KRYPTOWALUTY
WYBRANE KLUCZOWE ASPEKTY

Sygn. PAB/WIB 5/2023

Raport przygotowany na zlecenie
Fundacji Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY

Warszawa, kwiecień 2023

O raporcie

Raport **Kryptowaluty wybrane kluczowe aspekty** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy

Raport został opracowany przez zespół w składzie:

prof. dr hab. Mirosław Kutyłowski

dr Elżbieta Lewańska

dr inż. Przemysław Błaśkiewicz

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

Spis treści

PROGRAM ANALITYCZNO BADAWCZY

1. Struktura rynku kryptowalut

Kryptowaluty charakteryzują się dużą zmiennością wartości. W lutym 2023 roku kapitalizacja rynku kryptowalut oceniana była na 1,12 bln USD, choć zaledwie w listopadzie 2021 roku osiągała blisko 3 bln USD. W rozdziale przedstawiono charakterystykę trzech kryptowalut o największej kapitalizacji rynkowej: bitcoin, ether oraz tether. Omówiono również profil użytkowników kryptowalut. Raporty branżowe wskazują, że większość użytkowników kryptowalut stanowią młodzi mężczyźni, jednak udział innych grup stale rośnie (szczególnie udział kobiet). Rozdział kończy przedstawienie przykładowych firm działających na rynku kryptowalut oraz charakterystyka produktów i usług, które są przez nie oferowane.

1.1 Omówienie wielkości rynku (wartość, obroty, zmienność w czasie) w ujęciu globalnym oraz dla wybranych regionów

Rynek kryptowalut charakteryzuje się dużą zmiennością. Wartość globalna kapitalizacji rynkowej dla wszystkich kryptowalut i tokenów[1] 19 lutego 2023 roku wynosiła 1 121 720 516 306 USD (1,12 bln USD) – według platformy CoinMarketCap.com, która rejestruje dane o blisko 10 tys. kryptowalutach i tokenach (ok. 950 kryptowalut, blisko 8 tys. tokenów) z ponad 22 tys. istniejących monet, będących w obrocie na 534 giełdach2. Warto jednak wskazać, że w roku 2022 nastąpił znaczny spadek wartości dwóch największych kryptowalut, Bitcoin i Ethereum, co przełożyło się na spadek kapitalizacji rynkowej. W listopadzie 2021 roku była ona wyceniana nawet na blisko 3 bln USD, a Bitcoin miał wówczas kurs 65 tys. USD (Gemini, 2022). Szczegółowe dane można śledzić na witrynach, które agregują informacje o kapitalizacji, na przykład CoinMarketCap (https://coinmarketcap.com/charts/).

Rok 2021 wskazuje się jako przełomowy dla kryptowalut: globalnie ok 45% użytkowników kryptowalut ankietowanych na przełomie roku 2021 i 2022 deklarowało, że po raz pierwszy zainwestowało w kryptowaluty w 2021 r. (w Europie było to 40%) (Gemini, 2022).

Monety z najwyższą kapitalizacją rynkową na dzień 18 lutego 2023 roku przedstawione są w tabeli 1. Wskazano w niej też przykładowe historyczne kursy (sprzed 3, 6 i 12 miesięcy), co pokazuje wielkość zmian wartości na przestrzeni stosunkowo krótkiego okresu. Na rysunkach 1 i 2 przedstawione są wykresy przedstawiające wartość wybranych kryptowalut na przestrzeni lat. Należy zaznaczyć, że zmienność rynku kryptowalut jest na tyle duża, że zestawienie walut o największej kapitalizacji rynkowej zmienia się dynamicznie. Liderem jest Bitcoin, następnie Ether i Tether.

Obroty najpopularniejszych monet obecnie sięgają miliardów dolarów na dobę. Największe obroty notują Tether i Bitcoin (patrz tabela 2). Tether jest popularny, ponieważ jest to tzw. stabilna moneta (stable coin), której kurs jest powiązany z dolarem amerykańskim. Natomiast Bitcoin jest najlepiej zaadoptowany na rynku, ponieważ jest najlepiej rozpoznawalną i pierwszą powstałą kryptowalutą. Obie te monety zostały szerzej opisane w dalszej części tego rozdziału.

Bitcoin (BTC) jest pierwszą kryptowalutą, wprowadzono go na rynek w 2009 roku. Twórca (bądź twórcy) Bitcoin podpisuje się pseudonimem Satoshi Nakamoto. Do dziś nie jest znana jego prawdziwa tożsamość. Nakamoto brał aktywny udział w tworzeniu i zarządzaniu Bitcoin do końca 2010 roku. Bitcoin opiera się na zdecentralizowanej technologii peer-to-peer (P2P), a więc nie ma podmiotu, który byłby odpowiedzialny za jego emisję. Maksymalna podaż BTC została ustalona na 21 mln jednostek, co ma zapobiec inflacji tej kryptowaluty. Budowa sieci sprawia, że podaż bitcoin znacznie spada w czasie (mniej więcej o połowę co cztery lata). Połowa planowanej liczby bitcoinów została wyemitowana przed końcem roku 2013. Szacuje się, że emisja zostanie całkowicie zakończona ok. roku 2140, obecnie (stan na luty 2023 roku) wyemitowano 92% bitcoinów. Co ciekawe, według (Phillips, 2021) ok. 3,7 mln BTC zostało bezpowrotnie utraconych, ponieważ ich właściciele stracili dostęp do portfela, w których były przechowywane (przede wszystkim poprzez utratę klucza prywatnego, a więc brak możliwości odszyfrowania portfela). Spadająca w czasie wartość nagród w sieci Bitcoin (tj. rosnąca trudność generowania nowych jednostek) powoduje, że pierwsi użyt-

1 Kryptowaluty to jednostka wartości wymiany dla konkretnego protokołu blockchain. Tokeny to jednostki wartości generowane przez smart contracts na danym protokole. Potocznie nazwa kryptowaluty obejmuje oba te znaczenia. Dla uproszczenia wywodu, pod hasłem „rynek kryptowalut" należy rozumieć rynek kupna, sprzedaży, wymiany i przechowywania kryptowalut oraz tokenów. Kryptowalutu i tokeny nazywane są również monetami (ang. coins).

2 Stan na dzień 02.01.2023 według https://coinmarketcap.com/ . CoinMarketCap.com rejestruje szczegółowe informacje tylko o części kryptowalut i tokenów, jednak w statystykach kapitalizacji rynkowej podaje całkowitą sumę.

Tabela 1. Kursy wybranych kryptowalut

Nazwa	Kurs w USD (14.11.21)	kurs w USD (14.08.22)	kurs w USD (13.11.22)	kurs w USD (18.02.23)	Kapitalizacja rynkowa (18.02.23)	Ilość w obiegu (18.02.23)
Bitcoin (BTC)	65 466,84	24 319,33	16 353,37	21 788,20	420,3 mld	19,3 mln BTC
Ether (ETH)	4 626,36	1 936,80	1 221,82	1 515,03	185,4 mld	122,4 mln ETH
Tether (USDT)	1,00	1,00	0,9988	1	68,4 mld	68 386,6 mln USDT
Binance Coin (BNB)	650,92	317,99	276,58	312,93	49,4 mld	157,9 mln BNB
USD Coin (USDC)	0,9996	0,9998	1,00	1	41,2 mld	41 219,4 mln USDC
XRP (XRP)	1,19	0,3765	0,3403	0,3753	19,1 mld	50 799,1 mln XRP
Binance USD (BUSD)	0,9999	0,9999	1,00	1,00	16,2 mld	16 148,9 mln BUSD
Cardano (ADA)	2,04	0,5703	0,3301	0,3643	12,6 mld	34 626,9 mln ADA
Dogecoin (DOGE)	0,2629	0,08169	0,08489	0,08214	10,9 mld	132 670,8 mln DOGE
Polygon (MATIC)	1,73	1,00	0,8881	1,24	10,9 mld	8 734,3 mln MATIC

Źródło: opracowanie własne.

kownicy tej kryptowaluty mają ogromną przewagę nad tymi, którzy dołączyli do sieci później, i to właśnie oni najbardziej skorzystali na wzroście wartości bitcoina, który miał miejsce do połowy 2021 roku.

Bitcoin jest najpopularniejszą kryptowalutą, zarówno pod względem rozpoznawalności nazwy w społeczeństwie, jak i liczby użytkowników oraz obrotów. Efekt sieciowy sprawia, że pomimo coraz większej konkurencji na rynku kryptowalut, Bitcoin przez cały czas pozostaje na pierwszym miejscu pod względem kapitalizacji rynkowej. Jest to kryptowaluta o bardzo dużej płynności i jedna z nielicznych, które są akceptowane przez niektóre podmioty w handlu. Adopcja bitcoin na rynkach postępuje powoli, co jest związane z brakiem regulacji oraz dużą zmiennością wartości kryptowalut, jednak stopniowo się on upowszechnia. Przykładowo, El Salvador przyjął Bitcoin jako środek płatniczy w 2021 roku (BBC.com, 2021), jednak Międzynarodowy Fundusz Walutowy przestrzega przed dalszą adopcją kryptowalut (Golubova, 2023). Niektóre firmy, na przykład Balenciaga[3], zaczęły akceptować płatności w Bitcoin.

Ze względu na budowę sieci Bitcoin i użycie zdecentralizowanej bazy danych przechowującej transakcje,

3 Płatność w kryptowalutach jest dostępna tylko dla klientów ze Stanów Zjednoczonych, https://www.balenciaga.com/en-us

Tabela 2. Obroty wybranych kryptowalut (stan na dzień 19.02.2023)

Nazwa	Obroty 24h w mld USD	Obroty 7d w mld USD	Obroty 30d w mld USD
Bitcoin (BTC)	20,7	244,1	689
Ether (ETH)	6	77	200
Tether (USDT)	32,7	202,8	1068
Binance Coin (BNB)	1,54	10,74	37,44
USD Coin (USDC)	0,49	3,5	15,8
XRP (XRP)	0,55	7,8	18,7
Binance USD (BUSD)	5,9	38,5	196,7
Cardano (ADA)	0,3	2,12	9,5
Dogecoin (DOGE)	0,46	3,1	12,7
Polygon (MATIC)	0,6	4,6	25,7

Źródło: opracowanie własne na podstawie CoinMarketCap.com

Bitcoin uznawany jest za walutę bezpieczną i odporną na manipulacje wartością przez organizacje rządowe, finansowe lub prywatne. Jest jednak podatny na spekulacje ceną. Ponadto, sieć Bitcoin teoretycznie jest podatna na atak typu „51%" – tj. w przypadku przejęcia ponad 50% mocy obliczeniowej sieci Bitcoin będzie możliwe przejęcie nad nią kontroli. Przy obecnym poziomie technologicznym taki atak jest jednak bardzo mało prawdopodobny, ponieważ wymagałby ogromnych zasobów sprzętowych i energii elektrycznej – pozyskanie obu tych elementów wiązałoby się z olbrzymimi kosztami.

Jako że bitcoin był pierwszą kryptowalutą, to jego techniczna implementacja nie jest tak zaawansowana, jak innych sieci blockchain wprowadzonych później. Jedną z istotnych wad jest negatywny wpływ sieci Bitcoin na środowisko naturalne. Obliczanie PoW wymaga ogromnych ilości energii elektrycznej: jedna transakcja Bitcoin zużywa w przybliżeniu tyle energii, co gospodarstwo domowe w USA przez miesiąc, a roczny ślad węglowy jest porównywalny z produkowanym przez Finlandię (Portal Digicomist, 2023). Rozbudowa sieci wymaga też zakupu sprzętu komputerowego o dużej mocy obliczeniowej.

Transakcje Bitcoin są jawne, ale anonimowe (tj. znany jest czas i kwota transakcji, ale właściciele środków pozostają anonimowi). Są one również nieodwracalne, tj. nie ma możliwości ich cofnięcia w przypadku popełnienia błędu.

Rysunek 1 przedstawia wykres cen bitcoin wyrażonych w USD od 2015 roku do połowy lutego 2023 roku. Badania (Auer, Cornelli, i in., 2022) prowadzone w latach 2015–2022 wskazują, że wzrost wartości Bitcoin koreluje ze wzrostem liczby użytkowników kryptowalut (badania wskazują również, że wpływ innych czynników, na przykład sytuacji gospodarczej w danym kraju jest mniejszy, niż wzrost ceny Bitcoin). Autorzy wykorzystali statystyki dotyczące pobrań aplikacji giełd kryptowalut.

Ether (ETH) to nazwa kryptowaluty opartej na blockchain Ethereum (jednak w Internecie, również na giełdach kryptowalut, często również kryptowaluta nazywana jest Ethereum).

ETH nie ma ograniczenia podaży, więc może podlegać inflacji. Ethereum zostało wydane w 2015 roku (Tual, 2015). Aż 50 mln z początkowej podaży 72 mln zostało sprzedanych w publicznej sprzedaży[4]

4 ICO, Wstępna Oferta Monet, to metoda gromadzenia funduszy poprzez wygenerowanie pewnej początkowej puli tokenów i ich sprzedaż wczesnym inwestorom. Jest to rodzaj finansowania społecznościowego stosowany w przypadku kryptowalut.

Rysunek 1. Ceny bitcoin w USD

Źródło: opracowanie własne.

w 2014 roku. Pozwoliło to w krótkim czasie zebrać fundusze na rozwój platformy oraz zaangażować stosunkowo dużą grupę użytkowników. Ether ma wielu zwolenników i ugruntowaną pozycję na rynku. Niemal od początku istnienia, bo od 2016 roku, niezmiennie znajduje się na drugim miejscu pod względem kapitalizacji rynkowej. Jest to stabilna sieć, z dużą i aktywną społecznością deweloperów (Ethereum jest blockchainem typu open-source) i ma dobrze zdefiniowaną mapę rozwoju do 2030 roku[5].

Ethereum jest siecią zdecentralizowaną, jednak wskazuje się, że początkowa pula przekazana inwestorom (50 mln) wciąż stanowi aż 40% udziału w rynku ETH (obecna podaż to ok. 122 mln jednostek).

Od grudnia 2022 roku Ethereum wykorzystuje mechanizm Proof-of-Stake zamiast Proof-of-Work, co pozwoliło obniżyć zużycie energii nawet o 99,9% w porównaniu do Bitcoin (Beekhuizen, 2021; De Vries, 2022).

W sieci Ethereum funkcjonują wysokie prowizje od transakcji, tzw. gas fee. Powodują one, że transakcje na małe kwoty nie są opłacalne, ale równocześnie stanowią zabezpieczenie przed atakami typu DDoS[6]. Wysokie opłaty za uruchomienie własnego węzła, wynoszące 32 ETH (w lutym 2023 roku było to ok. 45 tys. USD), chronią przed atakiem typu „51%", który pozwoliłby na przejęcie kontroli nad siecią.

Na Ethereum można uruchamiać aplikacje nazywane smart contracts i generować inne tokeny. Tether i USD Coin to przykłady tokenów wykorzystujących sieć Ethereum.

Rysunek 2 przedstawia wykres cen ether wyrażonych w USD od 2015 roku do połowy lutego 2023 roku.

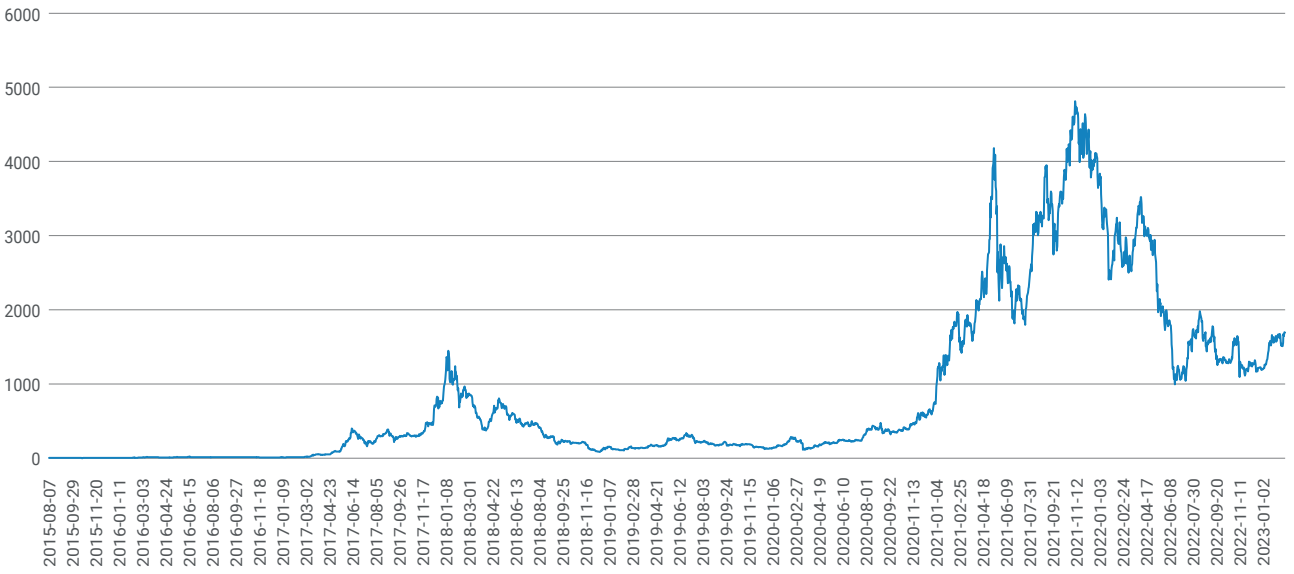
Tether (USDT) to tzw. stablecoin[7], którego wartość jest powiązana z dolarem amerykańskim (tj. 1 USDT ma w przybliżeniu wartość 1 USD). Tehter miał pierwszą emisję w 2014 roku, został opracowany przez firmę Tether Limited Inc., która z kolei należy do iFinex Inc. Więcej informacji o Tether można znaleźć w White Paper (Tether Limited Inc., 2022). W przeciwieństwie do bitcoin i ether,

5 https://ethereumroadmap.com/

6 Distributed denial of service, rozproszona odmowa usługi, atak polegający na zablokowaniu działania usługi lub serwera poprzez zajęcie wszystkich dostępnych zasobów, na przykład przez wysyłanie wielu zapytań równocześnie z rozproszonej sieci komputerów.

7 Stablecoins – tokeny zaprojektowane w sposób, który ma im umożliwić utrzymanie stałej mocy nabywczej. Cel ten jest realizowany poprzez powiązanie wartości stablecoina z wybraną walutą FIAT, produktem notowanym na giełdzie lub inną kryptowalutą. Mechanizm ten nie jest jednak niezawodny, w przeszłości były przypadki, kiedy stablecoin tracił istotnie na wartości (na przykład Terra, spadek z $1 do 26 centów).

Rysunek 2. Ceny ether wyrażone w USD



Źródło: opracowanie własne.

tether jest tokenem, a nie kryptowalutą. Jest również scentralizowany (tj. tokeny wypuszcza tylko firma Tether Ltd, nie są one wydobywane przez społeczność, jak w przypadku BTC i ETH). Jego twórcy deklarują, że utrzymują rezerwę dolarową równą emisji tether, jednak nie zostało to potwierdzone w przeprowadzonych audytach.

Tether jest bardzo popularny wśród użytkowników kryptowalut. Jest to spowodowane m.in. małą zmiennością wartości (tj. użytkownicy mogą niejako przechowywać oszczędności w tej walucie, nie martwiąc się o stratę wartości, ale też nie licząc na zyski ze spekulacji).

Tether zyskał popularność m.in. dlatego, że ma bardzo dużą płynność. Dzięki powiązaniu z USD pozwala obejść ograniczenia formalne nałożone na sprzedaż kryptowalut w niektórych krajach (użytkownicy mogą zamienić inną walutę na tether, przenieść go na giełdę, która umożliwi zamianę tether na USD i wypłacić; mogą też używać tether jako pośredniego kroku przy wymianie innych kryptowalut, bez użycia walut FIAT i bez konieczności wypłacania środków).

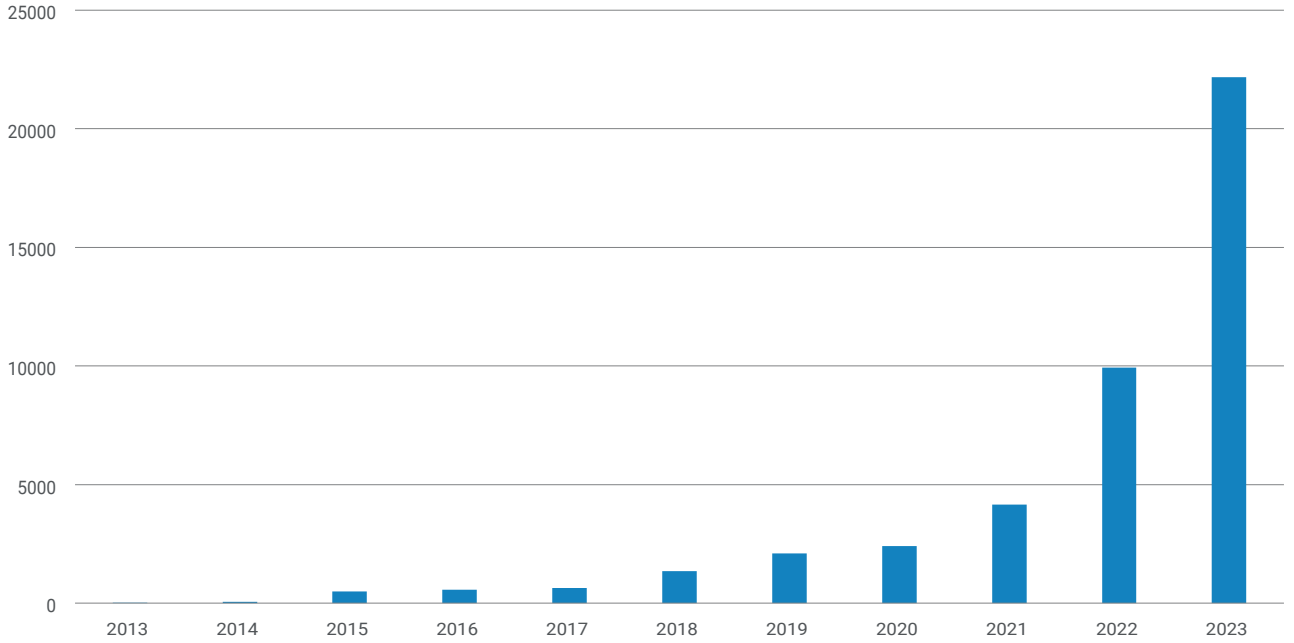
Z tetherem wiążą się również kontrowersje: firma iFinex jest również właścicielem giełdy Bitfinex. W 2019 roku iFinex zapłaciło 18,5 mln USD w ramach ugody w procesie o ukrywanie strat giełdy Bitfinex ze środków stanowiących rezerwę dla tether (firmę oskarżono o ukrywanie strat w wysokości 850 mln USD [Riley, 2021]).

Rynek kryptowalut rozwija się bardzo dynamicznie. Szczególnie w ostatnich dwóch latach obserwowany jest ogromny wzrost liczby kryptowalut i tokenów: z 4154 dostępnych na początku 2021 roku, do ponad 22 tys. w styczniu 2023 roku (patrz rysunek 3). Należy pamiętać, że część projektów upada lub jest wycofywana z rynku.

Duża zmienność wartości kryptowalut wynika m.in. z tego, że rynek wciąż nie jest bardzo duży, a monety spoza pierwszej dziesiątki pod względem kapitalizacji rynkowej mają umiarkowaną płynność. Liczbę użytkowników szacuje się na ok. 1 mld (więcej o demografii użytkowników w rozdziale 1.2), jednak należy pamiętać, że liczone są tutaj również osoby, które inwestują bardzo małe kwoty i nie zawierają wielu transakcji. Kryptowaluty są bardzo podatne na spekulacje i bardzo mocno reagują na zmiany w branży, na przykład problemy giełdy FTX i jej upadek spowodowały natychmiastowy spadek wartości bitcoin o ok. 25%. Zmienność wartości kryptowalut jest o wiele większa, niż walut fiat, złota czy największych indeksów giełdowych, co powoduje, że są one obecnie inwestycją bardzo wysokiego ryzyka (Auer, Farag, i in., 2022).

Wahania wartości kryptowalut powodują, że nie zyskują one dużej popularności jako środek płatniczy. Przykładowo – Tesla i Amazon początkowo zapowiadały wprowadzenie możliwości płatności w kryptowalutach, wycofały się jednak z tego pomysłu. Szczególny wpływ mają na tę decyzję wahania dzienne. Wskazuje się, że kryptowaluty nie staną się

Rysunek 3. Liczba kryptowalut i tokenów na rynku*



*Dane dla 2013 roku pochodzą z maja, pozostałe ze stycznia.

Źródło: opracowanie własne.

powszechnie zaadaptowanym środkiem płatniczym, jeżeli nie zostaną wcześniej uregulowane. Z tych samych powodów kryptowaluty nie są stosowane do wycen czy obliczania wskaźników ekonomicznych (Auer, Cornelli, i in., 2022).

Rynek kryptowalut jest rynkiem globalnym. Co prawda platformy wymiany kryptowalut działają tylko w wybranych krajach lub regionach (tj. oferują swoje usługi wyłącznie obywatelom wybranych krajów lub regionów), jednak nie da się wydzielić rynków lokalnych. Można za to analizować lokalizację nadawców i odbiorców transakcji, jak również udziały w rynku globalnym będące w posiadaniu użytkowników z różnych regionów. Firma Chainalysis opublikowała raport analizujący kryptowaluty pod względem geograficznym, jednak ostatnia dostępna wersja dotyczy roku 2021 (Chainalysis, 2021). Należy również mieć na uwadze, że analizy geograficzne opierają się częściowo na danych szacunkowych, szczególnie w odniesieniu do transakcji P2P. Raport ten wskazuje, że w 2021 roku kraje o najwyższym indeksie adaptacji kryptowalut[8], to: Wietnam, Indie, Pakistan, Ukraina, Kenia, Nigeria, Wenezuela, Stany Zjednoczone, Togo oraz Argentyna. Co ciekawe, podobny ranking, ale związany z adopcją rozwiązań DeFi, przedstawia się następująco: Stany Zjednoczone, Wietnam, Tajlandia, Chiny, Wielka Brytania, Indie, Holandia, Kanada, Ukraina, Polska. W raporcie Chainalysis można znaleźć również szacunki dotyczące udziału poszczególnych regionów w globalnym rynku kryptowalut (patrz rysunek 4).

1.2 Analiza demograficzna użytkowników (osób fizycznych) na podstawie danych udostępnianych przez giełdy kryptowalutowe

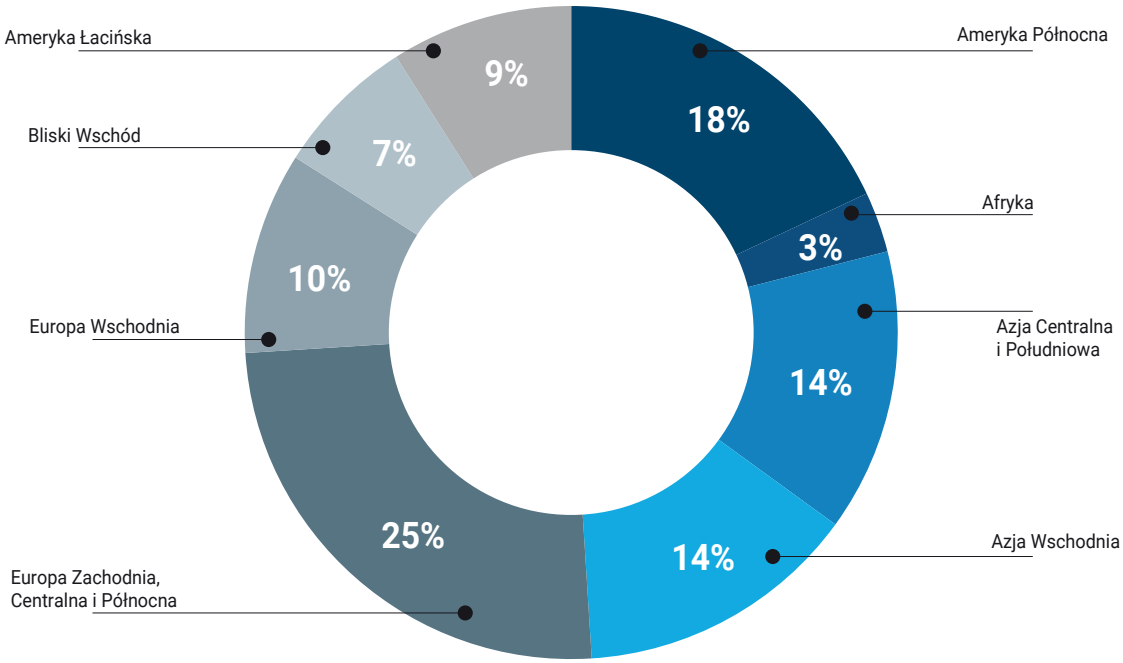
Według raportu portal crypto.com, liczba użytkowników kryptowalut na świecie miała przekroczyć 1 mld w roku 2022 (Hon i in., 2022), natomiast inni (Auer, Cornelli, i in., 2022) podają, że liczba użytkowników kryptowalut wzrosła z 5 mln w 2016 roku do ponad 220 mln w roku 2021.

Badania (Auer, Cornelli, i in., 2022) wskazują, że wśród użytkowników aplikacji platform wymiany kryptowalut[9] 40% stanowią młodzi mężczyźni (do 35 roku życia) – jest to równocześnie grupa, która wykazuje dużą akceptację ponoszenia ryzyka. Dla tej grupy motyw spekulacyjny jest bardziej istotnym po-

8 Jest to indeks obliczany przez Chainalysis, obejmujący wartość otrzymanych i przesłanych kryptowalut oraz obroty, ważonych wskaźnikiem siły nabywczej oraz liczby użytkowników internetu w danym kraju.

9 Dane pochodzą z 45 aplikacji na systemy Android i iOS, obejmują tylko aktywnych użytkowników w okresie I kw. 2020–II kw. 2022.

Rysunek 4. Regionalny podział transakcji przychodzących na rynku kryptowalut w czerwcu 2021 roku



Źródło: opracowanie na podstawie (Chainalysis, 2021).

wodem inwestycji w kryptowaluty, niż wskazywane w dalszej kolejności brak zaufania do publicznych instytucji finansowych czy przechowywania wartości. W sumie mężczyźni stanowią 68% użytkowników aplikacji platform wymiany kryptowalut, a osoby w wieku do 35 lat – 60%.

Ponadto, wskazuje się (Auer & Tercero-Lucas, 2021), że osoby, które wcześniej aktywnie używały bankowości cyfrowej są bardziej skłonne do inwestycji w kryptowaluty. To samo badanie nie potwierdziło popularnej tezy jakoby użytkownicy wybierali kryptowaluty z powodu obaw o bezpieczeństwo walut FIAT czy braku zaufania do systemu bankowego. Większość użytkowników kryptowalut nie traktuje ich też jako alternatywy dla walut tradycyjnych. Należy jednak podkreślić, że badanie (Auer & Tercero-Lucas, 2021) było prowadzone w USA. W tym badaniu wykazano, że osoby z wyższym wykształceniem oraz mężczyźni z większym prawdopodobieństwem posiadają kryptowaluty, niż pozostali. Natomiast prawdopodobieństwo znajomości choć jednej kryptowaluty rośnie wraz ze wzrostem poziomu dochodu oraz poziomu edukacji.

Jedna z wiodących na rynku giełd kryptowalut, Gemini, opublikowała na początku roku 2022 cykl raportów przedstawiających demografię użytkowników w różnych regionach świata oraz globalnie. Analizy te zostały przeprowadzone na reprezentatywnej grupie ankietowanych dla populacji osób dorosłych w wieku 18–75 lat osiągających roczny dochód min. 14 tys. USD (można przyjąć, że jest to wartość zbliżona do średniej pensji brutto w Polsce).

Choć wiele źródeł wskazuje, że typowi użytkownicy kryptowalut to młodzi, dobrze wykształceni mężczyźni (Auer & Tercero-Lucas, 2021), to w roku 2021 zauważalny był wzrost liczby kobiet wśród użytkowników. Raport Gemini (Gemini, 2022) wskazuje, że szczególnie w krajach rozwijających się odnotowuje się wysoki odsetek kobiet wśród użytkowników (na przykład 51% użytkowników w Izraelu, 51% w Indonezji, 50% w Nigerii, 40–45% w Brazylii, Kenii, Kolumbii, Meksyku, Singapurze, RPA). W krajach rozwiniętych odsetek kobiet wśród użytkowników wynosi ok. 30%, choć zdarzają się wyjątki, jak Francja gdzie wskaźnik ten osiąga 45%. Wskazuje się, że luka płciowa wśród użytkowników kryptowalut powoli się zamyka. Wśród ankietowanych, którzy deklarowali chęć zainwestowania w kryptowaluty w roku 2022 aż 47% stanowiły kobiety (rok wcześniej było to 40%).

Kryptowaluty są szczególnie popularne w krajach dotkniętych hiperinflacją: aż 59% ankietowanych

w Ameryce Łacińskiej i 58% w Afryce uważa, że kryptowaluty to pieniądz przyszłości (dla porównania w USA jest to tylko 23% ankietowanych, a w Europie niecałe 20%). Co więcej, w krajach, których waluta w ostatnich 10 latach dewaluowała względem dolara o 50% lub więcej, użytkownicy są pięciokrotnie bardziej skłonni do zakupu kryptowalut w przyszłości (Gemini, 2022). W krajach Ameryki Łacińskiej i Afryki aż 46% badanych uważa, że kryptowaluty to dobry sposób ochrony oszczędności przed inflacją. W USA i Europie jest to tylko 15–16% (według badań przeprowadzonych na przełomie lat 2021 i 2022 [Gemini, 2022]).

W momencie pisania tego raportu nie udało się znaleźć wiarygodnych i aktualnych szacunków odnoszących się do demografii użytkowników kryptowalut na rynku polskim.

Gemini opublikowała natomiast raport dotyczący demografii użytkowników kryptowalut w Wielkiej Brytani (jest to jedyny raport regionalny opublikowany przez Gemini dotyczący Europy [Gemini, 2021]). Jego wyniki są spójne z wynikami raportu globalnego: typowy użytkownik to mężczyzna w wieku 25–34 lata (choć kobiety stanowią aż 40% inwestorów na tym rynku). 40% użytkowników kryptowalut posiada w kryptowalutach mniej niż 1000 funtów, 37% posiada kryptowaluty o wartości od 1000 do 5000 funtów. Użytkownicy kryptowalut w Wielkiej Brytanii najczęściej pracują na pełen etat i są pracownikami w branżach: IT i telekomunikacja, architektura, inżynieria i budownictwo oraz retail. Są to również osoby zaliczane do grupy wcześniej przysposabiających innowacje (early adopters): 62,5% posiada samochód elektryczny lub hybrydowy, 67% korzysta z zabezpieczeń biometrycznych.

1.3 Charakterystyka najważniejszych firm działających na rynkach kryptowalut

Platformy wymiany kryptowalut

Wśród platform wymiany kryptowalut można wyróżnić:

- tradycyjne giełdy kryptowalut – pełnią rolę pośrednika między kupującymi i sprzedającymi, którzy zawierają transakcje po cenie rynkowej (podobnie jak giełdy papierów wartościowych). Giełda pobiera prowizję od każdej transakcji. Część z nich umożliwia również wymianę walut fiat na kryptowaluty;
- brokerzy – sprzedają i kupują kryptowaluty po cenie, którą proponuje broker (jest to zwykle cena rynkowa powiększona o marżę brokera);
- platformy wymiany bezpośredniej – pozwalają na transakcje P2P[10], nie korzystają z cen rynkowych, a z ustalonych między stronami (zazwyczaj narzuconych przez sprzedających). Jest to zazwyczaj rozwiązanie mniej korzystne dla kupujących, ale ze względu na ograniczenia prawne, w niektórych rejonach może być to jedyny sposób zakupu kryptowalut. Transakcje OTC[11] oferowane są również przez wybrane giełdy i brokerów.

Aktualnie działa ponad 500 platform wymiany kryptowalut. Różnią się one nie tylko pod względem liczby użytkowników i wolumenu transakcji, ale też liczby obsługiwanych monet, liczby obsługiwanych walut FIAT możliwości zamiany kryptowalut na waluty FIAT (niektóre giełdy umożliwiają tylko zakup kryptowalut i ich wymiany na inne, ale nie wypłaty w walutach FIAT), obszarem działalności (na przykład jedna z największych giełd, Bitfinex, nie obsługuje m.in. obywateli Stanów Zjednoczonych czy Kanady), opłatami oraz oferowanymi usługami. Tabela 3 przedstawia przykładowe platformy i ich charakterystyki.

Binance to obecnie największa giełda pod względem wolumenu transakcji, z ponad 90 mln użytkowników. Została uruchomiona w czerwcu 2017 roku w Chinach, obecnie składa się z ok. 20 spółek zarejestrowanych w różnych krajach, a oficjalna siedziba znajduje się na Kajmanach. Obsługuje transakcje spot, handel z dźwignią oraz inne usługi, takie jak karta płatnicza (Binance Visa Card), pożyczki w kryptowalutach[12], system płatności Binance Pay.

Coinbase Exchange należy do firmy Coinbase Global, Inc., założonej w 2012 roku w Stanach Zjednoczonych. Coinbase Exchange jest dostępna w ponad 100 krajach, jednak ze względu na regulacje prawne, w niektórych z nich użytkownicy nie mają dostępu do wszystkich funkcji. Giełda Coinbase wycofała się też z usługi handlu z dźwignią. Oferuje usługi powiązane, na przykład portfel, depozyty.

10 Ang. peer-2-peer, bezpośrednio między użytkownikami.

11 Ang. over the counter.

12 https://www.binance.com/pl/loan

Tabela 3 Przykłady platform wymiany kryptowalut

nazwa	typ	Wartość transakcji spot z 24h, w dniu 18.02.2023[13]	Wartość aktywów w dniu 06.02.2023	Liczba obsługiwanych monet	Liczba obsługiwanych walut FIAT
Binance[14]	giełda	16 mld USD	57,6 mld USD	384	11
Coinbase Exchange[15]	broker	1,1 mld USD	b/d	241	3
Kraken[16]	giełda	0,42 mld USD	b/d	221	7
KuCoin[17]	giełda	0,75 mld USD	3,35 mld USD	786	48
Bitfinex[18]	giełda	0,08 mld USD	7,97 mld USD	188	4
Zonda[19]	giełda	0,002 mld USD	b/d	57	4
BitMEX[20]	broker	0,0003 mld USD	b/d	18	0
Crypto.com[21]	giełda	0,24 mld USD	3,8 mld USD	228	0
eTORO[22]	broker	b/d	b/d	30	1

Źródło: opracowanie własne na podstawie https://coinmarketcap.com/rankings/exchanges/ oraz informacji ze stron domowych platform.

Kraken to giełda założona w 2011 roku, uruchomiona w 2013 roku w USA, właścicielem jest firma Payward Inc. Pozwala na transakcje SPOT (jako jedna z pierwszych zaczęła je oferować), handel z dźwignią, kontrakty futures, wkrótce ma też wprowadzić możliwość handlu NFT. Ma ok. 8 mln klientów. Kraken dostarcza kursy kryptowalut serwisowi Bloomberg. Planuje również otworzyć pierwszy bank kryptowalutowy w USA[23].

Twórcy giełdy **KuCoin** postawili sobie jako cel ułatwienie globalnego przepływu cyfrowych wartości, w związku z tym giełda reklamuje się jako posiadająca bardzo łatwy i krótki proces rejestracji użytkowników przy wysokim stopniu bezpieczeństwa. Działa od połowy 2017 roku. Jej siedziba znajduje się na Seszelach, ma biura w Hong Kongu i Singapurze. Ma ok. 200 mln użytkowników.

Bitfinex to jedna z dłużej działających giełd kryptowalut – funkcjonuje od 2012 roku. Należy do firmy iFinex Inc. Usługi Bitfinex są kierowane raczej do profesjonalistów, niż początkujących użytkowników (przykładowo nie oferuje wielu materiałów edukacyjnych). Oferuje handel z dźwignią (max 10-krotną, finansowaną przez rynek peer-to-peer, co oznacza, że użytkownicy giełdy mogą występować zarówno jako traderzy, jak i strona finansująca handel z dźwignią).

Zonda, wcześniej znana pod nazwą BitBay, to giełda założona przez Polaków w 2014 roku. Posiada licencję estońskiej Financial Intelligence Unit (według ich strony są pierwszą giełdą kryptowalut, która uzyskała tę licencję).

13 Wartość transakcji w przeliczeniu na USD jest zależna od wahań kursów kryptowalut, a nie jedynie liczby transakcji. W publikacjach można więc znaleźć wartości istotnie różniące się od powyższych.

14 https://www.binance.com/

15 https://pro.coinbase.com

16 https://www.kraken.com

17 https://www.kucoin.com

18 https://www.bitfinex.com

19 https://zondaglobal.com/

20 https://www.bitmex.com/

21 https://crypto.com/

22 https://www.etoro.com/pl/

23 https://www.kraken.com/bank

BitMEX to platforma skierowana do profesjonalistów. Ma rozwiniętą ofertę instrumentów pochodnych, na przykład pozwala na handel ze 100-krotną dźwignią. Wpłaty i wypłaty można realizować tylko w BTC. Firma będąca właścicielem BitMEX, HDR Global Trading Limited, jest zarejestrowana na Seszelach.

Crypto.com ma ok. 50 mln użytkowników z 90 krajów (ma jednak dużo ograniczeń, na przykład działa w Stanach Zjednoczonych, z wyjątkiem stanu Nowy Jork). Siedziba firmy znajduje się w Singapurze. Giełda oferuje pełen wachlarz produktów i usług, w tym programy VIP, program dla animatorów rynku, materiały edukacyjne.

Xtb to broker oferujący dostęp do ponad 5800 instrumentów finansowych: rynek forex, CFD na indeksy giełdowe oraz towary/surowce, akcje, ETFy, czy też kryptowaluty (w ofercie jest ok. 50 CFD na najpopularniejsze kryptowaluty: Bitcoin, Ether, Stellar itp.). Xtb jest przykładem firmy, która do swojej podstawowej działalności dodała usługi związane z kryptowalutami (działa od 20 lat i chwali się, że ma ponad 400 tys. klientów).

eToro jest brokerem, który pozwala inwestować nie tylko w kryptowaluty, ale też akcje, surowce, indeksy, fundusze ETF oraz waluty. Działa od 2007 roku, aktualnie ma 30 mln użytkowników.

Więcej informacji o produktach i usługach oferowanych na platformach wymiany kryptowalut znajduje się w rozdziale 1.4.

Należy pamiętać, że rynek platform wymiany kryptowalut zmienia się niemal równie dynamicznie, co sam rynek kryptowalut. W 2022 roku upadła giełda FTX, która była wówczas trzecią pod względem obrotów platformą wymiany kryptowalut na świecie. Zaledwie trzy lata po założeniu, w styczniu 2022 roku, została wyceniona na 32 mld USD, a jej założyciel Sam Bankman-Fried miał wówczas jedynie 29 lat (Robertson, 2022). Na początku listopada 2022 roku firma zaczęła mieć problemy z płynnością, 11 listopada 2022 roku złożyła wniosek o bankructwo. Równocześnie okazało się, że na rachunkach klientów brakuje środków o wartości kilku mld USD. Upadek giełdy FTX był ciosem dla rynku, pociągnął za sobą spadki cen największych kryptowalut i pod względem wpływu na rynek kryptowalut jest porównywany do wpływu upadku Lehman Brothers na rynki finansowe. W chwili tworzenia niniejszego opracowania sprawa upadku FTX nie została wyjaśniona. Więcej informacji można uzyskać w prasie branżowej (na przykład: Business Insider, 2022; Hetler, 2023; Napolitano & Cheung, 2022; Smith, 2023).

Fundusze kryptowalutowe

Fundusze kryptowalutowe to rodzaj funduszy inwestycyjnych, które inwestują w kryptowaluty, tokeny i inne instrumenty oparte na kryptowalutach. Pozwalają one klientom inwestować w kryptowaluty bez konieczności ich bezpośredniego kupowania i przechowywania, oddając zarządzanie portfelem w ręce specjalistów. Oferta funduszy skierowana jest do inwestorów, którzy chcą ulokować większe środki (minimalne wpłaty zależą od funduszu, ale wynoszą 100 tys. USD i więcej).

Według raportu PwC (PwC i in., 2022) w 2021 roku istniało ponad 300 kryptowalutowych funduszy hedgingowych. W porównaniu z rokiem 2020, w 2021 roku fundusze tego typu podwoiły średnią wartość zarządzanych aktywów, osiągając 58,6 mln USD (mediana 24 mln USD). W momencie tworzenia niniejszego opracowania, raport PwC za rok 2022 nie był jeszcze dostępny.

Przykładowe fundusze kryptowalutowe:

Grayscale Investments[24] należący do Digital Currency Group oferuje 17 różnych funduszy kryptowalutowych. Według danych opublikowanych na stronie domowej, w lutym 2023 roku spółka zarządzała aktywami o wartości 21 mld USD. Ponadto, firma zainwestowała w ponad 130 projektów związanych z kryptowalutami.

Polychain Capital[25] to fundusz hedgingowy założony w 2016 roku. Aktualnie zarządza aktywami o wartości 6,6 mld USD. Fundusz zainwestował w ponad 90 firm związanych z blockchain oraz ponad 100 tokenów. Oferuje pięć funduszy, w które można inwestować.

Pantera Capital[26] działa od 2003 roku, ale od 2013 roku koncentruje się na inwestycjach w obszarze kryptowalut i blockchain. Oferuje pięć różnych funduszy. Zainwestował w ponad 90 firm związanych z blockchain oraz ponad 100 tokenów.

24 https://grayscale.com/products/grayscale-bitcoin-trust/

25 https://polychain-cap.com/

26 https://panteracapital.com/funds/

Więcej informacji o rynku funduszy kryptowalutowych znajduje się w raporcie PwC (PwC i in., 2022).

Tokeny DeFi

DeFi to skrót od Decentralized Finance, co po polsku tłumaczone jest jako Zdecentralizowane Finanse lub Zdecentralizowane Monety. Jest to rodzaj aplikacji finansowych wykorzystujących blockchain i kryptowaluty do decentralizacji usług finansowych, jak pożyczki, ubezpieczenia, zakłady, crowdfunding, ale również związanych z zarządzaniem tożsamością na potrzeby procesów KYC i AML (Makarov & Schoar, 2022). Większość takich aplikacji działa jako smart kontrakty w sieci Ethereum.

Bitcoin umożliwił wykonywanie przelewów bezpośrednio pomiędzy użytkownikami, z pominięciem pośredników. Ruch DeFi (sieć 15 pierwszych projektów tego typu, powstałych w 2018 roku) idzie o krok dalej i dąży do stworzenia alternatywnego, zdecentralizowanego systemu finansowego, który byłby dostępny dla wszystkich, przejrzysty, bez udziału strony trzeciej, która mogłaby przejąć kontrolę nad środkami pieniężnymi.

Aktualnie DeFi ciągle znajdują się w początkowej fazie rozwoju. Kilka największych platform tego typu to:

- Zdecentralizowane giełdy (DEX), na których można handlować bez konieczności przechodzenia przez procedury KYC i AML, obsługują jednak niewiele kryptowalut. Przykłady: Totle[27], Newdex[28], KyberNetwork[29];
- Aplikacje pożyczkowe, na przykład Nexo[30];
- Marketplace, czyli platformy, na których wielu różnych sprzedawców może wystawiać swoje produkty lub usługi. W przypadku marketplace DeFi sprzedaje się cyfrowe tokeny NFT, które mogą reprezentować na przykład przedmioty w grach, cyfrowe dzieła sztuki, zdjęcia. Przykład takiego marketplace to OpenSea[31].
- Aplikacje do zarządzania tożsamością – pozwalają na przechowywanie danych o tożsamości czy danych finansowych w zdecentralizowanej sieci, co zmniejsza ryzyko przejęcia tożsamości. Rozwiązania tego typu nie są w tym momencie upowszechnione. Przykłady: Bloom[32], Civic[33].

Na stronie Ethereum można zapoznać się z listą aplikacji DeFi wykorzystujących ten właśnie protokół[34].

1.4 Przykładowe produkty i usługi oparte na kryptowalutach dostępnych na rynku, w szczególności takie, które są lub w przyszłości mogą być konkurencyjne dla produktów oferowanych przez banki

Firmy związane z rynkiem kryptowalut, przede wszystkim platformy wymiany kryptowalut, oferują cały wachlarz usług wzorowanych na usługach sektora bankowego, ale wykorzystujących kryptowaluty lub tokeny.

Część firm umożliwia branie pożyczek w kryptowalutach. Takie pożyczki wymagają zwykle zabezpieczenia (również w kryptowalucie, choć niekoniecznie w tej samej, którą klient chce pożyczyć), które przewyższa kwotę pożyczki, mają krótki termin (na przykład na Binance jest to od 7 do 180 dni), a odsetki naliczane są z dużą częstotliwością, na przykład co godzinę. Ze względu na duże wahania kursów kryptowalut, jeżeli wartość zabezpieczenia spadnie poniżej określonego poziomu, taka pożyczka jest zamykana lub klient musi uzupełnić zabezpieczenie do wymaganego poziomu. Co istotne, klient może występować w roli pożyczkobiorcy lub pożyczkodawcy, a giełdy są jedynie pośrednikiem w tych procesach. Warunkiem wzięcia pożyczki na rynku krypto jest jedynie posiadanie zabezpieczenia, nie jest badana zdolność kredytowa. Całym procesem sterują smart contracts (aplikacje). Pożyczki są popularne wśród klientów, ponieważ pożyczkobiorcom pozwalają na szybki dostęp do kapitału, a pożyczkodawcom zapewniają dochód pasywny z posiadanych kryptowalut. Wadami takich pożyczek, poza wahaniami wartości zabezpieczenia, co może powodować li-

27 https://www.totle.com/

28 https://newdex.io/

29 https://kyber.network/

30 https://nexo.io/borrow

31 https://opensea.io/

32 https://bloom.co/

33 https://www.civic.com/

34 https://ethereum.org/en/dapps/?category=finance#explore

kwidację pożyczki, jest podatność smart contracts na ataki hakerskie, które mogą powodować utratę środków). Istnieją również pożyczki typu flash, które nie wymagają zabezpieczenia, ale muszą być pobrane i spłacone w tym samym bloku.

Jedną z podstawowych usług bankowych jest możliwość deponowania środków. Ponieważ kryptowalut nie można obecnie przechowywać w bankach, ich użytkownicy muszą korzystać z innych rozwiązań. Jako najbezpieczniejszy sposób przechowywania kryptowalut uważane jest korzystanie z **portfeli sprzętowych**. Są to specjalnie urządzenia, które pozwalają na przechowywanie kryptowalut w postaci zaszyfrowanej, a najpopularniejsze umożliwiają też wykonywanie transakcji w wybranych kryptowalutach (pod warunkiem podłączenia takiego portfela do Internetu). Ich koszt waha się średnio od 50 do 150 USD. Choć urządzenia te są odporne na wirusy komputerowe, to wciąż mogą ulec zniszczeniu lub zostać w całości skradzione lub zgubione. Ze względu na niewielkie rozmiary można je przechowywać na przykład w sejfie, jednak nie każdy użytkownik taki posiada. Przykłady firm oferujących portfele sprzętowe, to: Trezor[35], Ledger[36].

Alternatywą mogą być **portfele cyfrowe**, czyli aplikacje desktopowe, mobilne lub przeglądarkowe. Takie portfele pozwalają na szybkie wykonywanie transakcji, ponieważ są cały czas podłączone do Internetu. Z drugiej strony, są one też częstym obiektem ataków hakerskich. Przykłady:

- portfele desktopowe: Electrum[37], Armory[38],
- portfele mobilne: Trust Wallet[39], mycelium[40], Enjin[41],
- portfele przeglądarkowe: Coinbase Wallet[42], 4coins[43], Paxful[44].

35 https://trezor.io/

36 https://www.ledger.com/

37 https://electrum.org/#home

38 https://www.bitcoinarmory.com/

39 https://trustwallet.com/

40 https://wallet.mycelium.com/

41 https://enjin.io/products/wallet

42 https://www.coinbase.com/pl/wallet

43 https://www.4coins.pl/

44 https://paxful.com/pl

Niektórzy użytkownicy decydują się również na korzystanie z tzw. **portfeli papierowych**, które są po prostu wydrukiem adresu publicznego posiadanych jednostek kryptowalut oraz klucza prywatnego. Jest to oczywiście rozwiązanie najmniej wygodne (żeby skorzystać z tak przechowywanych środków trzeba przepisać adres/klucz lub zeskanować specjalny kod), łatwo ulega też zniszczeniu.

Firmy oferujące portfele kryptowalut, promują również specjalne portfele cyfrowe przeznaczone dla przedsiębiorców. Mają one umożliwiać wygodne przyjmowanie płatności w kryptowalutach. Takie usługi świadczą na przykład Kriptomat[45], crypto.com[46], BinancePay[47].

Choć nie jest to zalecane, to część użytkowników przechowuje środki na giełdach kryptowalut lub portalach pośredników płatności. Takie rozwiązanie uznawane jest za bardzo ryzykowne, ponieważ firmy te nie podlegają nadzorowi. Ponadto, upadki takich firm, jak głośna afera związana z bankructwem giełdy FTX i domniemaną kradzieżą zdeponowanych tam środków, zmniejsza zaufanie do tej formy deponowania kryptowalut.

Bardziej zaawansowanym produktem oferowanym przez giełdy kryptowalut, jest tzw. **staking** (od ang. *stake*). Staking z punktu widzenia klienta można porównać do tradycyjnych lokat lub kont oszczędnościowych, jednak budowa produktu od strony oferującej (najczęściej giełdy), jest inna. Staking dostępny jest dla kryptowalut i tokenów z mechanizmem PoS. Polega on na tym, że użytkownik przeznacza część posiadanych przez siebie kryptowalut, aby brały udział w obliczaniu PoS. Takie środki pozostają własnością użytkownika, ale są niejako „zamrożone", tj. użytkownik deklaruje, że przez określony czas nie będzie z nich korzystał. W zamian otrzymuje nagrody (tj. pewną ilość stakowanej kryptowaluty, co można traktować jako odsetki). Wysokość nagrody różni się w zależności od ilości stakowanych środków, rodzaju kryptowaluty oraz zmienia się w czasie[48]. Istotne jest, że w przypadku stakingu użytkownik nie może stracić kryptowaluty, a jedynie ma ją zablokowaną na określony czas.

45 https://kriptomat.io/pl/kriptomatpay/

46 https://crypto.com/eea/pay-merchant

47 https://www.binance.com/pl/my/wallet/account/payment

48 Źródła branżowe podają, że można w ten sposób uzyskać odsetki w wysokości od 1% do 20% w skali roku, jednak na przykład giełda Binance 11.02.2023 oferowała najwyższe odsetki dla kryptowaluty AAVE w wysokości 5,9% rocznie, przy stakingu na 30 dni; przykładowa oferta: https://www.binance.com/pl/defi-staking

Tabela 4. Produkty i usługi oferowane na platformach wymiany kryptowalut

NAZWA	Transakcje spot	Handel z dźwignią	Instrumenty pochodne	OTC	staking	pożyczki	konkursy	NFT
Crypto.com	tak	tak, do 5x	tak	tak	tak	tak	tak, program Supercharger	tak
Binance	tak	tak, do 10x	tak	tak	tak	tak	nie (ale jest ranking traderów)	tak
CoinBase	tak	nie	tak	tak	tak	tak	nie	tak
Kraken	tak	tak, 5x	tak	tak	tak	nie	nie	tak
Bitfinex	tak	tak, 10x	tak	tak	tak	nie	nie	nie
KuCoin	tak	tak, 5x	tak	tak	tak	tak	tak	tak
BitMEX	tak	tak, do 100x	tak	nie	nie	nie	nie	nie
Zonda	tak	nie	nie	nie	nie	nie	nie	nie

Źródło: opracowanie własne.

Na stakingu budowane są również inne produkty związane z **depozytami kryptowalut**, na przykład Binance Simple Earn, który jest połączeniem depozytu i stakingu. Występuje w dwóch wariantach: depozyt „zablokowany", którego zerwanie przed końcem ustalonego czasu powoduje utratę naliczonych odsetek, oraz „elastyczny", który można zerwać w dowolnym momencie bez utraty odsetek. Roczna stopa zwrotu może wynieść nawet kilkadziesiąt procent (na przykład 11 lutego 2023 roku szacunkowa APR[49] dla depozytu AXS na 90 dni na giełdzie Binance wynosiła 39%[50]). Odsetki (również w tym produkcie nazywane „nagrodami") naliczane są raz dziennie. Należy podkreślić, że APR w tym produkcie jest zmienne, więc końcowy zysk może się znacznie różnić od szacowanego w momencie zakładania depozytu. Odsetki/nagrody naliczane są w walucie depozytu, co oznacza, że podlegają wahaniom kursów kryptowalut.

Podstawową usługą świadczoną przez giełdy kryptowalut są transakcje spot, jednak większość oferuje również handel z dźwignią, możliwość inwestowania w instrumenty pochodne[51], handel OTC[52] (tj. zawieranie transakcji pomiędzy użytkownikami z pominięciem rynku). Platformy konkurują o klienta i starają się zwiększać liczbę wykonywanych transakcji przez stosowanie różnych modeli biznesowych, na przykład organizowanie konkursów na największą liczbę transakcji w określonej walucie (nagrodą są kryptowaluty) lub publikowanie rankingu użytkowników uzyskujących najlepsze wyniki w handlu. Niektóre oferują premie za polecenie platformy nowym użytkownikom lub nagradzają kryptowalutami ukończenie szkoleń online.

Interesującym typem tokenów są tzw. NFT[53]. Są to tokeny, które reprezentują konkretne przedmioty materialne lub cyfrowe (na przykład dzieła sztuki, karty kolekcjonerskie lub przedmioty w grach). Są one niepodzielne i unikatowe. Tokeny NFT są wykorzystywane przez artystów, kluby sportowe, marki luksusowe i inne. Część giełd oferuje możliwość handlu takimi tokenami (jest to też możliwe na dedykowanych rynkach – platformach marketplace).

Porównanie produktów oferowanych przez kilka wybranych platform wymiany kryptowalut znajduje się w tabeli 4.

49 Ang. Annual Percentage Rate.

50 Więcej: https://www.binance.com/pl/simple-earn

51 Najczęściej kontrakty futures, rzadziej opcje, warranty i inne

52 Handel pozagiełdowy.

53 Ang. *non-fungible token*, token niewymienny.

Do kont kryptowalutowych zakładanych na giełdach wydawane są również **karty płatnicze**. Karty te mogą być debetowe lub kredytowe, umożliwiają rozliczenia w kryptowalucie lub w walutach FIAT (jednak premiują transakcje w kryptowalutach). Zalety takich kart to przede wszystkim błyskawiczne przewalutowanie kryptowalut na waluty FIAT i tym samym możliwość płacenia za wybrane produkty i usługi. Wadą może być kurs rozliczenia takich transakcji – ze względu na duże wahania kursów kryptowalut, użytkownik może mieć problem z oszacowaniem ceny, którą zapłaci po przeliczeniu na walutę FIAT. Przykładowe karty zostały zestawione w tabeli 5. Wiele z nich oferuje program cashback (naliczany w kryptowalucie). Jako wydawane przez Visa lub Mastercard, są powszechnie akceptowane w punktach handlowych (przy płatności następuje przewalutowanie na waluty FIAT), akceptowane m.in. przez Google Pay i Samsung Pay, pozwalają na wypłaty walut FIAT z bankomatów. Mają też wysokie limity płatności (nawet kilkadziesiąt tysięcy euro). Opłaty transakcyjne różnią się, ale opłaty za samo posiadanie karty są w większości przypadków zerowe. Wiele z nich nie wymaga też zdolności kredytowej, a jedynie konta na powiązanym z nimi portalu (tj. na giełdzie lub elektronicznym portfelu).

Tabela 5 Karty płatnicze obsługujące kryptowaluty

Nazwa karty	Wydawca	Typ	Dostępna w Polsce	link
Binance Visa Card	Visa	debetowa	tak	https://www.binance.com/pl/cards
Wirex	Visa	debetowa	tak	https://wirexas.com/en-us/card
Coinbase Card	Visa	debetowa	tak	https://www.coinbase.com/card
Nexo Card	MasterCard	kredytowa	tak	https://nexo.io/nexo-card
Crypto.com	Visa	debetowa	tak	https://crypto.com/eea/cards
Gemini Credit Card	MasterCard	kredytowa	nie	https://www.gemini.com/credit-card
Brex Card	MasterCard	korporacyjna	nie	https://www.brex.com/product/credit-card
Trastra Visa Card	Visa	debetowa	tak	https://trastra.com/card/

Źródło: opracowanie własne.

2. Rynek kryptowalut – szanse i zagrożenia dla sektora bankowego

Niniejszy rozdział przedstawia analizę powiązań pomiędzy sektorem bankowym a rynkiem kryptowalut. Wiele produktów opartych na kryptowalutach niejako naśladuje produkty sektora bankowego, jednak oferuje je w formie zdecentralizowanej, tj. bez pośrednictwa zaufanej organizacji pośredniczącej. Tego typu produkty w przyszłości mogą stać się konkurencją dla produktów bankowych, jednakże obecnie rynek ten jest zbyt zmienny i za mało uregulowany, trudno jest więc prognozować jak będzie przebiegał jego dalszy rozwój.

2.1 Identyfikacja powiązań pomiędzy sektorem bankowym a rynkiem kryptowalut (na przykład konkurencyjne produkty i usługi, które mogą prowadzić do przejmowania klientów)

Wraz z coraz szerszą adaptacją kryptowalut, pojawia się więcej powiązań tego rynku z sektorem bankowym. Najważniejszym punktem styku tych dwóch obszarów są przelewy walut FIAT z banków do giełd kryptowalut i przeciwnie. Pozwala to klientom tych instytucji na zakup kryptowalut. Na podstawie przelewów do giełd kryptowalut banki mogą ocenić jaki odsetek ich klientów korzysta z kryptowalut oraz oszacować jaką część posiadanych środków przeznacza na inwestycje w ten instrument.

Aby zakupić kryptowaluty należy posłużyć się aplikacją brokerską lub giełdą kryptowalut. Możliwe jest przelanie środków w walucie FIAT i wykorzystywanie ich do zakupu kryptowalut lub płacenie za zakup bezpośrednio podczas transakcji (na przykład wybierając płatność kartą). Część brokerów i giełd oferuje również tzw. subskrypcje, czyli cykliczne zakupy określonej ilości danej kryptowaluty po bieżącym kursie.

Kryptowaluty można oczywiście przekazywać pomiędzy użytkownikami, podobnie jak ma to miejsce w przypadku przelewów walut FIAT realizowanych z pośrednictwem banków, innych instytucji finansowych lub pośredników płatności (na przykład PayPal). Pobierane są prowizje od takich transakcji, jednak w przypadku przelewów międzynarodowych są one niższe, niż w bankach. Przelewy w kryptowalutach są też księgowane znacznie szybciej, ponieważ odbywają się całą dobę, niemal w czasie rzeczywistym. Powoduje to, że przelewy w kryptowalutach są konkurencją dla międzynarodowych przekazów pieniężnych, pomimo ryzyka wahań kursów.

Firmy związane z kryptowalutami już dzisiaj oferują usługi depozytów. Badania wskazują, że w krajach dotkniętych hiperinflacją adaptacja kryptowalut jest wyższa (Gemini, 2022). Użytkownicy korzystają ze stabilnych monet, na przykład tether powiązanego z USD, aby przechowywać oszczędności poza systemem bankowym. Podobne zjawisko obserwujemy w krajach o niestabilnej sytuacji ekonomicznej i będących w stanie wojny, na przykład na Ukrainie. Technologia niektórych blockchain pozwala na uzyskanie odsetek od depozytów – takie produkty wykorzystujące mechanizm stakingu (opisane w sekcji 1.4) są oferowane przez większość wiodących platform wymiany kryptowalut.

Z punktu widzenia użytkowników kryptowalut, ale również osób, które mogą być potencjalnie zainteresowane tym rynkiem, istotnym może okazać się również zaangażowanie największych wystawców kart płatniczych (Visa i Mastercard). Obecnie wiele platform oferuje karty płatnicze (debetowe i kredytowe), które pozwalają na płacenie kryptowalutami we wszystkich punktach, gdzie akceptowane są karty tych właśnie dostawców. Nie jest to aktualnie popularne rozwiązanie, ponieważ takie płatności są przewalutowywane na waluty FIAT w momencie płatności, co może być dla użytkownika bardzo niekorzystne. Warto zwrócić uwagę, że z punktu widzenia użytkownika końcowego, zaciera to granicę pomiędzy tradycyjnym sektorem finansowym oraz rynkiem kryptowalut.

Konkurencją dla sektora bankowego mogą w przyszłości stać się produkty i usługi oparte na tokenach DeFi. Są one z założenia projektowane na wzór produktów sektora finansowego (na przykład pożyczki, ubezpieczenia), jednak z pominięciem instytucji pośredniczącej. Ich celem jest zbudowanie zdecentralizowanego ekosystemu, w którym gwarancje (ale też kontrola) instytucji pośredniczącej nie będą potrzebne. Przykłady firm z ekosystemu DeFi zostały przedstawione w sekcji 1.3.

Badania (Auer, Cornelli, i in., 2022) prowadzone w latach 2015–2022 wskazują, że wzrost wartości Bitcoin koreluje ze wzrostem liczby użytkowników

kryptowalut (badania wskazują również, że wpływ innych czynników, na przykład sytuacji gospodarczej w danym kraju jest mniejszy, niż wzrost ceny Bitcoin)[54]. Równocześnie kryptowaluty są uważane za wysoce ryzykowny produkt inwestycyjny. Platformy wymiany kryptowalut prowadzą rozbudowane akcje marketingowe nakierowane na pozyskanie nowych klientów i utrzymanie obecnych, można się więc spodziewać, że produkty związane z kryptowalutami będą się dalej upowszechniały w społeczeństwie (zwłaszcza łatwo dostępne przelewy P2P oraz depozyty).

2.2 Analiza ryzyk i szans związanych z oferowaniem przez banki produktów opartych na kryptowalutach

Produkty oparte na kryptowalutach stają się coraz popularniejsze, szczególnie wśród młodych ludzi. Z roku na rok rośnie liczba użytkowników kryptowalut, liczba dostępnych monet, platform oferujących cały wachlarz produktów i usług opartych na kryptowalutach. Obecnie nie widać przesłanek, żeby ten trend wzrostowy miał się odwrócić.

Rynek kryptowalut jest w większości nieuregulowany, a po dużych spadkach wartości kryptowalut, które miały miejsce od połowy 2021 roku, wielu nowych użytkowników obawia się inwestycji na tym rynku. Aktualnie trwa dyskusja o konieczności wprowadzenia regulacji na rynku kryptowalut (PwC, 2022), które z jednej strony powinny pozwolić na kontrolę tego rynku, a z drugiej umożliwić adopcję kryptowalut na szerszą skalę.

Wsparcie dużych i znanych instytucji finansowych prawdopodobnie przyspieszyłoby adopcję kryptowalut, ale też spowodowało, że granica pomiędzy tradycyjną bankowością, a rynkiem kryptowalut, uległaby zatarciu. Ponadto, zaangażowanie instytucji finansowych (w szczególności banków) w rynek kryptowalut spowodowałoby niejako przeniesienie zaufania, które banki mają wśród swoich klientów, na produkty oparte na kryptowalutach. Równocześnie ewentualne straty, które klienci ponieśliby korzystając z produktów kryptowalutach, mogłyby pociągnąć za sobą spadek zaufania do banków.

Należy pamiętać, że kryptowaluty powstały jako alternatywa dla zcentralizowanych, tradycyjnych systemów finansowych, co podkreślone jest w pierwszym zdaniu manifestu Satoshi Nakamoto, twórcy Bitcoin: *„Pełnowartościowa wersja pieniądza elektronicznego oparta na modelu komunikacji sieciowej peer-to-peer pozwoliłaby na przesyłanie płatności online bezpośrednio od jednego podmiotu do drugiego bez konieczności przepływu transakcji przez instytucje finansowe”* (Nakamoto, 2008). Ta idea została rozwinięta i na inne produkty finansowe w tokenach DeFi (Makarov & Schoar, 2022). Trudno określić jaka część użytkowników wybiera kryptowaluty z powodu chęci ominięcie systemu bankowego.

Biorąc pod uwagę aktualny stan prawny kryptowalut oraz zmienność rynku, oferowanie przez banki produktów i usług bezpośrednio związanych z kryptowalutami, takich jak produkty inwestycyjne czy depozyty, wydaje się być bardzo ryzykowne. Ogromne wahania na rynku kryptowalut mogłyby doprowadzić do utraty zaufania do banków, a konkurencja ze strony największych platform specjalizujących się w kryptowalutach (sekcja 1.3) wymagałaby dużych nakładów na pozyskanie i utrzymanie klientów. Istotną barierą jest też aktualnie brak regulacji prawnych w tym zakresie.

Warte rozważenia są jednak usługi konsultingu i wsparcia merytorycznego dla użytkowników-inwestorów kryptowalut. (Auer, Cornelli, i in., 2022) wskazują, że według przeprowadzonych przez nich badań od 73 do 81% użytkowników poniosło stratę na inwestycji w kryptowaluty[55]. Z ich badań wynika, że w czasie wzrostu cen Bitcoin, „zwykli” użytkownicy w dużej mierze kupowali walutę (licząc, że będzie ona dalej rosła), natomiast tzw. duzi gracze sprzedawali odnotowując zyski kosztem niedoświadczonych użytkowników. Z przeprowadzonej analizy wynika, że było to spowodowane tym, że zwykli użytkownicy nie posiadali wystarczającej wiedzy o ryzyku związanym z inwestowaniem w kryptowaluty oraz ich zmienności. Ok. 40% ankietowanych wskazuje, że lepszy dostęp do zasobów edukacyjnych na temat kryptowalut pomógłby im rozpocząć inwesty-

54 Autorzy wykorzystali statystyki dotyczące pobrań aplikacji giełd kryptowalut.

55 Są to szacunki oparte na symulacjach, na podstawie danych o cenie Bitcoin w momencie pobrania przez użytkownika aplikacji giełdy kryptowalut.

cje w kryptowaluty, a tylko 22% chciałoby tę wiedzę czerpać od znajomych (Gemini, 2022).

Aktualnie największe bazy wiedzy o kryptowalutach to materiały przygotowane przez giełdy kryptowalut (na przykład https://coinmarketcap.com/alexandria) lub tzw. influencerów56. Popularne kanały YouTube o kryptowalutach posiadają nawet ponad 1 mln subskrybentów (na przykład globalne: Coin Bureau[57] 2,19 mln, BitBoy Crypto[58] 1,45 mln, Altcoin Daily[59] 1,29 mln, lub polskojęzyczne: Phil Konieczny[60] 302 tys., Piotr Ostapowicz[61] 174 tys.). Osobom początkującym trudno jest ocenić wiarygodność, kompetencje i doświadczenie influencerów. Ponadto, są to przeważnie entuzjaści kryptowalut, którzy przedstawiają je raczej w pozytywnym świetle. Natomiast portale branżowe wskazują Internet, a dokładniej portale o kryptowalutach i fora, jako najlepsze źródło informacji, podkreślając, że zmienność na tym rynku jest tak duża, że tradycyjne książki szybko się dezaktualizują. Niestety, informacje na portalach i forach są często publikowane anonimowo (szczególnie na forach), zwykły użytkownik nie ma więc możliwości aby szybko zweryfikować prawdziwość i aktualność prezentowanych tam treści, jak również kompetencje autorów.

Trudno jest określić, ilu użytkowników kryptowalut posiada wiedzę o inwestowaniu, a nie tylko o sposobie obrotu kryptowalutami. Brak wiedzy o finansach i inwestowaniu może przyczyniać się do podejmowania większego ryzyka przy inwestowaniu w kryptowaluty lub błędnej oceny tego ryzyka. Im takie zjawisko będzie powszechniejsze, tym mniej stabilny i podatny na oszustwa będzie rynek kryptowalut.

Do rozważenia mogłyby być również usługi pośrednio związane z kryptowalutami, tj. niezwiązane z handlem kryptowalutami, ale z samym ich przechowywaniem, na przykład usługa cyfrowego portfela kryptowalut (patrz sekcja1.4).

2.3 Kryptowaluty w rozliczeniach bankowych na przykładzie Ripple

Rozwój rynku kryptowalut stanowi konkurencję dla banków w kilku różnych obszarach (patrz sekcja 1.4 i 2.1), m.in. w realizacji przelewów międzynarodowych. Przelewy wykonywane za pośrednictwem kryptowalut są realizowane niemal natychmiast, przez całą dobę i 7 dni w tygodniu. Zwykle wiążą się też z mniejszymi opłatami, niż przelewy międzynarodowe realizowane za pośrednictwem banków.

Należy też mieć na uwadze, że wejście zdecentralizowanych kryptowalut do powszechnego użycia może stanowić zagrożenia dla polityki monetarnej, gdyż jest to zasób pieniądza pozostający poza kontrolą banków centralnych.

Z tego względu od kilku lat prowadzone są badania dotyczące możliwości adaptacji technologii blockchain przez banki, aby umożliwić im przyśpieszenie realizacji transakcji międzynarodowych i zmniejszyć ich koszty.

Wydaje się, że najbardziej zaawansowane prace dotyczą CBDC[62], czyli cyfrowych walut banku centralnego (Auer i in., 2021). Są to scentralizowane kryptowaluty emitowane przez banki centralne, powiązane z walutą FIAT. Ich celem jest wykorzystanie zalet blockchain, przy równoczesnym zachowaniu kontroli banków centralnych nad polityką monetarną. Według strony Atlantic Council[63] aktualnie 11 krajów wprowadziło już CBDC (Nigeria, Wspólnota Bahamów, Jamajka oraz 8 krajów ze wschodnich Karaibów), a 17 kolejnych jest na etapie pilotażu (m.in. Szwecja, Ukraina, Chiny, Indie, Arabia Saudyjska, Australia, Singapur, Rosja). W sumie aż 114 krajów prowadzi działania w kierunku wprowadzenia CBDC (Polska nie widnieje na tej liście Atlantic Council), w tym wszystkie kraje G7 i 18 z krajów G20 są na etapie opracowywania takiego rozwiązania.

Należy jednak podkreślić, że część zagadnień związanych z CBDC jest wciąż niejasnych, na przykład jakie wymusi zmiany w strukturze finansowej instytucji, jaki będzie wpływ wprowadzenia CBDC na stabilność systemu finansowego i na politykę monetarną,

56 Influencer to osoba, która w mediach społecznościowych posiada dużą liczbę obserwatorów (subskrybentów) i przez to jest w stanie oddziaływać na ludzi. Influencerzy często biorą udział w kampaniach marketingowych.

57 https://www.youtube.com/@CoinBureau

58 https://www.youtube.com/@BitBoyCryptoChannel

59 https://www.youtube.com/@AltcoinDaily

60 https://www.youtube.com/@PhilKonieczny

61 https://www.youtube.com/@PiotrOstapowicz1

62 central bank digital currency

63 https://www.atlanticcouncil.org/cbdctracker/

trwają też dyskusje o tym, jak daleko powinna być posunięta prywatność transakcji CBDC oraz jakie rozwiązania w zakresie cyberbezpieczeństwa powinny zostać równocześnie wdrożone.

Najpopularniejszym rozwiązaniem komercyjnym w tym zakresie jest produkt firmy Ripple[64]: projekt sieci płatniczej RippleNet oparty na blockchain z kryptowalutą XRP. RippleNet ma być elementem usprawniającym infrastrukturę bankową, zapewniając możliwość procesowania płatności, również międzynarodowych, w czasie rzeczywistym między instytucjami należącymi do sieci. Do RippleNet należy obecnie kilkaset instytucji finansowych, w tym również banki komercyjne. Poza siecią do transakcji międzynarodowych, Ripple oferuje również platformę CBDC.

Warte uwagi są publikacje Banku Rozrachunków Międzynarodowych na temat CBDC (na przykład Auer, Banka, i in., 2022; Auer i in., 2021; Bank for International Settlements' Committee on Payments and Market Infrastructures i in., 2022; BIS Innovation Hub Hong Kong Centre i in., 2022; Carstens, 2023; Cunliffe, 2023).

64 https://ripple.com/

PROGRAM ANALITYCZNO BADAWCZY

3. Ryzyka zarządzania portfelami, stabilność zabezpieczeń i zagrożenia związane z postępami technik kryptoanalitycznych

3.1 Poziom ryzyka w obrocie wynikający z możliwości kompromitacji procesu generowania i ochrony kluczy

Kluczowym pojęciem systemów kryptowalutowych, umożliwiającym przeprowadzanie operacji i identyfikującym rachunki jest para kluczy kryptograficznych: tajny, pozostający w pieczy posiadacza rachunku, oraz odpowiadający mu klucz publiczny. Pierwszy z tych kluczy umożliwia autoryzowanie (podpisywanie) zleceń transferu z własnego konta, drugi – jest swoistym identyfikatorem konta „adresata" lub odpowiada tokenowi, którego wartość poprzez transakcję zostaje przekazana komu innemu. Elementarną transakcję można opisać poniższym zdaniem:

*Niniejszym przekazuję na konto identyfikowane kluczem publicznym **KPubB** określoną kwotę. Potwierdzam to, podpisując to zlecenie moim kluczem tajnym **KSecA**, który to podpis można zweryfikować moim kluczem publicznym **KPubA**. Każdy, kto chce, może sprawdzić, że dysponowałem transferowaną kwotą na podstawie poprzednich transakcji zarejestrowanych w blockchaine.*

Tego typu operacja tworzy zamknięty obieg winien/ma, a obie strony transferu są jednoznacznie określone nie tylko w pojedynczej transakcji, ale przez całe życie użytych kluczy publicznych. Aby zapewnić anonimowość, systemy kryptograficzne korzystają ze struktury hierarchicznej (drzewiastej), umożliwiającej przechowywanie wielu kluczy prywatnych i odpowiadających im kluczy publicznych w taki sposób, że:

- wszystkie klucze powiązane z daną osobą wyprowadzane są deterministycznie od jednego klucza głównego (master key) – zapamiętanie tylko tej jednej informacji umożliwia odtworzenie całej struktury hierarchicznej;
- dla osoby postronnej niemożliwym jest stwierdzenie, czy dwa klucze publiczne należą do tej samej hierarchii kluczy;
- możliwe jest wygenerowanie bardzo dużej liczby kluczy w taki sposób, by praktycznie każdej operacji transferu można było przypisać inny klucz publiczny, a jednocześnie powiązania między tymi operacjami były związane z jednym kluczem prywatnym.

Ze względu na tak dużą wagę klucza master, twórcy systemów kryptowalutowych opracowali procedurę jego generowania, która z jednej strony zapewnia odpowiedni jego poziom entropii, a z drugiej strony umożliwia łatwe dla człowieka przechowanie jego kopii zapasowej. Szczegóły tej operacji zawarto w dokumentach BIP-19, BIP-32. Kroki tej procedury są następujące:

Generowany jest początkowy zalążek entropii 128 do 256 bitów. Jest to jedyne miejsce, w którym procedura wykorzystuje losowość.

Wyliczana jest suma kontrolna (SHA-256) zalążka i dołączana na jego końcu.

Tak otrzymany ciąg bitów dzielony jest na grupy po 11 bitów, które traktowane są jako liczby z zakresu 0–2047, stanowiące wskaźniki do tablicy słów kluczowych, zdefiniowanych w dokumencie BIP-39. Są to łatwe do zapamiętania słowa i każde z nich ma unikalne pierwsze cztery litery.

Otrzymuje się w ten sposób od 12 do 24 słów (w zależności od rozmiaru początkowego zalążka) z języka angielskiego[65] (mnemoników), deterministycznie zależnych od początkowo wylosowanego zalążka. Jest to „zdanie bezpieczeństwa", które zaleca się przechowywać w bezpiecznym miejscu, na przykład w formie wydrukowanej.

Tak wytworzone zdanie bezpieczeństwa poddaje się działaniu kryptograficznej funkcji skrótu (HMAC-SHA512), dodając dodatkowo wymyślone przez użytkownika hasło. Funkcję skrótu stosuje się 2048 razy w pętli, co ma na celu podniesienie złożoności tej procedury i utrudnienie ataków typu przeglądowego (ang. *brute-force*), których celem jest generowanie losowych zdań bezpieczeństwa i sprawdzanie, czy odpowiadają im jakieś istniejące konta kryptowalutowe. Wynikiem tej operacji jest 64-bajtowa wartość zalążka (ang. *seed*).

W ostatnim kroku zalążek ten ponownie przetwarzany jest kryptograficzną funkcją haszującą, a wynik tej operacji dzielony jest na dwie 32-bitowe liczby: główny klucz prywatny (ang. *master key*) oraz kod łańcucha (ang. *chain code*) – liczbę wykorzystywaną do generowania dalszych kluczy w hierarchii.

Nieprzewidywalność wartości seed zależy jedynie od dwóch czynników: źródła początkowej losowości (krok 1.) i ewentualnie zastosowanego hasła

65 BIP-39 ma wsparcie również dla 8 innych języków: japońskiego, koreańskiego, włoskiego, hiszpańskiego, czeskiego, portugalskiego, francuskiego oraz chińskiego (uproszczonego i tradycyjnego).

(krok 5.). O ile problem łamania haseł użytkowników jest ogólnie znany i rozumiany, warto nadmienić, że prawdziwie losowe wartości w wielu przypadkach są trudne do generowania. W publikacji (Kilgallin, Vasco, 2019) autorzy zidentyfikowali niższą od spodziewanej entropię źródła losowości przy generowaniu kluczy RSA jako silny czynnik ułatwiający kryptoanalizę: w grupie niemal 75 mln sprawdzonych certyfikatów RSA, 1 na 172 wykazywał tę podatność. O ile algorytm RSA nie ma bezpośredniego zastosowania przy generowaniu kluczy w systemach kryptowalutowych, to właśnie ten wykazany słaby element jest współdzielony przez oba te mechanizmy.

Fakt, że znajomość sekwencji wyrazów jest równoznaczna z uzyskaniem dostępu do konta został wykorzystany do organizacji gry w mediach społecznościowych[66]. Organizator przekazał adres konta bitcoin wraz z informacją, że zdanie bezpieczeństwa składa się z 12 wyrazów. Kolejne wyrazy miały być publikowane wraz z upływem czasu, a pierwsza osoba, która uzyska dostęp do konta, miała zdobyć zdeponowany na nim 1BTC. Przy opublikowanych ośmiu wyrazach zwycięzca był w stanie znaleźć rozwiązanie w czasie 30 godzin.[67]

Powyższa sześciopunktowa procedura generowania głównego klucza i wartości seed jest standardowo przeprowadzana w momencie inicjalizacji nowego portfela. W zależności od rodzaju portfela – sprzętowego, programowego czy w zdalnym hostingu – istnieje możliwość dostępu do zdania bezpieczeństwa lub kluczy prywatnych powiązanych z danym kontem. Dla portfeli typu *custodian* (z ang. dozorca, opiekun) – dostęp do tych informacji jest bezpośredni, gdyż tego typu rozwiązanie polega na zaufaniu posiadacza konta do trzeciej strony, która utrzymuje całość rachunku i wykonuje operacje na nim na żądanie właściciela. Większość giełd oferuje taką funkcjonalność w swoich hostowanych portfelach i jednocześnie jest najprostszą opcją umożliwiającą wejście w posiadanie i przeprowadzanie operacji na kryptowalucie. Jednak w naturalny sposób platformy te, oprócz posiadania de facto wszelkich danych umożliwiających korzystanie ze środków powierzonych im przez klientów, zdobywają też dodatkowe informacje o swoich klientach, na przykład dotyczące czasów logowania, zlecanych operacji, adresów e-mail służących do kontaktu itp.

Portfele typu *non-custodian* to często portfele programowe, uruchamiane na komputerach lub smartfonach przez danego użytkownika, lub portfele sprzętowe. Ich podstawowym założeniem jest to, że klucze prywatne i hasła dostępowe pozostają zawsze pod wyłączną kontrolą ich posiadacza. Niemniej jednak część portfeli tego typu ma zamknięty kod[68], co efektywnie uniemożliwia weryfikację poprawności działania aplikacji. Są przypadki udostępnienia części kodu (na przykład Exodus), ale utajnienia innej, co jest uzasadniane chęcią ochrony przed atakami typu scam, gdzie tworzone są imitacje oryginalnej aplikacji w celu wyłudzenia poufnych informacji. Z praktycznego punktu widzenia jednak, korzystanie z tego typu oprogramowania nie różni się niczym od korzystania z portfeli typu *custodian* – w obu przypadkach podstawowym elementem jest zaufanie klienta do twórcy portfela. Być może problem w tym przypadku jest większy, gdyż portfele uruchamiane lokalnie mają często możliwość prowadzenia wielu kont (tj. korzystania z wielu seedów jednocześnie), więc zakres potencjalnych strat w przypadku ich złośliwego działania jest znacznie szerszy.

Dostęp do pełnego kodu aplikacji wydaje się warunkiem niezbędnym do zapewnienia nie tylko zgodności pracy aplikacji ze specyfikacją, ale też braku jej dodatkowych funkcji, których skutek działania może być znacznie przesunięty w czasie. W kryptografii opracowano wiele metod tworzenia tzw. bocznych kanałów (ang. *subliminal channels*) (Simmons,1983), które umożliwiają wyciek poufnych informacji w ramach poprawnie realizowanego, bezpiecznego protokołu. Prace takie jak (Bellare i in., 2014) czy początkująca ścieżka kleptografii (Young, Yung, 1996) wykazują możliwość konstrukcji takich kanałów w algorytmach kryptografii symetrycznej i klucza publicznego. W pracy (Biryukov i in. 2019) wykazano istnienie takiego kanału dla zCash, a w (Verbücheln, 2015) opisano możliwość implementacji takiego kanału dla podpisów ECDSA w protokole Bitcoin. Niedawno opublikowana praca przeglądowa (Bangyao, 2022) przedstawia szereg możliwości budowania tego typu kanałów w technologiach korzystających z łańcucha bloków. W związku z powyższym, nie można wykluczać możliwości wbudowania w portfele mechanizmów wyciekają-

66 https://twitter.com/alistairmilne/status/1266037520715915267 wpis na koncie Alistera Milne z 28 maja 2020.

67 Szczegóły tego przedsięwzięcia opublikowano pod adresem https://medium.com/@johncantrell97/how-i-checked-over-1-trillion-mnemonics-in-30-hours-to-win-a-bitcoin-635fe051a752

68 na przykład Coinomi, Exodus, Enjin i in.

cych tajne klucze, a od środowiska deweloperów tych technologii należałoby oczekiwać wykorzystywania rozwiązań *secure-by-design* (bezpieczny z założenia) – gdzie brak tego typu ataków byłby dowodliwy lub ich obecność – możliwa do wykrycia.

Ostatnią formą portfeli są portfele sprzętowe. Są to urządzenia dedykowane do przechowywania tajnych danych dotyczących konta kryptowalutowego i zdolne wykonywać operacje kryptograficzne związane z tymi danymi (m.in. podpisywanie transakcji, a także generacja wartości *seed* zgodnie z opisanym powyżej algorytmem lub zaimportowanie istniejącego portfela na podstawie zdania bezpieczeństwa). Fizycznie są to niewielkie urządzenia, które współpracują z odpowiednim oprogramowaniem na komputerze udostępniającym użytkownikowi interfejs do przeprowadzania operacji i mającym łączność z Internetem. Pod kątem użyteczności portfele sprzętowe są mniej wygodne, ale uważane za najbezpieczniejsze, gdyż dostęp do poufnych danych jest chroniony przez rozwiązania sprzętowe, takie jak dedykowane koprocesory kryptograficzne, bezpieczne strefy obliczeniowe procesora, szyfrowana pamięć flash itp. Uznawany za najbezpieczniejszy na rynku portfel NGRAVE Zero[69] posiada certyfikację bezpieczeństwa EAL-7 a jedyną formą komunikacji między portfelem a obsługującą go aplikacją są wyświetlane przez nie kody QR. Inne znane marki takich portfeli to Ledger (certyfikowany przez NSSI) czy Trezor.

Nie należy jednak zakładać, że portfele sprzętowe są bezwarunkowo bezpieczne. Ich wykorzystanie odsuwa tajne dane od Internetu (uznawanego za główne źródło ataków), niemniej jednak znane są inne wektory ataku, oczywiście poza atakami na płaszczyźnie algorytmiczno-kryptograficznej, na którą będą podatne wszystkie portfele. Autorzy pracy (Dąbrowski i in., 2021) konstatują, że rozwiązania sprzętowych portfeli przenoszą zaufanie z twórców oprogramowania komputerowego na producenta sprzętowego portfela. Opisywany wcześniej problem zamkniętości oprogramowania w tym wypadku jest jeszcze poważniejszy: ze względu na własności IP upublicznienie całego oprogramowania takiego portfela może nie być możliwe. Z drugiej strony, jego analiza wymaga wyjątkowych umiejętności i aspekt kontroli społecznej jest tutaj znacznie osłabiony. A mając pełną kontrolę nad sprzętem, producent może z powodzeniem budować kanały kleptograficzne (Young, Yung, 1996), czy zmniejszając entropię losowości przy generowaniu nowych wartości *seed* osłabiać tym jakość kluczy prywatnych (Bednarek, 2019).

Autorzy pracy (Dąbrowski i in., 2021) wskazują także na problem zaufania do całego łańcucha producentów podzespołów wykorzystywanych w tych urządzeniach. W świetle ostatnich doniesień o możliwości nieuprawnionego zbierania danych przez telefony komórkowe wyposażone w podzespoły z pewnych źródeł, zapewnienie zaufania do takich komponentów, jak wyświetlacze dotykowe (posiadające własne kontrolery o zamkniętym oprogramowaniu) czy kamery – wydaje się być problematyczne. Należy też pamiętać o „zwykłych" podatnościach, które mogą zostać wykryte w produktach znanych firm. Na przykład niedawno wykryto względnie prosty atak na obszar bootloadera procesorów linii LPC firmy NXP, umożliwiający pominięcie zabezpieczeń przed odczytaniem kodu wykonywanego przez procesor[70]. Tą samą technikę wykorzystali badacze z laboratorium Kraken do wydobycia wartości seed z portfeli marki Trezor (Kraken, 2020).

Należy podkreślić, że systemy zarządzania portfelami, ze względu na potencjalnie wysoki zysk w przypadku sukcesu, są atrakcyjnym celem ataków hakerskich z całym wachlarzem możliwości. Przykładem może być incydent z portfelem non-custodian dostarczanym przez Slope, gdzie w połowie 2022 roku doszło do skutecznego ataku hakerskiego, skutkiem czego szereg portfeli został skompromitowany.[71] Jako przyczynę wskazano błędy w zabezpieczeniach aplikacji pochodzącej od firmy zewnętrznej, monitorującej pracę aplikacji Slope, przez co wrażliwe informacje zwracane przez aplikacje działające w systemie wyciekły poza bezpieczną domenę. Nie stwierdzono przy tym nadużyć w wewnętrznych protokołach komunikacyjnych samego dostawcy. Podobny mechanizm ataku, tj. przez wykorzystanie luk w aplikacji trzeciej strony miał miejsce w 2020 roku w sieci Trinity[72]. W sposób oczywisty uruchamianie aplikacji portfela na własnych urządzeniach również naraża je na ataki złośliwego oprogramowania, trojanów i innych „standardowych" zagrożeń związanych z systemami komputerowymi, a pro-

69 https://www.ngrave.io

70 Prezentacja z jest dostępna pod adresem https://av.tib.eu/media/32392

71 https://slope-finance.medium.com/slope-update-11-august-2022-31d678d7cd97

72 https://blog.iota.org/trinity-attack-incident-part-1-summary-and-next-steps-8c7ccc4d81e8/

blem zabezpieczenia przed nimi pozostaje po stronie użytkownika takiego portfela.

3.2 Kwestie przewidywalności postępów w kryptoanalizie i dostępności informacji o jej bieżącym stanie

Nieprzewidywalność postępów kryptoanalizy i niemożność rzetelnej oceny faktycznego bieżącego stanu techniki kryptoanalitycznej powinny być podstawowymi założeniami przy ocenie bezpieczeństwa systemów takich, jak kryptowaluty. Prognozowanie postępu metod kryptoanalitycznych tylko wtedy ma sens, gdy mowa jest o projektach implementacji nowych linii produktów hardware'owych. Przewidywanie odkryć o charakterze matematycznym nie jest możliwe.

Ponadto, należy brać pod uwagę czynniki nie leżące stricte w obszarze specyfikacji systemu określonej kryptowaluty, ale też potencjalnych rozbieżności pomiędzy specyfikacją a realnym stanem faktycznym wynikającym z czynników implementacyjnych. Obszar ten jest jednym z najbardziej prawdopodobnych miejsc występowania luk bezpieczeństwa.

Ujawnianie technik i wiedzy mogącej mieć wpływ na atak na kryptowaluty może mieć charakter skomplikowanej gry o charakterze strategicznym. Po pierwsze, nie widać powodów, dla których wiedza taka użyteczna w sensie komercyjnym i/lub strategicznym miałaby być upubliczniania. Wyjątkiem jest środowisko akademickie, gdzie nacisk na publikowanie powoduje zjawisko odwrotne: upubliczniane są wyniki prac nie tylko wartościowych, lecz również bezużytecznych, naciągniętych lub wręcz fałszywych. Dla przykładu – w przypadku obszarów takich, jak odporność na analizę typu side-channel możliwość weryfikacji wyników może wymagać sporych nakładów. W konsekwencji część wyników w istocie nie jest rzetelnie weryfikowana mimo istnienia teoretycznie ostrego systemu recenzowania. W ocenie jednego z wiodących specjalistów zjawisko to jest powszechne i blisko połowa wyników dotyczących analizy side-channel jest nie do końca rzetelna (komunikacja prywatna).

W drugim scenariuszu, przewaga pod względem wiedzy i technologii kryptograficznej może być ukryta i wykorzystywana w umiarkowany sposób, nie ujawniając swego istnienia. Historia uczy, że po stronie atakującego mogą być bardzo istotne zasoby nie tylko finansowe i sprzętowe, ale również zaawansowanej wiedzy. Znakomitym przykładem był atak FLAME (infekowanie komputerów poprzez wrogie aktualizacje z prawidłowym podpisem firmy dostarczającej system operacyjny), oparty na technikach ataku na funkcję haszującą MD5 w sposób bardziej wydajny niż metody znane z literatury. Systemy kryptowalutowe, inaczej niż inne obszary, dają tu więcej możliwości wykorzystania przewagi. Z jednej strony wiele danych jest explicite dostępnych dla atakującego poprzez blockchain. Z drugiej strony, w wielu przypadkach mechanizmy kryptowaluty gwarantują pierwszeństwo atakującemu. Na przykład, w przypadku złamania klucza publicznego użytkownika w systemie Bitcoin i użycia klucza prywatnego przez atakującego do transferu środków uniemożliwia nie tylko odzyskanie środków przez właściciela, ale również stawia go w pozycji osoby usiłującej dokonać oszustwa – powtórnego przekazania tych samych środków innemu kontrahentowi.

Trzeba również brać pod uwagę możliwości celowego wprowadzania w błąd poprzez fałszywe lub tylko przesadne informacje o możliwościach złamania określonych zabezpieczeń w niedalekiej przyszłości. Informacje takie mogą prowadzić do chaotycznych decyzji i pośpiesznego przejścia na nowe technologie, bez zachowania staranności, jaka byłaby właściwa dla takiego procesu.

W ocenie technik kryptograficznych i tzw. „dowodliwego bezpieczeństwa" trzeba być świadomym ograniczeń metod formalnych, w których dowód odnosi się jedynie do modelu bezpieczeństwa określonego przez autorów dowodu. Zazwyczaj model odnosi się do bardzo ograniczonego zbioru scenariuszy. Nawet w przypadku protokołów o fundamentalnym znaczeniu bywa, że wprowadzenie standardów nie jest poprzedzone rzetelnym procesem ewaluacji.

Pozytywnym wyjątkiem od tego typu sytuacji są konkursy prowadzone przez NIST na fundamentalne algorytmy kryptograficzne. Otwartość konkursów, spore zainteresowanie zdobyciem sławy poprzez złamanie określonego schematu, a także zażarta walka konkurencyjna niezwykle utrudniają przeforsowanie metody z wbudowanymi podatnościami. Nie oznacza to jednak, że wszystkie decyzje NIST są całkowicie pozbawione kontrowersji. Przykładem jest przyjęcie architektury SHA-3 pozwalającej na odwracanie przejść wewnętrznego stanu generatora haszy (warto tu zauważyć, że blockchain Bitcoina wykorzystuje SHA-2, choć być może powody są inne).

Z pewnością, brakuje podobnego transparentnego procesu projektowania i badania systemów kryptowalut. Dokumenty opisujące kryptowaluty (whitepapers) są wartościowe, ale mają zadanie promocyjne. Nie mogą być traktowane jako ocena bezpieczeństwa zgodnie z zasadą *nemo iudex in causa sua*.

3.3 Ryzyka związane z obliczeniami kwantowymi i niestandardowymi metodami obliczeniowymi

Bezpieczeństwo mechanizmów kryptograficznych, na jakich opierają się kryptowaluty są zazwyczaj analizowane w kontekście złożoności obliczeniowej złamania zabezpieczeń w modelu von Neumanna, opisującego standardowy uniwersalny procesor. Ze względu na możliwość wykorzystania koprocesorów kryptograficznych przyspieszających w bardzo znaczący sposób operacje kryptograficzne złożoność ataków opisuje się również biorąc pod uwagę samą liczbę operacji kryptograficznych abstrahując od ich kosztu zależnego od konkretnej implementacji. Niekiedy bierze się pod uwagę możliwość zrównoleglenia operacji wykonywanych w trakcie ataku, jednak w wielu przypadkach schematy kryptograficzne są budowane w taki sposób, aby zamykać możliwości tego typu postępowania (poza oczywistym przypadkiem ataku *brute force*, który zawsze da się zrównoleglić).

Poszukiwania słabości mechanizmów kryptograficznych opierają się na przyspieszeniu operacji trudnych w modelu von Neumanna bądź też budowie dedykowanych algorytmów zorientowanych na specyficzne urządzenia o niestandardowych możliwościach obliczeniowych.

W przeszłości już raz w istotny sposób takie niestandardowe urządzenia obliczeniowe wymusiły zmiany stosowanych algorytmów obliczeniowych. Z punktu widzenia kryptowalut warto wskazać na przykład przyspieszenia kryptoanalizy RSA poprzez zastosowanie urządzeń zaprojektowanych w pracach (Shamir, 2003) oraz (Lenstra, 2000). Pomysł polegał w tym wypadku na przyspieszeniu jednej z trudnych operacji w algorytmach opartych na przesiewaniu. Algorytmy te wykorzystują duże macierze stosunkowo łatwe do wygenerowania jednak zazwyczaj rzadkie (to jest, w których zdecydowana większość elementów to zera). Postęp w algorytmie uwarunkowany jest znalezieniem macierzy tego typu o stosunkowo dużej wadze. Dla klasycznej architektury komputera sprawdzenie czy określona macierz (wygenerowana na przykład w sposób równoległy) nie jest rzadka wymaga przeglądnięcia całej macierzy, co związane jest z szeregiem wolnych operacji na pamięci. Idea Twinkle to wykrywanie sumy elementów macierzy poprzez pomiar łącznej intensywności światła, gdy za każdy obszar macierzy odpowiada odrębny mikrokontroler i steruje diodą emitującą światło o natężeniu proporcjonalnym do łącznej wartości w tym obszarze. Sumowanie wartości odbywa się bez udziału układów elektronicznych z binarną logiką. W rzeczywistości, omawiane urządzenia nie zostały wprowadzone do produkcji przemysłowej. Skutkiem opublikowania ich koncepcji było dostosowanie parametrów RSA wymaganych dla praktycznych zastosowań.

Podobny charakter mają algorytmy kwantowej kryptoanalizy. Zastosowanie algorytmów kwantowych polega na sprawnym wykonaniu pewnych operacji w praktyce niewykonalnych w architekturze von Neumanna oraz na przetwarzaniu wyników już w klasycznej architekturze. W niniejszym raporcie nie odnosimy się do kwestii perspektyw postępów technologii i realnych możliwości pojawienia się na rynku komputera kwantowego.

Sukces rynkowy komputera kwantowego zależy od jego realnej praktycznej użyteczności. Ze względu na koszty (potencjalnie bardzo wysokie zarówno w zakresie ceny bieżącej eksploatacji, jak i pokrycia kosztów produkcji oraz zainwestowanych środków) konieczne jest wskazanie takich obszarów, gdzie wyniki obliczeń kwantowych posiadają wartość wyższą od kosztu ich wyprodukowania. W niektórych publikacjach wyrażane są opinie, że kwestia ta jest otwarta. Autorzy pracy (Lee i in., 2022) wskazują, że już samo przygotowanie stanu do obliczeń kwantowych dla modelowania procesów chemicznych może być tak trudne, że cały proces obliczeniowy staje się mało efektywny. Jeśli w tym zakresie nie zostanie odnotowany realny postęp, to pod znakiem zapytania stoi sens inwestowania w budowę komputerów kwantowych, bowiem zastosowania w zakresie kryptoanalizy efektywnie służą jedynie do destabilizacji obrotu cyfrowego.

W sytuacji powstania komputerów kwantowych (czy innej technologii o podobnych konsekwencjach) łamiących założenia kryptograficzne będące podstawą kryptowalut, nie jest wcale oczywiste, czy doprowadziłoby to do załamania rynku kryptowalut. Decydującym czynnikiem jest koszt dokonania ob-

liczeń skutkujących złamaniem określonego klucza publicznego. O ile zawartość portfela, do którego atakujący się włamie, jest niższa od kosztów włamania, atak nie ma bezpośredniego sensu ekonomicznego. W przeciwieństwie do obecnej architektury podpisów kwalifikowanych, kryptowaluty mogą elastycznie reagować na zagrożenia. Na przykład, wartość kryptoaktywów związanych z pojedynczą parą kluczy może być ograniczona. Problemem dla atakującego jest także sama struktura blockchaina oraz dodatkowe mechanizmy weryfikacji uczestników transakcji, które powinny się pojawić wskutek implementacji rozporządzenia (UE1, 2023).

Kolejnym podejściem do zagrożeń wynikających z obliczeń kwantowych jest przejście na algorytmy post-kwantowe. W obszarze tym należy pamiętać jednak o dodatkowej dozie ostrożności, ze względu na potencjalną niedojrzałość tych technologii i zastępowanie potencjalnych zagrożeń kryptoanalizy kwantowej przez technologie, gdzie istotne luki mogą istnieć już teraz i pozostawać nieznane w obszarze publicznym. Dobrym przykładem, że tego typu sytuacja nie jest tylko hipotetyczna, okazuje się historia algorytmu podpisu RAINBOW, jednego z finalistów konkursu NIST (Beullens, 2022). W 2022 roku pokazano wręcz, że możliwe jest złamanie klucza publicznego w kilkadziesiąt godzin na standardowym laptopie.

3.4 Praktyczne konsekwencje potencjalnego osłabienia zabezpieczeń kryptograficznych i możliwość zawalenia się całości bądź fragmentów rynku

Trzy zasadnicze komponenty kryptograficzne mają wpływ na bezpieczeństwo kryptowalut: problem dyskretnego logarytmu, siła generatorów liczb pseudolosowych oraz własności funkcji haszujących upodabniające je do wyroczni losowej (*random oracle*). Jedynie w kilku przypadkach stosowane są rozwiązania oparte na RSA (na przykład Hedera HBAR), gdzie konsekwencje złamania problemu faktoryzacji byłyby podobne jak w przypadku złamania problemu dyskretnego logarytmu.

Zawalenie się założeń kryptograficznych w każdym z wymienionych przypadków miałoby katastrofalne skutki.

Problem dyskretnego logarytmu. Możliwość obliczania dyskretnych logarytmów w określonej grupie algebraicznej G przez jakiegokolwiek uczestnika rynku daje nieograniczone możliwości przejęcia aktywów związanych z kluczami publicznymi, dla których obliczenia wykonuje się w grupie G. Do dokonania transakcji konieczne jest bowiem złożenie podpisu za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu przypisanemu do określonego konta (jak na przykład ma to miejsce dla Bitcoina), lub mającego charakter jednorazowy (jak to ma miejsce w przypadku Monero).

Należy zauważyć, że w przypadku podpisów elektronicznych używanych w obrocie prawnym do podpisywania dokumentów cyfrowych, sytuacja jest całkowicie odmienna. Po pierwsze, można dokonać unieważnienia certyfikatu przyporządkowującego określony klucz do jego posiadacza i zablokować możliwości pozytywnej weryfikacji podpisów utworzonych od tego momentu za pomocą unieważnionego klucza. Osoba będąca celem ataku może wygenerować nową parę kluczy, uzyskać certyfikat na nowy klucz publiczny i kontynuować posługiwanie się podpisem elektronicznym. Problemem są jedynie sfałszowane oświadczenia woli powstałe przed ich wykryciem przez ofiarę i unieważnieniem certyfikatu. W przypadku obrotu kryptowalutami sytuacja jest odmienna. Obecnie mamy do czynienia z prawami na okaziciela – nie ma powiązania prawowitego właściciela z kluczem publicznym.

Wartym uwagi jest fakt, że problem ten może być rozwiązany przez wprowadzenie zasad zawartych w projektowanych regulacjach (UE2, 2023) i (UE1, 2023). Możliwość identyfikacji uczestników każdej transakcji daje możliwości cofnięcia transakcji w przypadku wykrycia złamania określonego klucza publicznego. Co więcej, prawowity posiadacz klucza prywatnego może korzystać ze schematów pozwalających na udowodnienie, które podpisy weryfikujące się przy pomocy jego klucza publicznego zostały sfałszowane (przykład takiej techniki przedstawiliśmy w (Błaśkiewicz, 2022).

Należy podkreślić, że możliwości złamania klucza publicznego niekoniecznie musi być wykorzystana do przejęcie kryptowalut. W przypadku Monero, daje to możliwość przekazywania środków w sposób omijający wszelką potencjalną kontrolę. Mianowicie, nowy klucz publiczny adresata transakcji nie byłby tworzony za pomocą mechanizmu stealth address, tylko losowo. Odbiorcą byłaby osoba mogąca obliczać dyskretne logarytmy. Jednocześnie każdy uczestnik systemu Monero mógłby udowod-

nić, że nie jest adresatem transakcji zgodnie z mechanizmem *stealth address* (Kubiak, 2023).

Można oczekiwać, że przyszłe postępy w zakresie łamania problemu dyskretnego logarytmu będą miały charakter selektywny. Zagrożone mogą być zarówno określone grupy (określone krzywe eliptyczne) jak i pewne „*słabe klucze*" w tych grupach. Dla krzywych eliptycznych istnieje wiele przykładów „słabych grup". Stąd też organy takie, jak NIST wydają rekomendacje w zakresie wyboru krzywych eliptycznych.

Generatory liczb losowych. Większość kryptowalut opartych jest na jednym z dwóch schematów podpisu: ECDSA oraz EdDSA[73]. Drugi z nich jest schematem deterministycznym – do wygenerowania podpisu nie są potrzebne liczby losowe, tak więc ewentualne podatności generatorów liczb losowych nie stanowią zagrożenia. Jest to zresztą jedna z podstawowych cech przemawiających za stosowaniem EdDSA w wielu obszarach. W przypadku ECDSA gwarancje bezpieczeństwa podpisów obowiązują, gdy output generatora losowych parametrów jest nieodróżnialny od outputu idealnego generatora losowego. Co więcej, gdy atakujący może zgadnąć output generatora (nawet z prawdopodobieństwem takim jak 2^{-40}), wtedy atakujący może wyliczyć klucz prywatny użyty do złożenia podpisu ECDSA. Problem podatności związanych w ECDSA w praktyce jest omawiany w (Wang, 2020).

W przypadku stosowania deterministycznej wersji podpisu ECDSA według RFC 6979 (RFC, 2023) znika problem słabości generatora liczb losowych. RFC 6979 zostało zaadoptowane przez Bitcoin już w 2013 roku.

Słabością zarówno EcDSA, jak i deterministycznej wersji ECDSA jest to, że osoba weryfikująca podpis nie jest w stanie stwierdzić, jaki był proces generowania „losowego" komponentu i że odpowiada on specyfikacji EcDSA lub RFC 6979. Z tego względu w przypadku realizacji sprzętowej portfela kryptowalut należałoby się zastanowić nad potrzebą certyfikacji urządzeń.

Funkcje hashujące. Należy wziąć pod uwagę cztery fundamentalne zastosowania i cechy funkcji haszujących. Po pierwsze, są one stosowane jako komponent w podpisach cyfrowych. W tym wypadku niebezpieczeństwem jest ewentualna podatność w zakresie tzw. *second preimage resistance*. W przypadku tym atakujący dla zadanej transakcji M stara się znaleźć inną transakcję M' tak aby ich wartości przez funkcję haszującą były takie same. Atak taki mógłby potencjalnie zmienić transakcję przy zachowaniu tych samych gwarancji niezaprzeczalności przez blockchain. Margines bezpieczeństwa w tym przypadku jest jednak dość znaczny – nawet złamanie własności *second preimage resistance* nie gwarantowałoby, że alternatywne przeciwobrazy miałby postać sensownej transakcji, a tym bardziej transakcji atrakcyjnej z punktu widzenia atakującego. Co więcej, teoretyczne złożoności ataków na stosowane dziś funkcje haszujące różnią się dramatycznie dla znalezienia konfliktu i dla *second preimage resistance* (przykładowo podaje się złożoność 2^{128} w pierwszym przypadku dla funkcji SHA-256). Z drugiej strony, znalezienie konfliktu jest uważane za poważną przesłankę do zmiany algorytmu haszowania w powszechnych zastosowaniach.

Drugim obszarem zastosowania funkcji haszującej jest redukcja wielkości danych do bloku o ustalonej długości. Dla przykładu – konstrukcja bloku dla blockchaina Bitcoina przewiduje zbudowanie drzewa Merkla dla potwierdzanych transakcji i wpisanie do headera bloku jedynie wartości korzenia drzewa. Podobnie jak poprzednio, manipulacje mogłyby polegać na zamianie elementów drzewa w wypadku braku odporności na *second preimage resistance*. Tym samym poziom zagrożeń jest analogiczny jak w poprzednim wypadku.

Trzeci obszar, gdzie intensywnie wykorzystane są funkcje haszujące to protokół PoW omawiany w rozdziale 4. W tym wypadku nie jest konieczne łamanie funkcji haszującej, problemem staje się możliwość przyspieszenia poszukiwań. Fundamentalnym założeniem dla systemów PoW jest niemożność istotnego przyspieszenia poszukiwań ponad metodę prób i błędów. Dotychczasowe techniki rozwijane dla łamania funkcji haszujących nie wydają się wskazywać na jakieś istotne pomysły mogące zagrozić mechanizmowi PoW. Dotyczy to także obliczeń kwantowych. Gdyby nawet takie metody się pojawiły, warto zauważyć, że istnieje możliwość przejścia na mechanizmy PoS – co zresztą jest postulowane ze względu na olbrzymią konsumpcję energii przez mechanizm PoW.

Czwarty obszar zastosowania funkcji haszujących to proces wyprowadzania kluczy opisany w sekcji 3.1. Wielokrotne użycie funkcji haszującej ma za zadanie podnieść koszt ataków typu brute force

73 ethanfast.com/top-crypto.html

– w istocie przy małej entropii czy przewidywalności początkowego zalążka podanego przez posiadacza, wartość klucza może być odgadnięta i sprawdzona przez atakującego bez łamania funkcji haszującej. Dobra kryptograficzna funkcja haszująca gwarantuje jednak odporność na ataki polegające na zawężaniu listy kandydatów w następujący sposób:

- atakujący stwierdza, że określony klucz publiczny *Pub* spełnia pewną własność algebraiczną *A*,
- na tej podstawie stwierdza, że zarodek użyty do wygenerowania Pub spełnia własność *B* (z dużym prawdopodobieństwem),
- atakujący przeprowadza atak *brute force* wyprowadzając klucze prywatne i publiczne, ale ograniczając się jedynie do kandydatów na zarodek spełniających własność B.

O ile własność B byłaby mocno selektywna, to realna złożoność obliczeniowa ataku spadłaby w znaczący sposób. Należy jednak podkreślić, że istnienie tego typu zależności (relacja *A* i relacja *B*) natychmiast skutkowałoby negatywną oceną dla funkcji haszującej i wycofaniem jej z obrotu, gdyż funkcja ta stałaby się odróżnialna od wyroczni losowej. Los taki spotkał na przykład rosyjski standard GOST R dla funkcji haszującej (Cui, 2022).

Konkludując, można stwierdzić, że w obszarze tym najistotniejszym zagrożeniem dla pewności obrotu są kwestie złamania mechanizmów podpisów cyfrowych. W obliczu zagrożeń można myśleć o migracji na inne, bezpieczniejsze podpisy. Proces ten wcale jednak nie jest oczywisty. O ile w przypadku migracji z jednej krzywej eliptycznej na inną mamy do czynienia z podobnymi technologiami i dobrze rozpoznanym ryzykiem, przejście na nowe schematy, w tym post kwantowe, niesie ze sobą nowe wyzwania. Pierwszym wyzwaniem mogłaby być konieczność wymiany portfeli sprzętowych, gdy na przykład możliwości hardware'u nie pozwalają na implementację nowych algorytmów. Drugim problemem jest potencjalna podatność na ataki typu side channel pozwalające na odtworzenie klucza prywatnego (patrz na przykład atak [Berzati 2023]) na finalistę konkursu NIST). Trzecim problemem jest wykorzystanie generatorów liczb losowych (na przykład w standaryzowanym CRYSTALS-Dilithium istnieje możliwość użycia losowego ciągu 512 bitów). Nie do zlekceważenia jest także rozmiar podpisów – co niesie za sobą pewne zwiększenie kosztów pamięci potrzebnej do podtrzymania blockchaina.

3.5 Niebezpieczeństwo uwikłania sektora bankowego w odpowiedzialność finansową

Możliwości perturbacji na rynku kryptowalut mogą wynikać z wielu czynników, w tym z powodu czynników technicznych. W tej sytuacji naturalne jest pytanie w jakim zakresie instytucje finansowe uczestniczące w obrocie dochowują zasad należytej staranności i jaki może być zakres przerzucenia odpowiedzialności na te instytucje w przypadku strat poniesionych przez uczestników rynku, a w szczególności konsumentów. Pytanie to jest szczególnie ważne w kontekście prania brudnych pieniędzy, bowiem kryptowaluty są technologią niezwykle ułatwiającą tego typu proceder. Podobnie, brak jest gwarancji w postaci schematów certyfikacji i nadzoru nad emisją kryptowalut i usługami w zakresie kryptowalut. Sektor bankowy jako taki nie jest sektorem zorientowanym w sensie merytorycznego zakresu działania na samodzielną ocenę ryzyka rozwiązań kryptowalutowych pod kątem bezpieczeństwa technicznego. Tak więc jego decyzje w tym zakresie mogłyby być traktowane jako naruszenie zasad *due diligence*.

W bardzo dużym stopniu ryzyko zostałoby zredukowane poprzez wdrożenie projektowanych rozporządzeń (UE2, 2023) oraz (UE1, 2023). Zgodnie z nimi to jednostki wprowadzające kryptowaluty obarczone są szeregiem obowiązków mających zagwarantować bezpieczeństwo. Nadzór państwowy w tym zakresie i działanie na podstawie zezwolenia stwarzają sytuację, w której w sposób systematyczny, jednolity i transparentny powinno być szacowane ryzyko uczestnictwa w operacjach kryptowalutowych oraz wskazane właściwe drogi postępowania.

Osobnym tematem jest uczestnictwo sektora bankowego w usługach związanych z kryptowalutami. Wiele standardowych usług, które mogłyby być przedmiotem aktywności sektora bankowego podpada pod definicję „usług w zakresie kryptoaktywów":

- *„usługa w zakresie kryptoaktywów" oznacza jakąkolwiek usługę lub działalność związaną z jakimikolwiek kryptoaktywami spośród działalności wymienionych poniżej:*
- *przechowywanie kryptoaktywów i zarządzanie nimi w imieniu osób trzecich;*
- *prowadzenie platformy obrotu kryptoaktywami;*

- *wymiana kryptoaktywów na walutę FIAT będącą prawnym środkiem płatniczym;*
- *wymiana kryptoaktywów na inne kryptoaktywa;*
- *wykonywanie zleceń związanych z kryptoaktywami w imieniu osób trzecich;*
- *subemisja kryptoaktywów;*
- *przyjmowanie i przekazywanie zleceń związanych z kryptoaktywami w imieniu osób trzecich;*
- *doradztwo w zakresie kryptoaktywów".*

Rozdział 3 projektowanej regulacji określa obowiązki podmiotów świadczących usługi w zakresie kryptoaktywów. Zmierza to w kierunku korzystnej dla sektora bankowego i konsumentów sytuacji jednolitych reguł ostrożnościowych dla wszystkich usługodawców.

3.6 Ryzyko konieczności przebudowy systemów technicznych przez instytucje finansowe obsługujące rynek kryptowalut

Wspomniane już, a omawiane szerzej w rozdziale 5, projektowane regulacje (UE1, 2023) i (UE2, 2023) prowadzą do radykalnej zmiany rynku kryptowalutowego pod względem technicznym. Fundamentalną różnicą w stosunku do istniejących rozwiązań jest konieczność zapewnienia możliwości identyfikacji uczestników transakcji i przeprowadzenia procedur zgodnie z zasadami due dilligence w przeciwdziałaniu zjawiskom takim, jak finansowanie terroryzmu czy pranie brudnych pieniędzy. Anonimowe kryptowaluty mają być wyeliminowane z rynku europejskiego.

Konsekwencją postulowanych zmian jest konieczność zapewnienia powiązania pomiędzy rachunkiem, portfelem kryptowalutowym oraz wszelkimi innymi mechanizmami pozwalającymi na dokonywanie operacji z rzeczywistymi tożsamościami uczestników transakcji. Tego typu funkcjonalność wymaga stworzenia pewnego rodzaju infrastruktury klucza publicznego. W szczególności mogą to być na przykład rozwiązania oparte na schematach kryptograficznych typu *identity based* (Kiltz, 2008), dotychczas nie stosowane w praktyce w znaczącej skali.

Deanonimizacja nie wyklucza pseudonimizacji uczestników transakcji. W sytuacji dostępności danych o dokonywanych transakcjach w blockchainie, wydaje się to nawet warunkiem koniecznym nie tylko dla atrakcyjności rynkowej, ale także dla zachowania zasady bezpieczeństwa obrotu. Wymaga to zastosowania schematów pseudonimizacji umożliwiających automatyczne i efektywne odzyskanie tożsamości kryjącej się pod pseudonimem przez jednostki świadczące usługi w zakresie kryptoaktywów. Jedyną technologią kryptograficzną, która zdaje się spełniać wymagania tu stawiane jest koncepcja podpisu domenowego (pseudonimowego) zaproponowana przez niemiecki urząd BSI (BSI, 2021). Koncepcja ta może być zrealizowana z zachowaniem dostępu do klucza prywatnego tylko dla jego posiadacza (patrz przegląd [Błaśkiewicz i in. 2019]), co wydaje się warunkiem koniecznym w obrocie kryptowalutami (rozwiązanie z [BSI, 2023] tego warunku nie spełnia). Rozwiązania te są jednak obecnie dostępne jedynie w warstwie koncepcyjnej. Tym samym pierwsza faza realizacji regulacji (UE2, 2023) może być problematyczna pod względem znalezienia pragmatycznych metod realizacji idei.

4. Możliwości realizacji nadzoru nad obrotem finansowym a mechanizmy wspierające anonimowość w obrocie kryptowalutami

Rozważając działanie mechanizmów obrotu kryptowalutami należy brać pod uwagę nie tylko czynności dokonywane zgodnie z procedurami opisanymi w specyfikacji danej kryptowaluty, ale również wszelkie operacje, które zdają się przebiegać zgodnie ze specyfikacją, jednak realizują dodatkowe, ukryte funkcjonalności. Sytuacja jest o tyle skomplikowana, że mechanizmy kryptograficzne opierają się na sekretach (takich jak klucze kryptograficzne) i ujawnienie danych w sposób wykraczający poza specyfikację protokołu prowadzi co najmniej do załamania gwarancji bezpieczeństwa, a niekiedy do faktycznego załamania mechanizmów bezpieczeństwa. W sytuacji tej implementacje dające output nierozróżnialny kryptograficznie od implementacji zgodnych ze specyfikacją mogą być stosowane przez uczestników obrotu w sposób niewykrywalny dla podmiotów pośredniczących w obrocie oraz dla organów kontroli obrotu finansowego. Technologie kryptograficzne tego typu są znane od kilkudziesięciu lat i obejmują takie techniki, jak *subliminal channel* (Simmons, 1983), *kleptografię* (Young, 2004) oraz *kryptografię anamorficzną* (Persiano, 2022).

Opisane wyżej techniki są znane dla większości standardowych protokołów kryptograficznych. Tym samym należy brać pod uwagę możliwości ich wykorzystania przez uczestników obrotu kryptowalutami Jest to o tyle istotne, że sytuacja faktyczna w przypadku kryptowalut może mieć charakter krańcowo odmienny w stosunku do klasycznego obrotu finansowego, gdzie istotne dane o operacjach są widoczne dla jednostek kontroli finansowej.

Czynnikiem niezwykle sprzyjającym ukryciu operacji jest możliwość realizacji operacji na kryptowalutach za pomocą portfeli opartych na realizacji czysto software'owej. Liczba tego typu oferowanych portfeli jest dosyć spora. Część z nich to rozwiązania typu open source dające prawo do modyfikacji kodu. Najistotniejszy jest jednak dostęp do wysokopoziomego kodu w postaci bez obfuskacji (26 portfeli na 50 na stronie https://ethereum.org/). Znacząco obniża to wysiłek, jaki trzeba włożyć, aby zmodyfikować portfel do postaci realizującej dodatkowe, ukryte funkcjonalności, nie zawsze legalne.

4.1 Faktyczny poziom anonimowości na przykładzie Bitcoina, Ethereum i Monero

Podstawowym identyfikatorem uczestnika obrotu kryptowalutami nie jest rzeczywista tożsamość, ale kryptograficzny klucz publiczny (Bitcoin, Ethereum) lub zestaw kluczy publicznych (Monero). Możliwość działania w imieniu tej osoby oparta jest na posiadaniu klucza prywatnego lub kluczy prywatnych odpowiadających kluczowi lub kluczom publicznym. Tak więc klucz publiczny pełni rolę identyfikatora tożsamości elektronicznej, podobnie jak to ma miejsce w niektórych systemach zarządzania tożsamością (na przykład SPKI). Użycie kluczy kryptograficznych zamiast oficjalnych identyfikatorów uczestników podyktowane jest względami praktycznymi: z jednej strony pozwala to na uniknięcie ryzyka kolizji tożsamości z wysokim prawdopodobieństwem, a z drugiej strony nie wymaga budowy infrastruktury PKI potwierdzającej związek między osobami fizycznymi a kluczami publicznymi.

Efektem ubocznym jest brak bezpośredniego związku klucza publicznego uczestnika obrotu kryptowalutami z tożsamością tego uczestnika. Ponieważ generowanie kluczy kryptograficznych odbywa się w sposób niezależny od tożsamości osoby generującej klucze mamy do czynienia z procesem anonimizacji w sensie dyrektywy eIDAS (eIDAS, 2014) a nie pseudonimizacji. W przypadku generowania klucza za pomocą kodów mnemonicznych początkowy zestaw słów kodowych wybierany jest przez posiadacza klucza i wszelka ingerencja w ten proces powodowałaby zmniejszenie entropii, a tym samym mogła by doprowadzić do obniżenia poziomu nieprzewidywalności kluczy prywatnych.

Korzystanie z anonimowych identyfikatorów nie oznacza, że gwarantują one pełną anonimowość uczestników obrotu kryptowalutami. W przypadku kryptowalut, takich jak Bitcoin czy Ethereum, przepływ środków odbywa się pomiędzy kontami, których identyfikatorami/adresami są klucze publiczne używane do uwierzytelniania transakcji. Pozwala to na uzyskanie pełnego obrazu przepływów środków w systemie. Faktyczny poziom anonimowości w tym przypadku jest związany z informacjami, które mogą być uzyskane poprzez analizę ruchu środków. Wskazówką może być na przykład moment dokonywania transakcji (wskazujący na strefę czasową), brak transakcji w określonym czasie (szabat), kierunek przepływów (na przykład transakcje związane z okupem przekazywanym przez ofiary ransomware), wolumen transakcji, jak też transakcje z kontami, dla których znany jest właściciel. Sytuacja ta przypomina problem odkrycia faktycznej tożsamości użytkowników sieci komórkowych przez organy ścigania: w przypadku kontaktów w grupach przestępczych karty SIM mogą być rejestrowane na

osoby nie mające nic wspólnego z faktycznymi posiadaczami, jednak analiza dokonywanych połączeń może wskazywać na faktyczne tożsamości użytkowników.

Techniką, która może być stosowana do ograniczenia możliwości analizy przepływów, jest krótkookresowe korzystanie z adresów. W istocie mamy wtedy do czynienia z *mixem* w sensie teorio-informacyjnym: jeśli na konto X kierowane jest x jednostek kryptowaluty z kont A oraz B, a następnie po x jednostek jest transferowanych na konta C i D, to nie można stwierdzić, czy środki z konta A zostały przekazane na konto C czy na konto D. Konto X w takim przypadku działa jako konto techniczne służące anonimizacji przepływów.

Na ile ta technika jest skuteczna, zależy od poziomu wyrafinowania stosowanej metody. Sytuacja jest analogiczna do analizy ruchu w przypadku *Onion Routing*. Trzeba jednak pamiętać, że dla *Onion Routing* wysoki, dowodliwy poziom anonimowości można osiągnąć poprzez dostępność danych tylko z pewnej frakcji połączeń (Berman, 2015). W przypadku kryptowalut, dzięki istnieniu i dostępności danych z Blockchaina, analiza przepływów może być oparta na pełnej wiedzy dotyczącej przepływów.

W omawianym kontekście szczególną uwagę należy zwrócić na kryptowalutę Monero, gdzie celem projektowym było zapewnienie silnej anonimowości przepływu kryptowaluty XMR. Mechanizmy realizujące ten cel to: tzw. *stealth address* oraz specyficzny podpis pierścieniowy.

Każdy uczestnik systemu Monero posiada dwa podstawowe klucze publiczne i odpowiadające mu klucze prywatne stanowiące o możliwości dokonywania transakcji na koncie. System Monero oparty jest na zasadzie, że zarówno adres nadawcy jak i adres odbiorcy powinny pozostać ukryte na tyle, na ile to jest możliwe. Zasadniczą trudnością o charakterze matematycznym było tu wyeliminowanie możliwości wielokrotnego wykorzystania tych samych środków na koncie.

Dla ukrycia adresata transakcji Monero wykorzystuje mechanizm *stealth address*. Polega on na wygenerowaniu klucza publicznego, dla którego odpowiadający klucz prywatny może być wyprowadzony jedynie przez adresata transakcji. W szczególności nie jest on znany przez autora transakcji. Stealth address jest skonstruowany w taki sposób, że bez znajomości klucza prywatnego osoby B nie można odróżnić adresów przeznaczonych dla osoby B i adresów przeznaczonych dla innych osób. Gwarancje mają charakter nieodróżnialności obliczeniowej: przy realnych mocach obliczeniowych żaden algorytm nie jest w stanie przedstawiać odpowiedzi, które w sposób zauważalny byłyby lepsze od odpowiedzi losowych. Oczywiście dopóty, dopóki podstawowe założenia kryptograficzne o trudności problemu dyskretnego logarytmu nie zostały złamane.

Druga użyta technika dotyczy ukrycia autora transakcji. Tutaj efektywność mechanizmu anonimizacji jest niższa. Transakcja musi być możliwa tylko wtedy, gdy jest autoryzowana poprzez użycie określonego klucza prywatnego. Odpowiadający mu klucz publiczny powinien znaleźć się w danych transakcji choćby po to, by móc sprawdzić, że wykorzystywane są środki XMR, które faktycznie są w obrocie. Częściowe rozwiązanie problemu możliwe jest dzięki użyciu podpisu pierścieniowego. Podpis taki zawiera *pierścień kluczy publicznych* wybranych przez autora transakcji. Klucze te mogą być wybrane dowolnie, jednak z jednym zastrzeżeniem. Podpis pierścieniowy daje się utworzyć jedynie wtedy, gdy podpisujący użyje klucza prywatnego odpowiadającemu któremuś z kluczy publicznych w pierścieniu. Oczywiście, klucze publiczne w pierścieniu to klucze przypisane do jakichś poprzednich transakcji. Ostatnią własnością domykającą system jest mechanizm pozwalający na wykrycie, że dwa podpisy pierścieniowe zostały skonstruowane przy pomocy tego samego klucza prywatnego. Mechanizm ten zapewnia, że próba przekazania z konta tych samych środków XMR dwukrotnie zostałaby natychmiast wykryta. Własności kryptograficzne omawianego podpisu pierścieniowego dają gwarancje teorio-informacyjne, że nawet przy nieograniczonych mocach obliczeniowych nie da się stwierdzić, któremu kluczowi z pierścienia odpowiada klucz prywatny użyty przez podpisującego. Jedyna informacja dostępna dla obserwatora transakcji to fakt, że podpis został złożony przez osobę w posiadaniu klucza prywatnego odpowiadającego jednemu z kluczy z pierścienia.

Opisane powyżej gwarancje anonimowości autora transakcji nie są jednak tak silne, jak wynikałoby z własności podpisu pierścieniowego (Wijaya, 2018). Po pierwsze, dla posiadacza klucza prywatnego odpowiadającego danemu kluczowi publicznemu P wszystkie pierścienie zawierające klucz P efektywnie są mniejsze o ten właśnie klucz. Podobnie, gdy uzyskamy informację, że klucz prywatny odpowiadający kluczowi publicznemu P został już użyty, klucz P można wyeliminować analizując

nowe transakcje. Istotną rolę mogą odegrać koalicje uczestników obrotu wymieniające się tego typu informacjami. W krańcowych przypadkach utrata anonimowości może mieć charakter lawiny: o ile dojdziemy do wniosku, że wszystkie klucze oprócz klucza P w danym pierścieniu nie mogą odpowiadać kluczowi prywatnemu użytemu do wygenerowania podpisu, to nabieramy pewności, że klucz odpowiadający P został użyty właśnie w tym podpisie. W konsekwencji możemy wyeliminować P jako kandydata dla wszystkich innych pierścieni, w których występuje. Duże znaczenie w analizie może odegrać również czas, jaki upłynął od pierwszego wystąpienia określonego klucza. Przy wysokim tempie obrotu środkami, klucz niedawno powstały staje się naturalnym kandydatem na klucz odpowiadający przekazanym środkom. Tym samym, można przyjąć strategię wyboru do pierścienia kluczy stosunkowo świeżych. Z kolei, w przypadku użycia środków związanych z długo niewykorzystywanym kluczem, wspomniana wyżej strategia zmusza do użycia w pierścieniu wielu kluczy, które nie są świeże. Tego typu aspekty prowadzą do sytuacji, w której wybór kluczy publicznych do pierścienia staje się swoistą grą przeciwko jednostkom analizującym transakcje.

Warto na koniec dodać, że analiza transakcji pod kątem rzeczywistych autorów transakcji może co najwyżej prowadzić do sytuacji, w której znamy dokładnie przepływ XMR pomiędzy kluczami publicznymi. W odróżnieniu do Bitcoina i Ethereum, klucze te mają charakter jednorazowy – dla obserwatora nic nie wiąże kluczy wskazanych przez *stealth addresses* będących w posiadaniu tego samego uczestnika obrotu.

4.2 Techniczne możliwości wykorzystania kryptowalut do ukrytych transferów kryptowalut i danych

Zasadniczą zaletą kryptowalut pod kątem możliwości realizacji anonimowych transferów środków oraz danych jest dostęp do danych o transakcjach w blockchainie. Zasadnicza zaleta tej technologii – rozproszony sposób przechowywania informacji – daje możliwość realizacji anonimowej komunikacji, gdzie narzędzia analizy ruchu (*traffic analysis*) niewiele dają, bowiem dane z blockchaina są kopiowane do całej sieci.

Dla realizacji ukrytych przepływów zasadnicze znaczenie ma możliwość modyfikacji i kreatywnego wykorzystania oprogramowania stojącego po stronie klienta. Tak długo jak oprogramowanie to zachowuje się w sposób nieodróżnialny od oprogramowania zgodnego ze specyfikacją kryptowaluty, nie można stwierdzić odstępstw od specyfikacji. W istocie problem jest nieco głębszy. W przypadku techniki stealth address Monero organy nadzorcze mogą żądać przedstawienia danych umożliwiających sprawdzenie adresata transakcji. Teoretycznie pozwala to na sprawowanie określonego nadzoru finansowego.

Możliwości te dotyczą jednak tylko sytuacji, w której autor transakcji przestrzega specyfikacji technicznej. Autorzy transakcji, które mają zostać ukryte przed nadzorem finansowym, organami ścigania itp., mogą wykorzystać możliwości tkwiące w niestandardowym zakodowaniu transakcji, tak aby z przekazywanych środków mogła skorzystać inna osoba niż oficjalny odbiorca.

Możliwości realizacji tego scenariusza jest kilka. Jeden z nich to ukrycie kryptogramów w losowych fragmentach podpisu pierścieniowego użytego do uwierzytelnienia transakcji. O ile kryptogramy te są nieodróżnialne od losowych ciągów bitów (a zwykle tej własności żądamy od dobrych systemów szyfrowania), to możliwości odkrycia modyfikacji przez organy nadzorujące byłyby praktycznie zerowe. W konsekwencji autor transakcji mógłby udowodnić, że przekazuje środki do legalnego odbiorcy, zaś w istocie mógłby udostępnić je dowolnemu odbiorcy.

Ten sam mechanizm może być użyty do przekazywania w ukryty sposób dowolnych danych (na przykład danych wywiadowczych, kluczy do systemów teleinformatycznych itp). W tym przypadku, dane mogą być ukryte w losowych ciągach zawartych w podpisie pierścieniowym, zaś pozostała część transakcji miałaby charakter dokładnie zgodny ze specyfikacją. W odróżnieniu od standardowych metod wykorzystania kryptografii w takim celu, blockchain i szeroki zakres jego rozproszenia zapewnia silną anonimowość adresata.

W przypadku Ethereum (gdzie podpis nie zawiera ciągów (pseudo)losowych mogących być wprost zamienionych przez kryptogramy) mechanizm przekazania środków może być oparty na technikach kleptograficznych. W scenariuszu tym osoba przekazująca środki nie dokonuje transakcji typu stricte, jednak udostępnia adresatowi klucz prywatny związany z określonym swoim kontem. W ten sposób adresat efektywnie uzyskuje możliwość dysponowania środkami zgromadzonymi na koncie bez koniecz-

ności wykonania jakiejkolwiek transakcji z osobą, od której uzyskuje środki. Przekazanie klucza prywatnego adresatowi może być ukryte w jakiejkolwiek transakcji skierowanej do jakiejkolwiek osoby trzeciej. Pod względem technicznym można ten scenariusz zrealizować poprzez generowanie losowego elementu z podpisu ECDSA w sposób umożliwiający jego odtworzenie przez stronę, której ma być przekazany klucz prywatny. Przypomnijmy tu, że znajomość efemerycznej wartości losowej używanej w podpisie ECDSA pozwala na wyprowadzenie klucza prywatnego użytego do wygenerowania podpisu.

Warto zaznaczyć, że podobne mechanizmy mogą być zastosowane dla transakcji podpisanych za pomocą schematu Schnorra. Tym samym wszystko, co powiedzieliśmy powyżej, odnosi się w jednakowym stopniu do Bitcoina, bez względu na to, jaki schemat podpisu został zastosowany

Zarówno w przypadku Ethereum, jak i Bitcoina, możliwe jest wykorzystanie podpisu pod transakcją (ECDSA lub podpis Schnorra) tak aby utworzyć anamorficzny kanał informacji (Kutyłowski, 2023). Kanał ma mniejszą pojemność niż w przypadku Monero, jednak zagrożenie pozostaje.

4.3 Możliwości prania brudnych pieniędzy i omijania sankcji ekonomicznych za pomocą obrotu kryptowalutami oraz realne możliwości techniczne przeciwdziałania tym zjawiskom

Poziom anonimowości oferowany przez obrót kryptowalutami należy ocenić z punktu widzenia dwóch sytuacji. Pierwszą z nich są narzędzia informatyki śledczej, kryptoanaliza danych, analiza danych historycznych utrwalonych w blockchainenie itp. Drugim poziomem jest bieżące monitorowanie dokonywanych operacji. W pierwszym scenariuszu mówimy o analizie post factum, zaś w drugim o bieżącym monitorowaniu sytuacji i ewentualnym przeciwdziałaniu niepożądanym zjawiskom. Tak więc w pierwszym scenariuszu może chodzić o zgromadzenia dowodów do postępowania karnego, podczas gdy w drugim scenariuszu chodzi o blokowanie niepożądanego obrotu.

Pierwszym problemem jest brak powiązania tożsamości cyfrowej – konta/adresu/kluczy publicznych – z określonymi osobami fizycznymi lub organizacjami. Tym samym wszelka automatyczna kontrola uczestników operacji finansowych dokonywanych za pomocą kryptowalut jest niemożliwa. Brak jest również ograniczeń terytorialnych do dokonywanych transakcji kryptowalutami. W szczególności przedstawiane są argumenty, że zakup kryptowalut stanowił metodę obejścia ograniczeń dla wolumenu zakupu walut obcych i transferu środków finansowych z ChRL za granicę. W konsekwencji przeciwdziałanie ucieczce kapitału miało doprowadzić, jako jeden z kluczowych czynników, do zakazu obrotu kryptowalutami w ChRL we wrześniu 2021 roku (WEC, 2022).

Wymuszenie (na przykład poprzez regulacje ustawowe lub też zapisy umowne) powiązania tożsamości cyfrowej kont kryptowalutowych z tożsamością deklarowanych posiadaczy niewiele wnosi jako przeciwdziałanie niepożądanym zjawiskom w obrocie kryptowalutami. W istocie, jedynym dysponentem środków na koncie kryptowalutami pozostaje faktyczny posiadacz kluczy prywatnych do określonego klucza lub kluczy publicznych. Stanowi to istotną różnicę w stosunku do klasycznych rachunków finansowych, gdzie posiadacz konta pozostaje faktycznym dysponentem i w przypadku utraty narzędzi elektronicznych (w tym również narzędzi opartych na technikach kryptograficznych) służących do uwierzytelniania może dokonać dyspozycji z rachunku po uwierzytelnieniu się w alternatywny sposób. W przypadku kryptowalut takich możliwości nie ma. Dlatego osoba firmująca swą tożsamością operacje na określonym koncie kryptowalutowym nie może oszukać faktycznego właściciela środków i wyprowadzić środków. Jest to jedna z podstawowych faktycznych funkcjonalności kryptowalut.

Tak jak wskazaliśmy w poprzednim rozdziale, przepływ kryptowalut może odbywać się drogą zupełnie odmienną od tej opisanej w specyfikacji systemów. Jak zauważyliśmy, scedowanie środków na rzecz osoby trzeciej może być dokonane poprzez zdradzenie klucza prywatnego metodami kleptograficznymi. Do dokonania tego typu operacji konieczna jest jedynie znajomość pojedynczego klucza publicznego tej osoby w tej samej strukturze algebraicznej opartej na problemie dyskretnego logarytmu. Kluczem tym może być klucz przypisany do konta kryptowalutowego i używany do podpisywania transakcji, klucz jednorazowy związany z określoną kwotą XMR, jak i klucz publiczny spoza systemu kryptowalut (na przykład klucz publiczny do weryfikacji podpisu elektronicznego beneficjen-

ta). Taka operacja tworzy w istocie wspólne konto osoby udostępniającej klucz i osoby otrzymującej klucz z nieograniczonymi możliwościami dokonywania operacji przez któregokolwiek wspólnika. Co więcej, fakt przekazania klucza prywatnego nie wiąże się z jakimikolwiek operacjami wykraczającymi poza standardowe, legalne operacje na koncie. Ponadto, uczestnikiem tych operacji nie musi wcale być osoba otrzymująca klucz prywatny. Na koniec, warto dodać, że nawet w przypadku podejrzeń o takie działania użyty schemat kleptograficzny daje gwarancje nierozróżnialności transakcji kleptograficznych od transakcji zgodnych ze specyfikacją. Gwarancje te są skuteczne dopóty, dopóki nie zostaną obalone założenia kryptograficzne będące podstawą kryptowaluty. Gdyby tak jednak się stało, wtedy ta kryptowaluta traci wartość do poziomu trudności złamania klucza publicznego. Jest to sytuacja upadku kryptowaluty.

Sytuacja jest jeszcze trudniejsza w przypadku Monero. Tu, jak wskazaliśmy, środki mogą nominalnie przechodzić na legalne konto (autor transakcji może ujawnić wartości efemeryczne wskazujące kto powinien być odbiorcą transakcji), niemniej jednak faktycznym środków może być ktoś inny. Scenariusz ten może zrealizować wysyłający posługując się dwoma kontami, dla których posiada klucze prywatne. Operacja polegałaby na przerzucaniu niewinnych kwot pomiędzy własnymi rachunkami.

Mechanizm anonimizacji Monero pozwala też ukryć wypływ własnych środków. Nawet jeśli organ nadzorujący podejrzewa, że określony klucz publiczny P jest związany ze środkami w dyspozycji osoby A, zaś osoba A tworzy transakcję wykorzystującą klucz P w pierścieniu, to daje to pewność, że osoba A faktycznie wykorzystała środki powiązane z kluczem P. Ewentualne oskarżenie osoby A o łamanie sankcji, pranie brudnych pieniędzy itp. oparte na wykorzystaniu środków powiązanych z kluczem P, może być bardzo łatwo podważone jako dowód w postępowaniu przeciwko osobie A.

Należy podkreślić, że istnieje zasadnicza różnica pomiędzy sytuacją dla zaawansowanego podpisu elektronicznego a sytuacją dla obrotu kryptowalutami. W pierwszym przypadku regulacje prawne eIDAS (eIDAS, 2014) wymagają silnej ochrony klucza. W przypadku *bezpiecznego urządzenia do składania podpisu elektronicznego* nie ma możliwości uzyskania kopii klucza prywatnego nawet przez posiadacza tego urządzenia. W przypadku kryptowalut tego typu implementacja idei jest wykluczona – każde urządzenie kryptograficzne ma swój cykl życiowy i wskutek starzenia się komponentów z czasem musi ulec awarii. W tej sytuacji środki zgromadzone na koncie uległyby trwałemu zamrożeniu. Powyższa sytuacja jest powodem popularności rozwiązań opartych na kodach mnemonicznych, gdzie zarodek dla kluczy może być przez posiadacza przechowywany jako zapisany na papierze.

Warto zaznaczyć, że technicznie możliwa jest realizacja systemu opartego na bezpiecznych urządzeniach, w którym posiadacz urządzeń ani nikt inny nie ma dostępu do klucza, jednak posiadacz jest w stanie przenieść klucze do innego swojego urządzenia w trybie *post mortem* – tzn. gdy pierwotne urządzenie uległo awarii wraz ze zniszczeniem zawartego w nim klucza. Konkludując, należy jednak stwierdzić, że są to możliwości przyszłej ewolucji na rynku kryptowalut, nie mające odzwierciedlenia w obecnie oferowanych produktach.

4.4 Poziom odpowiedzialności instytucji finansowych w kontekście ich obowiązków prawnych

Istotne zmiany na rynku kryptowalut mogą być konsekwencją dwóch planowanych regulacji na poziomie europejskim: nowego rozporządzenia (UE1, 2023) w kontekście zabezpieczeń AML oraz rozporządzenia (UE2, 2023) ustanawiającego ramy dla funkcjonowania rynku kryptoaktywów (w tym kryptowalut). Regulacje te są odpowiedzią na dwa zjawiska:

- rozwój rynku kryptoaktywów w sposób zagrażający zasadom zdrowej konkurencji, interesom konsumentów, a jednocześnie wbrew zasadom wspólnego rynku;
- świadomość omijania zabezpieczeń mających na celu zwalczanie terroryzmu, pranie brudnych pieniędzy, sankcji i tym podobnych zjawisk za pomocą kryptowalut.

Propozycja (UE2, 2023) kładzie nacisk na uporządkowanie rynku w kierunku jego rozwoju, podczas gdy nowsza propozycja (UE1, 2023) już odzwierciedla świadomość złożoności sytuacji pod względem bezpieczeństwa finansowego.

W zasadzie najważniejszym postanowieniem (UE1, 2023) jest proponowany artykuł 58. W oryginalnym brzmieniu ma on postać:

„Article 58 Anonymous accounts and bearer shares and bearer share warrants 1. Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes, anonymity-enhancing coins or anonymous crypto-asset wallets as well as any account otherwise allowing for the anonymisation of the customer account holder. Owners and beneficiaries of existing anonymous accounts, anonymous passbooks, anonymous safe deposit boxes or crypto-asset wallets shall be subject to customer due diligence measures before those accounts, passbooks, deposit boxes or crypto-asset wallets are used in any way".

Artykuł ten w istocie jest zakazem stosowania większości kryptowalut obecnych na rynku, jako instrumentów o anonimowym charakterze. Zakaz dotyczy nie tylko instytucji emitujących kryptoaktywa i usługi z nimi związane, ale także posiadaczy aktywów w kryptowalutach. Posiadane kryptowaluty mogłyby być użyte dopiero po przeprowadzeniu wobec posiadacza procedur opisanych w projektowanej regulacji. Efekt faktyczny projektowanej regulacji byłby więc porównywalny z sytuacją na rynku finansowym CHRL, po zakazaniu obrotu kryptowalutami. Realizacja artykułu 58 to w istocie upodobnienie rynku kryptowalut do klasycznego obrotu finansowego poprzez wymianę aktywów pomiędzy kontami klientów. Podstawową różnicą pozostałoby to, że zawartość konta byłaby publicznie weryfikowalna na podstawie danych zawartych w blockchainie, a nie określana w istocie na podstawie oświadczenia zaufanej instytucji finansowej.

Można postawić pytanie na ile głębokie powinny być zmiany koncepcji kryptowalut, aby spełnić można było wymagania w zaproponowanej regulacji. Sama rezygnacja z anonimowości jako fundamentalnej cechy budowy kryptowaluty nie wystarcza do zachowania zgodności z projektowaną regulacją (UE1, 2023).

Po pierwsze, istotnym warunkiem zachowania należytej staranności jest identyfikacja i weryfikacja tożsamości beneficjenta transakcji (31) oraz (32a) w (UE1, 2023). O ile identyfikacja jest zadaniem relatywnie prostym, to weryfikacja tożsamości rzeczywistego beneficjenta danej transakcji może okazać się niezwykle trudna. Chodzi tu bowiem nie o beneficjenta formalnego, ale rzeczywistego – tzn. osoby posiadającej klucz prywatny, przy pomocy którego można wykorzystać kryptowaluty przekazane w transakcji. Każdy mechanizm oparty na posiadaniu klucza prywatnego może prowadzić do tego typu problemów.

Oczywiście można się starać uzupełnić ekosystem kryptowaluty o mechanizmy uzupełniające – w tym przypadku o mechanizm weryfikacji, że deklarowany odbiorca kryptowaluty faktycznie posiada przypisany mu klucz prywatny. Proste mechanizmy w tym przypadku zawodzą, gdyż badany beneficjent formalny może w istocie pełnić rolę proxy, pośrednicząc w komunikacji pomiędzy kontrolerem a beneficjentem rzeczywistym posiadającym klucz prywatny, o którym jest mowa.

Budowa wyszukanych metod kryptograficznych też nie do końca eliminuje zagrożenie – niemożliwe jest bowiem odkrycie sytuacji użyczenia dostępu do konta poprzez współdzielenie klucza prywatnego przekazanego metodami kleptograficznymi. O ile protokoły kryptograficzne dostarczają wielu narzędzi pozwalających na potwierdzenie, że dana osoba posiada określony klucz prywatny bez konieczności okazania go, brak jest rozwiązań pozwalających na stwierdzenie, że nikt inny nie zna tego klucza. Rozwiązaniem mogłoby być dopuszczenie kryptowalut jedynie opartych na portfelach zaimplementowanych w bezpiecznych urządzeniach kryptograficznych, ale to z kolei eliminuje wiele z zalet kryptowalut.

Na koniec, warto zauważyć, że omawiane badanie beneficjenta transakcji powinno odbywać się w zasadzie przed każdą transakcją – zgodnie z artykułem 19. Jest to związane z faktem, że w systemach opartych na znajomości klucza prywatnego sytuacja może się dynamicznie zmieniać.

Trzeba zaznaczyć, że zasady ostrożnościowe wynikające z polityki AML nie znajdują zastosowania do transakcji, które z tego punktu widzenia obarczone są niewielkim ryzykiem. Warto jednak zauważyć, że granica dla transakcji kryptowalutowych wyznaczona została na równowartość 1000 euro zamiast równowartości 10.000 euro obowiązującej w przypadku ogólnym. Świadczy to dobitnie, jak bardzo podejrzanym instrumentem są kryptowaluty w oczach autorów regulacji.

Prawdziwie niebezpieczne mogą okazać się obowiązki instytucji finansowej pod kątem budowania polityk, oceny ryzyka i monitorowania sytuacji. Zwrócić warto uwagę na artykuł 31a, który ze względu na wagę cytujemy w oryginale:

„Article 31a Measures to mitigate risks in relation to transactions with a self-hosted address

1. Crypto-asset service providers shall identify and assess the risk of money laundering and financing of terrorism associated with transfers of crypto-assets directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Crypto-asset service providers shall apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include one or more of the following:

(a) taking risk-based measures to identify, and verify the identity of, the originator or beneficiary of a transfer made from or to a self-hosted address or beneficial owner of such originator or beneficiary, including through reliance on third parties;

(b) requiring additional information on the origin and destination of the crypto-assets;

(c) conducting enhanced ongoing monitoring of those transactions;

(d) any other measure to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation and evasion of targeted financial sanctions and proliferation financing-related targeted financial sanctions".

W istocie postanowienia te stwarzają wygodną podstawę do obarczenia odpowiedzialnością instytucji finansowych za wszelkie nieszczelności w realizacji ograniczeń AML. Jest to o tyle istotne, iż kryptowaluty stwarzają okazję do obchodzenia zabezpieczeń przy pomocy implementacji protokołów kryptograficznych w sposób odmienny od specyfikacji, a zachowujących się zgodnie z oczekiwaniami kontrolera. Brak jest porównywalnych zagrożeń w sytuacji klasycznego obrotu finansowego.

Ustęp 2 tego samego artykułu 31a postanawia, iż AMLA (proponowana instytucja nadzoru) wyda wytyczne dotyczące środków, o których mowa w komentowanym powyżej ustępie 1, biorąc pod uwagę najnowsze osiągnięcia technologiczne. Wytyczne te mogą przyczynić się do harmonizacji rynku i zmniejszenia poziomu niepewności co do środków, jakie nadzór uzna za wystarczające. Z drugiej jednak strony istnieje ryzyko, że obecnie podejmowane decyzje projektowe mogą w przyszłości okazać się sprzeczne z wytycznymi.

PROGRAM ANALITYCZNO BADAWCZY

5. Kwestie energochłonności i skalowalności

Kryptowaluty po stronie klienta oparte są na standardowych algorytmch kryptograficznych: podpisie cyfrowym i funkcjach haszujących, które nie generują żadnych godnych uwagi problemów w kontekście skalowalności i zużycia energii.

Sytuacja jest całkowicie odmienna w przypadku procesów związanych z funkcjonowaniem blockchaina. Dla osiągnięcia podstawowego celu kryptowaluty – uniezależnienia od pojedynczego operatora lub grupy operatorów – blockchain musi być budowany i zarządzany w odpowiedni sposób. Ochrona przed manipulacjami już istniejącej i rozpowszechnionej części blockchaina jest stosunkowo łatwa i osiągana przez powiązania pomiędzy blokami: podpis i-tego bloku dotyczy nie tylko bieżących transakcji, ale też hasza z poprzedniego bloku. W sytuacji takiej, zmanipulowanie jakiegoś starego bloku wymaga przebudowania całego blockchain od modyfikowanego bloku do bloku zawierającego bieżące transakcje, albo znalezienia konfliktu dla funkcji haszującej.

Stosowane funkcje haszujące mają zapewnić, że drugi scenariusz nie ma szans powodzenia ze względu na trudności obliczeniowe, drugi zaś jest nierealistyczny ze względu na liczbę kopii i dynamikę wzrostu blockchaina.

Omawiany mechanizm tworzenia łańcucha haszy jest, tak jak samo tworzenie transakcji, stosunkowo łatwy w realizacji.

Miejscem, w którym napotykamy na fundamentalne trudności jest dodawanie nowych bloków do blockchaina. W realizowanej powszechnie strategii chodzi o losowe wyłonienie uczestnika bądź grupy uczestników, którzy dokonają rozszerzenia blockchaina lub nadzorują ten proces. Zastosowana metoda musi zapewnić niemożność uzyskania kontroli nad procesem dopisywania nowych bloków przez żadną ze stron ubiegających się o prawo do wydłużenia blockchaina. W przypadku wielu kryptowalut, o prawo do przeprowadzenia tej operacji może ubiegać się każdy uczestnik (*permissionless blockchain*), tak więc konieczny jest rodzaj konsensusu mocno odporny na działania nieuczciwych uczestników protokołu czy też tzw. *Sybil attack*, gdzie atakujący występuje pod wieloma anonimowymi tożsamościami. Ponieważ jak dotąd aktorzy w systemach kryptowalutowych występują bez powiązania ze swoją rzeczywistą tożsamością, *Sybil attack* jest możliwy. Linią obrony jest mechanizm tworzenia blockchaina, który nie pozwala atakującemu osiągnąć w ten sposób żadnych istotnych korzyści.

5.1 Strategie tworzenia distributed ledger/blockchaina. Ich specyfika i techniczne koszty

PoW (Proof-of-Work). Klasyczny system PoW opiera się na zadaniu obliczeniowym, które może być rozwiązane jedynie metodą *brute force*. Prawo do dodania bloków do blockchaina otrzymuje ten, kto rozwiąże zadanie obliczeniowe.

Bitcoin używa w tym celu zadania znalezienia ciągu bitów y takiego, że wartość funkcji Sha-256 obliczonej na wartościach z poprzedniego bloku, bieżących transakcji, stempla czasu oraz y jest ciągiem bitów rozpoczynającym się od pewnej liczby zer. W istocie, metoda ta opiera się na założeniu, że funkcja SHA-256 naśladuje dobrze tzw. *Random Oracle* i znalezienie argumentu y takiego, by wartość SHA-256 dla y wraz z ustalonymi innymi argumentami miała konkretne własności, może być prowadzone jedynie metodą prób i błędów. Nie jest to klasyczna własność funkcji haszujących rozważana w literaturze naukowej (takich jak na przykład *preimage resistance*), jednak jest ona wielokrotnie stosowana w praktyce obliczeniowej. Najgroźniejsze ataki polegające na przełamaniu ochrony danej przez funkcje haszujące wykorzystywały właśnie złamanie omawianego założenia (atak FLAME na certyfikaty podpisane z użyciem MD5). We wspomnianych przypadkach, osiągnięcie sukcesu w ataku było trudniejsze niż znalezienie kolizji dla MD5.

W świetle dotychczasowych badań kryptoanalitycznych trudno ocenić, co może nastąpić wcześniej (o ile w ogóle nastąpi): złamanie omawianej własności o niemożności poprawienia metody prób i błędów w poszukiwaniu ciągu y, czy złamanie którejś z klasycznych literaturowych własności (takich jak znalezienie kolizji). W przypadku powzięcia wątpliwości o sile SHA-256 nic nie stoi na przeszkodzie by zadanie obliczeniowe skomplikować, czy przerzucić się na inną funkcję haszującą, czy wręcz inne zadania obliczeniowe.

Słabością metody PoW jest nieuchronne powiązanie z dużą konsumpcją zasobów. Jest to nieuniknione ze względu na mechanizm ochrony przed Sybil attack: występowanie pod różnymi tożsamościami nie zmienia faktu, że szanse na pierwszeństwo są proporcjonalne do posiadanych zasobów obliczeniowych. Jedynym pocieszeniem jest fakt, iż oczekiwany łączny koszt obliczeniowy PoW na zatwierdzenie transakcji rośnie z liczbą uczestników w tempie niższym niż liniowy.

Proof-of-Space. Zasobem, który jest odporny na Sybil Attack, jest pamięć używana do obliczeń. Istnieją schematy kryptograficzne, które wymagają relatywnie niewielkiej liczby operacji (w stosunku do PoW), ale wykonane mogą być pod warunkiem używania dużego rozmiaru szybko dostępnej pamięci. Wyklucza to stosowanie takich urządzeń, jak karty graficzne czy FPGA, nagminnie stosowanych w procesach opartych na PoW – procesory tych urządzeń wykonujące obliczenia równolegle w przypadku klasycznych systemów PoW nie mogą być użyte, ze względu na brak dostępu do dużej, dedykowanej pamięci. W konsekwencji, urządzeniami predysponowanymi do wykonywania obliczeń Proof-of-Space są konwencjonalne komputery.

Reprezentatywną realizacją Proof-of-Space jest konieczność przygotowania tzw. plotu – obliczanych przy pomocy stosunkowo trudnej obliczeniowo funkcji haszującej. W momencie, w którym ma nastąpić uzupełnienie blockchaina, każdy z uczestników wylicza najmniejsze opóźnienie, które odpowiada wartościom zapisanym w plocie. Przed upływem tego czasu uczestnik nie może dokonywać rozszerzeń blockchaina. W międzyczasie inny uczestnik może już dokonać tej operacji dzięki mniejszej wartości opóźnienia. Mechanizm tworzenia plotów musi gwarantować, by uczestnik nie mógł manipulować jego wartościami. Mechanizm Proof-of-Space jest faktycznie wykorzystywany przez kilka kryptowalut będących w obiegu.

Proof-of-Space ma jednak istotną wadę w obszarze technicznym. W przypadku wykorzystania pamięci typu flash trzeba niestety wziąć pod uwagę fakt ograniczonej liczby zapisów takiej pamięci (na przykład 100 tys. zapisów w danym miejscu). W przypadku zwykłego użytkowania pamięci dyskowej nie jest to wada dyskwalifikująca – cykl życiowy urządzenia może być krótszy ze względu na starzenie się innych komponentów komputera. Proof-of-Space wymaga liczby zapisów w pamięci wykraczającej poza „standardowy użytek".

PoS (Proof-of-Stake). Proof-of-Stake jest w istocie powrotem do rozwiązań opartych na konsensusie w rozproszonym środowisku. Zamiast wyznaczania losowego zwycięzcy uzyskującego prawo przedłużenia blockchaina na podstawie zainwestowanego wysiłku obliczeniowego (prawdopodobieństwo proporcjonalne do wielkości tego wysiłku), realizowany jest algorytm rozproszonego konsensusu. Warunkiem wstępnym uczestnictwa w tym procesie jest złożenie zabezpieczenia w postaci jednostek kryptowaluty. Wymuszenie uczciwego zachowania podczas uzupełniania blockchaina oparte jest na koncepcjach teorii gier: uczestnik zachowujący się nieuczciwie traci złożone zabezpieczenie na podstawie decyzji większości (w domniemaniu uczciwej).

Mechanizm Proof-of-Stake nie wymaga tak dużego zaangażowania zasobów jak w przypadku PoW czy Proof-of-Space. Czynnik ten jest podawany jako podłoże decyzji o skomplikowanej operacji przejścia z PoW na PoS dokonanej w 2022 roku przez Ethereum.

Osiąganie uczciwego konsensusu w rozproszonym środowisku z niezależnymi aktorami jest zagadnieniem algorytmicznym, dla którego z jednej strony zaprojektowano wiele rozwiązań, z drugiej zaś pokazano ograniczenia w przypadku istnienia tzw. bizantyjskich uczestników działających niezgodnie z protokołem i usiłujących wypaczyć wynik działania algorytmu. Jeden z fundamentalnych wyników teoretycznych mówi, że osiągnięcie uczciwego konsensusu przez uczciwych uczestników jest niemożliwe, o ile nie mają oni większości $^2/_3$ wśród uczestników protokołu. Wynik ten nie może być zmieniony czy podważony przez zastosowanie technik kryptograficznych. Cytowane twierdzenie jest uzasadnieniem dla mechanizmu głosowania stosowanego przez Ethereum, gdzie wymagana jest większość $^2/_3$ głosów do zatwierdzenia bloku przedstawionego przez wyróżnionego uczestnika wybieranego w kontrolowalny, pseudolosowy sposób.

PoUW (Proof-of-Useful-Work). Zasadniczą wadą PoW jest fakt, iż kosztowne obliczenia wykonywane przez uczestników protokołu są bezużyteczne poza samym faktem wyłonienia zwycięzcy. Idea PoUW polega na tym, że obliczenia wykonywane w trakcie ubiegania się o prawo do wydłużenia blockchaina mają być pożyteczne dla całkiem innych celów. W sytuacji takiej koszty operacji rozkładają się na blockchain oraz na zlecającego dane zadanie obliczeniowe.

Atrakcyjna idea PoUW nie doczekała się dotychczas realizacji rynkowej o istotnym znaczeniu. Fundamentalne problemy pojawiają się w trakcie konkretnej realizacji tej koncepcji. Wybór zadania obliczeniowego jest rzeczą dosyć delikatną: należy ustrzec się sytuacji, w której zlecający zadanie formułuje je w taki sposób, że zna lub może łatwo poznać rozwiązanie problemu gwarantujące zwycięstwo w ubieganiu się o prawo do rozszerzania blockchaina. Rozwiązania odporne na tego typu

manipulacje idą często w kierunku poszukiwania rozwiązań opartych na problemach matematycznych odpornych na tego typu manipulacje. Prowadzi to jednak częstokroć do sytuacji, w której użyteczność obliczeń jest iluzoryczna – rozwiązywanie (ciekawych) zagadek matematycznych nie ma istotnej przewagi ekonomicznej nad klasycznym protokołem PoW używanym w przypadku Bitcoina.

Pewne nadzieje na przełamanie opisanych trudności można wiązać z rozwiązaniami zaproponowanymi w lecie 2022 roku (Fitzi, 2022). W proponowanym modelu zadanie obliczeniowe to instancja problemu SAT – problemu trudnego obliczeniowo, za pomocą którego stosunkowo łatwo można modelować wiele innych problemów obliczeniowych. W praktyce, mimo złożoności problemu SAT, skuteczne bywają algorytmy heurystyczne pozwalające na poszukiwania dobrych rozwiązań za pomocą błądzenia w przestrzeni rozwiązań. W opisywanym scenariuszu uczestnicy ubiegający się o prawo do przedłużenia łańcucha blockchaina poszukiwaliby rozwiązania dla instancji problemu SAT. Po pierwsze, autor tego zadania pokrywałby koszty obliczeń. Po drugie, sposób poszukiwania obliczeń – błądzenie losowe – odbywałoby się w sposób kontrolowany przez wspólny ciąg losowy. Tym samym każdy uczestnik byłby zmuszony do realizacji deterministycznej ścieżki poszukiwań. W szczególności nie daje to możliwości użycia dobrego rozwiązania z góry znanego przez autora zadania, w sytuacji gdy autorowi nie chodzi o rozwiązanie problemu, a o przejęcie kontroli nad wpisami w blockchainie.

5.2 Skalowalność rozwiązań i perspektywy stosowania dla masowych transakcji

Omawiane dotychczas rozwiązania miały na celu z jednej strony dopuścić nieograniczoną możliwość uczestnictwa w administrowaniu blockchainem, zaś z drugiej strony unieszkodliwić tak zwane *Sybil attack* – wykorzystanie wielu fikcyjnych tożsamości przez tego samego uczestnika. Rozwiązania tego problemu to procedury, w których prawdopodobieństwo zwycięstwa jest proporcjonalne do zaangażowanych zasobów.

Cele te są osiągane przez przedstawione mechanizmy jedynie częściowo. Pierwszy problem to olbrzymi koszt utrzymywania kryptowalut w sensie wydatków na zasoby obliczeniowe, w tym w szczególności energii elektrycznej oraz zużycia sprzętu komputerowego. O ile PoW opierać się miałby na funkcjach haszujących, to niewykorzystanie niestandardowych, niezbyt intensywnie przebadanych konstrukcji niosłoby za sobą ryzyko skutecznego ataku. Z kolei standardowe konstrukcje, rekomendowane przez NIST były zoptymalizowane pod kątem użycia na różnych platformach (patrz [NIST, 2012, str 38]). Tym samym nie nadają się do realizacji koncepcji użytej na przykład przez Proof-of-Space. Pewne nadzieje można by wiązać ze zmniejszaniem konsumpcji energii przez sprzęt obliczeniowy liczony jako koszt energii na operację (koncepcja „green computing"). Jednak postęp w tym obszarze nie może przynieść oszczędności o rzędy wielkości.

Szacunki energii elektrycznej zużytej dla funkcjonowania Bitcoina dostępne są pod adresem https://ccaf.io/cbeci/index (Cambridge Centre for Alternative Finance). Przykładowo 107 TWh podane jako szacunkowa wartość za 2022 rok należałoby porównać z rocznym zużyciem Polski (174 TWh). Zaskakująco, w dobie niepewności na rynku produkcji energii elektrycznej, mimo raportów renomowanych instytucji (Coroamă, 2021), dotychczasowe środki oszczędnościowe właściwie nie dotykały konsumpcji energii przez Bitcoin, koncentrując się na działaniach symbolicznych, takich jak na przykład nieoświetlanie pomników (reguły obowiązujące w Niemczech od września 2022 roku) czy obniżanie temperatury w pomieszczeniach biurowych w sektorze publicznym.

Kontekst kosztu PoW należy rozważyć w kontekście możliwych obszarów zastosowania w obrocie finansowym. O ile system taki miałby mieć realne znaczenie w obrocie (poza oczywistymi zastosowaniami, takimi jak omijanie regulacji AML, wymuszenia ransomware, omijanie sankcji czy ucieczka kapitału), liczba transakcji powinna wzrosnąć o rząd wielkości. Ponieważ wzrost produkcji energii elektrycznej w takiej skali jest nierealny, jedyną drogą musiałaby być przebudowa architektury systemu w kontekście większej przepustowości bez podnoszenia kosztu obliczeniowego.

Piętą Achillesową systemów kryptowalutowych jest tzw. „atak 51%". O ile w przypadku dużego systemu kryptowalutowego rola pojedynczego uczestnika w procesie PoW jest bardzo ograniczona, zasady optymalizacji finansowej skłaniają do łączenia się w tzw. farmy, gdzie uczestnicy dzielą się zyskiem z „kopania kryptowalut", stabilizując zysk z punktu widzenia jednostkowego uczestnika i minimalizując

ryzyko finansowe. W tej sytuacji naturalnym procesem jest zjawisko tworzenia się koalicji farm obejmujących coraz większy fragment rynku. W momencie, gdy koalicja obejmie więcej niż połowę mocy obliczeniowej, będzie w stanie przejąć całkowitą kontrolę nad rozszerzaniem blockchaina. Powodem jest mechanizm wyboru obowiązującego blockchaina: w przypadku rozdzielenia się (tzw. *fork*) jako prawidłowa uważana jest dłuższa gałąź. Koalicja „51%" w dłuższym okresie czasu zawsze może zdobyć przewagę nad resztą uczestników i unieważnić w tensposób alternatywną gałąź blockchaina.

„Atak 51%" dotyczy nie tylko systemów opartych na PoW, ale i PoS, jak przyznaje to strona zarządzająca Ethereum twierdząc jedynie, iż niebezpieczeństwo jest mniejsze:

„W modelu proof-of-stake zagrożenie atakiem 51% wciąż istnieje, lecz jest jeszcze bardziej ryzykowne dla napastników. Aby przeprowadzić taki atak, potrzebujesz kontroli nad co najmniej 51% zastawionych ETH. To nie tylko mnóstwo pieniędzy, ale prawdopodobnie spowodowałoby spadek wartości ETH. Motywacja do zniszczenia wartości waluty jest bardzo mała, jeżeli masz w tej walucie większościowy udział. Motywacja, aby utrzymać sieć bezpieczną i w dobrym stanie, jest mocniejsza".

Argument ten nie jest przekonywujący, bo sposobem na osiągnięcie zysku jest nie wzrost wartości kryptowaluty, ale wahania kursu, na które ma się istotny wpływ.

Rozwiązania alternatywne. Sytuacja może zmienić się radykalnie, o ile zbudowany zostanie w Europie system cyfrowej tożsamości wraz z powszechną implementacją pieczęci elektronicznej przypisanej do osób fizycznych i prawnych, a będącej deterministycznym podpisem cyfrowym (takim jak na przykład EdDSA). W sytuacji tej skomplikowane i kosztowne metody osiągania konsensusu opisane powyżej można zastąpić prostymi metodami: prawo do rozszerzenia blockchaina o nowe bloki otrzymywałby ten uczestnik, który przedstawiłby podpis pod referencyjnym ciągiem bitów wyznaczonym dla tego momentu, będący najmniejszą liczbą w reprezentacji binarnej. Rozwiązanie takie jest pośrednie pomiędzy publicznym a prywatnym blockchainem, jednak w przypadku wdrożenia cyfrowej tożsamości dodatkowy koszt byłby minimalny. Rozwiązanie takie jest technicznie możliwe nawet przy zachowaniu prywatności uczestników tego procesu (Hanzlik 2016).

5.3 Możliwości wprowadzenia ograniczeń/zakazu obrotu kryptowalutami

Sytuacja na europejskim rynku kryptowalut może drastycznie zmienić się pod wpływem dwóch projektowanych rozporządzeń (UE1, 2023) oraz (UE2, 2023). Pierwszym niezwykle istotnym czynnikiem jest wspomniany już art. 58 z (UE1, 2023), którego postanowienia ze względu na ich wagę warto przytoczyć bezpośrednio:

„1. Credit institutions, financial institutions and crypto-asset service providers shall be prohibited from keeping anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes, anonymity-enhancing coins or anonymous crypto-asset wallets as well as any account otherwise allowing for the anonymisation of the customer account holder.

Owners and beneficiaries of existing anonymous accounts, anonymous passbooks, anonymous safe-deposit boxes or crypto-asset wallets shall be subject to customer due diligence measures before those accounts, passbooks, deposit boxes or crypto-asset wallets are used in any way".

Regulacja ta w istocie zakazuje anonimowego obrotu kryptowalutami, istniejące obecnie instrumenty będą musiały zostać poddane deanonimizacji przed ich użyciem. Trudno bowiem mówić o akceptacji procesu jako „*due dilligence measure*" w kontekście projektowanego rozporządzenia, o ile nieznani są uczestnicy transakcji. Temat ten jest podejmowany również w omawianym wcześniej artykule 31a.

Deanonimizacja to proces, który wymagał będzie przebudowy systemów kryptowalut. Nie jest jasne jak zareagują państwa trzecie na projektowane regulacje. O ile dopuszczą istnienie kryptowalut w dotychczasowej anonimowej formie, to posiadacze kryptowalut w Unii Europejskiej znajdą się w trudnej sytuacji. Transakcje wykonywane przez tych uczestników w Europie podlegać będą prawu europejskiemu, tym samym usługodawca z państw trzecich uczestniczący w nich jako usługodawca powinien realizować obowiązki narzucone prawem europejskim. Oznacza to między innymi obowiązek uzyskania zezwolenia na działalność.

W tej sytuacji możliwe jest rozbicie rynku kryptowalut na odrębne ekosystemy. Możliwe jest powstanie w Europie podziemnego ekosystemu kryptowalut w dotychczasowym kształcie technicznym. Po-

wstać może sytuacja analogiczna do darknetu. Zapewne w niektórych przypadkach będziemy mieli do czynienia z „turystyką kryptowalutową" – aby dokonać transakcji, posiadacz kryptoaktywów będzie podróżował do kraju nie objętego restrykcjami europejskimi. Celem takich podróży mogą stać się miejsca na terenie geograficznym Europy nie podlegające rygorom prawa unijnego.

Projektowane rozporządzenie (UE2, 2023) zmierza do fundamentalnych zmian na rynku w UE, ustanawiając bardzo ostre reguły świadczenia usług w zakresie kryptoaktywów. Działalność taka będzie możliwa jedynie na podstawie zezwolenia. Podmioty świadczące takie usługi będą zobowiązane do przestrzegania wielu zasad mających na celu zagwarantowanie stabilności obrotu kryptowalutowego i interesów uczestników rynku. W istocie projektowane zmiany przekształcają anarchiczny rynek kryptowalutowy istniejący obecnie we fragment rynku finansowego oparty na odpowiedzialności i rozliczalności działań, transparentności wobec klientów oraz nadzorze państwowym.

Należy jednak podkreślić, że katalog usług w zakresie kryptoaktywów jest zamknięty i nie obejmuje operacji kolektywnego zarządzania blockchainem przez uczestników obrotu. Tym samym dostrzeżono, że rozproszone mechanizmy blockchaina są raczej zabezpieczeniem przed nieuczciwym obrotem niż obszarem zagrożeń. Nie zmienia to faktu, iż czynniki ekonomiczne wymuszą pragmatyczną realizację takiego rozproszonego rejestru ograniczając zarówno konsumpcję energii, jak i uodporniając na atak „51%".

6. Smart contracts

6.1 Smart contracts – mechanizm działania

Smart contracts (SC – inteligentne kontrakty) to działające w środowisku łańcucha bloków, automatycznie uruchamiane programy komputerowe. Powstają przy użyciu typowych języków programowania, takich jak C++, C# czy Java, a także w dedykowanych językach, takich jak wspierane przez platformę Ethereum Solidity i Vyper. Ideą kontraktów jest realizacja operacji typu „jeśli zaszedł warunek, to wykonaj akcję", przy czym warunkiem było pojawienie się określonej transakcji w łańcuchu bloków a akcją – stworzenie nowej transakcji. Programy te mogą współpracować ze sobą i tworzyć rozproszony system komunikacji i realizacji funkcjonalności, który to koncept funkcjonuje obecnie pod nazwą *Distributed Applications – DApps*. Uruchomienie kontraktu realizowane jest tak, jak inne transakcje w łańcuchu bloków, za pomocą podpisu, co zapewnia niezaprzeczalność podjęcia kontraktu przez stronę. Ciekawym zagadnieniem jest też to, że kontrakty operują jedynie w zakresie łańcucha bloków, w którym je uruchomiono, tj. nie mają dostępu do danych zewnętrznych, na przykład notowań walut, wyników wyścigów itp. Aby jednak umożliwić kontraktom działanie w odniesieniu do takich informacji, tworzone są tzw. kontrakty-wyrocznie (ang. *oracle contracts*), których zadaniem jest właśnie umieszczanie w łańcuchu bloków konkretnych danych zewnętrznych. Za jakość tych danych odpowiada (a raczej: ręczy) twórca takiej wyroczni, a zaufanie do tego źródła budowane jest na zasadzie zaufania między przedsiębiorcą a klientem (Kosinski, 2023).

Cykl życia kontraktu różni się od typowego programu. Kod źródłowy kontraktu jest tworzony przez programistę w języku wyższego poziomu i kompilowany do kodu bajtowego (ang. *bytecode*). W tej postaci przekazywany jest do łańcucha bloków jako transakcja bez adresata. Tak jak każda transakcja, kontrakt otrzymuje swój adres umożliwiający interakcję z nim innych użytkowników oraz kontraktów. Po przesłaniu (ang. *deployment*) bajtkodu struktura programu-kontraktu nie może zostać zmieniona[74], a sam kontrakt nie może zostać wycofany z łańcucha bloków. Istnieje możliwość pośredniej weryfikacji, czy dany bajtkod odpowiada deklarowanemu kodowi źródłowemu, poprzez samodzielną kompilację do bajtkodu i porównanie wartości hash otrzymanego kodu z tym opublikowanym. Funkcjonalność taką dostarczają platformy m.in. Etherscan czy Tenderly.

Niewątpliwie największym problemem technicznym kontraktów jest zapewnienie poprawności ich wykonania. Jako że są to programy uruchamiane automatycznie, a wynik ich działania trafia do łańcucha bloków w formie transakcji – błędne działanie (zamierzone lub nie) – jest praktycznie nieodwracalne. Klasycznym przykładem jest tutaj *casus* DAO z 2016 roku (Falcon 2017). Kontrakt o otwartym kodzie został uruchomiony w łańcuchu bloków, inicjalizując akcję crowdfundingową, która zebrała ok. 150 mln dolarów. Błąd w implementacji kontraktu pozwolił jednak na wykorzystanie podatności *reentrancy*, umożliwiającej wielokrotne wycofanie przez atakujących środków z konta DAO. Należy więc podkreślić, że kontrakty są niczym innym, jak programami komputerowymi, których skutek działania może dotykać szerokiej populacji użytkowników i mieć nieodwołalny wpływ na obiekty o znacznej wartości. Na tym poziomie można go porównywać do systemów informatycznych banków, jednak procedury tworzenia programów z obu tych grup są granicznie odmienne.

Wśród innych narzędzi zorientowanych na podniesienie bezpieczeństwa tworzonych kontraktów można wskazać projekt Slither[75] – zestaw narzędzi do statycznej analizy podatności w kodzie dla języka Solidity. Dużą rolę odgrywa też społeczna presja i kontrola utrzymania czystości i poprawności kodu kontraktów. Publikowane są listy kontaktowe[76], umożliwiające zgłaszanie nieprawidłowości wykrytych w opublikowanych kodach kontraktów. Istnieją też bazy „złych praktyk" programistycznych, na przykład Not-so-smart Contracts[77] – mające na celu propagowanie informacji i podniesienie świadomości deweloperów kontraktów.

Problematyką jakości kodu i bezpieczeństwa kontraktów interesuje się też społeczność akademicka. Opracowanie (Chen i in. 2021) dotyczy problemu utrzymywania kodu kontraktów już aktywnych w łańcuchu bloków. W (Wang i in. 2021) dostępny jest przegląd literatury z zakresu bezpieczeństwa środowiska wykonywania kontraktów i wykorzysty-

74 W rzeczywistości istnieją techniki umożliwiające zmianę kodu uruchamianego przez niezmienniczy kod samego kontraktu, zob. https://ethereum.org/en/developers/docs/smart-contracts/upgrading/

75 https://github.com/crytic/slither

76 Block Chain Security Contacts: https://github.com/crytic/blockchain-security-contacts

77 https://github.com/crytic/not-so-smart-contracts/

wania podatności ich warstwy logicznej. (Sayeed i in. 2020) przedstawiają klasyfikację ataków na kod kontraktów. Niektóre z nich wykorzystują problemy znane z „klasycznego" kodu (na przykład *reentrancy attack*, *overflow attack*), a inne są rezultatem specyfiki środowiska wykonania kontraktu (zależność kolejności transakcji, zależność znaczników czasu itp.). Jest to zatem zupełnie nowa klasa podatności programów, znacząco poszerzająca problematykę formalnej analizy poprawności programów o wielowątkowe, ściśle rozproszone obliczenia. W (Sharma i in. 2021) można znaleźć szerokie studium zarówno obszarów zastosowań kontraktów, jak i problemów związanych z ich bezpieczeństwem, a także szeroką listę innych publikacji poświęconych tym konkretnym zagadnieniom.

Struktura kontraktów dostępnych w łańcuchu bloków została dokładnie zbadana w pracy (Gustavo i in. 2020). Niestety brak jest podobnych analiz z późniejszego okresu, ale pewne wnioski z cytowanej pracy są dość interesujące i zdają się być uniwersalne. Badacze zauważyli, że spośród wszystkich dostępnych kontraktów niecałe 1% otrzymało ok. 80% wszystkich transakcji adresowanych do kontraktów, z czego zaledwie 8% można dalej uznać za aktywnie wykorzystywane kontrakty. Jeśli chodzi o odsetek zweryfikowanych dostępnych kontraktów to wynosił on zaledwie 2,2%, natomiast ok. 72% wszelkich transakcji adresowanych jest do kontraktów zweryfikowanych. Kreśli to obraz bardzo małej liczby rzeczywiście wykorzystywanych kontraktów o relatywnie dobrej przejrzystości kodu, które odpowiadają za przeważającą liczbę realizowanych transakcji.

Dalsze wnioski z (Gustavo i in. 2020) dotyczą przedmiotu działania i struktury kodu najaktywniejszych kontraktów. Otóż ok. 73% z nich to kontrakty zarządzające tokenami[78] o łącznej kapitalizacji rynkowej 12,7 mld dolarów (dane z 2020 r.), 41% aktywnych kontraktów to proste kontrakty działające na tokenach. Najaktywniejsze zweryfikowane kontrakty wyróżniają się na tle innych zweryfikowanych nieco większym stopniem złożoności kodu (w znaczeniu wykorzystywania innych kontraktów do realizacji swoich funkcjonalności), jednak jest to często niewielki, dobrze skomentowany kod źródłowy. Niemniej jednak badacze stwierdzili stały spadek proporcji ilości komentarzy do kodu na przestrzeni lat. Prowadzi to do wniosków, że pomimo dużej elastyczności formuły, kontrakty są przede wszystkim używane jako mechanizm wymiany dóbr (tokenów). Ich prosta struktura logiczna może być podyktowana chęcią zwiększenia ich dostępności dla podmiotów i osób o ograniczonej wiedzy na ich temat. Rysuje to jednak również inny obraz: podmiotów posiadających odpowiednią wiedzę i środki, by w takim środowisku móc wykorzystywać w znacznie większym stopniu kontrakty o bardzo złożonej strukturze. W naturalny sposób tego rodzaju przypadki będą nieliczne, a więc na tle pospolitego użycia, o którym piszą autorzy analizy, mogą pozostać niezauważone lub pomijalne.

6.2 Szanse demonopolizacji rynku opanowanego przez platformy sprzedażowe/pośredniczące oraz możliwości sektora finansowego rozwoju usług opartych na smart contracts

Użycie kontraktów smart posiada wiele cech pożądanych przez uczestników rynków finansowych, handlowych i innych, gdzie obrót dobrami polega w swojej istocie na przekazywaniu informacji (o stanie posiadania, zaistnieniu pewnych faktów, itp.), raczej niż fizycznych przedmiotów. W szczególności są to:

- natychmiastowość działania: w momencie realizacji kontraktu powiązane z nim transakcje stają się dostępne w łańcuchu bloków niemal od razu;
- nieodwołalność i niezaprzeczalność: wejście strony w kontrakt nie może być cofnięte, a wyniki zrealizowanych kontraktów są praktycznie niemożliwe do zmiany po ich opublikowaniu w łańcuchu;
- dostęp do historii: podmioty mogą pozostawiać ślad swoich transakcji, budując tym swoją reputację.

W efekcie podmioty na rynku mogą budować i weryfikować wzajemne zaufanie do siebie i przeprowadzić transakcje o natychmiastowych, nieodwołalnych skutkach.

W dwóch dużych pracach przeglądowych dotyczących kontraktów smart w łańcuchach bloków

78 Tokenem nazywa się wirtualny obiekt, któremu przypisuje się określoną wartość (na przykład jednego dolara), charakterystykę (na przykład punkt popularności osoby) lub prawo własności rzeczywistego przedmiotu. Dokumentacja tokenów w sieci Ethereum jest dostępna jako EIP-20: https://eips.ethereum.org/EIPS/eip-20

(Rouhani 2019) i (Sharma i in. 2023) badacze zidentyfikowali szereg obszarów, dla których istnieją badania w zakresie stosowalności kontraktów. W **sektorze ubezpieczeniowym** umowy mogą przyjmować postać jasno określonych kontraktów, realizowanych automatycznie po zaistnieniu zdarzeń ubezpieczeniowych, a łańcuch bloków ma zapewniać następstwo czasowe, co może przeciwdziałać praniu brudnych pieniędzy. To zapewnienie kolejności zdarzeń wydaje się być naturalnym wsparciem **łańcucha dostaw**, gdzie wszyscy uczestnicy realizują odpowiednio skonstruowany kontrakt, umożliwiający obserwację stanu dostawy, potwierdzenie pochodzenia i zarządzanie jakością. Postulowane zastosowania łańcucha bloków na **rynku zdrowia** to przede wszystkim mechanizmy utrzymywania danych medycznych pacjenta w formie zapewniającej poufność, niezaprzeczalność i kontrolę pacjenta nad udostępnianiem danych w razie potrzeby (Novikov i in. 2018). Z pokrewnych obszarów należy też wyliczyć **zarządzanie tożsamością** (w tym systemy reputacyjne i systemy prezentowania uprawnień), **zarządzanie danymi** czy zastosowanie w przetwarzaniu Internetu rzeczy (IoT).

Wszystkie te zastosowania mają ważną wspólną cechę, która jest czynnikiem dającym potencjał udanego wdrożenia usług przez duże podmioty o rozpoznawalnej marce w świecie rzeczywistym. Chodzi tu o oczywistą potrzebę wykorzystywania przez kontrakty smart danych spoza łańcucha bloków. A zatem, jak wspomniano w poprzedniej sekcji, istnieje potrzeba zaufanych źródeł informacji (kontraktów-wyroczni), które dostarczałyby danych do przetwarzania kontraktów. Będą to na przykład rzeczoznawcy wyceniający szkody ubezpieczeniowe, audytorzy certyfikujący pochodzenie i przetwarzanie towarów, placówki medyczne generujące dane medyczne pacjentów itd. A zatem wytworzenie ekosystemu usług opartych na łańcuchu bloków i kontraktach smart nie polega wyłącznie na powstawaniu samych usługodawców – potrzebny jest też ekosystem tworzony przez podmioty realizujące audyt i będące „źródłem jakości" – a zatem też zaufania. Techniczna propagacja zaufania między stronami usługi jest realizowana przez łańcuch bloków i logikę kontraktów jako cecha wbudowana w samo rozwiązanie.

Prawdopodobnie największym obszarem wykorzystania kontraktów smart jest sprzedaż detaliczna. Jak zaznaczono wcześniej, kontrakty przetwarzające tokeny stanowią wyraźną większość w łańcuchu bloków. W momencie pisania tego raportu Amazon podał[79], że rozpoczyna sprzedaż tokenów NFT (wiążących posiadanie dobra wirtualnego z rzeczywistym, które jest dostarczane klientom), czyli de facto dając możliwość kupna przedmiotów kolekcjonerskich za kryptowalutę. Co więcej, firma będzie dawać możliwość zakupu żetonów w ramach konta Amazon, bez wymogu posiadania portfela kryptowalutowego. Wśród głównych szans Amazona w realizacji tego przedsięwzięcia wymieniana jest jego pozycja na rynku sprzedażowym, rozpoznawalność marki i zaplecze informatyczne. To wydaje się dobrze podsumowywać możliwości rozwojowe z wykorzystaniem tej technologii: obecni duzi i rozpoznawalni gracze mają znaczną przewagę, ale małe podmioty mogą wykorzystać te narzędzia do budowania swojej pozycji zaufanego gracza. Warunkiem jest nieskazitelna historia działalności – weryfikowalnej i niezaprzeczalnej. Rozwiązanie kwestii technicznych związanych z bezpieczeństwem kontraktów opisanych w poprzednim podrozdziale, a także uczciwe podejście do prowadzenia biznesu przez podmioty – to dwa filary tej technologii, opartej na zaufaniu tworzonemu w ujęciu cyfrowym, a realizowanym w rzeczywistości.

79 Za: https://artplugged.co.uk/amazon-to-launch-nft-marketplace-in-april/

PROGRAM ANALITYCZ BADAWCZY

Wnioski i podsumowanie

Rynek kryptowalut jest niezwykle zmienny, co powoduje, że duża część użytkowników działa na nim w celach spekulacyjnych. Rynek ten charakteryzuje się bardzo dużym ryzykiem, znacznie większym niż na przykład inwestycje w waluty fiat lub akcje.

Równocześnie rynek kryptowalut, pomimo dużej zmienności, rozwija się bardzo dynamicznie. Z roku na rok rośnie liczba dostępnych kryptowalut i tokenów, platform pośredniczących w wymianie kryptowalut oraz oferowanych produktów. Duże firmy z sektora finansowego, na przykład Visa i Mastercard, współpracują z platformami wymiany kryptowalut i producentami portfeli kryptowalut.

Rynek kryptowalut nie jest wystarczająco uregulowany, przez co jego uczestnicy są narażeni na utratę zainwestowanych środków. Firmy działające na tym rynku, szczególnie platformy wymiany kryptowalut, nie posiadają funduszy gwarancyjnych. Pojawiające się propozycje w Unii Europejskiej mogą znacząco zmienić sytuację.

Wiele produktów i usług oferowanych na rynku kryptowalut jest wzorowanych na produktach i usługach sektora bankowego, jednak w formie zdecentralizowanej, tj. z pominięciem zaufanej organizacji pośredniczącej. Produkty tego typu mogą dawać użytkownikom złudne poczucie bezpieczeństwa poprzez skojarzenie ich ze znanymi produktami bankowymi, jednak są one podatne na wszystkie konsekwencje wahań kursów kryptowalut.

Ewentualne zaoferowanie przez banki produktów lub usług opartych na kryptowalutach (zakładając wprowadzenie regulacji prawnych, które to umożliwią) wiązałoby się z przeniesieniem zaufania do banków na kryptowaluty. W przypadku, gdyby klienci utracili ulokowane w ten sposób środki (na przykład na skutek dużych wahań kursów), mogłoby to spowodować spadek zaufania do całego sektora bankowego.

Technologia blockchain jest rozwijana i wdrażana przez banki centralne na całym świecie, w celu usprawnienia procesów wykonywania przelewów międzybankowych. Takie wdrożenie/badania są prowadzone przez większość banków centralnych na świecie, a 11 krajów wprowadziło już CBDC.

Kryptowaluty dają pewne możliwości skutecznego omijania kontroli w zakresie AML, nawet gdy uczestnicy obrotu są poddawani szczegółowej kontroli. Mogą oni wykazać, że transakcje są budowane w sposób zgodny ze specyfikacją, a zarazem powodujące niekontrolowany przepływ środków.

Zasadniczym niebezpieczeństwem z punktu widzenia uczestników obrotu jest ochrona kluczy autoryzujących transakcje. Żadna z technik nie daje gwarancji odpowiadających poziomowi ryzyka w przypadku obrotów o dużej wartości.

Postęp w zakresie kryptografii kwantowej może doprowadzić do znaczących perturbacji na rynku kryptowalut, jednak obecna sytuacja nie skłania do szybkich ruchów w tym zakresie.

Pod względem technicznym stoimy prawdopodobnie przed fundamentalną przebudową rynku, zmierzającą do eliminacji anonimowości. Realizacja po stronie technicznej jest sporym wyzwaniem technicznym.

Projektowane regulacje europejskie zmierzają w kierunku budowy rynku, na którym sektor bankowy będzie miał równiejsze warunki funkcjonowania. Należy oczekiwać wyeliminowania szeregu patologii wynikających z całkowitego braku kontroli i wyzyskiwania nieświadomości konsumentów.

Istotną niszą dla kryptowalut w przyszłości mogą być smart contracts. Największego wzrostu można upatrywać w tych obszarach, gdzie obecnie zaufana trzecia strona (na przykład platforma sprzedażowa) jest gwarantem prawidłowej realizacji wzajemnych zobowiązań.

PROGRAM ANALITYCZ BADAWCZY

Bibliografia

- Auer, R., Banka, H., Boakye-Adjei, N. Y., Faragallah, A., Frost, J., Natarajan, H., Prenio, J. (2022). *Central bank digital currencies: A new tool in the financial inclusion toolkit?* (Nr 41; FSI Insights, s. 1–39). BIS. https://www.bis.org/fsi/publ/insights41.htm

- Auer, R., Cornelli, G., Doer, S., Frost, J., Gambacorta, L. (2022). *Crypto trading and Bitcoin prices: Evidence from a new database of retail adoption* (Nr 1049; BIS Working Papers, s. 1–28). BIS. https://www.bis.org/publ/work1049.htm

- Auer, R., Farag, M., Lewrick, U., Orazem, L., Zoss, M. (2022). *Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies* (Nr 1013; BIS Working Papers, s. 1–25). BIS. https://www.bis.org/publ/work1013.htm

- Auer, R., Haene, P., Holden, H. (2021). *Multi-CBDC arrangements and the future of cross-border payments* (Nr 115; BIS Papers, s. 1–23). BIS. https://www.bis.org/publ/bppdf/bispap115.htm

- Auer, R., & Tercero-Lucas, D. (2021). *Distrust or speculation? The socioeconomic drivers of U.S. cryptocurrency investments* (Nr 951; BIS Working Papers, s. 1–52). BIS. https://www.bis.org/publ/work951.htm

- Du, B., He, D., Luo, M., Peng, C., Feng, Q. (2022): *The Applications of Blockchain in the Covert Communication.* W: Wireless Communications and Mobile Computing vol. 2022: Emerging Technologies towards Improving Confidentiality and Privacy in Blockchain. https://doi.org/10.1155/2022/4618007

- Bank for International Settlements' Committee on Payments and Market Infrastructures, BIS Innovation Hub, International Monetary Fund (IMF), & World Bank. (2022). *Options for access to and interoperability of CBDCs for cross-border payments* (s. 1–61) [Joint report to the G20]. BIS. https://www.bis.org/publ/othp52.htm

- BBC.com. (2021, czerwiec 9). *Bitcoin: El Salvador makes cryptocurrency legal tender.* BBC, News. https://www.bbc.com/news/world-latin-america-57398274

- Bednarek, A., Independent Security Evaluators: *Ethercombing: Finding Secrets in Popular Places* [online, dostęp: 15.03.2023] https://www.ise.io/casestudies/ethercombing/

- Beekhuizen, C. (2021, maj 18). Ethereum's energy usage will soon decrease by ~99.95%. *Ethereum Foundation Blog*. https://blog.ethereum.org/2021/05/18/country-power-no-more

- Bellare, M., Paterson, K.G., Rogaway, P. (2014): *Security of Symmetric Encryption Against Mass Surveillance*. W: CRYPTO 2014. Lecture Notes in Computer Science, vol. 8616, s. 1–19. Springer. https://link.springer.com/chapter/10.1007/978-3-662-44371-2_1

- Berman, R., Fiat, A., Gomułkiewicz, M., Klonowski, M., Kutyłowski, M., Levinboim, T., Ta-Shma, A. (2015): *Provable Unlinkability Against Traffic Analysis with Low Message Overhead*. Journal of Cryptology. 28(3): s. 623-640. https://link.springer.com/article/10.1007/s00145-013-9171-8

- Berzati, A., Viera, A.C., Chartouni, M., Madec, S., Vergnaud, D., Vigilant, D. (2023): *A Practical Template Attack on CRYSTALS-Dilithium*. W: IACR Cryptology ePrint Archive 2023: vol. 50. https://eprint.iacr.org/2023/050

- Beullens, W. (2022): *Breaking Rainbow Takes a Weekend on a Laptop*. CRYPTO (2) 2022: s. 464–479. https://link.springer.com/chapter/10.1007/978-3-031-15979-4_16

- Biryukov, A., Feher, D., Vitto, G. (2019): *Privacy Aspects and Subliminal Channels in Zcash*. W: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. https://dl.acm.org/doi/10.1145/3319535.3345663

- BIS Innovation Hub Hong Kong Centre, Hong Kong Monetary Authority, Bank of Thailand, Digital Currency Institute of the People's Bank of China, & Central Bank of the United Arab Emirates. (2022). Project mBridge: *Connecting economies through CBDC* (s. 1–50) [Joint report]. BIS. https://www.bis.org/publ/othp59.htm

- Błaśkiewicz, P., Hanzlik, L., Kluczniak, K., Krzywiecki, Ł., Kutyłowski, M., Słowik, M., Wszoła, M. (2019): *Pseudonymous Signature Schemes*. W: Advances in Cyber Security 2019: s. 185-255. https://link.springer.com/chapter/10.1007/978-981-13-1483-4_8
- Błaśkiewicz, P., Kutyłowski, M. (2022): *Chaining Electronic Seals – An eIDAS Compliant Framework for Controlling SSCD*. ACIIDS (2) 2022: s. 714–732. https://link.springer.com/chapter/10.1007/978-3-031-21967-2_57
- BSI: *TR-03110 eIDAS Token Specification*, [online, dostęp: 13.03.2023] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/BSITR03110-eIDAS_Token_Specification.html
- Business Insider. (2022, listopad 15). Po upadku giełdy kryptowalut FTX zniknęły miliardy dolarów. Jak to się w ogóle stało? *Business Insider*. https://businessinsider.com.pl/gospodarka/upadek-ftx-zniknely-miliardy-dolarow-jak-to-sie-w-ogole-stalo/lbm48m0
- Carstens, A. (2023, luty 22). *Innovation and the future of the monetary system* [BIS speech]. Monetary Authority of Singapore, Singapore. https://www.bis.org/speeches/sp230222.htm
- Chainalysis. (2021). *The 2021 Geography of Cryptocurrency Report. Analysis of Geographic Trends in Cryptocurrency Adoption and Usage*. Chainalysis. https://markets.chainalysis.com/
- Chen, J., Xia, X., Lo, D., Grundy, J., Yang, X. (2021): *Maintenance-related concerns for post-deployed Ethereum smart contract development: issues, techniques, and future challenges* W: Empirical Software Engineering vol. 26, No. 117. https://link.springer.com/article/10.1007/s10664-021-10018-0
- Coroamă, V. (2021): *Blockchain energy consumption An exploratory study*. Federal Department of the Environment, Transport, Energy and Communications DETEC Swiss Federal Office of Energy SFOE Energy Research and Cleantech Division [online, dostęp: 13.03.2023] https://ccaf.io/cbeci/index
- Cui, T., Wang, W., Wang, M. (2020): *Distinguisher on full-round compression function of GOST*. W: Information Processing Letters, vol. 156. https://www.sciencedirect.com/science/article/abs/pii/S0020019019301851?via%3Dihub
- Cunliffe, J. (2023, luty 7). *The digital pound* [Central bank speech]. UK Finance, London. https://www.bis.org/review/r230208a.htm
- Dabrowski, A., Pfeffer, K., Reichel, M., Mai, A., Weippl, E.R., Franz, M. (2021): *Better Keep Cash in Your Boots - Hardware Wallets are the New Single Point of Failure*. W: DeFi '21: Proceedings of the 2021 ACM CCS Workshop on Decentralized Finance and Security. November 2021, s. 1–8. https://dl.acm.org/doi/10.1145/3464967.3488588
- De Vries, A. (2023). Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. Patterns, 4(1), 100633. https://doi.org/10.1016/j.patter.2022.100633
- eIDAS: *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*, [online, dostęp: 13.03.2023] (2014) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32014R0910
- S. Falkon (2017): *The Story of the DAO—Its History and Consequences* [online, dostęp 15.03.2023]: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee
- Fitzi, M., Kiayias, A., Panagiotakos, G., Russell, A. (2022): *Ofelimos: Combinatorial Optimization via Proof-of-Useful-Work - A Provably Secure Blockchain Protocol*. CRYPTO (2) 2022: s. 339–369. https://eprint.iacr.org/2021/1379
- Gemini. (2021a). *Gemini State of UK Crypto Report 2021* [Market report]. Gemini. https://www.gemini.com/state-of-crypto
- Gemini. (2021b). *Gemini State of US Crypto Report 2021* [Market report]. Gemini. https://www.gemini.com/state-of-crypto

58

- Gemini. (2021c). *Gemini The State of Crypto in Singapore Report 2021* [Market report]. Gemini. https://www.gemini.com/state-of-crypto
- Gemini. (2022). *2022 Global State of Crypto* [Market report]. Gemini. https://www.gemini.com/state-of-crypto
- Golubova, A. (2023, luty 13). IMF warns El Salvador: Government should reconsider plans to increase Bitcoin exposure. *kitco*, News. https://www.kitco.com/news/2023-02-13/IMF-warns-El-Salvador-government-should-reconsider-plans-to-increase-Bitcoin-exposure.html
- Gustavo A. Oliva, Ahmed E. Hassan i Zhen Ming (Jack) Jiang (2020): *An exploratory study of smart contracts in the Ethereum blockchain platform. W: Empirical Software Engineering* vol. 25, s. 1864–1904. https://link.springer.com/article/10.1007/s10664-019-09796-5
- Hanzlik, L., Kluczniak, K., Kutyłowski, M., Dolev, S. (2016): *Local Self-Organization with Strong Privacy Protection*. Trustcom/BigDataSE/ISPA (2016): s. 775-782. https://ieeexplore.ieee.org/document/7847021
- Hetler, A. (2023, luty 1). FTX scam explained: Everything you need to know. *TechTarget*. https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know
- Hon, H., Wang, K., Bolger, M., Wu, W., & Zhou, J. (2022): *Crypto Market Sizing Report 2021 and 2022 Forecast* [Market report]. https://crypto.com/research/2021-crypto-market-sizing-report-2022-forecast
- Kilgallin, J., Vasco, R. (2019), *Factoring RSA Keys in the IoT Era* https://www.keyfactor.com/resources/factoring-rsa-keys-in-the-iot-era/
- Kiltz, E, & Neven, G. (2008): *Identity-Based Signatures*. W: Cryptology and Information Security Series on Identity-Based Cryptography (pp. 31–44). IOS Press. https://ebooks.iospress.nl/publication/27590
- Kosinski, John R. (2023): *Ethereum Oracle Contracts: Can We Trust the Oracle?* [online, dostęp: 15.03.2023] https://www.toptal.com/ethereum/oracle-contracts-tutorial-pt3
- Kraken Labs, *Kraken Identifies Critical Flaw in Trezor Hardware Wallets*, [online, dostęp: 15.03.2023] https://blog.kraken.com/post/3662/kraken-identifies-critical-flaw-in-trezor-hardware-wallets/
- Kubiak, P., Kutyłowski, M. (2023): *Threat of Anamorphic Channels in Monero Cryptocurrency*, w przygotowaniu
- Kutyłowski, M., Persiano, G., Phan, D.H., Yung, M., Zawada, M. (2023): *Anamorphic Signatures: Secrecy From a Dictator Who Only Permits Authentication*! złożone do druku
- Lee, S., Lee, J., Zhai, H., Tong, Y., Dalzell, A.,M., Kumar, A., Helms, P., Gray, J., Cui, Z-H., Liu, W., Kastoryano, M., Babbush, R., Preskill, J., Reichman, D.R., Campbell, E.T., Valeev, E.F, Lin, L., Chan, G.K-L. (2022): *Is there evidence for exponential quantum advantage in quantum chemistry?* [online, dostęp: 13.03.2023] https://arxiv.org/pdf/2208.02199.pdf
- Lenstra, A.K., Shamir, A. (2000): *Analysis and Optimization of the TWINKLE Factoring Device*. EUROCRYPT 2000: s. 35–52. https://link.springer.com/chapter/10.1007/3-540-45539-6_3
- Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and Decentralised Finance (DeFi)* (Nr 1061; BIS Working Papers, s. 1–79). BIS. https://www.bis.org/publ/work1061.htm
- Nakamoto, S. (2008). *Bitcoin: Elektroniczny System Pieniężny Typu Peer-to-Peer.* Bitcoin.org. https://bitcoin.org/en/bitcoin-paper
- Neapolitano, E., & Cheung, B. (2022, listopad 18): The FTX collapse, explained. *NBC News*. https://www.nbcnews.com/tech/crypto/sam-bankman-fried-crypto-ftx-collapse-explained-rcna57582
- NIST (2012), National Institute of Standards and Technology, USA: *NISTIR 7896, Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*. https://csrc.nist.gov/publications/detail/nistir/7896/final

- Novikov, S. P., Kazakov, O.D., Kulagina, N.A., Azarenko, N.Y. (2018): *Blockchain and Smart Contracts in a Decentralized Health Infrastructure*. W: 2018 IEEE International Conference „Quality Management, Transport and Information Security, Information Technologies". https://ieeexplore.ieee.org/document/8524970
- Persiano, G., Phan, D.H., Yung, M. (2022):
- *Anamorphic Encryption: Private Communication Against a Dictator*. EUROCRYPT (2) 2022: s 34–63, Lecture Notes in Computer Science, Springer. https://eprint.iacr.org/2022/639
- Phillips, D. (2021, styczeń 3): *Lost Bitcoin: 3.7 million Bitcoin are probably gone forever.* Decrypt. https://decrypt.co/37171/lost-bitcoin-3-7-million-bitcoin-are-probably-gone-forever
- Portal Digicomist. (2023). *Bitcoin Energy Consumption Index*. Digicomist. https://digiconomist.net/bitcoin-energy-consumption
- PwC. (2022): *PwC Global Crypto Regulation Report 2023. Towards global regulatory clarity* [Market report]. https://www.pwc.com/gx/en/about/new-ventures/global-crypto-regulation-report-2023.html
- PwC, Elwood, & CoinShares. (2022): *4th Annual Global Crypto Hedge Fund Report 2022* (Market report Nr 4). PwC. https://www.pwc.com/gx/en/financial-services/pdf/4th-annual-global-crypto-hedge-fund-report-june-2022.pdf
- RFC 6979: *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)* [online, dostęp: 13.03.2023] https://datatracker.ietf.org/doc/rfc6979/
- Riley, D. (2021, luty 23): IFinex agrees to pay $18.5M to settle New York Tether lawsuit. *siliconANGLE*. https://siliconangle.com/2021/02/23/ifinex-agrees-pay-18-5m-settle-new-york-tether-lawsuit/
- Robertson, H. (2022, luty 20). FTX's Sam Bankman-Fried explains how he built a $32 billion crypto exchange in 3 years after growing annoyed with „crappy" platforms – making him a multibillionaire at 29. *Markets Insider*. https://markets.businessinsider.com/news/currencies/sam-bankman-fried-ftx-crypto-exchange-valuation-billionaire-bitcoin-ethereum-2022-2
- Rouhani, S., Deters, R. (2019): *Security, Performance, and Applications of Smart Contracts: A Systematic Survey*. W IEEE Access, vol. 7. s. 50759–50779. https://ieeexplore.ieee.org/document/8689026
- Sayeed, S., Marco-Gisbert, H., Caira, T. (2020). *Smart Contract: Attacks and Protections*. W: IEEE Access, vol. 8, s. 24416-24427. https://ieeexplore.ieee.org/document/8976179
- Shamir, A., Tromer, E. (2003): *Factoring Large Number with the TWIRL Device*. CRYPTO 2003: s. 1–26. https://link.springer.com/chapter/10.1007/978-3-540-45146-4_1
- Sharma P., Jindal R. & Borah M.D. (2023): *A review of smart contract-based platforms, applications, and challenges*. W: Cluster Computing vol. 26, s. 395–421 (2023). https://link.springer.com/article/10.1007/s10586-021-03491-1
- Simmons, G.J. (1983): *The Prisoners' Problem and the Subliminal Channel*. CRYPTO 1983: s. 51–67, Plenum Press. (brak dostępu online)
- Smith, T. (2023, styczeń 5). FTX: An Overview of the Exchange and Its Collapse. *Investopedia*. https://www.investopedia.com/ftx-exchange-5200842
- Tether Limited Inc.,. (2022). *Tether: Fiat currencies on the Bitcoin blockchain.* Tether Limited Inc.,. https://tether.to/en/whitepaper/
- Tual, S. (2015, lipiec 15). Ethereum Launches. *Ethereum Foundation Blog*. https://blog.ethereum.org/2015/07/30/ethereum-launches

- UE1, *Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: Mandate for negotiations with the European Parliament.* [online, dostęp: 13.03.2023] https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf
- UE2, *Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937* [online, dostęp: 13.03.2023] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-CELEX%3A52020PC0593#
- Verbücheln, S. (2015): *How Perfect Offline Wallets Can Still Leak Bitcoin Private Keys*. W: MCIS 2015 Proceedings. https://arxiv.org/abs/1501.00447
- Wang, Z., Yu, H., Zhang, Z., Piao, J., Liu, J. (2020): *ECDSA weak randomness in Bitcoin*. Future Generation Computing Systems, vol. 102: s. 507–513. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17330030?via%3Dihub
- WEC, World Economic Forum, 31.1.2022: *What's behind China's cryptocurrency ban?* [online, dostęp: 13.03.2023] https://www.weforum.org/agenda/2022/01/what-s-behind-china-s-crypto-currency-ban
- Wijaya, D.A,, Liu, J.K., Steinfeld, R., Liu, D., Yuen, T.H. (2018): *Anonymity Reduction Attacks to Monero*. Inscrypt 2018: s. 86–100, W: Lecture Notes in Computer Science 11449, Springer. https://link.springer.com/chapter/10.1007/978-3-030-14234-6_5
- Young, A., Yung, M. (1996): *The dark side of „black-box" cryptography*, or: *Should we trust capstone*? W: CRYPTO'96, vol. 1109 of LNCS, pp 89–103. Springer, Aug. 1996. https://link.springer.com/chapter/10.1007/3-540-68697-5_8
- Young, A., Yung, M. (2004): *Malicious cryptography – exposing cryptovirology*. Wiley 2004, ISBN 978-0-7645-4975-5, I-XXIV, s. 1–392. https://www.wiley.com/en-us/Malicious+-Cryptography%3A+Exposing+Cryptovirology--p-9780764549755
- Wang Z., Jin, H., Dai, W., Raymond Choo, R. K-K., Zou, D. (2021): *Ethereum smart contract security research: survey and future research opportunities*. W: Frontiers of Computer Science vol. 15, No.: 152802. https://link.springer.com/article/10.1007/s11704-020-9284-9

PROGRAM
ANALITYCZNO
BADAWCZY

Raport przygotowany na zlecenie
Fundacji Warszawski Instytut Bankowości