nie podlegają transferowi, lecz pozostają powiązane z adresem lub rachunkiem rozproszonego rejestru posiadacza. Posiadacz natomiast udostępnia CASP środek dostępu do kryptoaktywów, najczęściej w postaci kryptograficznego klucza prywatnego powiązanego z adresem lub rachunkiem w DLT.

Prawodawca unijny w przepisach MiCAR nie określił, jaka jest różnica pomiędzy sprawowaniem pieczy a sprawowaniem kontroli. Powszechne znaczenie tych pojęć zarówno w języku polskim, jak i angielskim, wskazuje, że sprawowanie pieczy należy odnosić przede wszystkim do przechowania kryptoaktywów związanego z ich transferem do CASP lub przechowania samych środków dostępu do kryptoaktywa. Wskazywałoby na to w szczególności anglojęzyczny wyraz *safekeeping*, który słownikowo odnosi się do ochrony przed szkodą lub stratą („*Safekeeping*”, b.d.). Istotą kontroli z kolei jest posiadanie decyzyjności, władania nad kryptoaktywem (np. transferowania, wykonywania powiązanych z nim uprawnień).

Pojęcie kontroli. W celach porównawczych można wskazać, że zgodnie z *Zasadami dotyczącymi aktywów cyfrowych i prawa prywatnego* (dalej: „PDAPL”) przyjętymi przez Międzynarodowy Instytut Unifikacji Prawa Prywatnego (UNIDROIT 2023) dostawca usługi custody (ang. *custodian*) utrzymuje kryptoaktywo dla klienta, jeżeli sprawuje kontrolę nad tym kryptoaktywem lub powierza sprawowanie takiej kontroli podwykonawcy (ang. *sub-custodian*) (UNIDROIT 2023, s. 68–69). W przeciwieństwie do MiCAR, w PDAPL zdefiniowano pojęcie „kontroli”, przyjmując, że jest ona sprawowana w wypadku posiadania możliwości uzyskania zasadniczo wszystkich korzyści z aktywa cyfrowego lub uniemożliwienia innym osobom uzyskania takich korzyści, a także w wypadku posiadania wyłącznej możliwości przeniesienia takich możliwości na inną osobę (UNIDROIT 2023, s. 51–52). W tym kontekście zauważono, że pojęcie „kontroli” sprawowanej nad kryptoaktywem jest odpowiednikiem funkcjonującego w prawie prywatnym pojęcia „posiadania” rzeczy ruchomej. Oba pojęcia odnoszą się bowiem do władztwa o charakterze faktycznym, które może być sprawowane w oderwaniu od faktu posiadania praw majątkowych (UNIDROIT 2023, s. 52–54). Nie ma zasadniczych przeszkód, by w tożsamy sposób rozumieć „kontrolę”, o której mowa w art. 3 ust. 1 pkt 17 MiCAR.

Zakres kontroli. Jak słusznie zauważono w motywie 83 MiCAR, kontrola nad kryptoaktywem może przybierać charakter częściowy lub pełny, w zależności od tego, czy wejście w nią przez CASP stanowi przeszkodę do równoległego sprawowania jej przez klienta. Transfer kryptoaktywa na adres lub rachunek w rozproszonym rejestrze, kontrolowany wyłącznie przez CASP, będzie wiązał się z całkowitym przekazaniem kontroli. Udostępnienie CASP środków dostępu do kryptoaktywa nie wyklucza natomiast możliwości zachowania dostępu do kryptoaktywów przez klienta CASP, do czego wystarczy utrwalenie środków dostępu na dowolnym innym nośniku fizycznym lub cyfrowym. W takiej sytuacji wystąpi jedynie częściowa kontrola po stronie CASP.

Portfele niepowiernicze. W motywie 83 MiCAR *in fine* wyraźnie wskazano, że: *dostawcy sprzętu lub oprogramowania dla portfeli niepowierniczych nie powinni być objęci zakresem stosowania niniejszego rozporządzenia*. Portfele niepowiernicze (ang. *non-custody* lub *self-custody*) przyjmują przede wszystkim postać sprzętu (np. pendrive z wgranym oprogramowaniem⁷) lub oprogramowania (np. w postaci aplikacji mobilnej, dodatku do przeglądarki internetowej⁸), które ułatwiają zarządzanie środkami dostępu do kryptoaktywów. Portfele tego typu umożliwiają interakcję z protokołami zdecentralizowanych finansów, zarówno za pośrednictwem własnych interfejsów, jak i poprzez podłączenie portfela do innych aplikacji. Ich podstawową cechą jest to, że w przeciwieństwie do portfeli powierniczych, dają użytkownikom wyłączną kontrolę nad ich środkami dostępu do kryptoaktywów, i to użytkownicy są odpowiedzialni za zabezpieczenie tych środków. Dostawcy tego typu portfeli nie wchodzi w posiadanie ani samych kryptoaktywów poprzez ich transfer, ani środków dostępu do kryptoaktywów. Utrata środków dostępu przez

⁷ Np. produkt marki Ledger lub Trezor.

⁸ Np. produkt marki Metamask.

użytkownika zazwyczaj skutkuje trwałą utratą dostępu do kryptoaktywów (Europejski Urząd Nadzoru Bankowego 2025, s. 13). Taka sytuacja może wystąpić np. w razie zniszczenia pendrive'a przechowującego klucze prywatne.

Za najbezpieczniejszy rodzaj portfeli niepowierniczych uznawane są portfele sprzętowe, będące portfelami typu zimnego (ang. *cold*). W przeciwieństwie do portfeli przyjmujących postać oprogramowania, będących najczęściej portfelami typu gorącego (ang. *hot*), nie są one dostępne online, co czyni je bardziej odpornymi na ataki cybernetyczne z zewnątrz. Przykładowy schemat użycia portfela sprzętowego obejmuje jego połączenie z zewnętrznym urządzeniem służącym do przygotowywania transakcji, uruchomienie oraz wpisanie hasła zabezpieczającego dostęp do portfela. Z uwagi na to, że portfele tego typu nie mają aktywnego połączenia z siecią, podpisywanie transakcji zawsze musi poprzedzać uzyskanie do nich fizycznego dostępu. Nie działają one także w sposób autonomiczny, co oznacza, że przeprowadzenie transakcji wymaga współpracy z innym urządzeniem przygotowującym transakcję. Z uwagi na wszystko powyższe, portfele sprzętowe są najczęściej wykorzystywane do przechowywania większych ilości kryptoaktywów w długim horyzoncie czasowym.

Pozostałe usługi niepowiernicze. Rozważania przedstawione powyżej nie zawierają wyjaśnień w odniesieniu do tego, czy świadczenie usługi przechowywania kryptoaktywów i administrowania nimi w imieniu klientów będzie występować w wypadkach, w których CASP nie sprawuje pieczy lub nie kontroluje kryptoaktywa lub środka dostępowego do kryptoaktywa, a wykonuje wyłącznie inne czynności, które ewentualnie mogłyby mieścić się w niezdefiniowanych bliżej w MiCAR pojęciach „administrowania” kryptoaktywem. Opisane wyżej wyłączenie, które zostało zawarte w motywie 83 MiCAR *in fine*, odnosi się bowiem wyłącznie do portfeli niepowierniczych, a nie innych usług niepowierniczych. W naszej ocenie nie ma silnych podstaw, by sądzić, że wszelkie pozostałe usługi dodatkowe niezwiązane ze sprawowaniem kontroli nad kryptoaktywem, a jednocześnie niestanowiące innych usług regulowanych w rozumieniu MiCAR, powinny podlegać przepisom tego rozporządzenia. W szczególności należy zauważyć, że dostarczanie usług związanych z portfelami niepowierniczymi również może wiązać się z pewnymi ryzykami dla kryptoaktywa użytkownika (np. związanych z awarią urządzenia lub oprogramowania dostarczanego przez dostawcę). Celem uregulowania usługi zapewniania przechowywania lub administrowania kryptoaktywami nie jest zatem mitygowanie przez prawodawcę wszystkich istniejących na rynku ryzyk, a wyłącznie tych o najpoważniejszym charakterze indywidualnym lub systemowym.

Administrowanie związane z pieczą lub kontrolą. Wskazany powyżej problem nie będzie miał znaczenia dla usług, które można uznawać za polegające na podejmowaniu czynności „administrowania” kryptoaktywami, a których świadczenie wymaga jednoczesnego sprawowania nad nimi pieczy lub kontroli. Usługi takie powinny raczej podlegać wymogom MiCAR oraz nadzorowi publicznoprawnemu sprawowanemu w celu przestrzegania przepisów tego rozporządzenia, jako ściśle związane ze sprawowaniem kontroli nad kryptoaktywem. W literaturze wskazuje się, że do takich usług „administrowania” można zaliczyć usługi związane z uzna-

waniem wszelkich bezpośrednich korzyści dla klienta, wynikające z posiadania kryptoaktywów. Odnosić się to może w szczególności do obejmowania rzutów nagród (ang. *airdrops*), podejmowania decyzji w sprawie propozycji tzw. forków (tj. podziałów historii łańcucha bloków na oddzielne ścieżki), głosowania w sprawie inteligentnych kontraktów (ang. *smart contracts*) lub protokołów stakingu (Ossio, Nixon, Yates 2023, 14). Zastrzec należy jednak, że wskazane wyliczenie jest o tyle kontrowersyjne, że w wypadku czynności polegających na podejmowaniu dyskrejonalnych decyzji przez CASP w stosunku do kontrolowanych kryptoaktywów, uprawnione może być kwalifikowanie takich czynności również jako usługi zarządzania portfelem kryptoaktywów, tj. odrębnej usługi regulowanej za pośrednictwem przepisów MiCAR. Analiza wskazanego problemu nie mieści się jednak w ramach niniejszego opracowania.

Podsumowując powyższe rozważania, w naszej ocenie warunkiem koniecznym do kwalifikacji określonej usługi jako usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, jest co najmniej objęcie przez CASP kontroli nad kryptoaktywem lub środkiem dostępu do kryptoaktywa klienta. Cel takiego działania nie jest istotny, w tym może obejmować on wyłącznie zagwarantowanie klientowi, że jego kryptoaktywo lub środek dostępu do kryptoaktywa nie zostaną ukradzione lub w inny sposób utracone. Alternatywnie, świadczenie omawianej usługi może być operacyjnie związane ze świadczeniem innych usług w zakresie kryptoaktywów, w tym w szczególności służyć świadczeniu usług transferu kryptoaktywów czy zarządzania portfelem kryptoaktywów. Świadczenie omawianej usługi nie wystąpi natomiast w wypadku, w którym kontrola nad kryptoaktywem będzie sprawowana przez CASP w jego własnym imieniu, a nie jego klienta. Może to dotyczyć głównie umów odpowiadających umowom pożyczki lub umowom o ustanowienie zabezpieczenia rzeczowego zawieranych z klientem, z których bezpośrednie korzyści będzie odnosił CASP.

2. Publicznoprawne wymogi regulacyjne

Reglamentacja usługi. Zasadniczo świadczenie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów wymaga: 1) uzyskania zezwolenia na prowadzenie działalności w zakresie kryptoaktywów w ramach procedury opisanej w art. 62–63 MiCAR lub alternatywnie, 2) dopełnienia obowiązku notyfikacyjnego w ramach procedury opisanej w art. 60 MiCAR. Prawo do świadczenia omawianej usługi bez uzyskania zezwolenia, z zastrzeżeniem wypełnienia obowiązku notyfikacyjnego, przysługuje wyłącznie wybranym podmiotom finansowym, którymi są instytucje kredytowe (art. 60 ust. 1 MiCAR), centralne depozyty papierów wartościowych (art. 60 ust. 2 MiCAR), firmy inwestycyjne (art. 60 ust. 3 MiCAR) oraz instytucje pieniądza elektronicznego (art. 60 ust. 4 MiCAR). W stosunku do instytucji pieniądza elektronicznego w ramach art. 60 ust. 4 MiCAR zastrzeżono jednak, że omawiana usługa może być świadczona wyłącznie w stosunku do EMT. *A contrario* należy wnioskować, że w wypadku pozostałych trzech rodzajów instytucji finanso-

wych omawiana usługa może być świadczona bez względu na rodzaj kryptoaktywa będącego przedmiotem przechowywania lub administrowania.

Odpowiedniki w ramach TradFi. W wyżej przytoczonych przepisach MiCAR zastrzeżono wyraźnie, że odpowiednikami usługi przechowywania kryptoaktywów i administrowania nimi w imieniu klientów są: 1) w stosunku do centralnych depozytów papierów wartościowych – usługa prowadzenia lub obsługi rachunków papierów wartościowych w związku z usługą rozrachunku, o której mowa w sekcji B pkt 3 załącznika do CSDR⁹, natomiast 2) w stosunku do firm inwestycyjnych – sprawowanie pieczy nad instrumentami finansowymi oraz administrowanie nimi na rachunek klientów, o której mowa w sekcji B pkt 1 załącznika I do MiFID. W naszej ocenie konsekwencją zawarcia tych postanowień jest to, że świadczenie usługi przechowywania kryptoaktywów i administrowania nimi w imieniu klientów przez wyżej wymienione podmioty, wymaga dochowania nie tylko wymogów wymienionych w MiCAR, ale także wymogów przewidzianych dla wskazanych usług równoważnych w CSDR oraz MiFID. W wypadku centralnych depozytów papierów wartościowych wymogi dla świadczenia bankowych usług pomocniczych opisano w tytule IV CSDR i obejmują one przede wszystkim wymóg uzyskania zezwolenia. Również, zgodnie z art. 6 MiFID, zezwolenie udzielane firmie inwestycyjnej powinno określać zakres usług dodatkowych.

Wyjątek od zezwolenia/notyfikacji. Zgodnie z art. 4 ust. 5 MiCAR świadczenie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, z pominięciem uzyskania zezwolenia lub wypełnienia obowiązku notyfikacyjnego, możliwe jest wyłącznie w wypadku, w którym oferta publiczna danego kryptoaktywa innego niż ART i EMT podlega wyłączeniu na podstawie art. 4 ust. 3 MiCAR. Nie dotyczy to jednak takich kryptoaktywów, które kiedykolwiek w przeszłości podlegały już ofercie publicznej lub zostały dopuszczone do obrotu na platformie obrotu. Art. 4 ust. 3 MiCAR zawiera katalog czterech wypadków wyłączających obowiązek przeprowadzania oferty publicznej, do których należą: nieodpłatne oferowanie kryptoaktywa, oferowanie kryptoaktywa jako nagrody za utrzymywanie rejestru lub walidację transakcji, oferowanie tokena użytkowego (ang. *utility token*) zapewniającego dostęp do istniejącego towaru lub usługi czy oferowanie kryptoaktywów uznawanych wyłącznie w ograniczonej sieci akceptantów. *A contrario* zwolnienie z obowiązku uzyskania zezwolenia lub wypełnienia obowiązku notyfikacyjnego nie znajdzie zastosowania w wypadku zamiaru świadczenia omawianej usługi w stosunku do kryptoaktywów innych niż ART i EMT, do których stosuje się uproszczone zasady składania oferty publicznej w wypadkach określonych w art. 4 ust. 2 MiCAR.

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012, Dz.U. L 257 z 28.8.2014, s. 1–72.

Rozróżnienie wymogów. Dostawcy, chcący świadczyć usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, muszą wypełniać przewidziane w MiCAR: 1) wymogi ogólne, tj. znajdujące zastosowanie bez względu na rodzaj świadczonej usługi w zakresie kryptoaktywów, a także 2) wymogi szczególne, których wypełnienie związane jest wyłącznie z faktem świadczenia omawianej usługi. Najważniejsze wymogi o charakterze szczególnym zostały zawarte w art. 70 ust. 1 oraz 75 MiCAR. Wymogi te obowiązują jednolicie zarówno w odniesieniu do podmiotów finansowych wymienionych w art. 60 MiCAR, jak i pozostałych podmiotów, które muszą uzyskać zezwolenie. Oznacza to, że w założeniu prawodawcy unijnego użytkownik omawianej usługi powinien mieć zagwarantowany taki sam minimalny standard ochrony, niezależnie od tego, czy CASP oferujący jej świadczenie jest jednocześnie inną instytucją finansową wskazaną w MiCAR. Biorąc jednak pod uwagę fakt równoczesnego podlegania instytucji kredytowych innym regulacjom ostrożnościowym o charakterze szczególnym, w tym dotyczącym zarządzania ryzykiem operacyjnym czy restrukturyzacji i uporządkowanej likwidacji, to właśnie one będą zapewniały użytkownikom najwyższy standard ochrony rynkowej. Zgodność z tymi regulacjami będzie bowiem w praktyce wpływać także na działalność w zakresie kryptoaktywów.

Mechanizmy ochrony. Zgodnie z art. 70 ust. 1 MiCAR podstawowym obowiązkiem CASP jest wprowadzenie mechanizmów mających na celu zabezpieczenie praw własności klientów w odniesieniu do kryptoaktywów, w szczególności w przypadku niewypłacalności CASP oraz mających na celu zapobieżenie wykorzystywaniu kryptoaktywów należących do klienta na własny rachunek CASP. Mechanizmy takie powinny być opisane w polityce w zakresie przechowywania, o której mowa w art. 75 ust. 3 MiCAR. Uznać należy, że zgodnie z art. 75 ust. 3 MiCAR wskazana polityka powinna uwzględniać wszelkie relewantne ryzyka, zarówno o charakterze zewnętrznym, jak i wewnętrznym, w tym przykładowo wskazane przez prawodawcę unijnego ryzyka związane z oszustwami, cyberbezpieczeństwem lub zaniedbaniami. Przyjęte przez CASP środki ograniczania zidentyfikowanego ryzyka mogą, co do zasady, mieć różną naturę i obejmować przede wszystkim środki związane z wewnętrzną organizacją działalności CASP, jak również środki o charakterze technologicznym. W świetle art. 70 ust. 1 MiCAR wykorzystywanie przez CASP na własną rzecz powierzonych kryptoaktywów jest bezwzględnie wykluczone. Zabronione jest zatem również nabywanie za takie kryptoaktywa instrumentów finansowych w celach inwestycyjnych, niezależnie od poziomu ryzyka czy płynności takich instrumentów.

Mityganty ryzyka. Podczas, gdy dobór właściwych mitygantów powinien być uzależniony od indywidualnego poziomu zidentyfikowanych przez CASP ryzyk, MiCAR przewiduje szczególne środki, które CASP świadczący usługę zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów muszą uwzględnić w swojej działalności. Środki te sprowadzają się do segregacji (tj. oddzielenia) kryptoaktywów przechowywanych w imieniu klientów i środków dostępu do nich, od własnych kryptoaktywów, na trzech poziomach, tj. operacyjnym, technologicznym i prawnym (Kokorin 2023, s. 15–16). Segregacja operacyjna sprowadza się do przewidzianego w art. 75 ust. 2 MiCAR obowiązku prowadzenia

otwartego, w imieniu każdego klienta, rejestru pozycji odpowiadających prawom każdego klienta do kryptoaktywów. W rejestrze tym powinny być rejestrowane, możliwie jak najszybciej, wszelkie operacje wynikające z dyspozycji klientów CASP. Segregacja technologiczna sprowadza się natomiast do obowiązku przechowywania kryptoaktywów w ramach odrębnych rachunków (art. 75 ust. 7 akapit 1 MiCAR). CASP powinien także wydzielać kryptoaktywa prawnie, zgodnie z mającym zastosowanie prawem, aby wierzyciele CASP nie mogli zaspokajać swoich roszczeń z kryptoaktywów przechowywanych w imieniu klientów, głównie w przypadku niewypłacalności (art. 75 ust. 7 akapit 2 MiCAR).

Prawne wydzielenie kryptoaktywów. W naszej ocenie przewidziany w MiCAR wymóg prawnego wydzielenia kryptoaktywów klienta od kryptoaktywów CASP, stanowi wadę regulacji MiCAR w zakresie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów. Zaadresowanie dyspozycji art. 75 ust. 7 MiCAR wyłącznie do CASP powoduje wątpliwości, czy z przepisu tego można wywodzić obowiązek państw członkowskich UE do przyjęcia takich przepisów prawa publicznego, w tym szczególnie w zakresie obowiązujących procedur egzekucyjnych, które wyłączałyby możliwość przeprowadzania egzekucji roszczeń przysługujących wobec CASP z kryptoaktywów przechowywanych w imieniu jego klientów. Wątpliwości takie nie istnieją, natomiast zasadniczo chociażby w wypadku art. 10 ust. 1 lit. a *in fine* PSD2¹⁰, który odwołuje się do zasad ochrony środków pieniężnych użytkowników obowiązujących dostawców usług płatniczych. W naszej ocenie, jeżeli w świetle prawa danego państwa w ogóle można przeprowadzać egzekucję z kryptoaktywów (w szczególności biorąc pod uwagę możliwość występowania odmiennych ustaleń w stosunku do prywatnoprawnego charakteru takich aktywów), to przepisy takie powinny zostać przewidziane w porządku krajowym zgodnie z MiCAR. W przeciwnym razie CASP nie będzie w istocie dysponował wystarczającymi środkami ochrony kryptoaktywów przed roszczeniami wierzycieli CASP, a segregacja na poziomie prawnym będzie wyłącznie iluzoryczna.

Outsourcing. Ostatnim istotnym wymogiem regulacyjnym w stosunku do CASP, w związku ze świadczeniem usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, są szczegółowe zasady outsourcingu, które zostały przewidziane w art. 75 ust. 9 MiCAR. Zgodnie ze wskazanym przepisem korzystanie z usług innych dostawców usług w zakresie kryptoaktywów w ramach omawianej usługi, może odbywać się wyłącznie w wypadku, gdy tacy insourcerzy mają status CASP uzyskany na podstawie procedury zezwoleniowej lub notyfikacyjnej przewidzianej w MiCAR. W naszej ocenie wskazany wymóg odnosi się wyłącznie do sytuacji, w których dochodzi do przekazania pieczy lub kontroli nad kryptoaktywem lub środkiem dostępowym do kryptoaktywa innemu podmiotowi, którego w takim wypadku można określać anglojęzycznym pojęciem *sub-custodian*.

¹⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35–127.

Nie wydaje się bowiem zasadne rozciąganie tego wymogu na dostawców usług lub działań do celów wykonywania funkcji operacyjnych na mocy art. 73 MiCAR, biorąc pod uwagę, że art. 75 ust. 9 MiCAR wspomina wąsko o dostawcach usług w zakresie kryptoaktywów. W celu zastosowania zaostrzonych wymogów outsourcingu czynności wykonywane przez takiego insourcera na rzecz CASP muszą zatem kwalifikować się jako świadczenie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów w rozumieniu przyjętym w MiCAR.

3. Wymogi prywatnoprawne dotyczące umowy zawieranej z użytkownikiem

Wymogi ogólne. Jednym z nadrzędnych celów rozporządzenia MiCAR jest podniesienie poziomu ochrony posiadaczy kryptoaktywów. Mając na uwadze istniejącą i niejednorodną praktykę obrotu, z względu do rozporządzenia wprowadzono wiele norm o charakterze prywatnoprawnym. W szczególności, w art. 66 MiCAR, dotyczącym wszystkich CASP, wprowadzono reguły wymagające od CASP działania w sposób uczciwy, rzetelny i profesjonalny, zgodnie z najlepiej pojętym interesem swoich klientów i potencjalnych klientów (ust. 1), jak również obowiązek przekazywania swoim klientom uczciwych, jasnych i niewprowadzających w błąd informacji (ust. 2). Zgodnie z art. 66 ust. 4 MiCAR każdy CASP ma obowiązek udostępnić publicznie swoje polityki w zakresie cen, kosztów i opłat, zamieszczając je w widocznym miejscu na stronie internetowej. W konsekwencji należy założyć, że umowy w zakresie usługi zapewnienia przechowywania i administrowania kryptoaktywami będą, przynajmniej w części swych postanowień, miały charakter umów adhezyjnych.

Prywatnoprawna natura kryptoaktywów. Kwestia prywatnoprawnej kwalifikacji kryptoaktywów pozostaje wciąż nierozstrzygnięta w MiCAR a jej szczegółowe omówienie wykracza poza ramy niniejszego opracowania. Warto jednak zauważyć, że w ramach art. 70 ust. 1 MiCAR, dla CASP, którzy posiadają kryptoaktywa należące do klientów lub środki dostępu do takich kryptoaktywów, ustanowiono obowiązek wprowadzania odpowiednich mechanizmów mających na celu m.in. zabezpieczenie „praw własności klientów” (ang. *ownership rights*). Jednakże w świetle tego przepisu, jak i całokształtu regulacji, wydaje się, że unijny prawodawca unika wprowadzania jednoznacznej propozycji, co do rozstrzygnięcia statusu prywatnoprawnego kryptoaktywów. Materia ta wymaga więc rozstrzygnięcia na poziomie prawa krajowego.

Podobnie, w gestii krajowych ciał ustawodawczych oraz orzeczniczych powinno pozostawać rozstrzygnięcie, czy i w jakim zakresie do usług zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów, powinno stosować się krajowe przepisy dotyczące umowy przechowania, w zakresie w którym nie pozostają one sprzeczne z przepisami MiCAR. W polskim prawie prywatnym (art. 835 i n. ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny) umowa przechowania rzeczy ruchomych, chociaż również zakłada istnienie po stronie przechowawcy obowiązku sprawowania pieczy nad rzeczą ruchomą, to nie dotyczy jednak rzeczy

oznaczonych co do gatunku, które nie zostały zindywidualizowane przy ich przekazaniu¹¹. Cechą tokenów innych od NFT jest natomiast to, że mają charakter w pełni wymienialny i nie są dodatkowo indywidualizowane. Pomimo tego, zakaz dysponowania przekazanymi kryptoaktywami, zbliża jednak umowę na przechowywanie kryptoaktywów do klasycznej umowy przechowania, a nie umowy depozytu nieprawidłowego właściwej dla rzeczy oznaczonych co do gatunku.

Zawarcie umowy z użytkownikiem. Dalsze szczegółowe normy prywatnoprawne w zakresie usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów znajdują się w art. 75 MiCAR, który jest poświęcony wyłącznie CASP dostarczającym taką usługę. Zgodnie z art. 75 ust. 1 MiCAR CASP ma obowiązek zawarcia umowy z użytkownikiem, co implikuje co najmniej obowiązek udostępnienia treści umowy do jej akceptacji przez klienta. W tymże przepisie ustanowiono również minimalne wymogi co do treści umowy – CASP ma obowiązek wskazać m.in. swoją tożsamość, system uwierzytelniania klienta, opłaty i prawo właściwe.

Powstanie lub zmiana praw klienta. Specyficzną dla rynku kryptoaktywów regulacją jest art. 75 ust. 4 MiCAR, który ustanawia obowiązek CASP wobec ułatwienia wykonywania praw związanych z kryptoaktywami. Wszelkie zdarzenia mogące spowodować powstanie lub zmianę praw klienta mają być natychmiast rejestrowane w rejestrze pozycji klienta. W kolejnym akapicie tego przepisu uregulowano natomiast kwestię tzw. forków¹² rozproszonych rejestrów i tym podobnych zdarzeń na poziomie DLT. Przyjęto założenie, że klient jest uprawniony do wszelkich nowo utworzonych kryptoaktywów lub praw na podstawie i w zakresie pozycji klienta w momencie wystąpienia takiej sytuacji. Jest to przepis dyspozytywny, co oznacza, że strony mogą w umowie wyłączyć takie uprawnienie klienta.

Odpowiedzialność CASP. W art. 75 ust. 8 MiCAR uregulowano kwestię odpowiedzialności CASP wobec klientów. CASP, którzy zapewniają przechowywanie kryptoaktywów i administrowanie nimi w imieniu klientów, ponoszą wobec swoich klientów odpowiedzialność za utratę kryptoaktywów lub środków dostępu do kryptoaktywów w wyniku incydentu, który można im przypisać. Unijny prawodawca doprecyzował, że incydenty, których nie można przypisać CASP, obejmują wszelkie zdarzenia, w odniesieniu do których CASP wykaże, że miały miejsce niezależnie od świadczenia odpowiedniej usługi lub niezależnie od operacji CASP, takie jak problem nieodłącznie związany z eksploatowaniem rozproszonego rejestru, nad którym dostawca usług w zakresie kryptoaktywów nie sprawuje kontroli. Nie zostało to wprost przesądzone, natomiast takie uregulowanie kwestii odpowiedzialności

¹¹ Umowa przechowania nie dotyczy zatem pieniędzy, które nie zostały umieszczone w kopercie lub skarbonce oddanej do przechowania (Gudowski 2017, s. 448).

¹² Wyraz „fork” jest pożyczony z j. angielskiego i odnosi się do „rozwidlenia” DLT, przykładowo, podjęcia przez część społeczności utrzymującej DLT decyzji o wgraniu aktualizacji i kontynuowania rejestrowania transakcji w nowej wersji rejestru, podczas gdy stara wersja jest wciąż utrzymywana przez inną część społeczności. W MiCAR ujęte jako „zmiany w leżących u podstaw kryptoaktywów technologiach rozproszonego rejestru lub wszelkie inne zdarzenia, które mogą spowodować powstanie lub zmianę praw klienta”.

wydać się sugerować odwrócony ciężar dowodu, spoczywający na CASP. W sytuacji utraty kryptoaktywów lub utraty środków dostępu do kryptoaktywów, przechowywanych i administrowanych przez CASP, klient może mieć bowiem ograniczone możliwości dowodowe. Odpowiedzialność CASP jest natomiast ograniczona do wartości rynkowej utraconych kryptoaktywów w momencie wystąpienia utraty.

W MiCAR nie zdefiniowano pojęcia „incydentu”, o którym wyżej mowa, natomiast pewnych wyjaśnień dostarcza tutaj motyw 83 MiCAR, wskazujący, że CASP powinni ponosić odpowiedzialność za wszelkie straty wynikające z incydentów związanych z technologiami informacyjno-komunikacyjnymi (ICT), w tym incydenty spowodowane cyberatakami, kradzieżą lub jakąkolwiek awarią.

W naszej ocenie art. 75 ust. 8 MiCAR ma na celu przesądzenie często spornego charakteru odpowiedzialności CASP za szkody spowodowane incydentami, w tym cyberatakami. Klauzule wyłączające odpowiedzialność CASP we wskazanym powyżej zakresie będą nieważne, z uwagi na sprzeczność z przepisami MiCAR. Powyższy przepis nie wyłącza natomiast możliwości pociągnięcia CASP do odpowiedzialności na innej podstawie prawnej, w tym w wyniku niewykonania lub nienależytego wykonania zobowiązania lub na podstawie deliktowej. W zakresie odpowiedzialności za incydenty w przedstawionym powyżej zakresie CASP ma jednak prawo powołać się na art. 75 ust. 8 MiCAR jako *lex specialis*, dotyczące głównie przesłanek i wysokości jego odpowiedzialności za takie zdarzenia.

Podsumowanie

Zakres podmiotowy świadczenia usług zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów jest ograniczony z uwagi na wprowadzoną rozporządzeniem MiCAR reglamentację. Pozwala ona świadczyć tego typu usługę jedynie podmiotom mającym odpowiednie zezwolenie lub niektórym podmiotom finansowym realizującym adekwatne usługi poza rynkiem kryptoaktywów, po wywiązaniu się z obowiązku notyfikacyjnego względem właściwego organu nadzoru. Dalsze wymogi przewidziane w MiCAR stosuje się zasadniczo jednolicie, bez względu na rodzaj CASP.

Zakres przedmiotowy analizowanej usługi jest zagadnieniem, które może rodzić najwięcej problemów praktycznych, z uwagi na występujący w MiCAR brak konsekwencji terminologicznej pomiędzy tekstem motywów oraz definicją tejże usługi, jak również brakiem wyjaśnień w zakresie użytych w definicji sformułowań. Kwestie te będą zatem podlegać dalszemu wypracowaniu przez literaturę, stanowiska właściwych organów oraz orzecznictwo. Najważniejszym wnioskiem jest to, że omawiana usługa może obejmować wszystkie typy i kategorie kryptoaktywów w rozumieniu przyjętym w MiCAR, za wyjątkiem kryptoaktywów w sposób generalny wyłączonych spod zakresu stosowania tego rozporządzenia. Z jej zakresu będą wykluczone natomiast przede wszystkim usługi portfeli niepowierniczych oraz sytuacje, w których CASP wykonuje pieczę lub kontrolę nad kryptoaktywem

we własnym imieniu, a nie w imieniu klienta. Ponadto do świadczenia omawianej usługi nie może dojść, jeżeli CASP nie będzie sprawował efektywnej kontroli nad kryptoaktywem lub środkiem dostępowym do kryptoaktywa klienta również w wypadku wszelkich innych usług aniżeli dostarczanie portfeli niepowierniczych.

Na pozytywną ocenę zasługuje fakt, że MiCAR wprowadza dla CASP świadczących analizowaną usługę wiele istotnych obowiązków o charakterze publicznoprawnym. Za szczególnie istotne należy uznać obowiązki w zakresie operacyjnego, technologicznego i prawnego wydzielenia kryptoaktywów klientów, których praktyczne stosowanie może rodzić jednak wątpliwości. Przede wszystkim zapewnienie należytej ochrony klientów wobec wierzycieli CASP, szczególnie w wypadku upadłości lub restrukturyzacji CASP, dla swojej skuteczności wymaga podjęcia inicjatywy legislacyjnej właściwych państw członkowskich UE. W sferze prywatnoprawnej rozporządzenie MiCAR wprowadza z kolei minimalne wymagania dotyczące obowiązku zawarcia, jak i treści umowy CASP z odbiorcą usługi zapewniania przechowywania kryptoaktywów i administrowania nimi w imieniu klientów. W MiCAR ustanowiono również minimalne obowiązki informacyjne, a także w ograniczony sposób uregulowano kwestię odpowiedzialności CASP wobec klienta.

Wielość obowiązków nałożonych na CASP w MiCAR, które są inspirowane podobnymi rozwiązaniami obowiązującymi już w ramach TradFi, w zestawieniu z szerokim zakresem przedmiotowym omawianej usługi, pozwala sądzić, że regulacja ta zabezpieczy interesy użytkowników na co najmniej podstawowym poziomie. Na pozytywną ocenę zasługuje przy tym fakt, że wymagania stawiane CASP podlegają szczegółowemu badaniu w ramach procedury zezwoleniowej oraz notyfikacyjnej. W ich ramach podmiot ubiegający się o status CASP musi przedstawić wyczerpująco dowody zgodności z wypełnianiem obowiązków o charakterze zarówno prywatno-, jak i publicznoprawnym przewidzianych w MiCAR, w szczególności przedstawiając opis polityki w zakresie przechowywania i administrowania, a także opis procedury wyodrębnienia kryptoaktywów, zgodnie z wymogami odpowiednich rozporządzeń delegowanych 2025/303¹³ oraz 2025/305¹⁴. Ostatecznie to jednak praktyka stosowania regulacji MiCAR, w tym praktyka nadzorcza, będą pozwalały rozstrzygnąć, czy mechanizmy przewidziane w MiCAR okażą się skuteczne i znacząco przyczynią się do ograniczenia liczby występujących nadużyć rynkowych lub innych zdarzeń naruszających interesy klientów.

¹³ Rozporządzenie delegowane Komisji (UE) 2025/303 z dnia 31 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu do regulacyjnych standardów technicznych określających informacje, które mają być przekazywane przez niektóre podmioty finansowe w powiadomieniu o zamiarze świadczenia usług w zakresie kryptoaktywów, Dz.U. L, 2025/303, 20.02.2025.

¹⁴ Rozporządzenie delegowane Komisji (UE) 2025/305 z dnia 31 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu do regulacyjnych standardów technicznych określających informacje, które należy zawrzeć we wniosku o zezwolenie na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów, Dz.U. L, 2025/305, 31.03.2025.

Bibliografia

Arner D., Zetsche D., Buckley R., Kirkwood J. (2023), *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022–2023*, University of Hong Kong Faculty of Law Research Paper, 2023/19.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE, Dz.U. L 337 z 23.12.2015, s. 35–127.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE, Dz.U. L 156 z 19.06.2018.

Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS), Dz.U. L 302 z 17.11.2009, s. 32–96.

Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010, Dz.U. L 174 z 1.07.2011, s. 1–73.

Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz.U. L 173 z 12.06.2014, s. 349–496.

Europejski Urząd Nadzoru Bankowego (2025), Joint Report, Recent developments in crypto-assets (Article 142 of MiCAR), https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets__Art_142_MiCA_.pdf (dostęp: 10.05.2025).

Gudowski J. (2017), 'Art. 835', [w:] T. Bielska-Sobkowicz, H. Ciepla, P. Drapała, M. Sychowicz, R. Trzaskowski, T. Wiśniewski, C. Żuławska, J. Gudowski (red.), *Kodeks cywilny. Komentarz. Tom V. Zobowiązania. Część szczegółowa*, wyd II, Warszawa: Wolters Kluwer.

Kokorin I. (2023), *The Anatomy of Crypto Failures and Investor Protection Under MiCAR*, „Forthcoming in the Capital Markets Law Journal”.

Ossio D., Nixon L., Yates M. (2023), *Custody of Cryptoassets: Moving Towards Industry Best Practice*, <https://financialmarketstoolkit.cliffordchance.com/en/financial-markets-resources/resources-by-type/guides/custody-of-cryptoassets--moving-towards-industry-best-practice--.html> (dostęp: 10.05.2025).

Rozporządzenie delegowane Komisji (UE) 2025/303 z dnia 31 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu do regulacyjnych standardów technicznych określających informacje, które mają być przekazywane przez niektóre podmioty finansowe w powiadomieniu o zamiarze świadczenia usług w zakresie kryptoaktywów, Dz.U. L, 2025/303, 20.02.2025.

Rozporządzenie delegowane Komisji (UE) 2025/305 z dnia 31 października 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu

do regulacyjnych standardów technicznych określających informacje, które należy zawrzeć we wniosku o zezwolenie na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów, Dz.U. L, 2025/305, 31.03.2025.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937, Dz.U. L 150 z 9.06.2023, s. 40–205.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012, Dz.U. L 257 z 28.08.2014, s. 1–72.

„Safekeeping” (b.d.) Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/safekeeping> (dostęp: 10.05.2025).

UNIDROIT (Międzynarodowy Instytut Unifikacji Prawa Prywatnego) (2023), *Principles On Digital Assets And Private Law*, International Institute for the Unification of Private Law, <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf> (dostęp: 10.05.2025).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2024 r. poz. 1061 z późn. zm.).

Völkel O. (2023), *MiCAR versus MiFID – Wann ist ein vermögenswertreferenzierter Token kein Finanzinstrument?*, „Zeitschrift für Finanzmarktrecht“.