TRANSAKCJE

Kryptowaluty jako narzędzie prania brudnych pieniędzy

kancelarie rp

Anonimowa i zdecentralizowana forma przenoszenia wartości za pomocą kryptowalut powoduje, że mogą być wykorzystywane do prania „brudnych" pieniędzy lub do obchodzenia sankcji gospodarczych.

KRZYSZTOF ROŻKO
MATEUSZ PISARSKI

Wzrost popularności kryptowalut, ich zdecentralizowany charakter, anonimowa natura oraz ograniczona kontrola regulacyjna sprawiają, że coraz częściej stanowią one narzędzie legalizacji środków uzyskiwanych z działalności przestępczej. Ponadto sam obrót kryptoaktywami wiąże się z szeregiem ryzyk, do których zalicza się m.in. wysoką zmienność ich wartości, ich wysoce spekulatywny charakter, brak jednoznacznej i powszechnie akceptowalnej wartości ekonomicznej oraz przede wszystkim bardzo wysokie ryzyko nadużyć i utraty środków. Wynikają one przede wszystkim z braku nadzoru działalności giełd oraz kantorów kryptowalutowych ze strony KNF (poza obszarem świadczenia usług płatniczych). W Polsce, podobnie jak w większości krajów Unii Europejskiej, aktualnie brak jest bowiem regulacji działalności dostawców usług wymiany walut wirtualnych (tzw. Crypto Assets Service Providers, CASP), poza przepisami ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (dalej: AML).

Czym są kryptowaluty

Kryptowaluty są niematerialnymi, opartymi na kryptografii (a więc systemie szyfrowania), zapisami cyfrowymi (protokół danych). Swoją popularność zawdzięczają przede wszystkim możliwości dokonywania za ich pomocą niemal natychmiastowych transakcji. Do portfela innego użytkownika docierają bowiem bezpośrednio za pomocą komputerowego algorytmu (model peer-to-peer: P2P) bez pośrednictwa jakiegokolwiek centralnego ośrodka (np. banku). Przy czym, mimo pewnych wątpliwości terminologicznych, ustawodawca zalicza je do kategorii walut wirtualnych, obok scentralizowanych walut wirtualnych używanych np. w grach (np. WoW Gold, czy Linden Dollars).

Budowa kryptowalut opiera się na chronologicznym łańcuchu bloków (technologia Blockchain), w których poprzez ciąg znaków (34-cyfrowy) na stałe szyfrowane są informacje o dokonywanych kolejno transakcjach (wartości transakcji, adresy kryptowalutowych kont nadawców i odbiorców, kwoty transakcji oraz daty i godziny ich dokonania). Wobec tego, mimo że co do zasady charakteryzują się wysoką anonimowością oraz poufnością, to analiza blockchain-u pozwala na identyfikację konta, z którego najczęściej przeprowadzane są transakcje, a w konsekwencji na identyfikację podejrzanych aktywności, w tym związanych z praniem pieniędzy.

Pranie brudnych pieniędzy

Proces prania brudnych pieniędzy co do zasady obejmuje szereg czynności służących utajnieniu źródeł środków finansowych pochodzących z tzw. pierwotnych (bazowych) przestępstw, takich jak np. oszustwa, kradzieże czy handel narkotykami. Zazwyczaj składają się na niego trzy etapy, a mianowicie:

- lokowanie „brudnych" środków,
- maskowanie ich pochodzenia oraz
- integrowanie, czyli wtórne wprowadzanie do obrotu.

Stosunkowo anonimowa i zdecentralizowana forma przenoszenia wartości za pomocą kryptowalut powoduje, że mogą być wykorzystywane do prania „brudnych" pieniędzy lub też do obchodzenia sankcji gospodarczych (np. nakładanych na Rosję). Natychmiastowość transakcji realizowanych przy pomocy kryptowalut powoduje, że mogą stanowić narzędzie przestępców, w szczególności w fazie lokowania polegającego na wprowadzaniu nielegalnych funduszy do systemu finansowego oraz maskowania opierającego się na tworzeniu sieci transferów, celem ukrycia ich pierwotnego pochodzenia.

Najpopularniejszą metodą służącą tym celom jest tzw. mieszanie kryptowalut (ang. cryptocurrency tumbler) polegające na kumulowaniu szeregu krypto-transakcji, dokonywaniu ich wielokrotnego podziału oraz mieszaniu ze sobą, tak aby utrudnić prześledzenie ciągu dokonywanych z ich użyciem transakcji. Ułatwieniem tego procederu z pewnością może być wykorzystywanie kryptowalut typu „privacy" takich jak np. Monero i Zcash zaprojektowanych w celu zapewnienia ich posiadaczom zwiększonej prywatności, a ponadto lokowanie funduszy za pośrednictwem kryptowalutowych giełd typu offshore, zakładanych w rajach podatkowych nieposiadających odpowiedniego poziomu regulacji i nadzoru. Inną metodą stosowną przez przestępców jest także lokowanie środków pieniężnych na kontach bankowych za pośrednictwem tzw. słupów, a następnie nabywanie kryptoaktywów za pomocą fikcyjnych kont kryptowalutpwych z wykorzystaniem narzędzi maskujących tożsamość nadawców i odbiorców oraz ich adresy IP (sieć TOR, Darknet).

Inwestujący w tego typu aktywa powinni również uważać na nieuczciwe zbiórki wykorzystujące mechanizm ICO (emisja cyfrowych monet), w ramach których obiecywane kryptoaktywa nie zostają w rzeczywistości wyemitowane albo których emitenci po uzyskaniu finansowania „znikają" oraz na piramidy finansowe (schemat Ponziego) oferujące w zamian za wprowadzanie innych inwestorów do danego systemu kryptaktywów możliwość nabycia nieprzedstawiających realnej wartości kryptowalut.

Narzędzia przeciwdziałania praniu pieniędzy

Podmioty świadczące usługi w obszarze walut wirtualnych (wymiany pomiędzy walutami wirtualnymi, walutami wirtualnymi oraz walutami emitowanymi przez państwo oraz pośrednictwa w tym obszarze i prowadzenia rachunków), jako instytucje obowiązane w świetle przepisów ustawy AML, chcąc uchronić się przed ryzykiem wykorzystania ich usług do prania „brudnych" pieniędzy powinny poświecić szczególną uwagę: odpowiedniej aplikacji w ramach swoich struktur regulacji AML/CFT i procedur KYC, szczegółowej analityce danych, w tym dokonywanych przez klientów transakcji oraz podejmowaniu innych inicjatyw samoregulacyjnych i kampanii edukacyjnych. Przy czym w pierwszej kolejności powinny zadbać o dokonanie wpisu do rejestru walut wirtualnych prowadzonego przez Generalnego Inspektora Informacji Finansowej (art. 129m AML) oraz wytypowanie w ramach swoich struktur organizacyjnych osób odpowiedzialnych za realizację obowiązków i przestrzeganie procedur AML (art. 8 AML).

Ponadto każdej transakcji z zakresu obrotu walutami wirtualnymi powinno towarzyszyć badanie ryzyka AML ze szczególnym uwzględnieniem (zgodnie z art. 33 ust. 3 AML):

- rodzaju obsługiwanego inwestora,
- obsługiwanego obszaru geograficznego,
- przeznaczenia rachunku, na którym przechowywane są kryptoaktywa,
- ich rodzaju,
- sposobu dystrybucji,
- poziomu wartości majątkowych deponowanych przez inwestora lub wartości przeprowadzonych transakcji.

Z kolei wewnętrzne procedury AML powinny uwzględniać także możliwość anonimowego zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń przepisów AML (art. 53 ust. 1 AML).

Podmiot zajmujący się obrotem walutami wirtualnymi winien podejmować również czynności z zakresu identyfikacji inwestora i beneficjenta rzeczywistego środków pochodzących z kryptoaktywów (weryfikacja tożsamości i ustalanie struktury własności i kontroli) oraz monitorowania jego stosunków gospodarczych (analiza transakcji, źródeł pochodzenia wartości majątkowych, aktualizacja dokumentów, danych i informacji ich dotyczących) (art. 34 ust. 1 AML), w szczególności w przypadku udziału w transakcji okazjonalnej z wykorzystaniem waluty wirtualnej o równowartości 1000 euro lub większej (art. 35 ust. 1 pkt 2 lit. c AML).

Niemniej ważnymi obowiązkami podmiotu obowiązanego są również:

- wyjaśnianie rozbieżności między własnymi ustaleniami a danymi zawartymi w Centralnym Rejestrze Beneficjentów Rzeczywistych o beneficjencie rzeczywistym klienta oraz
- podejmowanie czynności celem wyjaśnienia ich przyczyn (art. 61 a ust. 1 AML), a także
- zapewnianie udziału osób wykonujących obowiązki związane z AML w programach szkoleniowych (w formie kursów e-learningowych lub szkoleń stacjonarnych) (art. 52 ust. 1 AML).

Ponadto tego typu podmioty powinny zwracać szczególną uwagę na informacje, jakimi posługują się w materiałach promocyjnych. Wbrew bowiem narracji, jaką posługują się niektóre z nich w przestrzeni medialnej, KNF nie licencjonuje, nie rejestruje ani nie nadzoruje giełd oraz kantorów kryptowalut. Komisja „nie zatwierdza" także tego rodzaju działalności ani nie jest wyposażona w narzędzia umożliwiające pomoc osobom poszkodowanym w wyniku ewentualnego upadku giełdy kryptowalut. Ponadto giełdy i kantory kryptowalut nie zapewniają ochrony środków klientów przewidzianej np. dla banków czy instytucji płatniczych, m.in. przed ewentualnymi roszczeniami wierzycieli tych podmiotów oraz nie są wyłączone z masy upadłościowej.

Kary i sankcje związane z AML a kryptowaluty

Za naruszenia przepisów AML podmioty obowiązane działające na rynku kryptowalut ponoszą przede wszystkim odpowiedzialność administracyjną. Przykładowo niewykonanie obowiązku rejestracyjnego przez podmiot prowadzący działalność w zakresie walut wirtualnych zagrożone jest karą pieniężną o wartości do 100 000 zł (art. 153b AML). Jednak kwalifikacja ich zachowania, jako czynu zabronionego, może prowadzić również do odpowiedzialności karnej zarówno osób nimi zarządzających, jak i osób odpowiedzialnych za zapewnienie zgodności ich funkcjonowania z regulacjami AML.

Pieniężne kary administracyjne nakładane na tego typu podmioty mogą sięgać nawet dwukrotności kwoty korzyści osiągniętej lub straty uniknięcie w wyniku naruszenia albo – gdy nie jest możliwe ustalenie kwoty tej korzyści lub straty – nawet 1 mln euro (art. 150 ust. 1 i 2 AML).

Z kolei w ramach odpowiedzialności karnej osoba niewywiązująca się z realizacji obowiązku przekazywania GIIF informacji o okolicznościach, tudzież transakcjach, rachunkach oraz osobach mogących wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu albo przekazująca nieprawdziwe lub zatajająca prawdzie dane dotyczące transakcji może zostać skazana na karę grzywny i/lub kary pozbawienia wolności od 3 miesięcy do 5 lat za (art. 156 ust. 10 AML). Przy czym kwalifikacja działania podmiotu odpowiedzialnego za realizację obowiązków AML jako przestępstwa prania pieniędzy może prowadzić do orzeczenia kary pozbawienia wolności od 6 miesięcy do 12 lat za przestępstwo w typie podstawowym oraz od roku do nawet lat 10 za popełnienie go w typie kwalifikowanym polegającym na działaniu w porozumieniu z innymi osobami lub na osiągnięciu z niego znacznej korzyści majątkowej (art. 299 ust. 1 – 6 k.k.). /®

ZDANIEM AUTORÓW

Krzysztof Rożko

radca prawny, Wspólnik Zarządzający w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

MAT.PRAS.

Mateusz Pisarski

radca prawny w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

MAT.PRAS.

Z 30 grudnia 2024 r. na obszarze Unii Europejskiej zacznie obowiązywać (z pewnymi wyjątkami) opublikowane 9 czerwca 2023 r. rozporządzenie Market in Crypto-Asset (MiCA). Jego celem jest przede wszystkim zwiększenie ochrony konsumentów przed ryzykiem związanym z inwestowaniem w kryptoaktywa. W przyszłości można spodziewać się również wprowadzania kolejnych regulacji ograniczających wykorzystywanie kryptowalut w procederach prania pieniędzy. Organizacje międzynarodowe (m.in. FATF oraz UE) oraz krajowe (KNF, GIIF, MF) stoją jednak przed trudnym wyzwaniem, ponieważ kolejne regulacje muszą pogodzić specyfikę kryptowalut, ochronę danych inwestorów, efektywność AML i dalszy rozwój technologii cyfrowych.

Niezależnie od powyższego z pewnością każda instytucja obowiązana winna dążyć do jak najszerszego wywiązywania się z obowiązków związanych z AML nie tylko ze względu na grożące w tym zakresie sankcje administracyjne, lecz również ze względu na możliwość kwalifikacji działań lub zaniechań osób odpowiedzialnych za realizację obowiązków AML w ramach jej struktur jako przestępstw zagrożonych nawet karą pozbawienia wolności. W tym zakresie, ze względu na złożoność przedmiotowych obowiązków oraz celem redukcji ryzyka prawnego, pomocne może okazać się zasięgnięcie pomocy podmiotów profesjonalnie zajmujących się aplikacją stosownych rozwiązań w strukturach jednostek obowiązanych.