

Krzysztof Chochowski
Sylwia Gwoździewicz

Wykorzystanie technologii blockchain w instytucjach finansowych i w cyberbezpieczeństwie w świetle polskich (krajowych) uregulowań prawnych

The use of blockchain technology in financial institutions and in cybersecurity in the light of Polish (national) legal regulations

Celem podjętej tematyki jest analiza technologii blockchain w aspekcie krajowego prawodawstwa oraz wskazanie praktyk wykorzystania tej technologii w instytucjach finansowych i w cyberbezpieczeństwie. W podjętych rozważaniach analizie poddano aktualny stan normatywny dotyczący technologii blockchain w celu potwierdzenia tezy, iż ta technologia w coraz szerszym zakresie staje się przedmiotem uregulowań prawnych, a zakres jej funkcjonalności powiększa się, co wymusza na prawodawcy stosowną reakcję normatywną. Następnie na wybranych przykładach przedstawiono zastosowanie technologii blockchain w instytucjach finansowych i w cyberbezpieczeństwie.

Słowa kluczowe: technologia blockchain, inteligentne kontrakty, tokeny płatnicze, kryptowaluty

The aim of the topic is to analyze blockchain technology in the aspect of national legislation and to indicate the practices of using this technology in cybersecurity and financial institutions. In the considerations undertaken, the current normative status regarding blockchain technology was analyzed in order to confirm the thesis that blockchain technology is increasingly becoming the subject of legal regulations and

the scope of its functionality is expanding, which forces the legislator to adopt an appropriate normative response. Then, examples show the use of blockchain technology in financial institutions and cybersecurity.

Key words: blockchain technology, smart contract, payment tokens, cryptocurrencies

Stan normatywny dotyczący technologii blockchain

Technologia blockchain nie doczekała się jeszcze w Polsce kompleksowego uregulowania. Istniejące przepisy prawa w omawianej materii odnajdujemy przede wszystkim w prawie cywilnym oraz finansowym, a także – już w znacznie ograniczonym zakresie – w prawie karnym.

W przestrzeni prawa cywilnego szczególnie wyraziście jawi się zagadnienie tzw. inteligentnych kontraktów (smart contract). W pierwotnej koncepcji sformułowanej przez N. Szabo, smart contracts to algorytmiczne ujęcie transakcji (umowy) w postaci kodu źródłowego programu komputerowego zabezpieczonego kryptograficznie lub w inny sposób, a jedną z głównych cech tego algorytmu jest samowykonalność¹.

Aktualnie pod tym pojęciem rozumie się „Skompilowany kod programistyczny, którego kopia wpisana jest w rejestr blockchain (np. sieci Ethereum) i reprezentujący zasady dokonania transakcji pomiędzy stronami. Raz rozpropagowany w ramach sieci, smart kontrakt jest uruchomiony na wszystkich węzłach jako program wykonywalny i uruchamia konkretną funkcję przewidzianą przez autora. Smart kontrakt jest cyfrową reprezentacją zasad lub procesów funkcjonujących w danej organizacji biznesowej, które regulują sposób dokonywania i przebieg transakcji. Smart kontrakty pełnią również rolę kontrolującą aktywa lub mogą wywoływać zdarzenia, ustalone za pomocą technik programistycznych (funkcje if... then... else...). Rozbudowany system smart kontraktów mający na celu autonomicznie zarządzać aktywami nazywany jest Zdecentralizowaną Autonomiczną Organizacją”².

W uproszczony sposób kwestię inteligentnych kontraktów prezentują M. Pecyna i A. Behan, zdaniem których „smart contracts to skompilowany

¹ N. Szabo, *Smart Contract: Formalizing and Securing Relationships on Public Networks*, View of Formalizing and Securing Relationships on Public Networks | First Monday (dostęp: 26.05.2023).

² *Leksykon pojęć na temat technologii blockchain i kryptowalut* – (ictbanking.net) (dostęp: 25.05.2023).

kod źródłowy programu zapisany na blockchainie, który zapewnia samowystarczalność oraz autonomiczną naturę postanowień przewidzianych i zdefiniowanych w kodzie, na warunkach w nich zawartych oraz zastosowanych do wartości majątkowych, które mogą być powiązane z blockchainem”³.

Inteligentny kontrakt, zdaniem J. Czarneckiego, „jest oprogramowaniem, które jest wykonywane za sprawą transakcji w danym blockchainie poprzez dokonanie zmian w tym blockchainie. Jest ono zapisane w blockchainie i wykonywane przez rozproszone węzły sieci, co eliminuje konieczność korzystania z zaufanej trzeciej strony. Modyfikacja albo wpłynięcie na działanie inteligentnego kontraktu wymaga zmiany konsensu całej sieci”⁴. Jak zatem widać, inteligentne kontrakty mocno eksponują kwestię bezpieczeństwa, zmiany bowiem, jak wskazano powyżej, wymagają zgody sieci.

J. Czarnecki, kontynuując swoje rozważania, stwierdza następnie, iż „Smart contract to więź prawna, która może samodzielnie funkcjonować w przestrzeni cyfrowej, bez potrzeby odwoływania się do świata realnego. W praktyce realizacja tej idei powinna zapewniać, że: „relacja prawna jest zawierana za pośrednictwem środków elektronicznych, bez potrzeby korzystania z papierowych dokumentów czy tradycyjnych podpisów, oraz może być w taki sposób zmieniana; również wykonanie tej relacji prawnej czy jej elementów nie musi być związane z jakimkolwiek działaniem w świecie realnym – jest ono automatyczne i podlega wyłącznie regułom ustalonym w danym inteligentnym kontrakcie”⁵.

Trafnie więc wskazuje D. Szostek, że inteligentne kontrakty to kolejny etap rozwoju umów online. Uwzględniają one wymóg zapewnienia kryptografii, automatyczność procesów oraz możliwość automatycznego „wykonania” kontraktu po przesłankach określonych w kodzie programistycznym⁶.

W tym miejscu warto przypomnieć, iż „Smart contract jest elementem rzeczywistości, natomiast umowa jest konstrukcją prawną i istnieje wtedy, gdy spełnione są określone w przepisach przesłanki. Do zaistnienia umowy potrzebna jest co do zasady zgodna wola stron (konsensus), tj. złożenie

³ M. Pecyna, A. Behan, *Smart Contracts – nowa technologia prawa umów?*, Transformacje prawa prywatnego 2020/3, s. 188–189.

⁴ J. Czarnecki, *Czym są inteligentne kontrakty i DAO*, 2016, s. 7, Blockchain, inteligentne kontrakty i DAO (wardynski.com.pl) (dostęp: 27.05.2023).

⁵ Tamże, s. 7.

⁶ D. Szostek, *Blockchain i prawo*, Baden – Baden 2019, s. 111.

przez strony oświadczeń woli o zgodnej treści. Oświadczenia woli nie muszą mieć formy pisemnej. (...) Smart contract może być więc formą wyrażenia zgodnej woli stron, ale nie musi. Jeżeli bowiem nie ma między stronami konsensu, to nie ma również umowy. Deployment smart contractu w blockchainie nie ma wtedy żadnego znaczenia prawnego w zakresie istnienia umowy. W konsekwencji, naszym zdaniem, zastosowanie smart contractu nie wyklucza w żadnym wypadku możliwości powołania się na błąd czy inne wady oświadczeń woli na gruncie ogólnych przepisów kodeksu cywilnego”⁷.

W zasadzie zbieżny pogląd prezentują M. Pecyna i A. Behan, twierdzą bowiem, że „smart contract jako taki nie jest umową i z umową w sensie prawnym nie powinien być utożsamiany. Natomiast smart contract może być uznany za sposób zawarcia i jednocześnie (samo)wykonania umowy, o ile taki jest jego cel i treść kodu (programu). Może być również sposobem wykonania umowy zawartej w inny sposób. Smart contracts mogą występować również jako niezależni (autonomiczni) „agenci”, którzy negocjują, dokonują wyboru smart contract, którego celem będzie zawarcie i wykonanie umowy lub innej czynności wywołującej skutki prawne”⁸.

Smart contracts nie stanowią jednolitej kategorii. D. Szostek dokonał podziału inteligentnych kontraktów w oparciu o poniższe kryteria. Pod względem dostępu i możliwości zawarcia umowy „inteligentne kontrakty” można sklasyfikować jako: otwarte – dostępne dla nieograniczonej grupy osób (w tym zagraniczne podmioty; częściowo otwarte (np. dla podmiotów z określonego terytorium, np. UE) lub zamknięte – tylko dla określonej grupy. Z kolei pod względem ilości stron „inteligentne kontrakty” można sklasyfikować jako dwustronne lub wielostronne. Natomiast w zakresie przedmiotu umowy „inteligentne kontrakty” można sklasyfikować jako: związane z gospodarką cyfrową; kojarzone z tradycyjną gospodarką lub hybrydy⁹.

Na podstawie powyższych uwag można stwierdzić, iż inteligentne kontrakty stanowią nowe i perspektywiczne rozwiązanie mieszczące się w ramach prawa cywilnego, dzięki którym można zwiększyć efektywność, szybkość i bezpieczeństwo obrotu gospodarczego.

⁷ P. Gałka, S. Ciach, *Blockchain a prawo: mapa drogowa najważniejszych zagadnień*, „Krytyka Prawa” tom 11, nr 2/2019, s. 70–71.

⁸ M. Pecyna, A. Behan, *dz. cyt.*, s. 207.

⁹ D. Szostek, *dz. cyt.*, s. 123.

Technologia blockchain powszechnie kojarzona jest z kryptowalutami (zwłaszcza z Bitcoinem), a zatem ze sferą finansów, która normatywnie ujęta jest w ramy prawa finansowego. Ta gałąź prawa oprócz walut wirtualnych, w tym kryptowalut, obejmuje także m.in. podatki z nimi związane, jak również giełdy kryptowalut oraz nadzór finansowy nad nimi. Kluczowego znaczenia nabiera więc zdefiniowanie kryptowalut i określenie ich istoty na podstawie obowiązujących przepisów prawa.

Waluty cyfrowe uznaje się w myśl art. 44 k.c. za postać mienia oraz inny niż pieniądź miernik wartości, na co wskazuje art. 358 § 2 k.c. Nie są przedmiotami materialnymi, a zatem nie mogą być uznane za rzeczy – są natomiast zwykłym prawem majątkowym.

Kryptowaluty jako tzw. tokeny płatnicze, w myśl stanowiska Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami z dnia 10 grudnia 2020 r., „służą jako środek wymiany za dobra lub usługi (zewnętrzne w stosunku do ekosystemu tego aktywa cyfrowego) i jako takie mogą pełnić rolę odpowiadającą środkom płatniczym. Nie stanowią jednak zalegalizowanego środka płatniczego (o ile nie będą spełniać wymogów formalnoprawnych określonych dla pieniądza elektronicznego) – nie są emitowane przez bank centralny lub inny organ publiczny, nie posiadają gwarantowanej przepisami prawa zdolności do umarzania zobowiązań pieniężnych, a „płatność” nimi może być dokonana jedynie wtedy, gdy wierzyciel wyrazi wolę przyjęcia takiej „płatności” i zwolnienia dłużnika z zobowiązania pieniężnego”¹⁰.

Legalną definicję kryptowaluty w polskim porządku prawnym odnaleźć można w art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu¹¹.

Zgodnie z przytoczonym przepisem pod pojęciem waluty wirtualnej rozumie się cyfrowe odwzorowanie wartości, które nie jest: prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej, międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące, pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, instrumentem finansowym

¹⁰ Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, Urząd Komisji Nadzoru Finansowego, wyd. 10 grudnia 2020 r. s. 12.

¹¹ Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. 2022.593).

w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, wekslem lub czekiem – oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego. Prawodawca, formułując powyższą definicję, przeciął wątpliwości związane z określeniem istoty kryptowalut i ujęciem jej w ramy prawne¹².

Wspomnieć należy jeszcze o kwestii opodatkowania kryptowalut. Otóż w Polsce przychody uzyskane ze sprzedaży kryptowalut przez osoby fizyczne podlegają opodatkowaniu podatkiem dochodowym od osób fizycznych¹³. Przychody te są opodatkowane według skali określonej w art. 27 przedmiotowej ustawy, w zależności od sumy przychodów podatnika, w danym roku podatkowym. Aktualnie pierwszy próg podatkowy wynosi 12% – w przypadku sumy dochodów brutto do 120 000 złotych, a drugi próg podatkowy – 32%, w przypadku sumy dochodów brutto przekraczającej tę kwotę.

Wspomnieć należy jeszcze, że w przypadku (dochodów) pochodzących z nieujawnionych źródeł, chociażby z DAO (kryptowalut), dochody te opodatkowuje się stawką 75% podatku dochodowego¹⁴. Kryptowaluty wraz z ich rozwojem mogą stać się w przyszłości poważnym źródłem dochodów Skarbu Państwa. Kwestia ta będzie z pewnością z upływem czasu nabierała znaczenia.

Odnosząc się do kwestii giełdy kryptoaktywów jako platformy obrotu wspomnianymi aktywami, zaznaczyć trzeba, że umożliwia ona uczestnikom platformy dokonania transakcji wymiany waluty fiducjarnej na kryptoaktywo bądź też wymianę kryptoaktywa na inne kryptoaktywo lub też ułatwia uczestnikom rynku dokonywanie takich transakcji czy też przekazywanie zleceń nabycia kryptoaktywa¹⁵. Jak trafnie wskazuje M. Strzelbicki, „Objęcie giełdy kryptowalut przepisami ustawy o usługach płatniczych ma tę konsekwencję dla podmiotu giełdę prowadzącego, że musi on dokonać wyboru jednej z form wykonywania działalności określonych przepisami ustawy (tak zwanego dostawcą usług płatniczych — zamknięty katalog dostawców zawarto w art. 4 ust. 2 ustawy

¹² Szerzej na ten temat patrz np. M. Wnęk, *Natura prawna kryptowaluty*, Warszawa 2023 z podaną tam literaturą.

¹³ Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz.U. 2022.2647).

¹⁴ J. Prokurat, *DAO a podatki – wybrane zagadnienia*, 2016, s. 39, Blockchain, inteligentne kontrakty i DAO (wardynski.com.pl) data dostępu 27.05.2023.

¹⁵ *Stanowisko KNF w sprawie wydawania i obrotu kryptoaktywami*, op.cit. s. 34.

o usługach płatniczych), spełnić warunki jej prowadzenia i ostatecznie uzyskać od KNF (Komisji Nadzoru Finansowego) stosowne zezwolenie, względnie wpis w rejestrze działalności regulowanej”¹⁶.

Prawodawca, wprowadzając wymóg uzyskania zezwolenia bądź wpisu na prowadzenie giełdy kryptowalut, dąży do zapewnienia minimum bezpieczeństwa obrotu gospodarczego dla jej uczestników. Rozwiązanie to, zdaniem autorów, należy uznać za zasadne, albowiem absolutna swoboda w tworzeniu powyższych platform i nadmierna anonimizacja podmiotów korzystających z ich usług ułatwia popełnianie szeregu przestępstw. Również poddanie działalności w zakresie walut wirtualnych wymogom niekaralności (art. 129n ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowania terroryzmu¹⁷, zwana dalej w skrócie upft) oraz posiadania odpowiedniej wiedzy lub doświadczenia (art. 129o upft) należy uznać za zasadne. Co więcej, ustawa ta formułuje odpowiedzialność karnoprawną za przestępstwa związane z niedopełnieniem obowiązków w niej określonych (art. 156 upft), a także za udaremnianie lub utrudnianie przeprowadzenie czynności kontrolnych (art. 157 upft). Wydaje się, że wprowadzenie możliwości zastosowania wobec sprawców przestępstw wskazanych w upft sankcji karnoprawnej zwiększa pewność obrotu gospodarczego i w pewnej mierze pełni funkcję prewencyjną oraz odstraszającą.

Na podstawie powyższych uwag jako zasadna jawi się teza, iż technologia blockchain w coraz szerszym zakresie staje się przedmiotem uregulowań prawnych. Zakres jej funkcjonalności powiększa się, co wymusza na prawodawcy stosowną reakcję normatywną. Nie bez powodu przecież uznano już w starożytności, iż prawo jest sztuką tego co dobre i słuszne (*Ius est ars boni et aequi* – Celsus), a zatem poddanie technologii blockchain powinno wywołać pozytywne rezultaty, z jednej strony zwiększając dostępność i szybkość realizowanych operacji, z drugiej zaś pewność i bezpieczeństwo podmiotów w nich uczestniczących.

¹⁶ M. Strzelbicki, *Kryptowaluty jako przedmiot działalności gospodarczej – wybrane uwagi*, „Acta Universitatis Wratislaviensis” No 3977 PRAWO CCCXXIX Wrocław 2019, s. 396.

¹⁷ Tekst jednolity Dz.U.2022.593.

Zastosowanie technologii blockchain w instytucjach finansowych – przykłady

Technologia blockchain coraz częściej jest wykorzystywana w instytucjach finansowych. Argumentami przemawiającymi za jej zastosowaniem są: bezpieczeństwo transakcji, szybkość rozliczeń, jak również zmniejszenie kosztów przesyłania pieniędzy. Pozwala zatem na oszczędzenie czasu i pieniędzy przez instytucje finansowe. Obecne rozwiązania blockchain zapewniają bowiem techniczne środki bezpieczeństwa dotyczące technik kryptograficznych, które łączą w sekwencje kolejno utworzone bloki danych; niezmiennie i odporne na manipulacje transakcje; protokół konsensusu w zdecentralizowanej sieci transakcji; replikowane dane i pełną ścieżkę audytu wykonanych transakcji; cyfrowe tożsamości i podpisy cyfrowe; inteligentne kontrakty – inteligentne transakcje¹⁸.

Jak wskazuje A. Czajkowski „Na polskim rynku jako pierwsze blockchain zaimplementowało PKO BP, które wydało decyzję o inwestycji w nośnik danych firmy Hyperledger Fabric. Ponadto, Bank przeznaczył fundusze na badania prowadzone przez Politechnikę Warszawską. Celem programu rozwojowego jest stworzenie skutecznego systemu obrotu wirtualnymi tokenami, które PKO chce wdrożyć do oferty w niedalekiej przyszłości. PKO BP ma zamiar uruchomić platformę nie tylko do obsługi tokenów, ale także tworzenia tzw. smart kontraktów. Mają one pozwolić na uproszczenie i przyspieszenie procesów niezbędnych do zawierania kontraktów. Smart kontrakty w przyszłości mają zastąpić tradycyjne polisy ubezpieczeniowe i akredytywy. Docelowo mogą także zastąpić standardowe umowy kredytowo-depozytowe. W ten sposób blockchain umożliwia diametralną redukcję kosztów obsługi”¹⁹. W ślad za bankiem PKO BP poszły inne instytucje finansowe, „Alior Bank po raz pierwszy wykorzystał blockchain publiczny, umożliwiając klientom sprawdzenie autentyczności dokumentów bankowych. Również ING Bank Śląski poinformował niedawno o wzięciu udziału w pilotażowej transakcji finansowania handlu w oparciu o technologię blockchain. W tyle nie pozostaje także bankowość spółdzielcza – Bank Spółdzielczy w Toruniu latem

¹⁸ B. Rutkowski, *Blockchain – aspekty technologiczne oraz przykłady zastosowań* (lazarski.pl) (dostęp: 02.06.2023).

¹⁹ Praktyczne zastosowania technologii blockchain | CrypS (dostęp: 02.06.2023).

2019 roku poinformował o wdrożeniu rozwiązania opartego na systemie bloków rozproszonych”²⁰.

Podzielić należy ponadto twierdzenie D. Zimnoch, iż „Ze względu na płynące korzyści banki (i inne instytucje finansowe) upatrują szansę wdrożenia i testują technologię blockchain m.in. w następujących obszarach: – płatności, – umowy, wnioski, kontrakty, – aktualizacja danych o kliencie, – procesy identyfikacji klientów (know your customer, KYC oraz przeciwdziałanie praniu pieniędzy – anti money laundering, AML), – finansowanie handlu, – ubezpieczenia i polisy”²¹.

Instytucje finansowe chętnie korzystają z technologii blockchain i wydaje się, że jest to stały trend. Technologia ta, coraz powszechniej stosowana, umożliwia szybszy, pewniejszy i bardziej bezpieczny obrót finansowy²². Zakres i możliwości jej stosowania przez świat finansów trudno jednoznacznie określić, granice są bowiem wciąż jeszcze płynne. Dalszy jej rozwój zależy od kreatywności i pomysłowości ludzkiej, która jest źródłem sukcesu każdej organizacji, w tym oczywiście i instytucji finansowych.

Wybrane problemy wykorzystania technologii blockchain w cyberbezpieczeństwie

W zakresie wykorzystania technologii blockchain w rozwiązaniach ICT instytucji finansowych należy wskazać znaczący argument związany z cyberbezpieczeństwem.

Jak w swoich badaniach wskazują m.in. N. Moosavi i H. Taherdoost²³, aplikacje blockchain mogą zapewnić rozwiązania w zakresie cyberbezpieczeństwa w różnych przypadkach i branżach takich jak IoT, opieka zdrowotna czy analizowany sektor finansowy. Należy mieć jednak na uwadze wnikliwą analizę tej technologii, która powinna opierać się

²⁰ *Blockchain – rewolucja w sektorze finansowym?* – Kochański & Partners (kochanski.pl) (dostęp: 02.06.2023).

²¹ D. Zimnoch, *Wpływ technologii Blockchain na efektywność banku*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach” 2016 nr 281, s. 227–228.

²² Szerzej na ten temat, patrz np.: P. Międlar, *Blockchain w systemie finansowym*, „Studia i Prace Kolegium Zarządzania i Finansów” 2019 Nr 173, s. 77–88, czy H. Kołodziejczyk, *Zastosowanie technologii blockchain w finansach*, [w:] K. Perez (red.), *Innowacja finansowe w gospodarce 4.0*, Poznań 2021, s. 9–27.

²³ N. Moosavi, H. Taherdoost, *Blockchain Technology Application in Security: A Systematic Review*, „Blockchains” 2023; 1(2):58–72. <https://doi.org/10.3390/blockchains1020005>.

na wyborze typu kategoryzacji blockchain (publiczny, prywatny, konsorcjum), różnych algorytmów konsensusu (PoW, PBFT, PoA) czy też możliwości wykorzystania otwartych platform blockchain, takich jak Ethereum i Hyperledger Fabric, oraz integracji blockchain z innymi technologiami opartymi na oprogramowaniu. Bardzo ważny jest zatem wybór rodzaju kategoryzacji blockchain według różnych wymagań i warunków różnych przypadków użycia. Jak wskazano w powyższych rozważaniach, blockchain dzieli się bowiem na trzy typy: publiczny, prywatny i konsorcjum. Publiczne łańcuchy bloków to łańcuchy bloków bez uprawnień, w których każdy użytkownik może wejść do sieci, w przeciwieństwie do sieci prywatnej, w której dostęp do sieci mogą uzyskać tylko autoryzowani użytkownicy jednej organizacji. Blockchain konsorcjum to połączenie łańcucha publicznego i prywatnego, w którym w sieci znajduje się więcej niż jedna organizacja²⁴. Wspomniani wyżej autorzy N. Moosavi i H. Taherdoost w swoich badaniach odpowiadają na różne pytania badawcze dotyczące kwestii bezpieczeństwa, np. w jakich znanych domenach stosowane są aplikacje zabezpieczające typu blockchain i jakie są ich konkretne przypadki użycia. Wyniki ich badań wykazują, że najczęstsze przypadki użycia rozwiązań bezpieczeństwa typu blockchain dla sieci IoT dotyczą uwierzytelniania i autoryzacji urządzeń oraz implementacji bezpiecznej sieci zapewniającej poufność danych²⁵. Podobne kwestie wykorzystania i użycia dla gwarantowania odpowiedniej ochrony przechowywania i zarządzania danymi osobowymi, może dotyczyć również każdego sektora infrastruktury krytycznej w tym instytucji finansowych.

Analizy dotyczące możliwości wykorzystania blockchain w bezpieczeństwie potwierdzają się w innych wynikach badań empatycznych np. dotyczących skalowalnych elektronicznych systemów głosowania opartych na blockchain, zgodnie z którymi technologia ta została wdrożona w wielu różnych obszarach jako część infrastruktury niektórych firm wymagających przejrzystości, integralności i niezawodności. Godne zaufania środowisko blockchain i przyjazna dla użytkownika sieć dają skuteczne wyniki, które zwiększają zaufanie między stronami²⁶. Cyber-

²⁴ Szerzej na ten temat, patrz np.: D. Yaga, P. Mell, N. Roby, K. Scarfone, *Blockchain technology overview*, National Institute of Standards and Technology, U.S. Department of Commerce 2018, <https://doi.org/10.6028/NIST.IR.8202>.

²⁵ N. Moosavi, H. Taherdoost, *Blockchain Technology Application in Security: A Systematic Review*, "Blockchains" 2023; 1(2):58–72. <https://doi.org/10.3390/blockchains1020005>.

²⁶ Por. U. Jafar, M.J. Ab Aziz, Z. Shukur, H.A. Hussain, *A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems*, Sensors 2022, 22, 7585.

bezpieczeństwo i ochrona danych osobowych mają ogromne znaczenie w sektorze finansowym, a technologia blockchain staje się w tym zakresie wyzwaniem. Od technik ochrony prywatności i technik szyfrowania po kompleksowe ramy kontroli dostępu, blockchain może zapewniać zatem rozwiązania w zakresie cyberbezpieczeństwa, np. w zakresie niezawodnego i bezpiecznego środowisko zarządzania danymi poprzez budowanie zaufania i zapewnienie zgodności z rygorystycznymi regulacjami prawnymi w zakresie cyberbezpieczeństwa. Mając na uwadze powyższe, należy wskazać, że niezbędną kwestią do pomyślnego przejścia na technologię blockchain jest jednak płynna integracja z istniejącymi systemami w danej branży.

Zakończenie

Artykuł miał na celu przedstawienie wybranych problemów wykorzystania technologii blockchain w instytucjach finansowych i w cyberbezpieczeństwie w świetle polskich (krajowych) uregulowań prawnych. Technologia blockchain stale się rozwija, pokonując różne wyzwania i przyczyniając się do rozwoju sektora finansowego w kierunku skutecznej, skoncentrowanej, bezpiecznej cyfrowej transakcji. Technologia blockchain będzie miała zatem wpływ na cyberbezpieczeństwo w miarę jej rozwoju, zmieniając sposób przechowywania, udostępniania, wykorzystywania danych. Od technik ochrony prywatności i technik szyfrowania po kompleksowe ramy kontroli dostępu, blockchain może dać podstawę rozwoju bezpiecznych systemów np. sektora finansowego. Zmiany te tworzą bardziej niezawodne i bezpieczne środowisko zarządzania sferą finansową poprzez budowanie zaufania i zapewnienie zgodności z rygorystycznymi przepisami prawa w zakresie cyberbezpieczeństwa np. względem nowej dyrektywy 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE (NIS 2).

Bibliografia

- Blockchain – rewolucja w sektorze finansowym?*, Kochański & Partners (kochanski.pl) (dostęp: 02.06.2023).
- Czarnecki J., *Czym są inteligentne kontrakty i DAO, Blockchain, inteligentne kontrakty i DAO* (wardynski.com.pl) (dostęp: 27.05.2023).
- Gałka P., Ciach Sz., *Blockchain a prawo: mapa drogowa najważniejszych zagadnień*, Krytyka Prawa, tom 11, nr 2/2019.
- Jafar, U.; Ab Aziz, M.J.; Shukur, Z.; Hussain, H.A. *A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems*. *Sensors* 2022, 22, 7585.
- Kołodziejczyk H., *Zastosowanie technologii blockchain w finansach* [w:] K. Perez (red.), *Innowacja finansowe w gospodarce 4.0*, Poznań 2021.
- Leksykon pojęć na temat technologii blockchain i kryptowalut*, (ictbanking.net) (data dostępu 25.05.2023).
- Międlar P., *Blockchain w systemie finansowym*, *Studia i Prace Kolegium Zarządzania i Finansów*, 2019 nr 173.
- Moosavi N, Taherdoost H. *Blockchain Technology Application in Security: A Systematic Review*. *Blockchains*. 2023; 1(2) <https://doi.org/10.3390/blockchains1020005>.
- Pecyna M., Behan A., *Smart Contracts – nowa technologia prawa umów?*, *Transformacje prawa prywatnego* 2020/3.
- Prokurat J., *DAO a podatki – wybrane zagadnienia*, 2016.
- Rutkowski B., *Blockchain – aspekty technologiczne oraz przykłady zastosowań* (lazarski.pl) (dostęp: 02.06.2023).
- Strzelbicki M., *Kryptowaluty jako przedmiot działalności gospodarczej – wybrane uwagi*, *Acta Universitatis Wratislaviensis*, No 3977 PRAWO CCCXXIX, Wrocław 2019.
- Szabo N., *Smart Contract: Formalizing and Securing Relationships on Public Networks*, *View of Formalizing and Securing Relationships on Public Networks | First Monday* (dostęp: 26.05.2023).
- Szostek D., *Blockchain i prawo*, Baden – Baden 2019.
- Wnęk M., *Natura prawna kryptowaluty*, Warszawa 2023.
- Yaga D., Mell P., Roby N., Scarfone K. *Blockchain technology overview*, *National Institute of Standards and Technology*, U.S. Department of Commerce 2018, <https://doi.org/10.6028/NIST.IR.8202>.
- Zimnoch D., *Wpływ technologii Blockchain na efektywność banku*, *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, 2016 nr 281.

Źródła prawa:

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tj. Dz. U. 2022.593).

Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tj. Dz.U. 2022.2647).

Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami, UKNF, dn. 10 grudnia 2020 r.

