

dr Jacek Charatynowicz

Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie

e-mail: j.charatynowicz@gmail.com

ORCID: 0000-0003-0484-4078

# Zagrożenia dla rynku finansowego związane z praniem pieniędzy a technologie FinTech – identyfikacja zjawiska oraz metody przeciwdziałania

## I. Wstęp

Współczesne, złożone i zmienne, środowisko bezpieczeństwa uwarunkowane jest wieloma zagrożeniami, procesami i trendami, istotnymi z punktu widzenia bezpieczeństwa państwa, jego obywateli, jak też organizacji międzynarodowych czy podmiotów pozapaństwowych. Zagrożenie – jak podaje *Słownik terminów z zakresu bezpieczeństwa narodowego* – to „sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenia: polityczne, ekonomiczne (gospodarcze), psychospołeczne, ekologiczne, wewnętrzne i inne”<sup>1</sup>.

Istotnym zagrożeniem dla bezpieczeństwa wewnętrznego państwa jest przestępczość w różnych jej wymiarach: ekonomicznym, kryminalnym, narkotykowym, korupcyjnym czy występującym w cyberprzestrzeni, zarówno o charakterze pospolitym, jak i zorganizowanym. Rozważając kwestię przyczyn rozwoju przestępczości, w tym przestępczości zorganizowanej, należy stwierdzić, iż główną jej determinantą jest korzyść finansowa uzyskiwana w wyniku działania przestępczego. Do tego należy dodać również czynniki społeczno-ekonomiczne,

psychologiczne, konflikty grupowe (walka o wpływy) oraz działania państw o charakterze totalitarnym.

Korzyści finansowe pochodzące z przestępczości mogą być wykorzystywane do następujących celów: (1) bieżącej konsumpcji; (2) nabywania nieruchomości, pojazdów, złota, dzieł sztuki czy innych dóbr luksusowych; (3) finansowania innych przedsięwzięć przestępczych; (4) korpupowania funkcjonariuszy państwowych; (5) użycia w obrocie gospodarczym.

Nielegalnie uzyskane korzyści mogą być ponadto legalizowane za sprawą różnego rodzaju przedsięwzięć organizacyjnych, finansowych czy gospodarczych. W tym celu sprawcy wykorzystują luki w systemie przeciwdziałania praniu pieniędzy oraz podatne instrumenty – wartości majątkowe, których specyfika konstrukcji technologicznej i prawnej sprzyja ich wykorzystaniu do działalności przestępczej. Pranie pieniędzy może powodować różne skutki w obrębie procesów mikro- i makroekonomicznych<sup>2</sup> dla rynku, jednak przede wszystkim proceder ten powoduje: (1) utratę wiarygodności państwa; (2) naruszenie stabilności systemu finansowego, z uwypukleniem systemu walutowego, podatkowego i bankowego; (3) zakłócenie działalności instytucji i mechanizmów gospodarki rynkowej; (4) wzrost zjawisk korupcyjnych w obrębie służby publicznej i w sferze prywatnej; (5) naruszenie zasad uczciwej konkurencji

oraz praktyk rynkowych; (6) destabilizację rynku i odpływ kapitału (mimo że w początkowym okresie pranie pieniędzy może stanowić czynnik kapitałotwórczy). Dlatego też legalizowanie korzyści pochodzących z różnych form przestępczości (przestępczości pospolitej, poważnej czy zorganizowanej) stanowi tak istotne zagrożenie dla bezpieczeństwa finansowego państwa.

Przedmiotem rozważań podejmowanych w niniejszym artykule będzie kwestia nowych technologii FinTech, wykorzystywanych przez grupy przestępcze do prania pieniędzy, a w szczególności wyodrębniony z tego systemu segment DeFi, czyli kryptoaktywów. Analizie poddane zostaną także sposoby przeciwdziałania temu zjawisku o charakterze regulacyjnym, operacyjnym czy też w kontekście działań strategicznych państwa.

W artykule wykorzystano metody teoretyczne związane z analizą i syntezą literatury przedmiotu, aktów prawnych, dokumentów analitycznych i strategicznych z obszaru kryptoaktywów, bezpieczeństwa oraz przeciwdziałania zagrożeniom. Artykuł rozpoczyna się od wprowadzenia, w którym zarysowano problematykę rynku DeFi i kryptoaktywów, natomiast w kolejnych częściach przedstawiono szczegółowe rozważania dotyczące prawnego i instytucjonalnego otoczenia kryptoaktywów, zagrożeń związanych z praniem pieniędzy oraz możliwych do zastosowania metod prawnych, organizacyjnych i operacyjnych, służących przeciwdziałaniu im.

## II. Identyfikacja zjawiska prania pieniędzy

Zagrożenia związane z praniem pieniędzy obejmują wszystkie działania służące ukrywaniu nielegalnych źródeł środków finansowych i nadawaniu im pozorów legalności w celu umożliwienia ich ponownego zainwestowania w legalnym obrocie gospodarczym<sup>3</sup>. Nie ma przy tym znaczenia, czy podejmowane działania mają charakter prosty czy złożony, czy realizowane są z udziałem transakcji gotówkowych, na rynku finansowym (transakcje bankowe, inwestycyjne, ubezpieczeniowe) czy pozafinansowym (nieruchomości, rynek dzieł sztuki, kryptowaluty). Ważne jest to, że ich jedynym celem jest nadanie pozorów legalności wartościom majątkowym pochodzącym z aktywności przestępczej.

Regulacje związane z prawnokarnym ujęciem przestępstwa prania pieniędzy pojawiły się w polskim systemie prawnym w latach dziewięćdziesiątych, przy czym były to przepisy fragmentaryczne, które nie stanowiły wystarczającego narzędzia dla służb państwowych w zakresie skutecznego ich ścigania i zwalczania<sup>4</sup>. W 1997 r. przestępstwo prania pieniędzy zostało umiejscowione w art. 299 Kodeksu karnego, w rozdziale *Przestępstwa przeciwko obrotowi gospodarczemu*. W Ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do

obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł<sup>5</sup> wprowadzono z kolei przepisy mające na celu administracyjne przeciwdziałanie praniu pieniędzy. Powołano wówczas Generalnego Inspektora Informacji Finansowej (GIIF) oraz stworzono system przeciwdziałania praniu pieniędzy, który wprowadził mechanizmy związane z identyfikowaniem podejrzanych transakcji i ich raportowności do GIIF.

Zgodnie z obowiązującymi przepisami prawa przez pranie pieniędzy należy rozumieć:

- przyjmowanie, posiadanie, używanie, przekazywanie lub wywożenie za granicę, ukrywanie, dokonywanie transferu lub konwersji środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innego mienia ruchomego lub nieruchomości, pochodzących z korzyści związanych z popełnieniem czynu zabronionego;
- pomaganie w przenoszeniu własności ww. wartości majątkowych lub ich posiadaniu;
- podejmowanie innych czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie przestępczego pochodzenia lub miejsca umieszczenia ww. wartości majątkowych, ich wykrycie, zajęcie albo orzeczenie przepadku.

W ten sposób opisano szeroki wachlarz sprawczy legalizowania korzyści z wykorzystaniem wielu *modi operandi*, jak również szerokiej gamy wartości majątkowych.

W związku z międzynarodowymi implikacjami zagrożeń związanych z praniem pieniędzy dla wiarygodności finansowej państw, korporacji, podmiotów gospodarczych czy też powiązań finansowych zachodzących pomiędzy wymienionymi podmiotami, zarówno w sferze stosunków międzynarodowych, jak również na poziomie operacyjnym, tworzone są rozwiązania instytucjonalne i prawne zmierzające do identyfikowania i mitygacji tych zagrożeń.

W 1989 r. podczas szczytu państw grupy G7 w Paryżu utworzono Grupę Specjalną ds. Przeciwdziałania Praniu Pieniędzy (The Financial Action Task Force, FATF), zajmującą się analizą i oceną zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu. Znacznym osiągnięciem grupy było wydanie czterdziestu rekomendacji określających standardy instytucjonalne i operacyjne w zakresie identyfikowania ryzyka prania pieniędzy oraz finansowania terroryzmu i proliferacji broni masowego rażenia.

FATF już w 2014 r. opublikował raport *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko w zakresie prania pieniędzy oraz finansowaniu terroryzmu*. Zdefiniowano w nim wirtualną walutę jako cyfrową reprezentację wartości, która może być przedmiotem obrotu cyfrowego i działa jako środek wymiany i/lub środek przechowywania wartości, ale nie posiada statusu

prawnego środka płatniczego w jakiegokolwiek jurysdykcji<sup>6</sup>. W związku z podobieństwem kryptoaktywów do tradycyjnych rozwiązań finansowych FATF alarmował, iż z uwagi na anonimowy charakter obrotu tym instrumentem może on implikować ryzyko prania pieniędzy. FATF rekomendował ponadto, aby podmioty uczestniczące w konwersji kryptowalut na walutę FIAT objąć rozwiązaniami prawnymi w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

Kolejnym podmiotem zaangażowanym w tworzenie i audyt międzynarodowych standardów w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest Komitet MONEYVAL (ang. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism), tj. Komitet Ekspertów ds. Ewaluacji Środków Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu. Organizacja ta jest utworzonym w 1997 r. organem Rady Europy, którego celem jest monitoring i ocena zgodności działalności państw członkowskich MONEYVAL z podstawowymi międzynarodowymi zasadami dotyczącymi AML/CTF, a także efektywności ich implementacji. Komitet jest ciałem regionalnym funkcjonującym podobnie jak FATF oraz członkiem stowarzyszonym tej organizacji<sup>7</sup>.

Instytucją europejską o charakterze policyjnym jest Europol, czyli organ ścigania Unii Europejskiej (UE), którego głównym celem jest przyczynianie się do zwiększania bezpieczeństwa obywateli/instytucji UE. Z danych Europolu wynika, że grupy przestępcze i terrorystyczne stanowią poważne zagrożenie dla bezpieczeństwa wewnętrznego UE oraz dla bezpieczeństwa i bytu jej obywateli. Największymi zagrożeniami dla tego bezpieczeństwa są: (1) terroryzm; (2) międzynarodowy nielegalny obrót środkami odurzającymi i pranie pieniędzy; (3) zorganizowane oszustwa; (4) fałszowanie euro; (5) przemyt ludzi<sup>8</sup>.

Europol oprócz koordynowania, analiz problematyki kryptoaktywów i inicjowania działań policji krajów UE organizuje konferencje naukowe dotyczące teoretycznych i praktycznych aspektów analizy *blockchain*. Ponadto dokonuje analizy obszarów i kierunków rozwoju przestępczości zorganizowanej, przestępczości finansowej i cyberprzestępczości. W ramach tych działań identyfikuje przypadki wykorzystywania kryptowalut do przestępczości finansowej, cyberprzestępczości, a w szczególności prania pieniędzy<sup>9</sup>.

### III. FinTech a kryptoaktywa

Zgodnie ze słownikiem pojęć Polskiego Funduszu Rozwoju termin FinTech (ang. *Financial Technology*) oznacza innowacyjne usługi finansowe działające wyłącznie w sieci opartej na technologii informacyjnej<sup>10</sup>. Termin ten nie określa precyzyjnie tego, jaki segment rynku obejmuje

przedmiotowe zagadnienie – może to być np. sektor bankowy, usług płatniczych, ubezpieczeniowy, pożyczek, płatności mobilnych czy internetowych. Ponadto nie jest istotne, czy sektor branży FinTech objęty jest nadzorem Komisji Nadzoru Finansowego (KNF) lub innego regulatora. Istotną kwestią jest za to innowacyjność rozwiązania FinTech w sektorze usług płatności, pożyczek, wymiany waluty, porównywarek internetowych itd.

Jednym z segmentów rynku FinTech jest rynek DeFi. DeFi (zdecentralizowane finanse) to zbiorczy termin dla usług finansowych opartych na publicznych łańcuchach bloków, głównie ethereum<sup>11</sup>. Od pierwszych transakcji zrealizowanych w 2009 r. rynek kryptowalut podlegał oddziaływaniom i przeobrażeniom prawnym, organizacyjnym, ekonomicznym i instytucjonalnym. Ewolucji, a w zasadzie swoistej rewolucji, uległa jego technologia, stanowiąca podstawę funkcjonowania kryptoaktywów.

Termin kryptoaktywo ma szersze znaczenie niż inne pojęcia odnoszące się do technologii zdecentralizowanych rejestrów, bowiem obejmuje kryptowaluty i tokeny, w tym tokeny płatnicze, inwestycyjne i użytkowe. Zgodnie z definicją opracowaną przez KNF „kryptoaktywo to cyfrowe odwzorowanie relacji zachodzących pomiędzy uczestnikami sieci DLT, któremu w ramach tej sieci można przypisać uprawnienia o zróżnicowanym charakterze, w tym np. uprawnienia o charakterze majątkowym. Z tego też względu może być ono akceptowane przez inne podmioty rynkowe oraz stać się między tymi podmiotami przedmiotem obrotu jako zapisane z wykorzystaniem zabezpieczeń kryptograficznych przy wykorzystaniu technologii DLT (w tym Blockchain), w ramach którego wiązka uprawnień związana z kryptoaktywem może przybrać postać określaną jako token”<sup>12</sup>.

Z raportu Chainalysis *The 2022 Geography of Cryptocurrency Report*<sup>13</sup> wynika, że Europa Wschodnia jest piątym co do wielkości rynkiem kryptowalut. Między lipcem 2021 a czerwcem 2022 r. przetransferowano tu 630,9 mld USD, co stanowi nieco ponad 10% globalnej aktywności transakcyjnej w badanym okresie.

Ze wspomnianego raportu wynika ponadto, że cztery największe rynki kryptoaktywów tworzyły: Europa (wartość transakcji 1,3 bln USD), Ameryka Północna (1,15 bln USD), Centralna i Południowa Azja i Oceania (932 mld USD) i Wschodnia Azja (777,5 mld USD).

W internetowych źródłach na temat rynku kryptowalut można natrafić na informację, iż w sieci Internet usługi w zakresie wymiany kryptowalut na walutę FIAT w języku polskim oferowało co najmniej 27 kantorów i 45 giełd kryptowalut<sup>14</sup>. Inne źródło podaje z kolei, że obecnie (stan na dzień 3 marca 2022 r.) w Polsce kryptowaluty na walutę FIAT można wymienić w co najmniej 204 bitomatach<sup>15</sup>. Zgodnie z informacją Izby Administracji Skarbowej w Katowicach 1 stycznia 2022 r. w rejestrze działalności w sektorze walut wirtualnych było

odnotowanych 136 podmiotów, natomiast 30 maja 2023 r. w tym samym rejestrze figurowało już 777 podmiotów.

Przedstawione dane wskazują, w jak szybkim tempie rozwija się rynek kryptoaktywów, co przy braku stosownych przepisów określających ich otoczenie regulacyjne (braku właściwego regulatora czy instytucji chroniących inwestora indywidualnego) sprawia, że rynek ten jest szczególnie zagrożony ryzykiem wykorzystania jego mechanizmów i instrumentów do różnego rodzaju przestępstw, w tym prania pieniędzy.

#### **IV. Przeciwdziałanie zagrożeniom związanym z kryptoaktywami – działania regulacyjne, instytucjonalne i operacyjne**

Kryptoaktywa – z uwagi na ich cechy charakterystyczne, takie jak anonimowy charakter obrotu, brak szczególnych wymogów regulacyjnych czy ograniczających obrót, szybkość realizowanych transakcji i ich kryptograficzne zabezpieczenie – mogą być wykorzystywane do działań niezgodnych z prawem. Zaliczyć do nich można: (1) ukrywanie mienia pochodzącego z różnego rodzaju przestępstw; (2) pranie pieniędzy; (3) nabywanie towarów, którymi obrót jest zabroniony; (4) czerpanie korzyści z wymuszeń rozbójniczych lub porwań czy też (5) różnego rodzaju oszustwa finansowe związane z emisją kryptoaktywów.

Aktem prawnym określającym zadania systemu podmiotów zaangażowanych w przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu jest Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (u.p.p.f.t.)<sup>16</sup>, na mocy której utworzono krajowy system przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Na system ten składa się działalność GIIF, instytucji obowiązanych i jednostek współpracujących.

Głównym elementem systemu jest GIIF. Do jego zadań należy uzyskiwanie, gromadzenie, przetwarzanie i analizowanie informacji w trybie określonym w ustawie oraz podejmowanie działań w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, jak również w szczególności:

- analizowanie informacji dotyczących wartości majątkowych, co do których Generalny Inspektor powziął podejrzenie, że mają związek z przestępstwem prania pieniędzy lub finansowania terroryzmu;
- przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku;
- żądanie przekazania informacji o transakcjach i ich udostępnianie;
- przekazywanie uprawnionym organom informacji i dokumentów uzasadniających podejrzenie popełnienia przestępstwa;

- wymiana informacji z jednostkami współpracującymi;
- sporządzanie krajowej oceny ryzyka prania pieniędzy i finansowania terroryzmu oraz strategii przeciwdziałania tym przestępstwom we współpracy z jednostkami współpracującymi i instytucjami obowiązany;
- sprawowanie kontroli nad przestrzeganiem przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
- wydawanie decyzji w sprawach wpisu na listę osób i podmiotów, wobec których stosuje się szczególne środki ograniczające wobec osób i podmiotów, lub skreślenia z niej oraz prowadzenie tej listy;
- współpraca z właściwymi organami innych państw, a także zagranicznymi instytucjami i międzynarodowymi organizacjami zajmującymi się przeciwdziałaniem praniu pieniędzy lub finansowaniu terroryzmu;
- nakładanie kar administracyjnych<sup>17</sup>.

Kolejnym elementem systemu są instytucje obowiązkowe, czyli instytucje finansowe i pozafinansowe, na które nałożono obowiązek w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu<sup>18</sup>, w tym m.in. w obszarze:

- stosowania wobec klientów tzw. środków bezpieczeństwa finansowego<sup>19</sup>;
- raportowania do GIIF informacji o transakcjach stanowiących równowartość 15 tys. euro (w przypadku realizacji transakcji gotówkowych – 10 tys. euro) i transakcjach podejrzanych;
- analizy ryzyka w zakresie identyfikowania transakcji podejrzanych;
- stworzenia technologicznych możliwości do wstrzymania transakcji/blokady rachunku.

Jednostki współpracujące to natomiast organy administracji rządowej, organy jednostek samorządu terytorialnego oraz inne państwowe jednostki organizacyjne, a także Narodowy Bank Polski, KNF i Najwyższa Izba Kontroli<sup>20</sup>.

Świadczenie usług w zakresie obrotu lub wymiany między kryptoaktywami a walutą fiducyjną traktowane jest jako działalność regulowana zapisami Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców i może być wykonywane po uzyskaniu wpisu do rejestru działalności w zakresie obrotu walutami wirtualnymi. Niespełnienie tego wymogu regulacyjnego implikuje karę administracyjną do kwoty 100 tys. zł. Zgodnie z nowymi przepisami działalność w zakresie obrotu walutami wirtualnymi może być prowadzona jedynie przez osoby fizyczne, które posiadają wiedzę lub doświadczenie w tym zakresie i nie zostały prawomocnie skazane za umyślne przestępstwa<sup>21</sup>.

Mankamentem tych rozwiązań jest brak przepisów prawnych, które penalizowałyby zachowanie polegające na prowadzeniu działalności gospodarczej w zakresie

obrotu walutami wirtualnymi bez wpisu do rejestru. Nie określono ponadto właściwego regulatora tego rynku, czyli organu nadzorczego, jakim mogłyby być KNF czy Narodowy Bank Polski.

Z uwagi na konieczność zapewnienia transparentności rynku kryptowalut oraz bezpieczeństwo uczestników transakcji konieczne było wprowadzenie do u.p.p.p.f.t. regulacji dotyczących kryptowalut, a w szczególności ich definicji ustawowej, definicji rachunku i transakcji.

Zgodnie z tą ustawą wirtualne waluty to „cyfrowe odwzorowanie wartości, które nie jest:

- a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
- b) międzynarodową jednostką rozrachunkową ustanowianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
- c) pieniądzem elektronicznym w rozumieniu Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,
- d) instrumentem finansowym w rozumieniu Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
- e) wekslem lub czekiem;

oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego”.

Warto zwrócić uwagę na ostatnią część przytoczonego fragmentu ustawy, gdyż zawiera on pierwszą w polskim prawodawstwie definicję waluty wirtualnej, która jest wykorzystywana pomocniczo przez nadzór finansowy czy organy podatkowe na potrzeby działań realizowanych na podstawie właściwych ustaw.

Na gruncie u.p.p.p.f.t. wprowadzono również definicję transakcji i rachunku wirtualnej waluty. Zgodnie z tymi regulacjami rachunek waluty wirtualnej to prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany. Transakcją to z kolei czynność prawna lub faktyczna, na podstawie której dokonuje się przeniesienia własności lub posiadania wartości majątkowych.

W kontekście przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu istotne było także wskazanie w ustawie podmiotów prowadzących działalność gospodarczą polegającą na świadczeniu usług w zakresie: (1) wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi; (2) wymiany pomiędzy walutami wirtualnymi; (3) pośrednictwa w wymianie; (4) prowadzenia rachunku.

Kolejnym aspektem regulacyjnym kryptoaktywów, istotnym z punktu widzenia przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, jest możliwość prowadzenia przez giełdy/kantory działalności gospodarczej w zakresie obrotu kryptowalutami na podstawie przepisów Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (u.u.p.). Określenie takiej formy działalności było wynikiem prac zespołu roboczego ds. rozwoju innowacji finansowych (FinTech), którego celem była identyfikacja barier natury prawnej, regulacyjnej i nadzorczej dla rozwoju branży FinTech w Polsce oraz przygotowanie propozycji sposobów ich eliminacji. Po konsultacjach prawnych ustalono najodpowiedniejszą formę prowadzenia działalności w obszarze kryptowalut, zgodną z zasadami określonymi w ustawie o usługach płatniczych, czyli małą instytucją płatniczą. Najistotniejszymi wymogami dla tej działalności są:

- uzyskanie wpisu do rejestru prowadzonego przez KNF;
- średnia całkowita kwota transakcji płatniczych wykonanych przez małą instytucję płatniczą, w tym przez agentów, za pośrednictwem których świadczy ona usługi płatnicze, nie może przekraczać kwoty 1 500 tys. euro miesięcznie w okresie 12 ostatnich miesięcy;
- posiadanie rozwiązań organizacyjnych pozwalających na wyliczenie całkowitej miesięcznej kwoty transakcji płatniczych;
- posiadanie rozwiązań w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
- łączna wysokość środków przyjętych dla jednego użytkownika nie może przekroczyć równowartości (w PLN) 2 tys. euro.

Ustawa nie wyklucza możliwości prowadzenia działalności gospodarczej przez podmioty działające na rynku kryptoaktywów w ramach innej formy usług płatniczych, np. krajowej instytucji płatniczej lub biura usług płatniczych, jednak podmioty te muszą spełniać już inne, bardziej rygorystyczne, wymogi regulacyjne.

Podmioty prowadzące działalność gospodarczą m.in. w oparciu o przepisy u.u.p. podlegają nadzorowi KNF. Celem nadzoru nad rynkiem finansowym jest zapewnienie jego prawidłowego funkcjonowania, stabilności, bezpieczeństwa i przejrzystości, a także podtrzymywanie zaufania do rynku finansowego i ochrona interesów jego uczestników<sup>22</sup>.

## V. Zagrożenia występujące na rynku DeFi – pranie pieniędzy

W odniesieniu do bezpieczeństwa rynku kryptoaktywów możemy wskazać zagrożenia o charakterze wewnętrznym, czyli „wynikające ze zbiorów różnego rodzaju okoliczności wewnętrznych, właściwych danemu podmiotowi,

które powodują lub mogą spowodować zakłócenie jego wewnętrznej stabilności i harmonijnego rozwoju w różnych przejawach jego aktywności, włącznie z osłabieniem pozycji lub nawet utratą możliwości przetrwania w środowisku jego funkcjonowania”, oraz zagrożenia zewnątrz, „wynikające ze zbiorów różnego rodzaju okoliczności pojawiających się w otoczeniu danego podmiotu, które powodują lub mogą spowodować podobne lub takie same skutki”<sup>23</sup>.

Z raportów Europolu na temat działalności zorganizowanych grup przestępczych (tzw. raport SOCTA) wynika, że wśród najczęściej wykorzystywanych metod prania pieniędzy – oprócz przemytu gotówki, wykorzystywania działalności gospodarczej i działalności wyspecjalizowanych grup – można odnotować także nowe metody płatności finansowych (w tym obrót kryptowalutami) umożliwiające ukrycie faktycznego beneficjenta transakcji.

Europol wyróżnia trzy najczęściej występujące mechanizmy wykorzystywania rynku kryptowalut do prania pieniędzy:

- wykorzystanie prowadzonej działalności gospodarczej (giełdy kryptowalutowej) w procesie legalizowania środków finansowych pochodzących z przestępczości zorganizowanej;
- wykorzystanie transakcji smurfingowych polegających na rozdrabnianiu wpłat gotówkowych na kontrolowane przez grupę przestępczą rachunki bankowe, a następnie mieszanie i transferowanie środków finansowych do giełd lub innych instytucji rynku kryptowalutowego;
- transfer środków finansowych w celu ich zalegalizowania w zagranicznych giełdach kryptowalutowych.

Uzupełniając tę kwestię, można wskazać, iż w celu zalegalizowania określonych wartości finansowych wykorzystywane są również osoby wyspecjalizowane do tworzenia szczególnych rozwiązań finansowych i pozafinansowych, jak również osoby nazywane potocznie „słupami” i „mułami”, których różni tylko świadomość uczestnictwa w procederze przestępczym.

Szczególnie istotne jest również przenikanie rynku kryptowalut do tradycyjnych rozwiązań finansowych – rynku funduszy inwestycyjnych, obrotu giełdowego, transakcji płatniczych, usług powierniczych czy emisji instrumentów kryptoaktywów – co utrudnia instytucjom obowiązany ocenę ryzyka w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

W ostatnim okresie wzrosła popularność tzw. NFT (niewymienialnych tokenów, ang. *non-fungible token*). NFT to unikatowy cyfrowy certyfikat przechowywany w łańcuchu bloków (*blockchain*), zapewniający określone prawa własności do aktywa, zwykle cyfrowego, np. cyfrowego dzieła sztuki<sup>24</sup>. NFT mogą przybierać postać

różnego rodzajów animacji, obiektów istniejących w wymiarze wirtualnym, akcji sportowych. Rekordowym jak dotąd dziełem kupionym za NFT jest wystawione na aukcji w domu aukcyjnym Christie's *Everydays – the first 5000 days* autorstwa Beeple. Jest to kolaż składający się z pięciu tysięcy grafik tworzonych przez artystę codziennie przez tyleż dni. Obraz został sprzedany na początku 2021 r. za 69 mln USD<sup>25</sup>.

Warto również wskazać, iż zagrożeniem w kontekście wykorzystania giełd/kantorów kryptowalutowych do prania pieniędzy są sankcje nakładane na obywateli Federacji Rosyjskiej odpowiedzialnych za agresję zbrojną na Ukrainę i pełniących istotne funkcje wojskowe i polityczne. „Rosjanie są jednymi z największych posiadaczy kryptowalut na świecie. Według Bloomberga, powołującego się na źródła pochodzące z ministerstwa finansów Rosji, aż 12 proc. wszystkich światowych zasobów kryptowalut znajduje się w ich rękach. Daje to więc zawrotną liczbę blisko 240 mld USD”<sup>26</sup>.

14 kwietnia 2022 r. KNF podjęła uchwałę nr 111/22 w sprawie okoliczności istotnych dla oceny rękojmi w sprawach z zakresu rynku finansowego w związku z agresją Federacji Rosyjskiej wobec Ukrainy. W dokumencie tym „rękojmia” oznacza gwarancję, zapewnienie o czymś, a więc obiektywny brak niedających się usunąć wątpliwości co do zaistnienia w przyszłości określonego stanu. Oznacza to, iż odnośnie podmiotu licencjonowanego, a także jego znaczących udziałowców oraz osób nim zarządzających – jako wywierających kluczowy wpływ na działalność tego podmiotu – nie mogą zachodzić jakiegokolwiek nieusuwalne wątpliwości, że działalność ta będzie prowadzona w sposób prawidłowy, czyli praworządny, uczciwy, transparentny, ostrożny i stabilny. Uchwała ta nie dotyczy jednak rynku kryptowalut, ponieważ nie jest on nadzorowany przez KNF.

31 lipca 2014 r. Rada UE wydała Rozporządzenie nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie, w ramach którego zastosowano ograniczenia dotyczące dostępu do rynku kapitałowego wobec niektórych instytucji finansowych. Rozporządzeniem Rady UE 2022/394 z dnia 9 marca 2022 r. w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie zmieniono zakres środków ograniczających, podkreślając, że użyte w rozporządzeniu wyrażenie „zbywalne papiery wartościowe” oznacza różne rodzaje papierów wartościowych, w tym w postaci kryptoaktywów, które podlegają zbyciu na rynku kapitałowym, z wyjątkiem instrumentów płatniczych.

W kontekście przeciwdziałania wykorzystywaniu kantoru/giełdy kryptowalutowej do prania pieniędzy oraz finansowania terroryzmu, jak również do innych przestępstw, do zadań instytucji obowiązanych należą: (1) stosowanie środków bezpieczeństwa finansowego (ustalenie

tożsamości, beneficjenta rzeczywistego i rodzaju stosunków gospodarczych); (2) sprawdzanie list sankcyjnych; (3) analiza metadanych w zakresie wykorzystywanych urządzeń i miejsc realizacji transakcji (powtarzalności tych danych i możliwości ich weryfikacji); (4) uwierzytelnianie logowania i transakcji; (5) ocena ryzyka transakcyjnego dla giełdy/kantoru; (6) analiza realizowanych transakcji kryptowalutowych; (7) analiza transakcji walutą FIAT; (8) ustalenie źródła pochodzenia wartości majątkowych lokowanych na giełdzie lub w kantorze.

GIIF 14 lipca 2014 r. wydał Komunikat w sprawie niebezpieczeństw związanych z walutami wirtualnymi w zakresie zagrożeń związanych z wykorzystaniem kryptowalut do prania pieniędzy, a ponadto sygnalizował ryzyko dotyczące możliwości wykorzystania kryptowalut w sprawozdaniach rocznych z realizacji u.p.p.p.ft.

Kwestia kryptowalut oraz ryzyka związanego z ich wykorzystaniem do prania pieniędzy, jak również finansowania terroryzmu znalazła odzwierciedlenie w opracowanej przez Komisję Europejską Ponadnarodowej ocenie ryzyka prania pieniędzy oraz finansowania terroryzmu z 27 października 2022 r. W dokumencie tym ustalono 43 rodzaje produktów i usług w ośmiu obszarach, które mogą być podatne na ryzyko prania pieniędzy oraz finansowania terroryzmu, i określono dla nich poziomy zagrożenia i podatności. W ocenie tej dla kryptoaktywów ustalono najwyższe ryzyko prania pieniędzy i finansowania terroryzmu<sup>27</sup>.

Istotną kwestią jest ujęcie ryzyka związanego z wykorzystaniem walut wirtualnych do prania pieniędzy w Krajowej ocenie ryzyka prania pieniędzy oraz finansowaniu terroryzmu. Zgodnie z rekomendacją nr 1 FATF kraj powinien identyfikować, rozumieć i oceniać ryzyko prania pieniędzy oraz finansowania terroryzmu; wyznaczyć organ lub wskazać mechanizm dla zapewnienia koordynacji działań w zakresie oceny tego ryzyka i jego mitygacji; stosować podejście oparte na ryzyku w celu zapewnienia, że środki służące przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu są odpowiednie do zidentyfikowanego ryzyka w tym obszarze. Obowiązek opracowania Krajowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu oraz jej zasady zostały wprowadzone w u.p.p.p.ft., w której określono m. in., że:

- opracowanie krajowej oceny ryzyka i jej aktualizacja muszą być dokonywane nie rzadziej niż co 2 lata;
- opracowywanie krajowej oceny dokonywane jest przez GIIF, instytucje obowiązane i jednostki współpracujące;
- opiniowanie krajowej oceny ryzyka spoczywa na Komitecie Bezpieczeństwa Finansowego, a sama ocena jest akceptowana przez ministra właściwego do spraw finansów publicznych;
- na podstawie krajowej oceny opracowuje się strategię przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu.

W Krajowej ocenie ryzyka prania pieniędzy oraz finansowania terroryzmu kryptowaluty zostały wskazane w scenariuszu ryzyka z wysokim poziomem zagrożenia. Zgodnie z przyjętą metodyką oceny poziomów zagrożenia i podatności prawdopodobieństwo wykorzystania wirtualnych walut do prania pieniędzy zostało ocenione jako wysokie (trzy punkty w czterostopniowej ocenie).

## VI. Podsumowanie

Według raportu firmy Chainalysis wartość transakcji transferowanych poprzez nielegalne adresy *blockchain* wzrosła z 18,1 mld USD w 2021 r. do 20,6 mld USD w 2022 r., a znaczna ich część (ok. 43%) pochodziła z działalności podmiotów objętych sankcjami finansowymi. Wzrosła również wartość kradzieży kryptowalut – w 2022 r. skradziono kryptowaluty o wartości ok. 3,8 mld USD, a rok wcześniej – 3,3 mld USD<sup>28</sup>.

Biorąc pod uwagę ilość kryptowalut wysyłanych z nielegalnych adresów na adresy hostowane przez usługi, można stwierdzić, że przestępcy zalegalizowali w 2022 r. kryptowalutę o wartości 23,8 miliarda USD, w stosunku do kwoty 14,2 mld USD w 2021 r.<sup>29</sup>

Polska policja nie gromadzi szczegółowych informacji statystycznych dotyczących wykorzystania kryptoaktywów do dokonywania oszustw czy prania pieniędzy. Ze sprawozdania GIIF z realizacji u.p.p.p.ft. wynika jednak, że kwota wartości majątkowych, które były przedmiotem podejrzenia przestępstwa, wyniosła w 2022 r. 2,87 mld zł, zaś rok wcześniej – 8,5 mld zł.

Mając na uwadze te dane, można wnosić, iż stale rozwijający się rynek kryptoaktywów może być wykorzystywany do legalizowania korzyści pochodzących z różnych form przestępczości.

Przełomem w zakresie prawnych aspektów rynku kryptoaktywów było przyjęcie 20 kwietnia 2023 r. w Parlamencie Europejskim rozporządzenia Markets in Crypto-assets<sup>30</sup>, które będzie kompleksowo regulować rynek kryptoaktywów w różnych jego obszarach (definicja kryptoaktywów, emitenta, tokena; wymogi względów emitentów i kryptoaktywów, regulacje prawnokarne w zakresie przeciwdziałania ujawnianiu i wykorzystywaniu informacji poufnych i manipulacji na rynku; ramy dokumentów informacyjnych opracowywanych przez emitenta).

Podsumowując rozważania podjęte w niniejszym artykule, należy stwierdzić, że w celu skutecznego identyfikowania i zapobiegania przestępczości związanej z obrotem kryptoaktywami konieczne jest podjęcie następujących działań:

- powołanie organu nadzoru właściwego w sprawach kryptoaktywów lub rozszerzenie kompetencyjne

- istniejącego już urzędu (np. KNF) w celu stworzenia ram prawnych dla działań nadzorczych i analitycznych;
- wprowadzenie sankcji prawno-karnych związanych z brakiem wpisu podmiotu gospodarczego do rejestru działalności w zakresie obrotu walutami wirtualnymi;
  - uregulowanie na poziomie krajowym emisji kryptoaktywów na realizację przedsięwzięć gospodarczych w celu ochrony prawnej i ekonomicznej inwestorów indywidualnych i instytucjonalnych;
  - wypracowanie optymalnej formy działalności gospodarczej w oparciu o przepisy u.u.p., w tym wymagania o charakterze organizacyjnym i kapitałowym, obostrzenia dotyczące przestrzegania przepisów w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, wymogi techniczne w zakresie bezpieczeństwa transakcji i przechowywanych aktywów oraz wymóg niekaralności osób zarządzających;
  - wzmocnienie współpracy pomiędzy instytucjami publicznymi, sektorem prywatnym oraz ośrodkami naukowymi w zakresie wymiany informacji dotyczących kryptoaktywów, analizy łańcucha *blockchain*, zagrożeń związanych z obrotem kryptoaktywami;
  - organizację współpracy międzynarodowej realizowanej przez poszczególne instytucje (jednostki analityki finansowej oraz nadzoru finansowego) oraz służby (np. Europol);
  - powoływanie wspólnych zespołów zadaniowych identyfikujących zagrożenia w obszarze obrotu kryptoaktywami oraz wypracowujących środki mitygujące o charakterze prawnym, organizacyjnym i operacyjnym.

## Przypisy

- 1 *Zagrożenie*, [w:] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Warszawa 2008, s. 172.
- 2 Na ten temat zob. P. Chodnicka, *Ekonomia Copernicana* 2011, nr 4, s. 74–75.
- 3 Komisja Specjalna ds. Przestępczości Zorganizowanej, Korupcji i Prania Pieniądzy, Dokument roboczy w sprawie prania pieniędzy, [nr] PE504.311, [http://www.europarl.europa.eu/mee-tdocs/2009\\_2014/documents/crim/dt/925/925991/925991pl.pdf](http://www.europarl.europa.eu/mee-tdocs/2009_2014/documents/crim/dt/925/925991/925991pl.pdf) (dostęp: 21.06.2021).
- 4 Takim aktem jest np. Zarządzenie nr 16/92 Prezesa Narodowego Banku Polskiego z dnia 1 października 1992 r. w sprawie zasad postępowania banków w razie ujawnienia okoliczności wskazujących na lokowanie w bankach środków pieniężnych lub innych wartości majątkowych pochodzących z przestępstwa lub mających z nim związek oraz przy dokonywaniu wypłat gotówkowych przekraczających określoną kwotę (Dz.Urz. NBP nr 18 poz. 40). Podobny charakter mają koncepcje umiejscowienia jednostki ds. przeciwdziałania praniu pieniędzy (Państwowej Agencji Informacji Finansowej) jako centralnego organu administracji państwowej.
- 5 Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz.U. nr 116 poz. 1216); Ustawa weszła w życie 23 czerwca 2001 r.
- 6 FATF, *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko w zakresie prania pieniędzy oraz finansowania terroryzmu*, 2014.
- 7 Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 r.
- 8 *Informacje o Europolu*, <https://www.europol.europa.eu/about-europol:pl> (dostęp: 21.06.2021).
- 9 Zob. np. Europol, *Cryptocurrencies Tracing the Evolution of Criminal Finances*, 2022.
- 10 *Fintech*, <https://pfr.pl/slownik/slownik-fintech.html> (dostęp: 20.09.2022).
- 11 *Co to jest DeFi?*, <https://www.coinbase.com/pl/learn/crypto-basics/what-is-defi> (dostęp: 15.10.2022).
- 12 Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, 10.12.2020, s. 7, [https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko\\_UKNF\\_ws\\_wydawania\\_i\\_obrotu\\_kryptoaktywami\\_71794.pdf](https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf) (dostęp: 22.06.2021).
- 13 *Chainalysis, The 2022 Geography of Cryptocurrency Report*, October 2022.
- 14 *Ranking giełd i kantorów kryptowalut*, <http://gieldekrypto-walut.pl/najwieksze-giedy-i-kantory-kryptowalut/> (dostęp: 21.06.2021).
- 15 Dla porównania w 2020 r. było ich 67. Zob. *Bitomaty*, <https://wymianakrypto.pl/bitomaty> (21.06.2021).
- 16 Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2019 poz. 1115). Ustawa weszła w życie 13 lipca 2018 r.
- 17 Pełny zakres zadań zawiera art. 12 u.p.p.f.t.
- 18 M. Hara, R. Kierzyńska, P. Kołodziejewski, *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2014, s. 25.
- 19 Środkami tymi są: identyfikacja klienta i weryfikacji jego tożsamości, identyfikacja beneficjenta rzeczywistego oraz weryfikacja prowadzonych przez klienta stosunków gospodarczych, a także bieżące monitorowanie transakcji z klientem w zakresie ich zgodności z jego dotychczasową działalnością.
- 20 Definicja jednostki współpracującej została zawarta w art. 2 ust. 2 pkt 8 u.p.p.f.t.
- 21 Art. 129b u.p.p.f.t. stanowi, że „Działalność na rzecz spółek i trustów może być wykonywana przez: osobę fizyczną, która nie została prawomocnie skazana za umyślne przestępstwo przeciwko działalności instytucji państwowych oraz samorządu terytorialnego, przeciwko wymiarowi sprawiedliwości, przeciwko wiarygodności dokumentów, przeciwko mieniu, przeciwko obrotowi gospodarczemu i interesom majątkowym w obrocie cywilnoprawnym, przeciwko obrotowi pieniędzmi i papierami wartościowymi, przestępstwo, o którym mowa w art. 165a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny, przestępstwo popełnione w celu osiągnięcia korzyści majątkowej lub osobistej lub umyślne przestępstwo skarbowe; osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, w której wspólnicy, którym powierzono prowadzenie spraw spółki lub uprawnieni do reprezentacji spółki, lub członkowie organów zarządzających nie zostali prawomocnie skazani za przestępstwo, o którym mowa w pkt 1, lub umyślne przestępstwo skarbowe”.
- 22 *Zadania KNF*, bip.knf.gov, 30.04.2021, [https://bip.knf.gov.pl/bip\\_portal/knf/zadania\\_knf](https://bip.knf.gov.pl/bip_portal/knf/zadania_knf) (dostęp: 20.10.2022).



- 23 W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011, s. 60.
- 24 *Najwyżej sprzedane dzieła NFT*, <https://desa.pl/pl/historie/najwyzej-sprzedane-dziela-nft/> (dostęp: 21.06.2021).
- 25 *Podstawy NFT*, <https://desa.pl/pl/historie/podstawy-nft/> (dostęp: 21.06.2021).
- 26 K. Wysota, *Kryptoluka w sankcjach*, „Puls Biznesu”, 1.03.2022.
- 27 Commission staff working document. Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 27.10.2022.
- 28 Chainalysis, *The 2023 Crypto Crime Report*, February 2023.
- 29 Tamże.
- 30 Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937, 24.09.2020.

## Bibliografia

### Akty prawne i administracyjne

- Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz.Urz. UE L 229/1).
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 2022 poz. 1138 z późn. zm.).
- Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz.U. nr 116 poz. 1216).
- Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. nr 199 poz. 1175).
- Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2019 poz. 1115).
- Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646).
- Uchwała nr 111/22 z dnia 14 kwietnia 2022 r. Komisji Nadzoru Finansowego w sprawie okoliczności istotnych dla oceny rękami w sprawach z zakresu rynku finansowego w związku z agresją Federacji Rosyjskiej wobec Ukrainy.
- Zarządzenie nr 16/92 Prezesa Narodowego Banku Polskiego z dnia 1 października 1992 r. w sprawie zasad postępowania banków w razie ujawnienia okoliczności wskazujących na lokowanie w bankach środków pieniężnych lub innych wartości majątkowych pochodzących z przestępstwa lub mających z nim związek oraz przy dokonywaniu wypłat gotówkowych przekraczających określoną kwotę (Dz.Urz. NBP nr 18 poz. 40).

### Dokumenty i raporty

- Chainalysis, *The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime*, February 2022.
- Chainalysis, *The 2022 Geography of Cryptocurrency Report*, October 2022.
- Chainalysis, *The 2023 Crypto Crime Report*, February 2023.
- Commission staff working document. Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 27.10.2022.
- Europol, *Cryptocurrencies Tracing the Evolution of Criminal Finances*, 2022.

FATF, *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko w zakresie prania pieniędzy oraz finansowania terroryzmu*, 2014.

- Komisja Europejska, *Ponadnarodowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu z 26 czerwca 2017 r.*
- Komunikat Generalnego Inspektora Informacji Finansowej z 14 lipca 2014 r. w sprawie niebezpieczeństw związanych z walutami wirtualnymi.
- Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu, 2019.
- Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2020 r.
- Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 r.
- Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937, 24.09.2020.

### Opracowania

- Chodnicka P., *Ekonomika prania brudnych pieniędzy*, „Oeconomia Copernicana” 2011, nr 4.
- Hara M., Kierzyńska R., Kołodziejki P., *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2014.
- Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Warszawa 2011.
- Zagrożenie, [w:] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Warszawa 2008.
- Wysota K., *Kryptoluka w sankcjach*, „Puls Biznesu”, 1.03.2022.

### Internet

- Bitomaty*, <https://wymianakrypto.pl/bitomaty> (dostęp: 21.06.2021).
- Co to jest DeFi?*, <https://www.coinbase.com/pl/learn/crypto-basics/what-is-defi> (dostęp: 15.10.2022).
- Fintech*, <https://pfr.pl/slownik/slownik-fintech.html> (dostęp: 20.09.2022).
- Informacje o Europolu*, <https://www.europol.europa.eu/about-europol/pl> (dostęp: 21.06.2021).
- Komisja Specjalna ds. Przestępczości Zorganizowanej, Korupcji i Prania Pieniądzy, Dokument roboczy w sprawie prania pieniędzy, [nr] PE504.311, [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/crim/dt/925/925991/925991pl.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dt/925/925991/925991pl.pdf) (dostęp : 21.06.2021).
- Najwyżej sprzedane dzieła NFT*, <https://desa.pl/pl/historie/najwyzej-sprzedane-dziela-nft/> (dostęp: 21.06.2021).
- Podstawy NFT*, <https://desa.pl/pl/historie/podstawy-nft/> (dostęp: 21.06.2021).
- Ranking giełd i kantorów kryptowalut*, <http://gieldekryptowalut.pl/najwieksze-gieldy-i-kantory-kryptowalut/> (dostęp: 21.06.2021).
- Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, 10.12.2020, [https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko\\_UKNF\\_ws\\_wydawania\\_i\\_obrotu\\_kryptoaktywami\\_71794.pdf](https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf) (dostęp: 22.06.2021).
- Zadania KNF*, bip.knf.gov, 30.04.2021, [https://bip.knf.gov.pl/bip-portal/knf/zadania\\_knf](https://bip.knf.gov.pl/bip-portal/knf/zadania_knf) (dostęp: 20.10.2022).

**Abstrakt**

Nowe technologie, w tym rynek DeFi (zdecentralizowanej technologii *blockchain*), to nowy obszar płatniczy, pożyczkowy i inwestycyjny. Autor prezentuje funkcjonowanie nowych technologii, których wiele aspektów uregulowanych jest przez przepisy krajowe i unijne, skupiając się na analizie ryzyka użytkowników indywidualnych i instytucjonalnych w kontekście możliwości utraty aktywów, braku gwarancji, zmienności wartości czy braku ich powszechnej akceptowalności. Podkreśla także, że z uwagi na cechy technologiczne architektury systemu może być on wykorzystywany do legalizowania korzyści pochodzących z przestępstw (pranie pieniędzy). Artykuł jest również próbą przedstawienia obszarów zadań państwa w zakresie organizacyjnym, legislacyjnym i operacyjnym, które należy podjąć w celu przeciwdziałania potencjalnym zagrożeniom

**Słowa kluczowe:** kryptoaktywa, rynek DeFi, FinTech, strategia przeciwdziałania praniu pieniędzy

**Abstract**

***Threats to the financial market related to money laundering and FinTech technologies – identification of the phenomenon and methods of counteracting***

New technologies, including the DeFi (decentralized blockchain technology) market, are a new area of payments, loans and investments. In this article, the author presents the functioning of new technologies, many aspects of which are regulated by national and EU regulations, focusing on the risk analysis of individual and institutional users in the context of the possibility of losing assets, lack of guarantees, volatility of value, or lack of universal acceptance. In addition, due to the technological features of the system architecture, it can be used to legalize the proceeds of crime (money laundering). The article in question is also an attempt to present the areas of tasks of the state in the legislative and operational organizational scope, necessary to be undertaken in the field of counteracting potential threats.

**Keywords:** cryptocurrency, DeFi market, FinTech, anti-money laundering strategy

**Jacek Charatynowicz** – dr nauk społecznych, adiunkt w Wyższej Szkole Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, autor publikacji z zakresu kryptoaktywów. W pracy badawczej specjalizuje się w zagadnieniach dotyczących identyfikowania zagrożeń związanych z nowymi technologiami wykorzystywanymi do realizacji usług finansowych (kryptoaktywa). Ponadto analizuje występowanie trendów i tzw. czarnych łabędzi oraz ich wpływ na opracowywane przez państwo strategie bezpieczeństwa.