STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 193

193/2023
s. 201–225

Szkoła Główna Handlowa w Warszawie
Kolegium Zarządzania i Finansów
https://econjournals.sgh.waw.pl/SiP

Jakub Wróblewski
Citibank Europe PLC

Czesław Bartłomiej Martysz
Szkoła Główna Handlowa w Warszawie
ORCID: 0000-0003-2461-0121

Kryptowaluty a finansowanie przestępczości i pranie pieniędzy

Streszczenie

Celem artykułu jest identyfikacja najważniejszych przestępstw związanych z kryptowalutami oraz praniem pieniędzy przy użyciu infrastruktury opartej na blockchainie. Postęp technologiczny w dziedzinie zdecentralizowanych finansów przed długi czas wyprzedzał regulatorów, którzy dopiero przy gwałtownym wzroście wartości rynku zaczęli działać wprowadzając ograniczenia i zasady znane z tradycyjnych finansów. Mimo tych działań skala przestępstw z wykorzystaniem tych aktywów cały czas rośnie – wzrost zainteresowania detalicznych inwestorów tworzy sprzężenie zwrotne, gdyż coraz częściej padają oni ofiarami przestępstw i dostarczają płynności koniecznej do wyprania pieniędzy.

Słowa Kluczowe: blockchain, pranie pieniędzy, cyberprzestępczość, kryptowaluty
Kody klasyfikacji JEL: G18, G19, G29, G59

1. Wprowadzenie

Za wdrażanie innowacji na rynku finansowym początkowo odpowiedzialne były duże instytucje – kompanie handlowe, banki inwestycyjne czy instytucje prowadzące giełdy. Nowe klasy aktywów były wpierw przyjmowane przez inwestorów instytucjonalnych, by następnie trafić do inwestorów indywidualnych. Jednak w drugiej dekadzie XXI wieku ten trend się odwrócił – kryptoaktywa (powszechnie zwane kryptowalutami) trafiły do głównego nurtu finansów, przechodząc drogę od owocu prac informatyków-entuzjastów, chcących pozbawić państwo i banki centralne kontroli nad ich środkami, do efektów zaangażowania tysięcy spekulantów widzących w tym szanse na wielokrotne pomnożenie swoich pieniędzy.

Temat kryptoaktywów poruszany jest nie tylko w kontekście rynków finansowych, ogromnych stóp zwrotu, czy szans na usprawnienie systemów płatniczych [Kauflin, 2019], lecz także coraz częściej w kontekście wspomagania finansowania organizacji przestępczych i terrorystycznych poprzez łatwe i szybkie transfery wartości [Malik, 2018]. Jest to związane z gwałtownie zmieniającym się otoczeniem regulacyjnym, możliwościami, jakie daje piorącym pieniądze ten względnie młody rynek, typami przestępstw dokonywanych przy wykorzystaniu kryptoaktywów oraz nadal niedoskonałymi metodami śledczymi wykorzystywanymi w celu ustalenia tak zwanego *money-trail*.

Teza artykułu brzmi: zwiększenie popularności aktywów opartych na blockchain zwiększa możliwości prania pieniędzy i tworzy nowe, bezpieczniejsze dla przestępców metody pozyskiwania kapitału. Artykuł pokrywa lukę badawczą, ponieważ łączy zarówno opis różnych typów (cyber) przestępstw, zwykle towarzyszących rozwijającemu się rynkowi kryptoaktywów, jak i opis metod prania pieniędzy pochodzących z tych przestępstw przy użyciu blockchaina. Metodą badawczą artykułu jest analiza piśmiennictwa.

2. Istota blockchain

Blockchain to zdecentralizowana, rozproszona, publiczna, cyfrowa księga, na którą składa się wiele wpisów zwanych blokami. Jej użycie pozwala na jednoczesne rejestrowanie transakcji w całej sieci komputerów, tak aby żaden zaangażowany blok nie mógł być zmieniony wstecz, bez zmiany wszystkich kolejnych bloków [Armstrong, 2016]. Pozwala to użytkownikom na niezależną i stosunkowo niedrogą weryfikację i audyt transakcji. Baza danych blockchain jest zarządzana autonomicznie, tzn. bez istnienia jakiejkolwiek centralnej instytucji, za pomocą sieci peer-to-peer i rozproszonego serwera znacznika czasu. Są one uwierzytelniane przez masową współpracę napędzaną zbiorowym interesem użytkowników. Konstrukcja blockchain ułatwia efektywny przepływ informacji i sprawia, że niepewność użytkowników co do bezpieczeństwa danych jest znikoma. Zastosowanie blockchain usuwa cechę nieskoń-

czonej odtwarzalności z aktywów cyfrowych[1]. Zapobiega to największemu problemowi związanemu z cyfrowymi walutami – problemowi podwójnego wydawania pieniędzy. Blockchain opisano jako protokół wymiany wartości [Library of Congress].

Konstrukcję blockchain można rozpatrywać z kilku perspektyw [IBM]:

1) dane (bloki, transakcje) – pakiety prawidłowych transakcji tworzących łańcuch, które są hashowane i kodowane w specjalnej strukturze (drzewo Merkle'a) [Binance Academy, 2020];
2) sieci (wykrywanie węzłów, propagacja i weryfikacja informacji) – integralności danych i wiarygodność sieci są utrzymywane dzięki współdzieleniu tej samej, dystrybuowanej globalnie, księgi transakcji pomiędzy różnymi **węzłami (ang. nodes)** w rozproszonej sieci blockchain; węzły przechowują kopię transakcji w sieci i mogą wykonywać podstawowe funkcje, takie jak weryfikacja i uwierzytelnianie transakcji;
3) konsensusu (proof of work, proof of stake) – wszystkie węzły utrzymują tę samą księgę transakcji; w rozproszonej sieci blockchain każdy węzeł jest zarówno hostem jak i serwerem i musi wymieniać informacje z innymi węzłami, aby osiągnąć konsensus (w rodzaju *proof-of-work* oraz *proof-ofstake*);
4) infrastruktury (sprzęt komputerowy) – szczególne wymagania sprzętowe potrzebne do wydobywania kryptowalut (mining) oraz tworzenie wspólnych grup „górników" łączących moce obliczeniowe;
5) inteligentnych kontraktów (smart contracts) – programy przechowywane na blockchainie, które uruchamiają się, gdy spełnione są wcześniej ustalone warunki, wykorzystywane zwykle do automatyzacji wykonania umowy, dzięki czemu wszyscy uczestnicy mogą być natychmiast pewni wyniku (np. zwolnienie funduszy do odpowiednich stron, wysyłanie powiadomień, wystawienie biletu itp.).

3. Pranie pieniędzy a waluty cyfrowe i aktywa wirtualne

Pranie pieniędzy to wprowadzenie do legalnego obrotu wartości majątkowych uzyskanych z nielegalnych źródeł bądź służących finansowaniu nielegalnej działalności, polegając w szczególności na utrudnianiu stwierdzenia przestępnego pochodzenia tych wartości[2]. Nielegalne czynności takie jak przemyt, działalność przestępczości zorganizowanej, obrót narkotykami i sieci prostytucji, defraudacje, *insider trading*, łapówkarstwo i oszustwa komputerowe mogą generować duże zyski i stwarzać zachętę do legitymizacji nielegalnych dochodów właśnie poprzez pranie pieniędzy, które umożliwia kontrolowanie wartości majątkowych bez zwracania uwagi na działalność będącą źródłem tych wartości lub na zaangażowane w nią

[1] W przeciwieństwie do innych baz danych, bazy blockchain uniemożliwiają powielania tych samych wpisów – transakcja, w wyniku której zostaje przesłana jednostka wartości pomiędzy dwiema stronami o danym czasie nie może pojawić się w bazie danych dwukrotnie.

[2] Definicja prania pieniędzy pochodzi z art. 299 Kodeksu karnego [Dz.U. 2022, poz. 1138] w związku z art. 2 ust. 2 pkt 14 Ustawy o przeciwdziałaniu praniu pieniędzy (…) [Dz.U. 2023, poz. 1124].

osoby. Przestępcy robią to poprzez ukrycie źródeł, zmianę formy lub przeniesienie funduszy w miejsce, gdzie prawdopodobieństwo zwrócenia na nie uwagi jest mniejsze. Istnieje wiele metod prania pieniędzy, a wiele z nich (w tym blending, smurfing, structuring, wykorzystanie firm „słupów" czy transakcji na rynku nieruchomości) jest doskonale opisanych w literaturze przedmiotu [Martysz, 2021]. Pojawiają się jednak nowe techniki prania pieniędzy, gdzie kluczową rolę odgrywają nowoczesne technologie, w tym waluty cyfrowe i aktywa wirtualne, którym autorzy chcieliby poświęcić więcej uwagi. Coraz większa liczba rynków internetowych przyjmuje nowe metody płatności online, gdzie warunki rozliczeń i rozrachunków nie oferują ochrony konsumenta ani regulacji finansowych (gdzie transakcje za pośrednictwem usługodawców są uznawane za ostateczne). To właśnie takich systemów płatności poszukują osoby popełniające oszustwa internetowe.

Waluty cyfrowe (ang. *virtual currencies*) to waluty będące przedmiotem obrotu tylko w formacie cyfrowym – są to zarówno kryptowaluty jak i środki wymiany w specyficznych systemach (np. w grach czy sieciach społecznościowych). Waluta cyfrowa nie jest uznawana za prawny środek płatniczy, bo nie jest emitowana ani zabezpieczona przez żaden organ władzy publicznej, lecz tworzona niemal wyłącznie przez instytucje pozabankowe, ma zerową wartość wewnętrzną i jest transferowana zwykle za pośrednictwem rozproszonego rejestru [BIS, 2015]. Zrównywanie waluty cyfrowej z walutą wirtualną, kryptowalutą czy jakąkolwiek inną walutą jest akceptowalne jedynie w języku potocznym [Piech, 2017]. Jedną z najpopularniejszych walut cyfrowych jest bitcoin, kryptowaluta wykorzystująca sieć peer-to-peer (P2P), która pozwala użytkownikom na wysyłanie jednostek waluty do innych użytkowników online, bez konieczności korzystania z tradycyjnej instytucji finansowej [Financial Action Task Force, 2014].

W polskiej ustawie o przeciwdziałaniu praniu pieniędzy zdefiniowano **walutę wirtualną**, węższą pojęciowo od waluty cyfrowej, rozumianą jako cyfrowe odwzorowanie wartości, niebędące prawnym środkiem płatniczym banków centralnych, międzynarodową jednostką rozrachunkową, pieniądzem elektronicznym, instrumentem finansowym ani wekslem czy czekiem, ale wymienialne w obrocie gospodarczym na prawne środki płatnicze, akceptowane jako środek wymiany i mogące być przechowywane elektronicznie [Dz.U. 2023 poz. 1124, art. 2 ust. 2 pkt 26]. Coraz częściej można także spotkać pojęcie **waluty cyfrowej banku centralnego (CBDC)**, które zapewne zastąpi pierwotne znaczenie waluty cyfrowej[3].

Waluty cyfrowe są często narażone na ryzyko prania pieniędzy, ponieważ wiele z nich funkcjonuje jako międzynarodowe systemy płatności P2P, które przekraczają granice jurysdykcji, co stwarza trudności dla władz prowadzących działania o charakterze egzekucyjnym lub prawnym. Podmioty piorące pieniądze mogą próbować zacierać ślady, rozdzielając waluty cyfrowe pomiędzy wiele adresów – unikatowych identyfikatorów (reprezentujących miejsca docelowe, gdzie waluta może zostać wysłana) lub portfeli cyfrowych w złożonych transak-

[3] Ang. *Central bank digital current* (CBDC), czyli cyfrowa waluta banku centralnego, której wartość jest powiązana z oficjalną (papierową) walutą banku centralnego [McKinsey&Company, 2023].

cjach. Z uwagi na stadium rozwoju, waluty cyfrowe zwykle podlegają mniej rygorystycznym regulacjom niż tradycyjne płatności za pośrednictwem instytucji finansowych. Wiele jurysdykcji wymaga jednak od dostawców usług, którzy wymieniają lub w inny sposób obracają walutami cyfrowymi, aby posiadali skuteczne praktyki identyfikacji klienta lub prowadzenia dokumentacji [Bonderud]. Waluty cyfrowe nie zapewniają całkowitej anonimowości, dlatego są rzadko promowane przez usługodawców.

Istotną trudnością w skutecznym wykrywaniu przypadków prania pieniędzy za pomocą walut cyfrowych jest różnorodność tych walut. W maju 2013 r. międzynarodowe organy ścigania doprowadziły do zamknięcia Liberty Reserve, popularnego serwisu walut cyfrowych z siedzibą w Kostaryce. Zdaniem prokuratorów Liberty Reserve działał jako nielicencjonowany serwis transakcji finansowych – jego niedbałe procesy AML pozwoliły wyprać 6 mld USD nielegalnych aktywów od momentu powstania serwisu w 2001 r. [United States Attorney's Ofice, 2013]. Jednak wkrótce po tym zamknięciu przestępcy znaleźli alternatywne serwisy sprzyjające praniu pieniędzy, takie jak Perfect Money [Flitter, 2013]. Ponieważ ci usługodawcy działają online, mogą w krótkim czasie rozpocząć działalność w krajach o bardziej liberalnych przepisach finansowych. Ponadto wiele z najbardziej popularnych walut cyfrowych, w tym bitcoin, są praktycznie niemożliwe do zamknięcia z punktu widzenia organów ścigania, ponieważ działają one w zdecentralizowanej sieci P2P.

Po wzroście popularności bitcoina zaczęło pojawiać się wiele alternatywnych walut cyfrowych. Wiele z nich ma różne cechy, więc potencjał prania pieniędzy jest w nich różny. Ogólnie rzecz biorąc, waluty cyfrowe umożliwiają [ACFE, 2021]:

a) za niewielką opłatą lub bez opłaty transakcyjnej wysyłanie i przyjmowanie płatności od każdego użytkownika na świecie posiadającego dostęp do internetu;
b) wysyłanie i odbieranie płatności bez konieczności podawania jakichkolwiek informacji identyfikujących (poza losowo wygenerowanymi adresami użytkowników);
c) przeprowadzanie transakcji w bardzo dużej liczbie;
d) potwierdzanie transakcji w nie więcej niż kilka minut;
e) dystrybucję środków pomiędzy wieloma adresami lub portfelami cyfrowymi, aby tworzyć trudne do prześledzenia złożone transakcje.

Aktywa wirtualne są podobne do walut cyfrowych, ale są to zazwyczaj wartości niematerialne i prawne związane z konkretną usługą lub społecznością internetową. Na przykład strona internetowa z grami hazardowymi może oferować swoją własną zastępczą walutę, lub gra online może rozprowadzać wirtualne aktywa, której gracze mogą kupować. Często aktywa wirtualne zyskują wartość poza swoim pierwotnym kontekstem (tj. zyskują wartość w świecie rzeczywistym), ponieważ są rzadkie i można je sprzedać innym osobom za pośrednictwem rynków internetowych. Proces prania pieniędzy z wykorzystaniem aktywów wirtualnych często przypomina pewną odmianę poniższej sytuacji [Kuchta, 2020]:

a) nielegalne aktywa są wykorzystywane do zakupu wirtualnej waluty lub przedmiotów od stron trzecich; alternatywnie, organizacja przestępcza wynajmuje ludzi do samodzielnego gromadzenia wirtualnych zasobów;

b) jeśli wirtualne aktywa są kupowane od osób trzecich, sprzedawca przekazuje wirtualne przedmioty na konto kontrolowane przez przestępcę;
c) przestępca może albo sprzedać wirtualne aktywa za rzeczywiste pieniądze, albo przekazać informacje o wirtualnym koncie innemu przestępcy w celu przekazania wartości.

Choć rzeczywista cena sprzedaży wirtualnej waluty lub przedmiotów zwykle nie jest wysoka (niewielki odsetek transakcji przekracza kilka tysięcy USD) to profesjonalni pracze pieniędzy mogą rozbijać transakcje na niższe kwoty.

4. Kryminalne wykorzystanie kryptowalut – wprowadzenie

Skala wykorzystania kryptowalut w przestępstwach jest trudna do oszacowania. Narzędzia ułatwiające korzystanie z kryptowalut są powszechnie dostępne, dlatego przestępcze wykorzystanie kryptowalut nie oznacza wyłącznie działań związanych z samą cyberprzestępczością, ale przede wszystkim jest związane z przekazywaniem wartości pieniężnych [Europol, 2021]. Prywatna firma śledcza Chainalysis przygotowuje coroczne raporty na temat przestępczości na rynku kryptowalut. W 2022 r. wartość (wolumen) transakcji przestępczych w kryptowalutach osiągnął najwyższy w historii poziom 20,6 mld USD (rysunek 1), z dominującym udziałem oszustw typu scam[4]. Choć udział liczby transakcji wykorzystujących kryptowaluty w nielegalnej działalności zmniejsza się (przeważnie były to pranie pieniędzy oraz handel online nielegalnymi towarami i usługami), to jednak bezwzględna wartość „przestępczych" transakcji zapewne będzie rosła, nie tylko w związku z rozwojem przestępczości per se, ale również w związku z odkrywaniem nowych adresów kojarzonych z nielegalną działalnością[5]. Warto pamiętać, że 43% wolumenu nielegalnych transakcji w 2022 r. pochodziło z działalności związanej z podmiotami objętymi sankcjami.

Należy również zauważyć, że powyższe statystyki nie obejmują wpływów z przestępstw niezwiązanych z kryptowalutami, np. konwencjonalnego handlu narkotykami z wykorzystaniem kryptowaluty jako środka płatniczego [Chainalysis, 2023]. Ogółem udział nielegalnych transakcji w kryptowalutach oscyluje w ostatnich latach poniżej 1% i wykazuje tendencję spadkową (rysunek 1), co może wynikać ze spadku koniunktury – prawdopodobnie dlatego, że ofiary są bardziej pesymistyczne i mniej skłonne do wiary w obietnice wysokich zysków w czasach, gdy ceny aktywów spadają [Chainalysis, 2023].

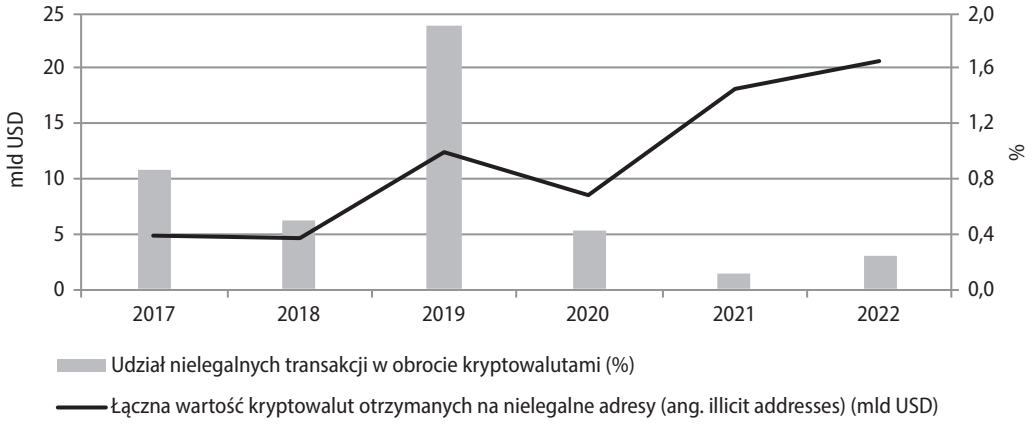
Warto przytoczyć badanie z końca kwietnia 2017 r. wskazujące, że 26% użytkowników bitcoinów (tj. ok. 27 mln osób) i blisko 46% transakcji bitcoinowych była związana z nielegalną działalnością [Foley, Karlsen, Putniņš, 2019]. Pamiętajmy jednak, że 28.04.2017 r. udział bit-

[4] Scam to oszustwo, w którym transakcja jest autoryzowana przez ofiarę w wyniku wprowadzenia ofiary w błąd (przeciwieństwem jest fraud, gdzie transakcja nie jest autoryzowana).

[5] Na przykład wartość „nielegalnych" transakcji w 2021 r. wyniosła 14 mld USD według raportu z 2022 r., ale później statystyki dotyczące 2021 r. wzrosły do 18 mld USD w kolejnej edycji raportu z 2023 r., głównie z powodu odkrycia nowych oszustw kryptograficznych.

-coina w rynku kryptowalut wynosił ok. 60,8%, na koniec 2020 r. 69,4%, ale już tylko 38,6% na koniec 2021 r. i 38,5% na koniec 2022 r. [CoinGecko, 2023].

Rysunek 1. Wolumen i udział nielegalnych transakcji w obrocie kryptowalutami



Źródło: opracowanie własne na podstawie [Chainanalysis, 2023].

5. Malware (złośliwe oprogramowanie) a kryptowaluty

Malware to złośliwe oprogramowanie działające zwykle bez wiedzy ofiary. Przestępstwa wykorzystujące malware mogą być proste jak kradzież informacji lub pieniędzy, ale mogą być również o wiele bardziej złożone. Na przykład operatorzy złośliwego oprogramowania, po zainfekowaniu dużej liczbę urządzeń mogą wykorzystywać je jako sieć botów do prowadzenia ataków typu **DDOS (distributed denial-of-service)**, popełniać oszustwa reklamowe lub wysyłać spam, aby dalej rozprzestrzeniać złośliwe oprogramowanie.

W przypadku kryptowalut większość ataków przy użyciu malware jest przeprowadzanych przez mniej wyrafinowanych hakerów, którzy mogą stosować tańsze, masowe podejście, w przeciwieństwie do skomplikowanych ataków dla okupu. Próbując zainfekować miliony potencjalnych ofiar, kradną oni mniejsze kwoty w krótszych interwałach. Wiele rodzajów malware można kupić w darknecie, co jeszcze bardziej ułatwia początkującym hakerom wykorzystanie ich przeciwko potencjalnym ofiarom [Crowdstrike, 2022a]. Przykładem jest oprogramowanie Redline – sprzedawca oferuje cyberprzestępcom miesiąc dostępu do Redline za 150 USD oraz dostęp dożywotni za 800 USD. Kupujący otrzymują również dostęp do Spectrum Crypt Service – narzędzia opartego na komunikatorze Telegram, które pozwala cyberprzestępcom zaszyfrować Redline tak, aby oprogramowanie antywirusowe ofiar trudniej wykryło go po pobraniu. Rozpowszechnienie taniego dostępu do malware (takiego jak Redline) dodatkowo utrudnia pracę wymiarowi sprawiedliwości, gdyż doprowadza ono do pomieszania działalności producenta oprogramowania z działalnością klientów [Viettel Security,

2022]. Wszystkie poniższe rodzaje malware służą do kradzieży krytpowaluty od ofiar, jednakże różnią się innymi zastosowaniami oraz działaniem [Chainalysis, 2022b]:

1) **information stealer** – zbiera zapisane dane uwierzytelniające, pliki, historię autouzupełniania i portfele kryptowalut z zainfekowanych komputerów,
2) **clipper** – zastępuje skopiowany przez użytkownika do schowka adres innym adresem, dzięki czemu hakerzy przekierowują transakcje do własnych portfeli,
3) **cryptojacker** – wykorzystuje bezprawnie moc obliczeniową komputera ofiary do wydobywania kryptowalut,
4) **trojan** – wirus, który wygląda jak legalny program, ale infiltruje komputer ofiary, aby zakłócić pracę, wykraść dane lub wyrządzić inne szkody.

Aż 98% operatorów malware otrzymuje płatności ofiar na adresy prywatnych portfeli. Reszta hakerów korzysta z adresów hostowanych przez większe serwisy, używając adresów hostowanych przez giełdy – głównie giełdy wysokiego ryzyka mające niskie lub zerowe wymagania KYC. Po otrzymaniu kryptowaluty od ofiar, operatorzy złośliwego oprogramowania wysyłają większość środków na adresy na scentralizowanych giełdach.

Giełdy otrzymały tylko 54% środków wysłanych z adresów operatorów malware w 2021 r., co oznacza spadek z 75% w 2020 r. Protokoły DeFi stanowią znaczną część różnicy – 20% w 2021 r., po tym jak w 2020 r. otrzymały znikomy udział w środkach pochodzących ze złośliwego oprogramowania. Nielegalne usługi pozornie niezwiązane ze złośliwym oprogramowaniem – głównie rynki darknetowe – są również znaczącą drogą prania pieniędzy dla operatorów malware'u, otrzymując około 15% wszystkich funduszy wysyłanych z tej grupy w 2021 r. Kradzież kryptowalut oparta na malware jest trudna do zbadania, częściowo ze względu na dużą liczbę mniej wyrafinowanych cyberprzestępców, którzy mogą wynająć dostęp do tych rodzajów malware. Badanie, w jaki sposób cyberprzestępcy piorą skradzioną kryptowalutę, może być dla śledczych najlepszym sposobem na znalezienie oszustów. Korzystając z analizy blockchain, śledczy mogą śledzić fundusze, znaleźć adresy depozytowe, których cyberprzestępcy używają do wypłacania pieniędzy, i wezwać podmioty świadczące usługi hostingu tych adresów w celu zidentyfikowania hakerów [Chainalysis, 2022b].

6. Ransomware (oprogramowanie okupowe) a kryptowaluty

Ransomware to złośliwe oprogramowanie, które blokuje sprzęt komputerowy lub dane ofiary i żąda okupu w zamian za ich odblokowanie (tzw. ransomware z pojedynczym wymuszeniem). W 2021 r. ataki ransomware stanowiły 21% wszystkich cyberataków [Braue, 2022] przynosząc straty ok. 20 mld USD [IBM]. Tworzenie kopii zapasowych niweluje skutki najprostszych ataków ransomware, dlatego niemal wszystkie dzisiejsze ataki ransomware, jak wynika z raportu 2022 X-Force Threat Intelligence Index [IBM, 2022a], to ataki z podwójnym wymuszeniem, zawierające dodatkową groźbę publicznego ujawnienia danych. Rośnie też liczba ataków typu „potrójne wymuszenie" (atakujący informuje klientów ofiary, że posiada

ich wrażliwe dane) oraz ataki typu *distributed denial of service* (DDoS), przeprowadzane równocześnie z wielu komputerów w celu znacznego spowolnienia systemów ofiary, by uniemożliwić prowadzenie działalności gospodarczej [United States Senate Comittee on Homeland Security & Goverment Affairs, 2022]. Po uzyskaniu przez hakerów dostępu do sieci komputerowej, atak ransomware zazwyczaj przebiega w następujących krokach [Murphy, 2021]:

1) **Rozpoznanie** – atakujący szuka w internecie informacji o pracownikach firmy (np. listy pracowników na firmowej stronie www, adresy e-mail pracowników oraz ich posty w mediach społecznościowych, komentarze na blogach i inne informacje), które mogą być wykorzystane do oszukania pracowników, aby ci kliknęli na złośliwy link lub otworzyli niebezpieczny załącznik. Atakujący analizują także ogłoszenia o pracę, informacje prasowe i raporty firmowe, informacje o kontrahentach, dostawcach i innych współpracujących z docelową firmą.
2) **Penetracja** – atakujący przeprowadzają ataki typu *spear phishing*, *social engineering* oraz *business e-mail compromise* na osoby w firmie. Atakujący tworzy e-maile, które brzmią autentycznie, ponieważ odnoszą się do osób, firm lub usług, z którymi cel jest zaznajomiony. Oszust tworzy również złośliwy program zaprojektowany specjalnie w celu obejścia kontroli bezpieczeństwa w firmie. Najlepszymi celami są zarządzający jednostką (np. dyrektorzy generalni lub dyrektorzy finansowi).
3) **Fortyfikacja** – po wejściu do sieci napastnicy ukrywają dowody swojego wejścia i szukają dodatkowych sposobów na uzyskanie dostępu do urządzeń firmowych, a także metod ponownego zainfekowania maszyn oprogramowaniem ransomware. Mogą nawet posunąć się do ochrony niektórych urządzeń przed innymi atakami, aby inny haker nie zwrócił przypadkiem uwagi na ich działania.
4) **Infiltracja** – atakujący uzyskują dostęp do wrażliwych informacji, a także do zasobów, które mogą być wykorzystane do zakłócenia procesów tworzenia kopii zapasowych i archiwizacji. Niektórzy cyberprzestępcy kradną na tym etapie dane, które mogą zostać sprzedane lub wykorzystane w kolejnych atakach. Dodatkowo, często dochodzi do kradzieży danych uwierzytelniających administratorów.
5) **Likwidacja** – napastnicy zmieniają procedury tworzenia kopii zapasowych w taki sposób, że kopie te wydają się działać, ale nie chronią danych docelowych. Atakujący mogą na tym etapie usuwać niektóre dane, wprowadzają błędy do oprogramowania, aby utrudnić przeprowadzenie przywracania, a także modyfikują dokumentację kopii zapasowych, aby zespoły przywracające dane nie mogły znaleźć właściwych informacji.
6) **Okup** – w fazie okupu atakujący umieszczają oprogramowanie ransomware w magazynach danych, w których znajdują się docelowe dane biznesowe. Okup jest zaplanowany na dzień, w którym będzie miał największy wpływ, np. tuż przed ważnym ogłoszeniem, podczas fuzji i przejęć lub w okolicach audytów. Atakujący wymazują archiwalne kopie danych i upewniają się, że wszystkie dane docelowe są zaszyfrowane, gdy dane są rozproszone na wielu serwerach, urządzeniach lub lokalizacjach. Czyszczą wszelkie pozostałe dowody swojej obecności, potencjalnie pozostawiając pewne możliwości na ponowny atak,

a następnie składają żądanie okupu. Nota okupu zawiera instrukcje dotyczące sposobu zapłacenia okupu, zwykle w kryptowalucie, w zamian za klucz deszyfrujący lub przywrócenie normalnego funkcjonowania.

Specjaliści w dziedzinie cyberbezpieczeństwa wyróżniają zazwyczaj **5 podstawowych typów oprogramowania ransomware**, od którego zależy też specyfika ataku, a także wysokość potencjalnego okupu. Typy te wymienione są poniżej [Crowdstrike, 2023]:

1) **Crypto ransomware lub encryptors** – jeden z najbardziej znanych i szkodliwych wariantów – szyfrowanie plików i danych w systemie, czyniąc zawartość niedostępną bez klucza deszyfrującego.
2) **Lockers** – całkowicie blokują użytkownika z systemu, więc jego pliki i aplikacje są niedostępne. Na ekranie blokady wyświetlane jest żądanie okupu, ewentualnie z zegarem odliczającym, aby zwiększyć pilność i skłonić ofiary do działania.
3) **Scareware** – fałszywe oprogramowanie, które informuje, że wykryło wirusa lub inny problem na komputerze i kieruje użytkownika do zapłacenia w celu rozwiązania problemu. Niektóre rodzaje scareware blokują komputer, podczas gdy inne po prostu zalewają ekran wyskakującymi alertami bez faktycznego uszkadzania plików.
4) **Doxware lub leakware** – grozi publiczną dystrybucją wrażliwych informacji sprawiając, że ofiary wpadają w panikę i płacą okup. Jedną z odmian jest ransomware o tematyce policyjnej, który wyświetla komunikaty jakoby użytkownikiem zainteresowały się organy ścigania (np. ze względu na nielegalne oprogramowanie lub niedozwoloną działalność online) – program informuje, że można uniknąć sankcji, płacąc grzywnę na specjalny rachunek w kryptowalucie.
5) **RaaS (Ransomware as a Service)** – złośliwe oprogramowanie hostowane anonimowo przez „profesjonalnego" hakera, który w zamian za część okupu kompleksowo zajmuje się atakiem, od dystrybucji ransomware do zbierania płatności i przywracania dostępu.

Metody podwójnego i potrójnego wymuszenia, zwiększona dostępność rozwiązań typu „ransomware-as-a-service", a przede wszystkim rozpowszechnienie się kryptowaluty jako trudnej do śledzenia formy płatności [IC3, 2021] przyczyniły się do gwałtownego wzrostu liczby incydentów ransomware. FBI Internet Crime Complaint Center odnotowało wzrost liczby zgłoszonych incydentów ransomware w latach 2013–2021 o około 276% [IC3, 2021]. Ofiary ransomware i negocjatorzy niechętnie ujawniają kwoty okupu, jednak wedle szacunków urosły one do kwot siedmio- i ośmiocyfrowych. W bardziej ekstremalnych przypadkach firmy mogą zapłacić nawet 40–80 mln USD za przywrócenie kontroli nad danymi [IBM, 2022b]. Średnia wielkość okupu za ransomware wyniosła ponad 118 tys. USD w 2021 r., w porównaniu z 88 tys. USD w 2020 r. i 25 tys. USD w 2019 r. [Peng, 2022]. Duże płatności, takie jak rekordowe 40 mld USD otrzymane przez Phoenix Cryptolocker [Mehrotra, Turton, 2021], napędzają ten rekordowy trend. Płatności okupu to nie jedyny koszt infekcji ransomware – według danych firmy IBM, średni koszt skutków ataku ransomware w 2021 r. bez samego okupu wyniósł 4,62 mln USD, a w pierwszej połowie 2022 r. wynosił on 4,54 mln USD [IBM, 2022c].

Jedną z przyczyn rosnących okupów jest koncentracja atakujących za pomocą oprogramowania ransomware na zakrojonych atakach przeciwko dużym organizacjom, wykorzystując narzędzia zewnętrznych dostawców. Narzędzia te obejmują zarówno nielegalne pomoce hakerskie, jak i legalne produkty, w tym:

a) anonimowy hosting oraz dostawców usług poczty email;
b) gotowe zestawy narzędzi pozwalające na wykorzystanie już znanych słabości zabezpieczeń w sieciach potencjalnych ofiar;
c) dane personalne, hasła itp., które dostały się do domeny publicznej w wyniku uprzedniego ataku hakerskiego bądź wycieku.

W 2021 r. ponad 16% (vs. 6% w 2020 r.) wszystkich środków wysłanych przez operatorów oprogramowania ransomware wydano na narzędzia i usługi w celu umożliwienia bardziej skutecznych ataków, a także usprawnienie procederu prania pieniędzy. Na przełomie drugiej i trzeciej dekady XXI wieku większość przestępców wykorzystujących ransomware prała wymuszone fundusze, wysyłając je na scentralizowane giełdy. Niektóre z nich należą do kategorii wysokiego ryzyka (liberalne procedury compliance), ale zwykle są to giełdy z tzw. mainstreamu compliance. Widoczne są również znaczne środki wysyłane do mikserów i na adresy związane z innymi formami nielegalnej działalności. Od 2020 r. aż 56% funduszy wysłanych z adresów ransomware trafiało do 6 firm krytowalutowych [Raj, 2022]:

a) trzy duże, międzynarodowe giełdy,
b) jedna giełda wysokiego ryzyka z siedzibą w Rosji,
c) dwa tzw. Mixery.

7. Geopolityczne wykorzystanie ransomware

Większość ataków ransomware ma motywacje stricte finansowe, jednak wartym poruszenia jest temat wykorzystania tego rodzaju złośliwego oprogramowania poprzez grupy działające pod protekcją lub/i na zlecenie państw. Ataki przeprowadzone przez takie grupy mają zazwyczaj na celu osłabienie zaufania do państwa, sianie paniki i zakłócenie działania kluczowych elementów infrastuktury. Nie można wykluczyć jednak motywu finansowego, w szczególności w przypadku Korei Północnej, dla której w obliczu niefektywnej gospodarki, handlu narkotykami, porwania oraz wymuszenia przy użyciu ransomware stanowią znaczące źródło finansowania programu zbrojeniowego [Department of Homeland Security – Cybersecurity and Infrastructure Security Agency, 2022]. Przykładem celu stricte geopolitycznego jest atak ransmoware ze strony Rosji na infrastukturę komputerową Ukrainy miesiąc przed wybuchem wojny [Computer Emergency Team of Ukraine, 2022]. Co ciekawe, dzień po wybuchu wojny – 25 lutego 2022 r. – inwazję poparła rosyjska grupa hakerska Conti specjalizująca się w atakach ransomware – w maju 2021 r. przeprowadziła 16 ataków na amerykańskie szpitale oraz systemy reagowania [Bing, 2022].

Przestępcy powiązani z Rosją nie są jedynymi, którzy wykorzystują ransomware do celów geopolitycznych. Analitycy ds. bezpieczeństwa cybernetycznego z firm Crowdstrike [2022a] i Microsoft [2021] stwierdzili, że wiele ataków ransomware powiązanych z Iranem, skierowanych głównie na organizacje w Stanach Zjednoczonych, Unii Europejskiej i Izraelu, jest ukierunkowanych bardziej na powodowanie zakłóceń lub służenie jako pretekst do ukrycia działalności szpiegowskiej. Ogólnie rzecz biorąc, w ciągu ostatniego roku odnotowano znaczny wzrost liczby ataków ransomware przypisywanych irańskim cyberprzestępcom – w gruncie rzeczy Iran odpowiada za więcej pojedynczych zidentyfikowanych ataków niż jakiekolwiek inne państwo. Wiele z tych irańskich ataków ransomware należy do konwencjonalnych, motywowanych finansowo i przeprowadzanych przez irańskich cyberprzestępców. Iran ma wysoko wykształconą populację, ale ograniczone możliwości zawodowe, co prawdopodobnie przyczynia się do rozwoju oprogramowania ransomware. Jednak niektóre ataki służą bardziej jako narzędzia szpiegostwa, wyłudzając od ofiar znikome kwoty kryptowaluty. Inni analitycy wcześniej zidentyfikowali przypadki grup powiązanych z Chinami, takich jak ColdLock, przeprowadzających podobne ataki geopolityczne na organizacje tajwańskie [Culpan, 2021].

Ransomware jest użyteczną „przykrywką" dla strategicznego sabotażu przeciwko wrogim państwom, ponieważ takie ataki są stosunkowo niedrogie a jako ich mocodawców można łatwo wskazać nie tyle służby państwowe lecz zwykłych cyberprzestępców. Ale nawet ataki ransomware przeprowadzane z powodów niefinansowych pozostawiają ślad na blockchainie, dlatego ważne jest, by istniały instytucjonalne możliwości śledzenia funduszy za pomocą analizy blockchain. Pozwala ona zidentyfikować osoby fizyczne i instytucje zaangażowane w ataki oraz sposoby prania wszelkich środków wymuszonych od ofiar.

8. Inne popularne cyberprzestępstwa związane z kryptowalutami

Cyberoszustwa stanowią jedno z największych zagrożeń dla dalszego upowszechniania się kryptowalut i są najczęstszym nielegalnym rodzajem działania opartego na kryptowalutach pod względem wolumenu transakcji (>7,7 mld USD w kryptowalutach przejętych od ofiar na całym świecie). Stanowi to wzrost o 81% w porównaniu z 2020 r., w którym aktywność w zakresie oszustw znacznie spadła w porównaniu z 2019 r., w dużej mierze z powodu braku jakichkolwiek wielkoskalowych schematów Ponziego [Chainalysis, 2021b]. Zmiana, która przyczyniła się do wzrostu przychodów z oszustw w 2021 r. to schemat *rug pull*, stosunkowo nowe oszustwo szczególnie powszechne w ekosystemie DeFi (*decentralized finance*), w którym twórcy rzekomo nowatorskiego projektu kryptowalutowego – zazwyczaj nowego tokena – niespodziewanie go porzucają, zabierając ze sobą fundusze użytkowników [Binance Academy, 2023]. Oszustwa w sferze kryptoaktywów zazwyczaj nie różnią się od tych internetowych czy ze świata rzeczywistego. Oparcie swojego działania na chciwości potencjalnych

ofiar pozwala cyberprzestępcom na zdobywanie dużych kwot przy niewielkim zaangażowaniu pracy i kapitału. Często spotykane typy oszustw to:

1) **Giveaway//Bitcoin doubler** – ofiara jest kuszona otrzymaniem w krótkim czasie, za darmo (*giveaway*) lub podwojeniem wpłaconej kwoty (*Bitcoin doubler*), dużej wartości w kryptowalucie. Przestępcy używają logotypów znanych marek z rynku kryptowalut, a także wizerunków znanych osób (np. Elona Muska) i stylizują stronę, tak aby dać ofierze poczucie autentyczności – ofiara jest nakłaniana do podania swojego klucza prywatnego, który później służy przestępcom do zlecenia transferów z portfela ofiary.
2) **NFT Minter** – tworzenie strony, na której można się zapisać na limitowaną kolekcję obrazków NFT (zazwyczaj są to małpy ze względu na sukces Bored Ape Yacht Club). Oszuści na prostej stronie umieszczają licznik pokazujący, jaka część puli została przydzielona (licznik z każdym odświeżeniem strony zaczyna liczyć od zera) i przycisk służący do podłączenia portfela w celu wysłania transferu, zazwyczaj w kryptowalucie ETH. Podobnie jak w przypadku giveaway'ów przestępcy szukają swoich ofiar na portalach społecznościowych i komunikatorach takich jak Telegram czy Discord.
3) **Rug pull (podciąganie dywanu)** – twórcy rzekomo nowatorskiego projektu DeFi przy użyciu masowego i intensywnego marketingu swojego dzieła w social media windują cenę tokenu na którym opiera się projekt. Gdy poziom emocji jest wysoki, a projekt ma dostęp do płynności, oszuści mają dwie opcje – sprzedać swoje tokeny po wysokiej cenie i pozbawić rynek całej płynności, albo nawet użyć furtek w inteligentnych kontraktach, aby okraść inwestorów. Bez wystarczającej płynności inwestorzy zmagają się ze sprzedażą swoich tokenów lub są zmuszeni sprzedać je po niskiej cenie[6].
4) **Romance – pig butchering scam (oszustwo zarzynania świni)** – celem są użytkownicy aplikacji randkowych i portali społecznościowych. Oszuści działają dwutorowo – po pierwsze wykorzystują zdjęcia atrakcyjnych fizycznie kobiet (zwykle Azjatek), aby długoterminowo i cierpliwie uwodzić ofiary, by potem „przy okazji" zainteresować ofiary inwestowaniem w kryptowaluty na fałszywej stronie internetowej lub aplikacji inwestycyjnej. Po drugie, oszuści odgrywają także rolę „obsługi klienta" tych fałszywych aplikacji czy stron, aby za pomocą podstępu i socjotechniki namówić ofiary do przekazywania coraz większych sum pieniędzy, grożąc ofiarom pozwem sądowym, powiadomieniem bliskich a nawet uszkodzeniem ratingu kredytowego ofiary czy koniecznością zapłacenia z góry podatku od rzekomych zysków [Ropek, 2022].
5) **Schemat Ponziego** – jest to oszustwo inwestycyjne przypominające parabank lub fundusz inwestycyjny, kuszące inwestorów obietnicą ponadprzeciętnych stóp zwrotu z interesującego i rzekomo legalnego lecz faktycznie nieistniejącego (fikcyjnego) przedsięwzięcia, gdzie wypłacane zyski dla „starych" inwestorów pochodzą z wpłat „nowych inwestorów". Schemat Ponziego upada z powodu utraty płynności, tj. niekorzystnej (zbyt dużej)

[6] Ciekawym przykładem rug pulla jest Squid Game Token, stworzony w październiku 2021 r. w szczycie popularności serialu Squid Game – oszuści wzbogacili się o ponad 3 mln USD [Cheng, 2021].

proporcji wypłat w stosunku do wpłat [Martysz, Królikowska, 2021]. Fasadowe modus operandi schematu Ponziego może być np. oparte na innowacyjnych usługach inwestowania na dynamicznie rozwijającym się rynku kryptowalut, którego wielu ludzi nie rozumie i który jest powszechny w przekazie medialnym. Z tego powodu łatwiej jest oszukać inwestorów obietnicami nierealnych zysków. Schemat Ponizego Bitconnect, obiecujący „inwestorom" 40% miesięcznych zwrotów z inwestycji, spowodował ponad 2 mld USD strat [United States Attorney's Office, 2021].

6) **Cloud mining** – stworzenie puli wydobywczej (mining pool) przy użyciu komputerów użytkowników z całego świata, którzy w zamian za udział w zysku ze sprzedaży kryptowalut udostępniają swoją moc obliczeniową i ponoszą koszty energii. Ofiara jest niedostatecznie wynagradzana lub traci wszystko. Przestępcy poza zdobyciem darmowego źródła mocy obliczeniowej zwiększają straty ofiar nakłaniając je do zakupu członkostwa premium, mającego rzekomo zwiększyć udziały w zyskach [Rees, 2022].

Nawiązując do rysunku 1, przyrost przychodów z oszustw kryptowalutowych w latach 2020–2021 wynika głównie z oszustw typu rug pull, jednak liczba wpłat na adresy związane z oszustwami (i tym samym liczba ofiar) spadła z niecałych 10,7 mln do 4,1 mln. W tym samym czasie liczba aktywnych[7] oszustw kryptowalutowych wzrosła z 2052 do 3300 [Chainalysis, 2022a]. Przeciętne oszustwo było aktywne przez zaledwie 70 dni w 2021 r. (vs. 192 dni w 2020 r.). Jednym z powodów może być to, że śledczy są bardziej skuteczni w prowadzeniu dochodzeń i ściganiu oszustw. We wrześniu 2021 r. CFTC (komisja nadzorująca rynek instrumentów pochodnych w USA) wniosła zarzuty przeciwko 14 oszustom inwestycyjnym, którzy twierdzili, że świadczą zgodne z przepisami usługi obrotu instrumentami pochodnymi kryptowalut, podczas gdy w rzeczywistości nie zarejestrowali się w CFTC [Commodity Futures Trading Commission, 2021]. Wcześniej te oszustwa mogły być w stanie kontynuować działalność przez dłuższy czas. Ponieważ oszuści stają się świadomi tych działań, mogą czuć większą presję, aby zamknąć działalność, zanim zwrócą uwagę organów regulacyjnych i organów ścigania. Jednocześnie obserwuje się koniec długotrwałego związku statystycznego między cenami aktywów kryptowalutowych a aktywnością oszustów. Oszustwa zazwyczaj pojawiają się w falach odpowiadających trwałemu wzrostowi cen popularnych kryptowalut, takich jak bitcoin i Ethereum, które zazwyczaj prowadzą również do napływu nowych użytkowników – aktywność oszustów wzrosła po hossie w latach 2017 i 2020. Nowi, mniej obeznani użytkownicy, przyciągnięci wzrostem cen kryptowalut są bardziej podatni na oszustwa niż bardziej doświadczeni użytkownicy. Zależność między cenami aktywów a aktywnością oszustów może już obecnie zanikać [Walk-Morris, 2022].

[7] Status aktywny oznacza, że adresy otrzymywały środki w danym roku.

9. Sposoby prania pieniędzy z przestępstw wykorzystujących kryptowaluty

Giełdy kryptowalut zapewniają niezbędną płynność na rynkach kryptowalut jako ważne ogniwo łączące systemy walut FIAT[8] i kryptowalut, dlatego też nieuchronnie pojawiają się w procesie prania kryptowalut. Financial Task Force (FATF) podkreśla szczególne ryzyko pochodzące z nieuregulowanych giełd lub tych, które nie mają kontroli AML / CTF, ponieważ „przestępcy wykorzystali luki w systemach AML/CTF (…), przenosząc swoje nielegalne fundusze do VASP-ów[9] mających siedzibę lub działających w jurysdykcjach o nieistniejących lub minimalnych regulacjach AML/CTF" [Financial Action Task Force, 2020]. Nielicencjonowane i prowadzone niezgodnie z przepisami giełdy generują istotne ryzyko prania pieniędzy, chociaż legalne giełdy również mogą posłużyć do prania pieniędzy.

Przestępcy celowo szukają giełd o niskich wymaganiach w zakresie AML w przekonaniu, że możne je bez większych przeszkód wykorzystać do transakcji między pieniędzmi FIAT a kryptowalutami lub pomiędzy różnymi kryptowalutami. Cechy takich giełd są następujące [Carlisle, 2022a]:

a) celowe lekceważenie przepisów i wymogów rejestracyjnych;
b) umożliwienie klientom zakładania rachunków przy jednoczesnym niewielkim lub żadnym wymogiem przedstawienia informacji identyfikacyjnych;
c) klienci otwierający rachunki nie muszą przestrzegać przepisów w żadnej jurysdykcji;
d) siedziba giełdy w kraju wysokiego ryzyka, do których należą:
   - kraje z wysokim ogólnym ryzykiem prania pieniędzy i finansowania terroryzmu – zwykle w Afryce, Europie Wschodniej lub na Bliskim Wschodzie,
   - kraje podlegające międzynarodowym sankcjom, embargu i innym ograniczeniom,
   - kraje na liście jurysdykcji wysokiego ryzyka i braku współpracy FATF,
   - kraje bez regulacji AML/CTF obejmujących kryptowaluty lub z nieefektywnymi ramami regulacyjnymi.

Oto typowe modus operandi prania pieniedzy przez giełdę kryptowalut [Europol, 2017]:

1) Przestępca pragnie wyprać nielegalnie uzyskane kryptowaluty (np. z ransomware).
2) Przestępca zakłada konto na nielicencjonowanej lub działającej niezgodnie z przepisami giełdzie, aby wymienić swoje kryptowaluty, czasami skorzystawszy uprzednio z mixerów. Na takich giełdach przestępca zakłada całkowicie anonimowe konta[10] lub używając pseudonimów lub/i fałszywych informacji identyfikacyjnych (np. fikcyjnego adresu).

[8] FIAT – pieniądz fiducjarny, legalny środek płatniczy, którego wartość ustalana jest przez rząd.

[9] VASP (ang. *virtual asset service provider license*) – licencja podmiotu organizującego wymianę aktywów wirtualnych na waluty fiducjarne, inaczej dostawcy usług wirtualnych aktywów. W Polsce taki rejestr prowadzi Dyrektor Izby Administracji Skarbowej w Katowicach [*Rejestr działalności w zakresie walut wirtualnych*].

[10] Należy podkreślić, że choć w świecie kryptowalut każdy użytkownik systemu posiada indywidualny identyfikator, to największą trudność sprawia przypisanie tego identyfikatora konkretnej osobie. Przypomina to sytuację, w której znamy numer telefonu, z którego ktoś próbował nas oszukać, ale nie wiemy, na kogo ten telefon jest zarejestrowany ani z kim de facto rozmawialiśmy.

3) Przestępca wymienia brudne kryptowaluty na waluty FIAT lub na inne kryptowaluty.
4) Przestępca może wypłacić środki z giełdy bezpośrednio na konto bankowe lub korzystać z wypłaty przy użyciu usług finansowym takich jak PayPal. Często wszelkie wiadomości lub tytuł towarzyszące transferom środków mogą być specjalnie przygotowane, aby ukryć powiązanie przelewanych środków z handlem kryptowalutami.
5) Alternatywnie, przestępca może najpierw przesłać nowe „czyste" kryptowaluty na legalną giełdę, z której może następnie dokonać wypłaty. Często obejmuje to wymianę kryptowalut na blockchainach umożliwiających śledzenie, takich jak bitcoin i Litecoin, na kryptowaluty prywatnościowe, takie jak Monero.

We wrześniu 2021 r. OFAC[11] podjęło akcję sankcyjną, która wyraźnie wskazywała na rolę, jaką odgrywają nieuregulowane giełdy kryptowalut w ułatwianiu prania pieniędzy. Wówczas OFAC nałożyło sankcje na SUEX OTC – czeską firmę handlującą kryptowalutami, która oferowała usługi w Rosji. Przy ograniczonej obecności w internecie, giełda SUEX OTC reklamowała butikowe usługi dla klientów pochodzących z rosyjskiej strefy wpływów, takie jak zakup kryptowalut za pomocą kart kredytowych online lub osobiście w gotówce. SUEX wydawał się być małym biznesem kryptowalutowym o niewielkim znaczeniu, lecz w rzeczywistości był filarem ekosystemu ransomware, który umożliwiał przestępcom pranie nielegalnych zysków. Według OFAC, firma umożliwiła pranie pieniędzy związanych z co najmniej ośmioma rodzajami ransomware, a aż 40% jego ogólnej działalności było związane z nielegalną działalnością [United States Department of the Treasury, 2022]. Analiza Elliptic (firmy dostarczającej oprogramowanie do śledztw kryptowalutowych) wskazuje, że od 2018 r. SUEX zaangażował się w transakcje kryptowalutowe warte ponad 934 mln USD, przetwarzając ponad 370 mln USD w nielegalnych transakcjach w ciągu zaledwie trzech lat, co jest znaczną sumą dla względnie małej giełdy [Carlisle, 2022b]. W ramach działań sankcyjnych skierowanych przeciwko SUEX, OFAC wpisał na swoją listę sankcyjną 25 adresów służących do przyjmowania i wysyłania BTC, ETH i USDT, aby dać prawne uzasadnienie dla zablokowania transakcji z SUEX. Ponieważ firma prowadziła handel OTC, otwierając rachunki na większych giełdach, sankcje OFAC mają realny wpływ – inne giełdy muszą zaprzestać transakcji z SUEX lub ryzykować karami za naruszenie sankcji.

Przestępcy zdają sobie sprawę, że przejrzystość blockchainów czyni je podatnymi na śledzenie i wykrywanie. Aby uniknąć wykrycia, przestępcy rutynowo starają się korzystać z tak zwanych **mixerów kryptowalut**, które mieszają fundusze od różnych użytkowników, utrudniając ustalenie ich pierwotnego źródła. Instytucje i osoby nadzorujące zgodność zachowań uczestników rynku kryptowalut z regulacjami oraz organy ścigania wykorzystują przejrzystość publicznych blockchainów do identyfikacji i przeciwdziałaniu praniu pieniędzy i innym działaniom związanym z przestępstwami finansowymi. Ta przejrzystość pozwala na wgląd

[11] OFAC (ang. *The Office of Foreign Assets Control*) – agencja Departamentu Skarbu USA, która zarządza sankcjami gospodarczymi i handlowymi oraz je egzekwuje, wspierając cele związane z bezpieczeństwem narodowym i polityką zagraniczną USA.

w nielegalną działalność w całym ekosystemie DeFi. Jednak przestępcy działający w przestrzeni DeFi szybko wykorzystali mixer Ethereum **Tornado Cash** do zacieranie śladu funduszy, utrudniając rozszyfrowanie ich działalności[12]. 8 sierpnia 2022 r. OFAC wpisał Tornado Cash na listę sankcyjną. Żaden amerykański obywatel ani przedsiębiorstwo nie mogą legalnie korzystać z Tornado Cash a wszelkie środki pochodzące z tej usługi uznaje się za brudne [United States Department of the Treasury, 2022]. Z usług Tornado Cash korzystali rzekomo m.in. północnokoreańscy cyberprzestępcy z Grupy Lazarus a łączną wartość wypranych w Tornado Cash kryptowalut szacuje się na mld USD[13]. Regulowane giełdy, w ramach swoich obowiązków związanych z zapobieganiem praniu pieniędzy, w kontekście korzystania z mixerów zwracają uwagę, że [Carlisle, 2022a]:

a) klient otrzymuje częste przelewy przychodzące z mixera, takiego jak Tornado Cash, i nie chce lub nie jest w stanie podać informacji o pierwotnym źródle środków;
b) klient dokonuje częstych transferów do Tornado Cash lub innych mixerów bez racjonalnego wytłumaczenia dla takiej aktywności;
c) klient, którego działalność wiąże się z częstymi transakcjami na zdecentralizowanych giełdach, dokonuje również transakcji z mixerami.

Typowy modus operandi prania pieniędzy przy użyciu mixerów wygląda następująco:

1) przestępca uzyskuje ether lub tokeny operate na Ethereum, na przykład poprzez zhakowanie platformy pożyczkowej DeFi;
2) przestępca wysyła skradzione środki na adres mixera (np. Tornado Cash);
3) przestępca otrzymuje nowe środki z mixera (np. Tornado Cash);
4) nowe tokeny deponuje się i wymienia na scentralizowanej platformie na FIAT.

W dniu 19 sierpnia 2021 r. cyberprzestępcy ukradli z japońskiej giełdy kryptowalut Liquid kryptowaluty warte ponad 97 mld USD, w tym 45 mln USD w tokenach opartych na Ethereum, które hakerzy przekonwertowali na ether na zdecentralizowanych giełdach takich jak Uniswap i SushiSwap, co zapobiegło zablokowaniu środków przez emitentów tokenów. Po przekształceniu funduszy w ether, hakerzy następnie wyprali fundusze o wartości około 20 mln USD właśnie poprzez wspomniany mikser Tornado Cash [Elliptic, 2021].

Jednym z nieodłącznych ograniczeń blockchainów jest to, że transakcje w ramach konkretnej sieci – takiej jak Ethereum – są ograniczone do tokenów opartych na tym blockchainie. Innymi słowy, blockchainy nie są wzajemnie kompatybilne, a użytkownik nie może używać

[12] Tornado Cash był do niedawna najpopularniejszym mixerem – łączył „brudne" środki z „czystymi" w jednej puli, a następnie rozsyłał je na nowe adresy, co uniemożliwiało skuteczne śledzenie tych pierwszych. Aby skorzystać z Tornado Cash należało przesłać na adres utrzymywany przez tę usługę 0,1; 1; 10; bądź 100 ETH wraz z prowizją. Następnie, po ustalonym czasie, Tornado wysyłał na inny adres użytkownika odpowiednią kwotę. Stałość kwot oraz opóźnione przesyłanie wymieszanej kwoty skutecznie uniemożliwiało śledzenie środków [Wade, Lewellen, Van Valkenburgh, 2022].

[13] Usługę Tornado Cash reklamowano tak, że zapewnia niemożliwe do wyśledzenia anonimowe transakcje finansowe. Twórcy mixera R. Storm i R. Semenov świadomie nie wdrożyli programów „poznaj swojego klienta" (ang. KYC, know your customer) ani programów przeciwdziałania praniu pieniędzy zgodnie z wymogami prawa. W sierpniu 2023 r. nowojoroscy prokuratorzy oskarżyli R. Storma i R. Semenova o wypranie 1 mld USD [United States Attorney's Office, 2023].

bitcoina do transakcji z decentralizowanymi aplikacjami opartymi na Ethereum. Ogranicza to praktyczną użyteczność systemów operatych na blockchain dla wielu użytkowników, którzy mogą chcieć transferować fundusze przez wiele z nich. Rozwiązaniem tego problemu są **cross-chain bridge**, które pozwalają na to, aby aktywa na jednym blockchainie były reprezentowane jako token na innym [Ethereum Foundation, 2023]. Popularne cross-chain bridge krzyżowe to między innymi RenBridge, VoltSwap i WanBridge. Zamiast polegać na scentralizowanej giełdzie, aby wymienić bitcoin na Ethereum, użytkownicy mogą wysłać swoje bitcoiny do adresu utrzymywanego przez cross-chain bridge, aby uzyskać tokeny bitcoinów w sieci Ethereum, a także uniknąć konieczności oddania kontroli nad swoimi kryptowalutami lub poddania się KYC, co byłoby wymagane w przypadku transakcji za pośrednictwem scentralizowanej giełdy.

Ta zdolność do wymiany kryptowalut pomiędzy blockchainami, bez konieczności poddawania się wymogom KYC, stanowi korzyści dla przestępców, którzy mogą próbować prać dochody z przestępstwa w formie jednej kryptowaluty na inną (np. tokeny oparte na Ethereum). Ten krzyżowy ruch funduszy stanowi wyzwanie dla analityków śledczych, którzy chcą monitorować ślad tych funduszy. Oto typowy **modus operandi prania pieniędzy przy użyciu cross-chain bridge'ów:**

1) przestępca uzyskuje bitcoiny z nielegalnego źródła (np. ransomware lub sprzedaż narkotyków w darkwebie);
2) przestępca wysyła bitcoiny z nielegalnego źródła do cross-chain bridge'a;
3) przestępca otrzymuje nowe „czyste" tokeny na innym blockchainie z cross-chain bridge'a w zamian za przesłanego wcześniej bitcoina;
4) nowe tokeny mogą być wysyłane dalej i wymieniane na zdecentralizowanych giełdach lub wymieniane na gotówkę na scentralizowanych giełdach.

Powstałe w 2018 r. oprogramowanie ransomware Ryuk jest wykorzystywane przez wiele grup przestępczych do wyłudzenia dziesiątek mln USD w postaci płatności za okup w bitcoinach. Ich dochody zostały wyprane na wiele sposobów – w tym przy użyciu mikserów i nieregulowanych giełd. W lipcu 2021 r. bitcoin z Ryuk zaczął być wysyłany do RenBridge, który jest zdecentralizowanym cross-chain bridge'em. Co najmniej 125 BTC – wówczas warte około 4 mln USD – w środkach pochodzących z płatności za okup zostało przesłane przez Ren, umożliwiając ich użycie na innym blockchainie, takim jak Ethereum [Seth, 2022].

Ostatnią metodą prania pieniędzy z wykorzystaniem kryptowalut są **Tokeny NFT**. Są one formą reprezentacji własności unikatowego aktywa cyfrowego, jak dzieło sztuki cyfrowej, kolekcje sportowe, przedmioty zakupione w grach online i inne. NFT stwarzają nowe możliwości dla powszechnego przyjęcia kryptowalut. Poprzez powiązanie infrastruktury leżącej u podstaw aktywów cyfrowych z widocznymi produktami, tokeny NFT umożliwiają coraz większej liczbie osób zaangażowanie się w ekosystem kryptowalut. Firmy zajmujące się NFT (np. Dapper Labs i OpenSea) należą do najszybciej rozwijających się firm w branży kryptowalut. W 2021 r. rynek NFT był warty około 41 mld USD, co jest wartością porównywalną z rynkiem tradycyjnej sztuki [Dailey, 2022]. NFT pomagają również w rozwoju modnego

konceptu Metaverse – np. handel sztuką cyfrową, kupno ziemi w grze online i inne przypadki użycia NFT zwiększają immersję podczas eksploracji światów wirtualnych dostępnych dla przeciętnego człowieka.

NFT niosą ze sobą również ryzyko, ponieważ umożliwienie kupna i sprzedaży sztuki cyfrowej i towarów stwarza nowe okazje do oszustw, prania pieniędzy i uchylania się od sankcji. Rynki NFT charakteryzują się również brakiem jednolitego nadzoru regulacyjnego, podczas gdy niektóre rynki mogą być objęte wymogami AML dotyczącymi handlu dziełami sztuki, pośrednictwa w obrocie papierami wartościowymi lub innych działań regulowanych, brakuje jasności regulacyjnej w odniesieniu do przestrzeni NFT. To dodaje dodatkową warstwę podatności na zagrożenia dla rynków NFT, gdzie przestępcy mogą próbować wykorzystać brak spójnego nadzoru [Akartuna, Nadini, DePow, Annison, 2022].

Rynki NFT są bardzo płynne, a oszacowanie ich godziwej wartości jest bardzo trudne. Niektóre NFT sprzedają się za duże kwoty, takie jak dzieło „Everydays: The First 5000 Days", autorstwa Beeple, która w marcu 2021 r. sprzedała się za ponad 69 mln USD [Palumbo, 2022]. Rynki, na których można szybko przenosić znaczne kwoty pieniędzy, są narażone na pranie pieniędzy. Rynki NFT mogą być w szczególności narażone na pranie pieniędzy, polegające na kupowaniu towarów i usług w celu ukrycia nielegalnych dochodów. Metody te są rozpowszechnione w świecie sztuki fizycznej i antyków, stąd rynki NFT są również narażone na podobne, a nawet większe ryzyko. Typowy **modus operandi prania pieniędzy przy użyciu NFT** jest następujący:

1) Przestępca posiada nielegalne kryptowaluty pochodzące z działalności takiej jak hakowanie giełd kryptowalut.
2) Przestępca używa mixera do prania skradzionego etheru lub tokenów opartych na Ethereum, otrzymując w zamian „czyste" środki.
3) Przestępca przesyła nowy, czysty ether na rynek NFT i kupuje NFT.
4) Przestępca może próbować sprzedać NFT, nawet za większą cenę. Wpływy ze sprzedaży NFT pozwalają przestępcy wykazać je jako swoje oficjalne źródło funduszy.

10. Podsumowanie

Celem artykułu była identyfikacja najważniejszych przestępstw związanych z kryptowalutami oraz praniem pieniędzy przy użyciu technologii blockchain, która jest wygodnym narzędziem dla znacznej grupy przestępców i terrorystów. Przy utrzymaniu trendu wzrostu wartości rynku kryptoaktywów bez jednoczesnego, jeszcze szybszego, rozwoju regulacji, technologia blockchain umożliwiłaby nieskrępowany dostęp do płynności dla przestępców. Widoczne jest zaangażowanie rządów bogatych krajów w zwiększaniu wymogów regulacyjnych dla kluczowych ogniw tego systemu, czyli giełd kryptowalut – umożliwia to przyjęcie technologii wśród biznesu i konsumentów zabierając przestępcom dostęp do finansowania – co najmocniej jest widoczne w spadku udziału nielegalnych środków w wolumenie

transkacji na blockchainach. Z drugiej strony wzrasta wartość okupów zdobytych przy użyciu oprogramowania ransomware, a także liczba prostych oszustw, których ofiarami padają przeciętni konsumenci. W odpowiedzi na to rządy na całym świecie, na czele z USA, koncentrują uwagę na dostawcach usług służących do prania pieniędzy oraz we współpracy z rynkiem prywatnym rozwijają swoje metody śledcze pozwalające deanonimizować użytkowników blockchaina, a następnie wymierzać im wyroki.

Podsumowując, rozpowszechnienie się aktywów opartych na blockchain zwiększa możliwości prania pieniędzy, jak i tworzy nowe, bezpieczniejsze dla przestępców metody zdobywania kapitału. Jednym z rozwiązań tego problemu mogłoby być zwiększenie reżimu regulacyjnego oraz szerzenie wiedzy o cyberprzestępczości wśród pracowników instytucji finansowych odpowiedzialnych za przeciwdziałanie praniu pieniędzy. Pamiętajmy jednak, że cyberprzestrzeń daje przestępcom globalne możliwości i dużą dozę anonimowości, co nie tylko potencjalnie napędza oszustwa, wymuszenia i ataki hakerskie na różną skalę, ale także utrudnia pozyskanie wiarygodnych danych o skali i rodzajach dokonywanych nadużyć. Pamiętajmy jednak, że kryptoaktywa tracą wszyscy – od przypadkowych ludzi, którzy zaufali nieznajomemu z portalu społecznościowego, poprzez dużych prywatnych inwestorów, aż po przedsiębiorstwa krytyczne dla gospodarki i bezpieczeństwa państwa (*vide* atak hakerski na rurociąg Colonial w Stanach Zjednoczonych, w którym okupem było 75 bitcoinów) [United Stated Department of Energy, 2021].

Bibliografia

1. Akartuna E.A., Nadini M., DePow C., Annison T. [2022], *NFTs and Financial Crime: Money Laundering, Market Manipulation*, Scams & Sanctions Risks in Non-Fungible Tokens.
2. Armstrong S. [2016], *Move over Bitcoin, the blockchain is only just getting started*, https://www.wired.co.uk/article/unlock-the-blockchain (dostęp: 31.03.2023).
3. Association of Certified Fraud Examiners [2021], *Fraud Examiners Manual 2021 Edition*.
4. Bank for International Settlements (BIS) [2015], *Digital currencies*, Committee on Payments and Market Infrastructures, https://www.bis.org/cpmi/publ/d137.pdf (dostęp: 10.10.2023).
5. Binance Academy [2020], *Merkle Trees and Merkle Roots Explained*, 6 July, https://academy.binance.com/en/articles/merkle-trees-and-merkle-roots-explained (dostęp: 7.01.2022).
6. Binance Academy [2023], *Rug Pull*, https://academy.binance.com/uk/glossary/rug-pull (dostęp: 31.03.2023).
7. Bing C. [2022], *Russia-based ransomware group Conti issues warning to Kremlin foes*, https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022–02–25/ (dostęp: 3.08.2023).
8. Bonderud D., *The importance of KYC for crypto exchanges*, https://withpersona.com/blog/kyc-crypto (dostęp: 23.01.2023).

9. Braue D. [2022], *Global Ransomware Damage Costs Predicted To Exceed $ 265 Billion By 2031*, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (dostęp: 2.08.2023).
10. Carlisle D. [2022a], *Preventing Financial Crime in Cryptoassets: The Definitive Practical Guide for Governance*, Risk and Compliance Professionals.
11. Carlisle D. [2022b], *OFAC Ransomware Crackdown Targets SUEX Crypto Exchange That Has Received More than $ 900 Million*, https://www.elliptic.co/blog/ofac-ransomware-crackdown-targets-suex-crypto-exchange-that-has-received-more-than-900-million (dostęp: 24.08.2023).
12. Chainalysis [2021a], *The 2021 Crypto Crime report*, https://go.chainalysis.com/2021-Crypto-Crime-Report.html (dostęp: 31.03.2023).
13. Chainalysis [2021b], *The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs*, https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/ (dostęp: 3.08.2023).
14. Chainalysis [2022a], *The 2022 Crypto Crime Report*, https://go.chainalysis.com/2022-Crypto-Crime-Report.html (dostęp: 31.03.2023).
15. Chainalysis [2022b], *Meet the Malware Families Helping Hackers Steal and Mine Millions in Cryptocurrency*, https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/ (dostęp: 22.08.2023).
16. Chainalysis [2023], *The 2023 Crypto Crime Raport*, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf (dostęp: 31.03.2023).
17. Cheng A. [2021], *'Squid Game' – inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam*, https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/ (dostęp: 3.08.2023).
18. Commodity Futures Trading Commission [2021], *CFTC Charges 14 Entities for Failing to Register as FCMs or Falsely Claiming to be Registered*, Release Number 8434–21, 29.09.2021, https://www.cftc.gov/PressRoom/PressReleases/8434–21 (dostęp: 4.08.2023).
19. Computer Emergency Team of Ukraine [2022], *Fragment of the investigation into cyber attacks 14.01.2022*, https://cert.gov.ua/article/18101 (dostęp: 3.08.2023).
20. Crowdstrike [2022a], *Global Threat Report*, https://www.crowdstrike.com/global-threat-report/ (dostęp: 31.03.2023).
21. Crowdstrike [2022b], *What is Crypto-Malware?* https://www.crowdstrike.com/cybersecurity-101/malware/crypto-malware/ (dostęp: 22.08.2023).
22. Crowdstrike [2023], *Take a Hike Ransomware, Deter ransomware with CrowdStrike protection for your AWS environments*, https://www.crowdstrike.com/wp-content/uploads/2023/06/crowdstrike-aws-ransomware-ebook.pdf (dostęp: 31.03.2023).
23. Culpan T. [2021], *Beware the Chinese Ransomware Attack With No Ransom*, https://www.bloomberg.com/opinion/articles/2021–11–17/what-a-chinese-ransomware-attack-tells-us-about-the-future-of-cyber-warfare (dostęp: 31.03.2023).
24. Dailey N. [2022], *NFTs ballooned to a $ 41 billion market in 2021 and are catching up to the total size of the global fine art market*, https://markets.businessinsider.com/news/currencies/nft-market-41-billion-nearing-fine-art-market-size-2022-1?op=1 (dostęp: 26.08.2023).

25. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency [2022], *North Korea Cyber Threat Overview and Advisories*, https://www.cisa.gov/uscert/northkorea (dostęp: 3.08.2023).
26. Elliptic [2021], *Liquid Exchange Hacked: $97 Million Stolen*, https://www.elliptic.co/blog/liquid-exchange-hacked-94-million-stolen (dostęp: 20.08.2023).
27. Ethereum Foundation [2023], *Blockchain bridges*, https://ethereum.org/en/bridges/ (dostęp: 25.08.2023).
28. Europol [2017], *Virtual Currencies Money Laundering Typologies: Targeting Exchanges and Other Gatekeepers*.
29. Europol [2021], *Internet Organised Crime Threat Assessment (IOCTA)*, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads (dostęp: 31.03.2023).
30. Financial Action Task Force [2014], *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (dostęp: 31.03.2023).
31. Financial Action Task Force [2020], *Virtual Assets. Red Flag Indicators of Money Laundering and Terrorist Financing*, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html (dostęp: 31.03.2023).
32. Flitter E. [2013], *Hackers switch to new digital currency after Liberty Reserve*, https://www.reuters.com/article/net-us-cybercrime-digital-currency idUSBRE9780GM20130809 (dostęp: 23.01.2023).
33. Foley S., Karlsen J.R., Putniņš T.J. [2019], *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?* „The Review of Financial Studies", vol. 32(5), s. 1798–1853, https://doi.org/10.1093/rfs/hhz015.
34. CoinGecko [2023], *Global Cryptocurrency Market Cap Charts*, https://www.coingecko.com/en/global-charts (dostęp: 31.03.2023).
35. IBM [2022a], *X-Force Threat Intelligence Index* 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ (dostęp: 31.03.2023).
36. IBM [2022b], *Definitive guide to ransomware* 2022, https://www.ibm.com/downloads/cas/EV6NAQR4 (dostęp: 31.03.2023).
37. IBM [2022c], *Cost of a Data Breach Report*, https://www.ibm.com/reports/data-breach (dostęp: 30.06.2023).
38. IBM, *What is blockchain technology?* https://www.ibm.com/se-en/topics/what-is-blockchain (dostęp: 7.01.2023).
39. IC3 [2021], *Internet Fraud Report*, https://www.ic3.gov/media/pdf/annualreport/2021_IC3Report.pdf (dostęp: 31.03.2023).
40. Kauflin J. [2019], *Visa Enters The $125 Trillion Global Money Transfer Market With New Blockchain Product*, https://www.forbes.com/sites/jeffkauflin/2019/06/11/visa-targets-swift-with-new-blockchain-product-for-global-money-transfers/ (dostęp: 7.01.2023).
41. Kuchta R. [2020], *Video games, virtual currencies, and money laundering*, https://newtech.law/en/video-games-virtual-currencies-and-money-laundering/ (dostęp: 23.01.2023).
42. Library of Congress, *Cryptocurrency & Blockchain Technology*, https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain (dostęp: 7.01.2023).

43. Malik N. [2018], *How Criminals And Terrorists Use Cryptocurrency: And How To Stop It*, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/ (dostęp: 7.01.2023).
44. Martysz C. [2021], *Charakterystyka wybranych nadużyć na rynku finansowym*, w: Ostaszewski J., Iwanicz-Drozdowska M. (red.), *Finanse u progu trzeciej dekady XXI wieku*, Tom I, Difin, Warszawa.
45. Martysz C.B., Królikowska A. [2021], *Piramidy finansowe (PF) i schematy Ponziego (SP) a marketing wielopoziomowy (MLM)*, w: Wielgórska-Leszczyńska J., Matusewicz M. (red.), *Nauki ekonomiczne przed, w czasie i po pandemii*, Oficyna Wydawnicza SGH, Warszawa.
46. McKinsey&Company [2023], *What is central bank digital currency (CBDC)?* 1 March, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-central-bank-digital-currency-cbdc (dostęp: 10.10.2023).
47. Mehrotra K, Turton W. [2021], *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, https://www.bloomberg.com/news/articles/2021–05–20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack (dostęp: 3.08.2023).
48. Microsoft [2021], *Evolving trends in Iranian threat actor activity*, https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/ (dostęp: 3.08.2023).
49. Murphy B. [2021], *Living Off the Land Ransomware Attacks: A Step-By-Step Plan for Playing Defense*, https://www.cyberark.com/resources/blog/living-off-the-land-ransomware-attacks-a-step-by-step-plan-for-playing-defense (dostęp: 2.08.2023).
50. Palumbo J. [2022], *First NFT artwork at auction sells for staggering $69 million*, https://edition.cnn.com/style/article/beeple-first-nft-artwork-at-auction-sale-result/index.html (dostęp: 25.08.2023).
51. Peng I. [2022], *Hackers Nabbed $1.3 Billion in Ransom Over 2 Years, a New Report Says*, https://www.bloomberg.com/news/articles/2022–02–10/hackers-nabbed-1–3-billion-in-ransom-over-2-years-report-says (dostęp: 3.08.2023).
52. Piech K. (red.) [2017], *Podstawy korzystania z walut cyfrowych*, Instytut Wiedzy i Innowacji, https://cyfrowaekonomia.pl/wp-content/uploads/2017/12/Podstawy-walut-cyfrowych.pdf (dostęp: 1.10.2023).
53. Raj A. [2022], *Russian hackers profited the most from ransomware payments*, https://techhq.com/2022/02/russian-hackers-ransomware-payments/ (dostęp: 3.08.2023).
54. Rees K. [2022], *What Are Crypto Cloud Mining Scams?* https://www.makeuseof.com/what-are-crypto-cloud-mining-scams/ (dostęp: 4.08.2023).
55. *Rejestr działalności w zakresie walut wirtualnych*, https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych (dostęp: 1.10.2023).
56. Ropek L. [2022], *What Is 'Pig Butchering,' the Crypto Scam That's Flooding the FBI's Phone Lines?* https://gizmodo.com/what-is-a-pig-butchering-crypto-scam-1849316921 (dostęp: 3.08.2023).
57. Seth A. [2022], *A $540 m Crypto Scam Using RenBridge Has Come to Light*, Coindaily, https://dailycoin.com/a-540 m-crypto-scam-using-renbridge-has-come-to-light/ (dostęp: 25.08.2023).

58. United States Attorney's Office [2021], *Director and Promoter of BitConnect Pleads Guilty in Global $ 2 Billion Cryptocurrency Scheme*, 1 September, https://www.justice.gov/usao-sdca/pr/director-and-promoter-bitconnect-pleads-guilty-global-2-billion-cryptocurrency-scheme (dostęp: 4.08.2023).
59. United States Attorney's Office [2013], *Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $ 6 Billion Money Laundering Scheme*, 28 May, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest (dostęp: 23.01.2023).
60. United States Attorney's Office [2023], *Tornado Cash Founders Charged With Money Laundering And Sanctions Violations*, 23 August, https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations (dostęp: 10.10.2023).
61. United States Department of Energy [2021], *Colonial Pipeline Cyber Incident*, Office of Cybersecurity, Energy Security, and Emergency Response, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident (dostęp: 2.08.2023).
62. United States Department of the Treasury [2022], *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, 8 August, https://home.treasury.gov/news/press-releases/jy0916 (dostęp: 24.08.2023).
63. United States Senate Comittee on Homeland Security & Goverment Affairs [2022], *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns*, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC Majority Cryptocurrency Ransomware Report_Executive Summary.pdf (dostęp: 30.06.2023).
64. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz.U. 2022, poz. 1138).
65. Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2023, poz. 1124).
66. Viettel Security [2022], *Leaking Critical Personal Information Due to Various Types of Information-stealing Malware*, *Redline Stealer*, https://viettelcybersecurity.com/wp-content/uploads/2022/02/Report-Redline-Stealer.pdf (dostęp: 20.06.2023).
67. Wade A., Lewellen M., Van Valkenburgh P. [2022], *How does Tornado Cash work*, https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ (dostęp: 25.08.2023).
68. Walk-Morris T. [2022], *Scammers have been around forever. Then came crypto*, https://www.grid.news/story/technology/2022/06/22/scammers-have-been-around-forever-then-came-crypto/ (dostęp: 4.08.2023).

Cryptocurrencies v. financing crime and money laundering

Summary

The aim of this article is to identify the most important types of crime related to cryptocurrencies and money laundering, utilizing the infrastructure based on blockchain technology. The development in the area of decentralized finance for a long time preceded the decisions of regulators, which only when the market increased in value substantially started to act, implementing limits and rules known from traditional finance. Despite these measures, the scale of crimes using the assets has been on the rise all the time: the growing interest of retail investors creates a feedback loop, as they increasingly become victims of crimes and provide the liquidity necessary for money laundering.

Keywords: blockchain, money laundering, cybercrime, cryptocurrencies