DOI: 10.15611/2023.38.1.04

Rozdział 4

Zagrożenia bezpieczeństwa związane z kryptowalutami i technologią blockchain

Marcin Brol

Uniwersytet Ekonomiczny we Wrocławiu
e-mail: marcin.brol@ue.wroc.pl
ORCID: 0000-0003-2203-4036

Cytuj jako: Brol, M. (2023). Zagrożenia bezpieczeństwa związane z kryptowalutami i technologią blockchain. W: W. Michalczyk (red.), *Ku kryptofinansom? Poszukiwanie miejsca kryptowalut we współczesnych finansach międzynarodowych* (s. 97-110). Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Streszczenie: Bezpieczeństwo wymiany to ogół warunków sprzyjających zawarciu transakcji rynkowej. Dotyczy to przede wszystkim zaufania między uczestnikami wymiany oraz jej przejrzystości. Wraz z rozwojem technologii informatycznych zaistniała możliwość zbliżenia tych warunków do modelu idealnego. Kamieniem milowym okazał się rozwój sieci internetu i digitalizacja procesów gospodarczych. Kolejnym ważnym krokiem było wprowadzenie transakcji opartych na łańcuchach blokowych (*blockchain*). W niniejszym rozdziale omówiono zagadnienie bezpieczeństwa związane z tą właśnie technologią.

Słowa kluczowe: bezpieczeństwo wymiany, wymiana rynkowa, spekulacje, blockchain, *peer-to-peer*.

4.1. Wprowadzenie

Technologia blockchain znana jest przede wszystkim z zastosowań związanych z funkcjonowaniem kryptowalut. Tymczasem spektrum związanych z nią możliwości jest o wiele szersze. Ze względu na to, że opiera się na protokole *peer-to-peer*, z powodzeniem może być i jest wykorzystywana wszędzie tam, gdzie przedmiotem obrotu są dobra cyfrowe lub do transakcji dochodzi przy użyciu danych w postaci cyfrowej, a więc w przypadku wszystkich transakcji księgowanych lub rejestrowanych w systemach komputerowych. Potencjał tej technologii pozwala na sformułowanie hipotezy, że w gospodarce sieciowej stanie się ona odpowiednikiem „niewidzialnej ręki", utożsamianej z wymianą rynkową. Chodzi tu przede wszystkim o autonomiczność

dokonywanych za jej pomocą transakcji. Celem niniejszego rozdziału jest wskazanie związanych z technologią blockchain istniejących już i potencjalnych niebezpieczeństw wynikających z obrotu kryptowalutami.

4.2. Zastosowania technologii blockchain w zapewnieniu bezpieczeństwa wymiany

Jak dotychczas podstawowym zastosowaniem dla technologii blockchain są kryptowaluty i to z nimi jest ona utożsamiana. Stało się tak dlatego, że w tym przypadku technologia ta została zastosowana po raz pierwszy. Jednakże blockchain ma także wiele innych zastosowań. Odnosi się to przede wszystkim do usług finansowych, takich jak ubezpieczenia, giełdy i bankowość. W tych domenach działalności ekonomicznej niezwykle ważne jest zarówno bezpieczeństwo, jak i przewidywalność transakcji.

Aby wskazać niebezpieczeństwa związane z blockchainem, w pierwszej kolejności konieczne jest scharakteryzowanie technologii, która stała się jej podstawą, a mianowicie *peer-to-peer*, często oznaczanej jako P2P. Dotyczy ona rozproszonych systemów oprogramowania, które składają się z węzłów (pojedynczych komputerów), dzięki którym ich moc obliczeniowa jest bezpośrednio dostępna dla innego węzła. Dołączając do systemu *peer-to-peer,* użytkownicy zamieniają komputery w węzły systemu, które są równorzędne pod względem swoich uprawnień i ról. Chociaż użytkownicy mogą różnić się pod względem wnoszonych do systemu zasobów, to i tak wszystkie węzły w systemie mają takie same możliwości funkcjonalne (Czetwertyński, 2017). Dlatego komputery wszystkich użytkowników są zarówno dostawcami, jak i konsumentami zasobów. W takim systemie niepotrzebny staje się każdy pośrednik między wytwórcą dóbr cyfrowych a ich konsumentem. Jest to o tyle istotne, że współcześnie coraz więcej przedmiotów codziennego użytku zyskuje postać cyfrową. Najlepszym tego przykładem jest zmiana, jaka dokonała się na rynku muzycznym. W 2017 r. po raz pierwszy w historii globalne wpływy ze sprzedaży muzyki w formie streamingu były wyższe od wpływów ze sprzedaży tejże muzyki na nośnikach tradycyjnych (CD, płyty winylowe). Wyniosły one odpowiednio 6,6 mld USD oraz 5,2 mld USD (Sweney, 2018). I chociaż na tym rynku w dalszym ciągu funkcjonują pośrednicy (Spotify, Apple Music i inni), to upowszechnienie technologii *peer-to-peer* umożliwiło dystrybucję bezpośrednią wielu artystom, którzy nie są związani z żadną wytwórnią płytową. Podobna zmiana dokonała się na rynku produktów finansowych (usługi bankowe, pożyczki, ubezpieczenia itp.), a także w przypadku usług administracyjnych świadczonych za pomocą platform e-administracji (w Polsce takich, jak: ePUAP, PUE ZUS, CEIDG, eKRS i kilkadziesiąt innych).

Technologia ta przyczyniła się jednocześnie do rozwoju tzw. nieautoryzowanego kopiowania, czyli powielania dóbr informacyjnych bez zgody ich autorów (Czetwer-

tyński, 2017). Przy użyciu takich programów, jak: BitTorrent, uTorrent czy eMule, możliwe stało się pobieranie plików przy ich jednoczesnym udostępnianiu. W ten sposób za pomocą protokołu P2P w niekontrolowany i nieautoryzowany sposób obracano dobrami cyfrowymi, takimi jak: filmy, pliki graficzne i muzyczne, oprogramowanie komputerowe. Jak twierdzi S. Czetwertyński, skutkiem tego była „nietransakcyjność produktów wirtualnych" (2017). Brak możliwości sprzedaży produktów cyfrowych wymusiła na właścicielach praw autorskich zmianę sposobu ich dystrybucji. Zamiast oczekiwać na np. nieautoryzowane umieszczenie teledysku w serwisie YouTube, sami zaczęli udostępniać swoje produkcje, licząc na dochód, którym podzieli się z nimi serwis streamingowy. W ten sposób technologia *peer-to-peer* z oazy internetowego piractwa stała się platformą umożliwiającą legalną i natychmiastową wymianę danych i plików.

Zmiana sposobu funkcjonowania rynku produktów wirtualnych nie oznaczała jednak braku problemów bezpieczeństwa wymiany. Zdecentralizowana i otwarta dla każdego użytkownika sieć P2P umożliwiała w bardzo łatwy sposób przekazywanie informacji fałszywych lub zawierających tzw. złośliwe oprogramowanie, czyli takie, które jest zaprojektowane do uszkadzania lub wykorzystania dowolnego programowalnego urządzenia lub sieci. Obrót wirtualnymi produktami finansowymi w takich warunkach byłby niezwykle ryzykowny, gdyż w dowolnym momencie można zmienić nieszyfrowaną zawartość pliku zawierającą informacje o jego właścicielu, kwocie transakcji i jej warunkach, stopie procentowej itp. Rozwiązanie tego problemu przyniosła integracja technologii *peer-to-peer* i kryptografii w postaci blockchainu.

Blockchain, po polsku nazywany „łańcuchem blokowym", to baza danych działająca na zasadzie *open source*, za pośrednictwem internetu, oparta na architekturze *peer-to-peer*, służąca do zapisywania (księgowania) transakcji. Jej charakterystyczną cechą jest jej decentralizacja. Oznacza to, że nie ma konkretnego miejsca przechowywania danych, jest jawna i publiczna, zakodowana za pomocą algorytmów kryptograficznych. To swoista cyfrowa księga, składająca się z wielu zapisów. Decentralizacja oznacza też, że dokonywanie jakichkolwiek wpisów odbywa się na wielu komputerach, przez co nie można zmienić zapisanych już bloków. Każdy blok zawiera kryptograficzny skrót poprzedniego bloku w całym łańcuchu bloków.

Rozproszone systemy *peer-to-peer* mogą wykorzystywać łańcuch bloków jako narzędzie porządkujące w sposób trwały i przejrzysty wszystkie zachodzące w ich ramach interakcje. Blockchain można zatem uznać za narzędzie do osiągnięcia i utrzymania integralności w różnego typu systemach rozproszonych. Informatycy definiują technologię blockchain jako „rozwiązanie umożliwiające utrzymanie rozproszonej bazy danych o stale rosnącej liczbie danych, które są potwierdzane przez uczestniczące w nim węzły" (Yli-Huumo, Ko, Choi, Park i Smolander, 2016, s. 2).

Taka charakterystyka omawianego systemu oznacza, że może on działać w pełni autonomicznie. Brak konkretnego, centralnego miejsca przechowywania danych

oznacza, że nie można ich fizycznie skasować. Zapisanie ich w wielu węzłach, czyli w komputerach połączonych siecią *peer-to-peer*, uniemożliwia też jakiekolwiek fałszerstwa danych. Zazwyczaj systemy te są projektowane tak, że jeden lub nawet kilka zapisów blokowych różniących się od większości innych są odrzucane jako błędne (Drescher, 2017). Cecha ta uwidocznia komercyjny potencjał blockchaina. Pojęcie „blok" oznaczać bowiem może jedną lub wiele transakcji ze sobą powiązanych (Singhal, Dhameja i Panda, 2018). A to z kolei prowadzi do wniosku, że autonomiczny system zaszyfrowanych, powiązanych ze sobą bloków-transakcji gwarantuje pełne bezpieczeństwo wymiany (Drescher, 2017).

Dlatego też pierwotnym celem twórcy technologii blockchain było wyemitowanie własnej waluty, której wartość zależałaby tylko i wyłącznie od liczby stworzonych jednostek pieniężnych i skali popytu. Tak powstała kryptowaluta o nazwie bitcoin. Jej cechą jest rozproszony, szyfrowany system księgowy oraz wirtualny charakter. Istotą działania tego systemu są jego węzły, zwane portfelami (*wallets*), do których dostęp ma tylko jeden użytkownik dysponujący unikalnym, zaszyfrowanym kluczem (*cryptographic hash*) (Nakamoto, 2009). Tym samym ma on pełną kontrolę nad jego zawartością, tak jak w przypadku tradycyjnego portfela zawierającego gotówkę. Wszystkie przepływy w ramach poszczególnych kryptowalut (obecnie jest ich bardzo wiele, w tym co najmniej kilkanaście o znacznej kapitalizacji rynkowej) są rejestrowane w ramach ich wewnętrznych algorytmów.

4.3. Bezpieczeństwo wymiany kryptowalut

Niezbędnym elementem każdej sieci jest zaufanie. Jeśli w ramach sieci występuje większe zaufanie, połączenia są tworzone łatwiej, a transakcje zachodzą z większą płynnością, co zwiększa jej rozmiar. Obniżając koszty połączeń i zapewniając większą absorpcję wiedzy i *know-how*, sieci o wysokim poziomie zaufania są w stanie szybciej dostosowywać się do zmian rynkowych i technologicznych. Zjawisko to zostało szczegółowo omówione przez C. Hidalgo (2015). Blockchain w tym przypadku jest mechanizmem, który pozwala na wymuszone szyfrowaniem wykonanie uzgodnionych umów. Nie jest tu potrzebny konsensus między uczestnikami transakcji, ponieważ technologia ta oferuje mechanizm kontroli, który w znacznym stopniu ogranicza potrzebę zaufania i wymusza przejrzystość (Davidson, de Filippi i Potts, 2016).

Pomimo istnienia technicznych mechanizmów i założeń dotyczących bezpieczeństwa wymiany, niemalże od samego początku funkcjonowania kryptowalut pojawiły się dwa zasadnicze problemy związane z ich wymianą. Odnosi się to do olbrzymiej zmienności ich kursów oraz do oszustw związanych z Initial Coin Offering (ICO), czyli metody pozyskiwania kapitału w postaci kryptowalut lub tokenów w celu finansowania swojego przedsięwzięcia.

Duża zmienność ceny jakichkolwiek aktywów może być zachętą do spekulacji. Stało się tak również w przypadku bitcoina i innych kryptowalut. W pewnym momencie stały się one niemalże synonimem inwestycji spekulacyjnych, a nie środka płatniczego (McDonald, 2021). W przypadku bitcoina okres boomu i krachu wystąpił w przeszłości już 2-krotnie: pierwszy na przełomie 2013 i 2014 r., który zakończył się głośnym włamaniem na giełdę Mt Gox, a drugi na przełomie 2017 i 2018 r., kiedy kapitalizacja rynkowa bitcoina, ethera i innych kryptoaktywów osiągnęła najwyższą notowaną wartość na poziomie 830 mld USD (McDonald, 2021). Choć, jak twierdzą niektórzy, w tym okresie było nawet 5 baniek spekulacyjnych (Huber i Sornette, 2022).

Przyczyną tych wahań według większości ekonomistów jest brak centralnego organu regulującego cenę i wolumen obrotu (Li, Tao, Su i Lobonţ, 2019). Pozbawione regulatora rynki, szczególnie te o dużej płynności, podatne są na spekulacyjne transakcje, czyli działania polegające na zakupie dóbr po okazyjnych cenach z perspektywą ich odsprzedania na tym samym rynku, lecz za cenę wyższą. W przeszłości zjawisko to dotyczyło przede wszystkim rozmaitych rynków papierów wartościowych, walut oraz nieruchomości. W przeciwieństwie do tych tradycyjnych obszarów zainteresowania spekulantów rynek kryptowalut pozwala na wygodniejsze dokonywanie operacji kupna–sprzedaży, bez obaw o interwencję podmiotów zewnętrznych, takich jak nadzorcy rynków finansowych.

Mechanizm spekulacyjny, którego skutkiem jest tworzenie się baniek, przedstawiony został przez Eugene'a Famę już w 1970 r., w odpowiedzi na tzw. hipotezę rynku efektywnego, zgodnie z którą rynek jest efektywny, gdy ceny danego aktywa odzwierciedlają wszystkie dostępne informacje, a nowe informacje są szybko włączane do cen rynkowych przez racjonalnych inwestorów. Nie jest możliwe, aby inwestorzy systematycznie uzyskiwali wyższy zwrot niż zysk w sytuacji równowagi rynkowej, wykorzystując informacje historyczne, informacje publiczne i informacje wewnętrzne (Fama, 1970). Mając na uwadze tę zasadę, żaden inwestor nie może prześcignąć innych i generować ponadprzeciętnych zysków przez dłuższy czas. Zgodnie z tą hipotezą rynki finansowe są zmienne, ponieważ systematycznie pojawiają się nowe informacje, które zmieniają preferencje inwestorów, a w konsekwencji również ceny rynkowe. W związku z tym, że pojawienie się nowych informacji jest w zasadzie niemożliwe do przewidzenia, zmiany cen rynkowych także powinny być losowe i nieprzewidywalne (Fama, 1965).

Jedną z głównych konsekwencji wynikających z hipotezy rynku efektywnego jest to, że żadna bańka spekulacyjna nie może tworzyć się na stałe, ponieważ zostałaby szybko wyeliminowana przez racjonalnych uczestników rynku, wtedy gdy ceny aktywów odbiegają od ich wartości fundamentalnych. Ta koncepcja, jedna z najbardziej wpływowych teorii w literaturze finansowej, była testowana i intensywnie analizowana w literaturze akademickiej przez kilku innych uczonych, m.in. przez R. Shillera

(2015). Zwrócił on uwagę, że w latach 90. ubiegłego wieku w sektorze technologicznym nastąpiło znaczne rozwarstwienie cen akcji i ich fundamentalnej wartości. Użył nawet w tym kontekście terminu „irracjonalny entuzjazm". Co więcej, bańki mogą być nie tylko wynikiem euforii gospodarczej, ale mogą także „zarażać" optymizmem inne rynki (Kindleberger i Aliber, 2015). Zagrożeniem w tym przypadku nie jest samo tworzenie się baniek, lecz właśnie rozprzestrzenianie się ich na inne rynki, niekoniecznie związane z nowoczesnymi technologiami.

W związku z tym problemem zaobserwowano cykliczną powtarzalność zjawiska baniek spekulacyjnych, co wydaje się charakterystyczne dla rynku kryptowalut. Zwrócili na to uwagę w swoich badaniach T. Huber i D. Sornette. Według nich cykle technologicznej adopcji bitcoina, napędzane bańkami, można skonceptualizować jako wzór zagnieżdżonych krzywych, z których każda reprezentuje nową grupę inwestorów – przyszłych spekulantów, którzy nie będą pozbywać się aktywów w czasie kolejnego krachu. Według nich „hipercykle", charakterystyczne dla bitcoina, są wbudowane w sam jego protokół. W projekcie Nakamoto co cztery lata następuje bowiem zmniejszenie o połowę nagrody dla „górników" zajmujących się tworzeniem bitcoina. Mechanizm ten został wbudowany w protokół w celu kontrolowania inflacji, a wszystkie poprzednie takie zdarzenia zbiegały się w czasie z ogromnym wzrostem kapitalizacji tej waluty (Huber i Sornette, 2022). Deflacyjny charakter podaży bitcoina i regularne zmniejszanie o połowę nagród za jego tworzenie, nazwać można adaptacją spekulacyjną. Wynikająca z tego hierarchiczna sekwencja powtarzających się, rosnących wykładniczo serii baniek, które pojawiły się w ciągu ostatniej dekady od jego powstania, spowodowała nowe fale napływu spekulacyjnych inwestorów.

Następnym zagrożeniem związanym z kryptowalutami jest wykorzystanie ICO w celu wyłudzenia pieniędzy na projekt, który w rzeczywistości nigdy nie zostanie zrealizowany. Istota tego narzędzia została opisana w innym rozdziale niniejszej książki, dlatego też w tej części zostaną przedstawione jedynie kwestie związane z zagrożeniem utraty środków finansowych przez inwestorów.

Całkowita kapitalizacja ICO osiągnęła swoje maksimum w 2017 r. i wyniosła 1 bln USD. W kolejnych okresach wartość ta znacząco się zmniejszyła, co dało początek dyskusji na temat tego, jakie były powody spadku popularności tej metody pozyskiwania kapitału (Roosenboom, van der Kolk i de Jong, 2020). W związku z tym wielu przedstawicieli branży kryptowalut wyraziło przekonanie, że spora część ICO wiązała się ze zwykłym oszustwem, co zniechęciło potencjalnych inwestorów. W badaniach branżowych posunięto się nawet do stwierdzenia, że 80% wszystkich ICO to w rzeczywistości oszustwa (Dowlat, 2018). Jednakże część badaczy uważa, że tak wysoki odsetek oszustw nie jest możliwy, tłumacząc, że często za oszustwo uważa się sytuację, w której przedsięwzięcie będące przedmiotem finansowania po prostu nie odniosło sukcesu rynkowego, nie zapewniając tym samym oczekiwanej przez

inwestorów stopy zwrotu. Ci sami naukowcy twierdzą równocześnie, że po analizie liczby pozwów, złożonych przez zawiedzionych inwestorów, można stwierdzić, że jedynie mniej niż 7% wszystkich ICO zaoferowanych do końca 2016 r. należy przyjąć za oszustwo (Liebau i Schueffel, 2019). Wydaje się, że tę hipotezę potwierdzają badania dotyczące „przeżywalności" nowych przedsięwzięć, przeprowadzone przez A. J. Timmonsa i S. Spinellego (2012). Ich zdaniem jedynie 60% przedsięwzięć przetrwa przez pierwszy rok swojego istnienia, a zaledwie 10% kolejne 5 lat. Do zbliżonych wniosków doszli M. Song, K. Podoynitsyna, H. van der Bij i J. Halman (2008) w odniesieniu do start-upów. Według nich do 5 roku funkcjonowania dotrwa 21,9% wszystkich przedsięwzięć tego typu. Podnoszenie tego zjawiska do rangi niebezpieczeństwa jest zatem niewłaściwe, ponieważ dotyczy ono w takim samym stopniu innych start-upów z sektora wysokich technologii. W przyszłości natomiast potencjalnym zagrożeniem może być awersja do ryzyka w odniesieniu do tego typu inwestycji ze względu na niskie prawdopodobieństwo ich sukcesu. Nie jest to jednak zagrożenie znaczące. Jak twierdzi A. Kuźmińska-Haberla, niektóre spośród ICO są bardziej udane niż inne. Do tej grupy należą projekty blockchain na wczesnym etapie, platformy *blockchain-as-a-service*, zajmujące się konkretnymi zastosowaniami zaawansowanej technologii w świecie rzeczywistym oraz projekty zapewniające najwyższą prywatność kryptowalut. Ponadto zdecentralizowane rynki predykcyjne wspierane przez technologię blockchain, oddaną społeczność programistów oraz innowacyjne, nowe projekty stwarzają szansę na przyniesienie sukcesu i wysokie zwroty inwestorom (Kuźmińska-Haberla, 2021).

Sytuacja na rynku kryptowalut wydaje się przypominać tzw. bańkę technologiczną z początku wieku. Jak argumentuje R. Shiller (2015), wzrost cen akcji spółek z branż technologicznych był napędzany irracjonalną euforią wśród inwestorów indywidualnych, podsycaną przez media, które maksymalizowały oglądalność telewizji i zaspokajały zapotrzebowanie inwestorów na „pseudowiadomości". Z podobną sytuacją mamy do czynienia także dzisiaj, gdy indywidualni gracze mogą nie znać zasad, na jakich działają kryptowaluty. Pozwala to przypuszczać, że w przyszłości częstotliwość tworzenia się baniek spekulacyjnych może być niższa, podobnie jak to miało miejsce w przypadku akcji spółek technologicznych. Częstotliwość ich wahań cenowych wydaje się obecnie dużo niższa niż jeszcze 20 lat temu. Spostrzeżenie to pokrywa się z wnioskami, jakie z analiz zachowań inwestorów w tych latach wyciągnęli M. Brunnermeier i S. Nagel (2004). Zwrócili uwagę na dwa istotne aspekty. Po pierwsze, oprócz inwestorów indywidualnych, to fundusze hedgingowe napędzały bańkę technologiczną, a po drugie, zmniejszały one swoje udziały w tym rynku zanim spadły ceny, co sugeruje, że zarządzający funduszami rozumieli, że ceny akcji nieuchronnie się obniżą. Ich ustalenia są zgodne z poglądem, że nastroje inwestorów napędzających spekulacje były do pewnego stopnia przewidywalne i że fundusze hedgingowe, będące podmiotami wysokiego ryzyka, wykorzystały okazję do szybkiego zarobku. Bańki spekulacyjne, które stanowią zagrożenie dla rynku

kryptowalut, w rzeczywistości mogą okazać się zatem „chorobą wieku dziecięcego", która skończy się wraz z pogłębieniem wiedzy na temat kryptowalut przez inwestorów i zmierzchem efektu nowości.

4.4. Niewymienne tokeny

Na wypowiedzi w alarmistycznym tonie można natrafić w mediach w przypadku *non-fungible token* (NFT). Jest to rodzaj kryptowaluty wywodzącej się z inteligentnych kontraktów Ethereum (Wang, Li, Wang i Chen, 2021). NFT różni się od klasycznych kryptowalut, takich jak bitcoin, podstawowymi cechami. W przypadku bitcoina wszystkie monety są równoważne i nie do odróżnienia. W przeciwieństwie do niego NFT jest unikatowe i nie można go wymienić na podobne, równoważne, niepodlegające wymianie jednostki, dzięki czemu rozwiązanie to nadaje się do identyfikacji konkretnych dóbr w sposób szczególny. Używając NFT w przypadku inteligentnych kontraktów, twórca może łatwo udowodnić istnienie i własność zasobów cyfrowych w postaci filmów, obrazów, dzieł sztuki, biletów na wydarzenia itp. Ponadto twórca może również otrzymywać tantiemy za każdą transakcję na dowolnym rynku NFT lub przez wymianę *peer-to-peer*. Ich zaletą jest pełna przejrzystość, duża płynność oraz interoperacyjność. Cechy te sprawiają, że NFT jest wygodnym rozwiązaniem chroniącym własność intelektualną i umożliwiającym obrót produktami wirtualnymi. Pomimo że NFT mogą mieć ogromny wpływ na obecne, zdecentralizowane rynki i przyszłe możliwości biznesowe, technologie te są wciąż na bardzo wczesnym etapie rozwoju. Niesie to ze sobą wiele niebezpieczeństw.

Do końca 2018 r. rynek NFT był w pełni zdominowany przez cyfrowe dobra artystyczne, a w szczególności przez kolekcję CryptoKitties. Od stycznia 2019 r. na popularności zaczęły zyskiwać inne kategorie dóbr, zarówno pod względem całkowitego wolumenu wymiany, jak i liczby transakcji. Ogólnie rzecz biorąc, w okresie od stycznia 2019 r. do lipca 2020 r. około 90% całkowitego wolumenu wymiany na NFT zostało podzielone na kategorie: „sztuka", „gry" i „Metaverse", przyczyniając się odpowiednio do 18%, 33% i 39% całkowitego obrotu. Od połowy lipca 2020 r. na rynku w dużej mierze dominowały NFT sklasyfikowane jako „sztuka", które od tego czasu stanowiły około 71% całkowitego wolumenu transakcji, a następnie „aktywa kolekcjonerskie" stanowiące 12%. Co ciekawe, struktura rynku jest zupełnie inna, jeśli chodzi o liczbę transakcji. Od lipca 2020 r. najczęściej wymieniane NFT należą do kategorii „gry" i „kolekcje", które stanowią 44% i 38% transakcji. Od 2020 r. rośnie udział wartości NFT klasyfikowanych jako „sztuka", podczas gdy ilość tych dóbr maleje (Nadini i in., 2021). Rozbieżność między wolumenem a transakcjami uwidacznia to, że ceny przedmiotów zaliczonych do tej kategorii stają się coraz wyższe w porównaniu z innymi kategoriami. Zjawisko to wskazuje na potencjalne tworzenie się baniek spekulacyjnych, zagrażających bezpieczeństwu i ograniczających rozwój rynku NFT.

Na ich tworzenie się wskazywać mogą głośne w 2021 i 2022 r. transakcje na rynku NFT, takie jak np. sprzedanie przez artystę, ps. Beeple, cyfrowego dzieła sztuki za 69 mln USD (Christie's, 2021) czy sprzedanie przez dyrektora generalnego Twittera, J. Dorseya, jego pierwszego tweeta za 2,9 mln USD (CNBC, 2021). O ile trudno dyskutować z gustami nabywców sztuki, o tyle trudno uznać zakup wpisu na portalu Twitter, który i tak w każdej chwili jest powszechnie dostępny, a treść którego można swobodnie kopiować i powielać, za zakup racjonalny. Jest to raczej spekulacja obliczona na odsprzedaż i szybki zarobek związany z rosnącą popularnością tokenów. Zresztą wspomniane dzieło sztuki także może być swobodnie oglądane i jest dostępne dla każdego w internecie. A zatem inaczej niż w przypadku tradycyjnych dzieł sztuki, których właściciel może nimi dowolnie rozporządzać i w ten sposób także czerpać z nich dochody.

Z badań przeprowadzonych przez A. Lennart (2021) wynika, że rynki NFT są napędzane przez inne rynki NFT. Projekty o bardzo zróżnicowanych treściach mogą mieć na siebie znaczący wpływ, co jak wskazuje autor badania wydaje się być sprzeczne z intuicją. Niezależnie od tej konkluzji pod uwagę trzeba wziąć nieuchronne, jak się wydaje, konsekwencje tego stanu rzeczy – rozrost i pęknięcie bańki spekulacyjnej w przypadku jednego tylko z aktywów NFT pociągnie za sobą krach na całym rynku. Jest to o tyle prawdopodobne, że jak wynika z analiz D.-R. Kong i T.-Ch. Lin (2022), inwestowanie w NFT zwykle wiąże się z bardzo dużą zmiennością, a ujemna korelacja zwrotów między transakcjami NFT a powszechnymi instrumentami zabezpieczającymi (np. złotem i obligacjami) wskazuje, że transakcje te przypominają pod tym względem inwestycje wysoce ryzykowne.

4.5. Bezpieczeństwo inteligentnych kontraktów

Sposób działania blockchaina można porównać do pośrednika rynkowego, który pomaga ustalić warunki wymiany i egzekwuje ich wykonanie. Zaletą tej technologii jest pełna autonomiczność. Cyfrowy pośrednik działa bowiem niezależnie, według zaprogramowanego schematu, a szyfrowanie transakcji oraz przechowywanie jej zapisu (śladu) w wielu miejscach jednocześnie uniemożliwia jakiekolwiek oszustwo. Umożliwia to realizację wiarygodnych i nieodwracalnych transakcji bez osób trzecich. Umowy zawierane za pomocą kryptografii zyskały nawet miano *smart contracts*, czyli inteligentnych kontraktów. Ich koncepcja narodziła się już w 1994 r. (Szabo, 1997), a szerokie zastosowanie znalazły wraz z powstaniem bitcoina. Jednakże dopiero powstanie ethera opierało się w pełni na protokołach inteligentnych kontraktów w celu ulepszenia funkcji transakcyjnej. Kontrakty te to wykonywalne kody, które działają na łańcuchu blokowym w celu ułatwienia, wykonania i egzekwowania umowy między niezaufanymi stronami bez angażowania zaufanej strony trzeciej (Alharby i van

Moorsel, 2017). Handlowcy mogą wspólnie projektować i opracowywać lepsze decyzje transakcyjne, aby zwiększyć efektywność swojej współpracy. Proces ten jest często określany jako Blockchain 2.0 (Angelis i da Silva, 2019).

W ciągu kilku ostatnich lat idea inteligentnych kontraktów znalazła zastosowanie przy tworzeniu zdecentralizowanych autonomicznych organizacji (DAO). Są to podmioty zorganizowane zgodnie z regułami zapisanymi w algorytmie komputerowym, który jest przejrzysty, kontrolowany przez akcjonariuszy i niepodlegający jakimkolwiek wpływom administracyjnym oraz regulacjom zewnętrznym. Organizacje takie mogą działać w sposób zdecentralizowany z pominięciem pośredników, poświadczających transakcję, takich jak: notariusz, bank centralny, agent rozliczeniowy, giełda itp. (Brol, 2020). Technologia blockchain wpływa na sposób zawierania i wykonywania niektórych umów, zmniejszając koszty związane z menedżerami-agentami, a nawet zasadniczo zmienia sposób zarządzania niektórymi firmami (Murray, Kuban, Josefy i Anderson, 2021).

Odniesienie do teorii agencji nie jest w tym przypadku nadużyciem. Zjawisko to w syntetyczny sposób opisał S. A. Ross. Według niego relacja ta jest „jednym z najstarszych i najpowszechniejszych skodyfikowanych sposobów interakcji społecznej" (Ross, 1973, s. 134). Kluczową różnicą w stosunku do koncepcji *homo oeconomicus* była konstatacja, że wszelkie decyzje indywidualne są podejmowane w warunkach niepewności. Tyczy się to szczególnie relacji między dwoma podmiotami, które mogą dysponować innymi, często rozbieżnymi informacjami, co może posłużyć do realizacji własnych – odmiennych celów. Jak twierdzi J. Stiglitz, korzyści pełnomocnika różnią się od korzyści mocodawcy. W konsekwencji pełnomocnik może nie podjąć działań, jakich oczekuje od niego mocodawca, a informacji odnośnie do swoich zamiarów nie ujawniać. Skłonność pełnomocnika do pracy zależeć będzie przede wszystkim od zaproponowanego systemu motywacyjnego (Stiglitz, 1987).

W ostatnich latach połączono system wieloagencyjny z technologią blockchain, aby wykorzystać jego funkcje bezpieczeństwa i prywatności. Wśród opracowanych aplikacji znajdują się m.in. systemy carpoolingu, monitorowania zużycia energii, a także łańcucha dostaw żywności oraz głosowania elektronicznego (Soufiene, Abdullah, Trad i Youssef, 2020). Rezultatem tego było ograniczenie niektórych kosztów, w tym przede wszystkim kosztów zawierania umów i agencji (Murray i in., 2021).

Można zatem zaryzykować stwierdzenie, że inteligentne kontrakty są dla kryptowalut instytucjami rozumianymi jako zbiór zasad i wzorców postępowania. Co więcej, ze względu na autonomiczny, bezosobowy i bezstronny ich charakter są niemalże idealnym „strażnikiem" funkcjonowania rynków, których działanie zależy od technologii blockchaina. Być może staną się one sposobem na przeciwdziałanie jednemu z największych problemów związanych z kryptowalutami, jakim jest organizacja obrotu nimi. Chodzi tu o dwa zasadnicze problemy. Po pierwsze o ataki hakerskie na

aplikacje i strony internetowe będące platformami wymiany, a po drugie o same giełdy, które zarejestrowane w krajach o słabych instytucjach państwowych i regulacyjnych mogą w sposób niekontrolowany upaść.

Kwestia ataków hakerskich na infrastrukturę sieciową, oprogramowanie komputerowe i aplikacje mobilne nie jest sprawą nową, jednakże do niedawna nie były prowadzone żadne analizy dotyczące skali tego zjawiska w przypadku giełd kryptowalut. Pierwsze takie opracowanie przygotowała w 2020 r. grupa chińskich badaczy skupionych wokół Pekińskiego Uniwersytetu Poczty i Komunikacji. Ustalili oni, że w przeszłości pojawiło się ponad 1500 domen kolportujących około 300 fałszywych aplikacji, podszywających się pod giełdy kryptowalut. Następnie, badając związek między oszukańczymi domenami a fałszywymi aplikacjami, zidentyfikowali 94 rodziny domen oszukańczych i 30 rodzin fałszywych aplikacji. Zauważyli także, że fałszywe aplikacje zostały przemycone na główne rynki aplikacji mobilnych (w tym Google Play) w celu zainfekowania urządzeń niczego niepodejrzewających użytkowników (Xia i in., 2020).

Od kilku lat trwają też prace nad uregulowaniem rynku pośredników w handlu cyfrowymi walutami. Działania takie mogą mieć dwojaki skutek. Z jednej strony regulacje mogą powodować ograniczenia dla uczestników rynku, negatywnie wpływając na rynek, z drugiej strony mogą go ożywić przez wzmocnienie jego wiarygodności i stabilności (Kim, Bilgin i Ryu, 2021). Celem tych regulacji ma być zapobieżenie takim zjawiskom jak niedawny upadek jednej z największych giełd, jaką była FTX Cryptocurrency Exchange. W związku z krążącymi na przełomie października i listopada 2022 r. plotkami, że fundusz założony przez ikonę branży, Sama Bankmana-Frieda, nie był w stanie zaspokoić swoich wierzycieli, nastąpiła masowa wyprzedaż oferowanych przez tę giełdę aktywów ze strony użytkowników platformy, co tylko przyspieszyło upadek firmy oraz dodatkowo pogłębiło trend spadkowy kursów innych kryptowalut.

Jak pisze A. Bris, upadek tak dużego podmiotu jak FTX może mieć kluczowe znaczenie dla przyszłości rynku kryptowalut. Po pierwsze dlatego, że w przeciwieństwie do tradycyjnych instytucji finansowych i giełd, w których pieniądze inwestorów i deponentów są chronione, giełdy kryptowalut są znacznie bardziej ryzykowne, a ewentualne roszczenia inwestorów mogą pozostać niezaspokojone (FTX było zarejestrowane na Bahamach). Po drugie złożenie wniosku o upadłość poprzedził tydzień paniki związanej z kondycją finansową giełdy i gwałtowny wzrost wypłat, co pogorszyło sytuację finansową także innych giełd. Po trzecie epizod FTX może oznaczać kolejny krok w kierunku ostatecznego upadku emitowanych prywatnie kryptowalut. Po czwarte wreszcie, zdarzenie to niesie ze sobą odkrycie, że kryptowaluty mogą nie być źródłem przychodów dla inwestorów oczekujących szybkiego i znacznego zwrotu z dokonanej inwestycji (Bris, 2022). To ostatnie spostrzeżenie uznać należy za dobrą wiadomość. Upadek FTX może doprowadzić do przyś-

pieszenia procesu regulacji rynków kryptowalut, a wykorzystanie w tym celu koncepcji inteligentnych kontraktów może zmniejszyć potencjalne niekorzyści z tytułu regulacji.

4.6. Podsumowanie

Celem rozdziału, sformułowanym we wstępie, było wskazanie związanych z technologią blockchain, na której jest oparte funkcjonowanie kryptowalut, istniejących i potencjalnych niebezpieczeństw wynikających z ich obrotu. Jak wykazano, główne zagrożenia dla funkcjonowania rynków kryptowalut leżą poza samą technologią blockchain. Mają one najczęściej tradycyjne, ekonomiczne podłoże, a sprzyja im brak regulacji. Kluczową sprawą wydaje się wykorzystywanie niewiedzy lub też braku umiejętności radzenia sobie z powszechnymi w sieci internetu zagrożeniami. Problemem jest też nadmierny optymizm dotyczący możliwości osiągania ponadnormatywnych zysków przez inwestorów. Zazwyczaj prowadzi on do tworzenia się baniek spekulacyjnych, w wyniku których swoje środki traci większość podmiotów zaangażowanych na rynku. Optymizm ten mogą wykorzystywać zawodowi uczestnicy rynków kapitałowych, tacy jak fundusze hedgingowe, którzy, podbijając nastroje inwestorów indywidualnych, dążą do maksymalizacji własnych zysków. Ostatnim z zagrożeń jest brak międzynarodowych regulacji związanych z funkcjonowaniem giełd kryptowalut – międzynarodowych, ponieważ lokalne, krajowe regulacje nie miałyby sensu w warunkach, w których podmiot prowadzący giełdę może być zarejestrowany w dowolnym państwie, a prowadzić działalność *de facto* w sposób globalny. Konsekwencją braku regulacji są problemy związane z niemożnością utrzymania należytej płynności finansowej tych podmiotów, przeinwestowaniem, zagwarantowaniem realizacji zleceń i wypłat należności itp.

Bibliografia

Alharby, M. i van Moorsel, A. (2017). *Blockchain-based smart contracts: A systematic mapping study*. arXiv:1710.06372.

Angelis, J. i da Silva, E. R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, *62*(3), 307-314.

Bris, A. (2022). *Five takeaways from the FTX crypto exchange collapse*. IMD Business School. Pobrane z https://www.imd.org/ibyimd/finance/five-takeaways-from-the-ftx-crypto-exchange-collapse

Brol, M. (2020). The influence of blockchain technology on exchange safety and costs. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, *64*(2), 21-31.

Brunnermeier, M. i Nagel, S. (2004). Hedge funds and the technology bubble. *The Journal of Finance*, *LIX*(5), 2013-2040.

Christie's. (2021). *Christie's announces Beeple's HUMAN ONE: The artist's first-ever dynamic physical artwork + video NFT*. Pobrane z https://www.christies.com/about-us/press-archive/details?-PressReleaseID=10268&lid=1

CNBC. (2021). *Jack Dorsey sells his first tweet ever as an NFT for over $2.9 million*. Pobrane z https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html

Czetwertyński, S. (2017). *Paradoks cenowy produktów wirtualnych*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Davidson, S., de Filippi, P. i Potts, J. (2016). *Economics of blockchain*. Public Choice Conference, Fort Lauderdale. Pobrane z http://dx.doi.org/10.2139/ssrn.2744751

Dowlat, S. (2018). *Cryptoasset market coverage initiation: network creation*. Pobrane z https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

Drescher, D. (2017). *Blockchain Basics*. New York: Apress.

Fama, E. F. (1965). The behavior of stock-market prices. *Journal of Business*, *38*(1), 34-105.

Fama, E. (1970). Efficient capital markets: A review of theory and empirical work. *Journal of Finance*, *25*(2), 383-417.

Hidalgo, C. (2015). *Why information grows: The evolution of order, from atoms to economies*. Philadephia: Basic Books.

Huber, T. A. i Sornette, D. (2022). Boom, bust, and bitcoin: Bitcoin-bubbles as innovation accelerators. *Journal of Economic Issues*, *56*(1), 113-136.

Kim, D., Bilgin, M. H. i Ryu, D. (2021). Are suspicious activity reporting requirements for cryptocurrency exchanges effective? *Financial Innovation*, *7*(1), 1-17.

Kindleberger, C. P. i Aliber, R. Z. (2015). *Manias, panics and crashes: A history of financial crises*. Basingstoke, Hampshire: Palgrave MacMillan.

Kong, D.-R. i Lin, T.-C. (2022). *Alternative investments in the fintech era: The risk and return of non-fungible token (NFT)*. SSRN. Pobrane z https://ssrn.com/abstract=3914085

Kuźmińska-Haberla, A. (2021). Initial Coin Offerings in practice. W: W. Michalczyk (red.), *Cryptocurrencies in the global economic and financial system. Initial Coin Offerings as an innovative tool of crowdfunding and promotion* (s. 146-169). Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Lennart, A. (2021). Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations. *Blockchain Research Lab Working Paper Series*, (22). https://doi.org/10.1080/10438599.2022.2119564

Li, Z., Tao, R., Su, C.W. i Lobonţ, O.R. (2019). Does Bitcoin bubble burst? *Quality & Quantity: International Journal of Methodology*, *53*(5/1), 91-105.

Liebau, D. i Schueffel, P. (2019). Cryptocurrencies & Initial Coin Offerings: Are they scams? – An empirical study. *The Journal of the British Blockchain Association*, *2*(1). https://doi.org/10.31585/jbba-2-1-(5)2019

McDonald, O. (2021). *Cryptocurrencies: Money, trust and regulation.* Newcastle: Agenda Publishing.

Murray, A., Kuban, S., Josefy, M. i Anderson, J. (2021). Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives*, *35*(4). https://doi.org/10.5465/amp.2018.0066

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. i Baronchelli, A. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific Reports*, *11*, 20902. https://doi.org/10.1038/s41598-021-00053-8

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. Pobrane 15 października 2022 z https://bitcoin.org/bitcoin.pdf.

Roosenboom, P., van der Kolk, T. i de Jong, A. (2020). What determines success in Initial Coin Offerings? *Venture Capital, An International Journal of Entrepreneurial Finance*, *22*(2), 161-183.

Ross, S. A. (1973). The economic theory of agency: The principal's problem. *American Economic Review*, *62*, 134-139.

Shiller, R. (2015). *Irrational exuberance* (revised and expanded 3rd ed.). Oxford, Princeton: Princeton University Press.

Singhal, B., Dhameja, G. i Panda, P. S. (2018). *Beginning Blockchain*. New York Apress.

Song, M., Podoynitsyna, K., Bij, H. van der i Halman, J. (2008). Success factors in new ventures: A meta-analysis. *Journal of Product Innovation Management*, *25*(1), 7-27.

Soufiene, B. O., Abdullah, A. B., Trad, A. i Youssef, H. (2020). PEERP: A priority-based energy-efficient routing protocol for reliable data transmission in healthcare using the IoT. *Procedia Computer Science*, *175*(2), 373-378.

Stiglitz, J. (1987). Principal and agent. W: *The new Palgrave: Dictionary of economics* (s. 966-971). London: MacMillan Press.

Sweney, M. (2018, 24 kwietnia). Slipping discs: music streaming revenues of $6.6bn surpass CD sales. *The Guardian*. Pobrane z https://www.theguardian.com/technology/2018/apr/24/music-streaming-revenues-overtake-cds-to-hit-66bn

Szabo, N. (1997). The idea of smart contracts. *Nick Szabo's Papers and Concise Tutorials*, *6*(1).

Timmons, A. J. i Spinelli, S. (2012). *New venture creation: Entrepreneurship for the 21st century*. New York: McGraw-Hill/Irwin.

Wang, Q., Li, R., Wang, Q. i Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *Tech Report*, (21). https://doi.org/10.48550/arXiv.2105.07447

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., Luo, X. i Xu, G. (2020). Characterizing cryptocurrency exchange scams. *Computers & Security*, (98), 1-17. https://doi.org/10.1016/j.cose.2020.101993

Yli-Huumo, J., Ko, D., Choi, S., Park, S. i Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. *PLoS ONE*, *11*(10).

Safety Risks Related to Cryptocurrencies and Blockchain Technology

Abstract: The term "exchange safety" refers to an array of conditions favourable to performing a market transaction, especially trust between the exchange participants and transparency of the exchange. The IT development allows the exchange conditions to approach the perfect model. The rise of the internet and digitalisation of economic processes were the key factors here, and another important factor was the introduction of blockchain transactions. This chapter deals with safety issues related to this technology.

Keywords: exchange safety, market exchange, speculations, blockchain, *peer-to-peer*.