Ewelina Melaniuk[1]

Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103359_18

ROLA WIRTUALNEGO PIENIĄDZA W ROZWOJU GOSPODARKI CYFROWEJ

THE ROLE OF VIRTUAL CURRENCY IN THE DEVELOPMENT OF THE DIGITAL ECONOMY

Streszczenie

Wirtualny pieniądz stanowi istotny komponent infrastruktury gospodarki cyfrowej, jednocześnie generując nowe wyzwania w obszarze cyberbezpieczeństwa. Celem rozdziału jest analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy bezpieczeństwa systemów informatycznych, ochrony transakcji oraz zarządzania ryzykiem cybernetycznym. Badanie oparto na analizie literatury naukowej, raportów zespołów CERT, instytucji nadzorczych oraz dokumentów branżowych. W rozdziale dokonano klasyfikacji form wirtualnego pieniądza, obejmującej kryptowaluty, stablecoiny, waluty wirtualne platform cyfrowych oraz cyfrowe waluty banków centralnych (CBDC), z uwzględnieniem ich podatności na zagrożenia takie jak phishing, malware, ransomware, ataki na giełdy kryptowalut oraz nadużycia

[1] https://orcid.org/0009-0002-9434-6258, e-mail: e.melaniuk@dyd.akademiabialska.pl

związane z kradzieżą kluczy kryptograficznych. Wyniki analizy wskazują, że wirtualny pieniądz przyczynia się do rozwoju gospodarki cyfrowej, lecz równocześnie zwiększa powierzchnię ataku oraz złożoność architektury bezpieczeństwa. Wnioski podkreślają konieczność integracji mechanizmów cyberochrony, w tym kryptografii, monitorowania transakcji, edukacji użytkowników oraz ram regulacyjnych, jako warunku bezpiecznego rozwoju ekosystemów finansów cyfrowych.

Słowa kluczowe: wirtualny pieniądz, cyberbezpieczeństwo, zagrożenia cyfrowe, kryptografia, bezpieczeństwo transakcji, gospodarka cyfrowa

Abstract

Virtual money constitutes a critical component of the digital economy infrastructure while simultaneously introducing new challenges in the field of cybersecurity. The aim of this chapter is to examine the role of virtual money in the development of the digital economy from the perspective of information system security, transaction protection, and cyber risk management. The study is based on a review of academic literature, CERT reports, supervisory authority publications, and industry documents. The chapter provides a classification of virtual money forms, including cryptocurrencies, stablecoins, virtual currencies of digital platforms, and central bank digital currencies (CBDCs), with particular attention to their exposure to threats such as phishing, malware, ransomware, attacks on cryptocurrency exchanges, and abuses related to the theft of cryptographic keys. The findings indicate that while virtual money supports the growth of the digital economy, it also expands the attack surface and increases the complexity of security architectures. The conclusions emphasize the necessity of integrating cybersecurity mechanisms, including cryptography, transaction monitoring, user awareness, and regulatory frameworks, as a prerequisite for the secure development of digital finance ecosystems.

Keywords: virtual money, cybersecurity, digital threats, cryptography, transaction security, digital economy

Wstęp

Wraz z dynamicznym rozwojem technologii informacyjno-komunikacyjnych i cyfryzacją gospodarki tradycyjne formy pieniądza ulegają zasadniczym przemianom. Coraz większe znaczenie zyskują formy pieniądza wirtualnego, obejmujące kryptowaluty, waluty wirtualne w ekosystemach

cyfrowych oraz cyfrowe waluty banków centralnych (Central Bank Digital Currencies, CBDC). Te instrumenty finansowe stają się nie tylko medium wymiany, ale również kluczowym elementem infrastruktury gospodarki cyfrowej, w której transakcje finansowe, handel elektroniczny i usługi finansowe są realizowane głównie w środowisku cyfrowym. Kryptowaluty takie jak Bitcoin czy Ethereum zrewolucjonizowały postrzeganie pieniądza, oddzielając go od formy fizycznej i podkreślając jego cyfrową naturę jako środka wymiany i przechowywania wartości (Ryś, 2023).

Wirtualny pieniądz, zwłaszcza w postaci CBDC, staje się przedmiotem rosnącego zainteresowania banków centralnych i regulatorów na całym świecie. Banki centralne podejmują prace nad cyfrowymi wersjami pieniądza fiducjarnego, które mają potencjał usprawnienia płatności detalicznych i transgranicznych, zwiększenia efektywności systemów płatniczych oraz poprawy inkluzji finansowej. Jednak równocześnie pojawiają się istotne wyzwania w obszarze cyberbezpieczeństwa, integralności systemów, ochrony prywatności oraz ryzyka technicznego (Gasz, Smalara, 2025).

Bezpieczeństwo cyfrowych systemów pieniężnych jest kluczowe dla ich stabilności i zaufania społecznego. Badania wskazują, że wprowadzenie CBDC oraz innych form pieniądza cyfrowego wiąże się z szeregiem zagrożeń cybernetycznych, takich jak kradzież lub przejęcie danych uwierzytelniających, podatności na ataki typu „double spending", denials-of-service oraz naruszenia integralności systemu transakcyjnego (WEF, 2021; IMF, 2024). Jednocześnie infrastrukturę tych systemów mogą stanowić atrakcyjne cele dla cyberprzestępców, co wpływa na konieczność wdrożenia kompleksowych mechanizmów ochronnych, w tym zaawansowanej kryptografii, monitorowania anomalii w czasie rzeczywistym oraz odporności na incydenty (Fed, 2022).

W literaturze podkreśla się również kwestie prawne i regulacyjne związane z emisją i wdrażaniem CBDC oraz kryptowalut, których brak harmonizacji w skali globalnej stanowi barierę dla ich powszechnego przyjęcia oraz efektywnego nadzoru ryzyka (Karpiuk-Wawryszuk, 2023). Ponadto intensywna cyfryzacja systemów finansowych zwiększa powierzchnię ataku, co wymaga od instytucji finansowych i regulatorów sprostania zarówno tradycyjnym, jak i nowym zagrożeniom w cyberprzestrzeni.

Celem niniejszego rozdziału jest analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy cyberbezpieczeństwa

i zarządzania ryzykiem. Podjęto próbę kompleksowego ujęcia tego zjawiska poprzez klasyfikację form wirtualnego pieniądza oraz wskazanie, w jaki sposób ich adopcja wpływa na funkcjonowanie cyfrowych systemów finansowych, a także jakie ryzyka cybernetyczne i organizacyjne są z tym związane. Przyjęte podejście opiera się na przeglądzie literatury naukowej, analizie raportów instytucjonalnych oraz przeglądzie istotnych badań w obszarze finansów cyfrowych i bezpieczeństwa informatycznego.

Znaczenie wirtualnego pieniądza w rozwoju gospodarki cyfrowej

Wirtualny pieniądz, obejmujący kryptowaluty, stablecoiny i cyfrowe waluty banków centralnych (CBDC), odgrywa coraz istotniejszą rolę w transformacji cyfrowej gospodarki. Umożliwia szybkie i bezpośrednie transakcje finansowe, rozwój innowacyjnych modeli biznesowych, zwiększa płynność rynków i wspiera ekspansję globalną przedsiębiorstw (IMF, 2024; Schär, 2021). Poniżej przedstawiono cztery kluczowe obszary wpływu wirtualnego pieniądza na gospodarkę cyfrową: wspieranie zdecentralizowanych finansów (DeFi), tokenizacja aktywów, integracja z płatnościami cyfrowymi i e-commerce oraz wyzwania cyberbezpieczeństwa i zaufania.

Zdecentralizowane finanse (DeFi) stanowią jedno z najważniejszych zastosowań wirtualnego pieniądza. Umożliwiają bezpośrednie transakcje peer-to-peer, bez potrzeby angażowania pośredników bankowych. Eliminuje to koszty pośrednictwa, skraca czas realizacji transakcji oraz zwiększa efektywność systemów finansowych (Schär, 2021).

Platformy takie jak Ethereum i Binance Smart Chain pozwalają tworzyć smart kontrakty – samowykonujące się umowy kodowane w blockchainie – które mogą obsługiwać pożyczki, ubezpieczenia czy wymianę tokenów. Smart kontrakty automatyzują procesy, minimalizując ryzyko błędów ludzkich oraz opóźnień w transakcjach. Przykładem jest protokół Aave, który umożliwia użytkownikom zdeponowanie środków i udzielanie pożyczek bez pośrednictwa banku, z pełną kontrolą nad własnym kapitałem i transparentnym systemem odsetek (Schär, 2021).

W kontekście cyberbezpieczeństwa, DeFi stawia przed uczestnikami rynku wyzwania związane z lukami w smart kontraktach i ryzykiem ataków typu flash loan, które mogą prowadzić do strat finansowych w krótkim

czasie. Dlatego istotna jest integracja mechanizmów audytu kodu, monitoring transakcji i edukacja użytkowników (Raz i in., 2025).

Tokenizacja aktywów realnych stanowi kolejny istotny obszar wpływu wirtualnego pieniądza na gospodarkę cyfrową. Poprzez reprezentowanie fizycznych aktywów, takich jak nieruchomości, dzieła sztuki, obligacje czy papiery wartościowe, w postaci tokenów cyfrowych, możliwe staje się frakcjonowanie własności i zwiększenie płynności rynkowej (OECD, 2024). Przykładem jest projekt tokenizacji nieruchomości w Singapurze (2024), który umożliwił globalnym inwestorom zakup udziałów w lokalnych obiektach komercyjnych. Dzięki tokenizacji inwestorzy mogą nabywać ułamkowe udziały, co znacznie obniża barierę wejścia na rynek nieruchomości i umożliwia łatwiejszą dywersyfikację portfela inwestycyjnego (OECD, 2024).

Tokenizacja wspiera także rozwój cyfrowych rynków kapitałowych, w tym emisji tokenów reprezentujących akcje lub obligacje. Umożliwia przyspieszenie procesu pozyskiwania kapitału, automatyzację rozliczeń i zwiększenie przejrzystości transakcji. Z punktu widzenia bezpieczeństwa cybernetycznego, niezbędne są mechanizmy kryptograficzne chroniące przed manipulacją danymi, zabezpieczanie portfeli cyfrowych i audyt smart kontraktów (ENISA, 2023).

Stablecoiny i CBDC odgrywają kluczową rolę w usprawnianiu płatności cyfrowych, szczególnie w handlu transgranicznym. Pozwalają na szybkie, niskokosztowe i bezpieczne transakcje, co zwiększa efektywność przedsiębiorstw i poprawia doświadczenie klienta (IMF, 2024). Przykładem praktycznego zastosowania jest projekt CBDC w Bahrajnie (Project Dinar), który umożliwił przeprowadzanie transgranicznych płatności w czasie rzeczywistym, skracając czas rozliczenia z kilku dni do kilku minut. Integracja wirtualnego pieniądza z systemami e-commerce pozwala również na wdrażanie nowych modeli biznesowych, takich jak mikropłatności w usługach cyfrowych, subskrypcje w grach online czy tokenizacja lojalności klientów.

W kontekście cyberbezpieczeństwa, systemy płatnicze muszą zapewniać integralność i poufność transakcji, odporność na ataki typu man-in-the-middle oraz skuteczny monitoring sieci w czasie rzeczywistym. CBDC i stablecoiny wprowadzają też nowe wyzwania regulacyjne, wymagając współpracy międzynarodowej w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (FATF, 2022).

W miarę jak wirtualny pieniądz staje się powszechny, rośnie także ryzyko ataków cybernetycznych, błędów w systemach oraz utraty zaufania społecznego (ENISA, 2023). Zagrożenia obejmują kradzież kluczy prywatnych, manipulacje smart kontraktami, ransomware na giełdach kryptowalut oraz ataki typu 51% w zdecentralizowanych sieciach blockchain.

Bezpieczeństwo systemów wirtualnego pieniądza wymaga:

- integracji zaawansowanych technologii kryptograficznych,
- monitoringu transakcji w czasie rzeczywistym i wykrywania anomalii,
- audytów smart kontraktów i zabezpieczeń portfeli cyfrowych,
- edukacji użytkowników w zakresie bezpiecznego korzystania z cyfrowych aktywów,
- regulacji minimalizujących ryzyko oszustw i cyberprzestępczości (Gasz, Smalara, 2025; Raz i in., 2025).

Zaufanie uczestników rynku jest warunkiem rozwoju wirtualnego pieniądza w gospodarce cyfrowej. Bezpieczeństwo, przejrzystość i zgodność regulacyjna są kluczowe, aby wirtualny pieniądz mógł wspierać innowacje, inwestycje i ekspansję cyfrowych usług finansowych.

Zagrożenia cyberbezpieczeństwa w systemach wirtualnego pieniądza

Wprowadzenie wirtualnego pieniądza do gospodarki cyfrowej wiąże się z istotnymi ryzykami w obszarze cyberbezpieczeństwa. Systemy oparte na kryptowalutach, CBDC i platformach cyfrowych zwiększają powierzchnię ataku, stwarzając nowe wyzwania dla instytucji finansowych i użytkowników końcowych.

Podstawowym zagrożeniem są ataki skierowane na infrastrukturę systemów płatniczych i giełd kryptowalutowych. Przykłady obejmują kradzież środków z portfeli cyfrowych w wyniku błędów w smart kontraktach lub luk w zabezpieczeniach giełd (np. atak na platformę Binance w 2022 r., gdzie skradziono kryptowaluty o wartości ok. 6,5 mln USD) (Binance, 2022). Ataki te mogą prowadzić do strat finansowych oraz do utraty zaufania do całego systemu cyfrowych płatności (Kshetri, Bhushal, Pandey, 2022).

Kolejnym istotnym zagrożeniem jest przejęcie kluczy prywatnych użytkowników oraz ataki phishingowe. W cyberprzestrzeni powstają

wyspecjalizowane kampanie malware, które wyłudzają dane uwierzytelniające do portfeli cyfrowych. Przykładem jest kampania „CryptoStealer" z 2023 r., w której zainfekowano setki komputerów i przejęto dostęp do portfeli kryptowalutowych użytkowników (ENISA, 2023).

Wirtualne pieniądze, szczególnie kryptowaluty w sieciach zdecentralizowanych, narażone są na double-spending, czyli próbę wielokrotnego wydania tej samej jednostki cyfrowej. Takie ataki mogą być przeprowadzane przez podmioty kontrolujące znaczną część mocy obliczeniowej sieci (atak 51%), jak miało to miejsce w przypadku kryptowaluty Ethereum Classic (Sayeed, Marco-Gisbert, 2019).

Cyfrowe waluty banków centralnych (CBDC) wprowadzają nowe ryzyka, związane z integracją systemów bankowych z infrastrukturą cyfrową. Problemy techniczne, awarie serwerów oraz błędy w protokołach bezpieczeństwa mogą powodować przerwy w świadczeniu usług płatniczych i ograniczać zaufanie użytkowników. IMF (2024) podkreśla, że wdrażanie CBDC wymaga rygorystycznych testów odpornościowych i ciągłego monitorowania zagrożeń cybernetycznych.

Platformy handlu kryptowalutami i giełdy cyfrowe stają się celem ransomware, które może wymuszać okup w kryptowalutach. Przykład ataku na giełdę w Korei Południowej w 2022 r. pokazał, że złośliwe oprogramowanie może sparaliżować systemy płatnicze i wymusić znaczące straty finansowe (ESET, 2022).

Brak ujednoliconych ram regulacyjnych na poziomie międzynarodowym zwiększa ryzyko wykorzystywania wirtualnego pieniądza do prania pieniędzy, finansowania terroryzmu i działań przestępczych (FATF, 2022). Integracja mechanizmów cyberbezpieczeństwa z polityką regulacyjną jest więc niezbędna, aby zminimalizować ryzyka i zwiększyć odporność systemów (Gasz, Smalara, 2025).

Zagrożenia cyberbezpieczeństwa w systemach wirtualnego pieniądza mają charakter wielowymiarowy: obejmują aspekty techniczne (ataki na infrastrukturę, kradzieże kluczy), operacyjne (błędy integracyjne, niewłaściwe zarządzanie ryzykiem) oraz regulacyjne (niewystarczająca ochrona prawna i brak globalnych standardów). Efektywna adaptacja wirtualnego pieniądza w gospodarce cyfrowej wymaga więc integracji mechanizmów kryptograficznych, monitoringu transakcji, edukacji użytkowników oraz spójnych ram regulacyjnych.

Mechanizmy ochrony i rekomendacje dla cyberbezpieczeństwa w systemach wirtualnego pieniądza

W obliczu rosnących zagrożeń cybernetycznych związanych z wirtualnym pieniądzem konieczne jest opracowanie i wdrożenie kompleksowych mechanizmów ochrony, obejmujących aspekty techniczne i regulacyjne oraz edukacyjne.

Podstawowym elementem ochrony w systemach wirtualnego pieniądza jest wykorzystanie silnych mechanizmów kryptograficznych, takich jak algorytmy szyfrowania klucza publicznego, podpisy cyfrowe i wielopoziomowa weryfikacja transakcji (multi-signature). Systemy CBDC i kryptowaluty powinny również korzystać z protokołów odporności na ataki typu man-in-the-middle, a infrastruktura giełd i portfeli cyfrowych – z zaawansowanych firewalli, systemów wykrywania włamań (IDS/IPS) oraz segmentacji sieci (IMF, 2024; EBA, 2022).

Ważnym mechanizmem ochrony jest ciągłe monitorowanie transakcji w czasie rzeczywistym w celu wykrywania działań nietypowych lub podejrzanych. Systemy oparte na analizie zachowań użytkowników (UBA – User Behavior Analytics) oraz algorytmach sztucznej inteligencji mogą identyfikować próby nieautoryzowanych transferów, ataki phishingowe lub ransomware skierowane na portfele cyfrowe (ENISA, 2023). Przykładem skutecznej implementacji takich rozwiązań jest monitorowanie giełdy Coinbase, która w 2022 r. wykorzystała algorytmy AI do wczesnego wykrycia próby kradzieży środków i zatrzymania ataku.

Ochrona systemów wirtualnego pieniądza wymaga również odporności infrastruktury IT, osiąganej poprzez redundancję serwerów, segmentację sieci i stosowanie technologii chmurowych z geograficznym rozproszeniem danych. Dzięki temu w przypadku awarii lub incydentu cybernetycznego, dostęp do kluczowych funkcji systemu pozostaje zachowany, a ryzyko całkowitej utraty środków minimalizowane (Fed, 2022).

Najczęstszym wektorem ataków są błędy ludzkie, takie jak kliknięcie w złośliwy link w phishingu lub przechowywanie kluczy prywatnych w niechronionych lokalizacjach. Dlatego edukacja użytkowników i personelu instytucji finansowych jest kluczowa. Szkolenia powinny obejmować rozpoznawanie zagrożeń, bezpieczne korzystanie z portfeli cyfrowych, praktyki silnych haseł i uwierzytelniania dwuskładnikowego (2FA) (ESET, 2022).

Skuteczna ochrona cybernetyczna wymaga również spójnych ram regulacyjnych, które narzucają obowiązki w zakresie bezpieczeństwa, raportowania incydentów oraz przeciwdziałania praniu pieniędzy (AML) i finansowaniu terroryzmu (CFT). W Europie ramy MiCA (Markets in Crypto-Assets Regulation) oraz wytyczne FATF stanowią podstawę regulacyjną dla systemów wirtualnego pieniądza, zapewniając równowagę między innowacyjnością a bezpieczeństwem (KarpiukWawryszuk, 2023; FATF, 2022).

Rekomendacje strategiczne dla instytucji:

- integracja rozwiązań bezpieczeństwa w architekturze systemów transakcyjnych i giełd kryptowalut,
- stałe testy penetracyjne i audyty bezpieczeństwa w celu wykrycia luk w systemach,
- współpraca z zespołami CERT i organami nadzoru w celu szybkiego reagowania na incydenty,
- wdrożenie mechanizmów szybkiego backupu i odzyskiwania danych w razie ataku ransomware,
- monitorowanie nowych zagrożeń, w tym ataków wykorzystujących sztuczną inteligencję i automatyzację transakcji.

Bezpieczeństwo wirtualnego pieniądza wymaga wielowarstwowego podejścia, obejmującego kryptografię, monitorowanie transakcji, odporność infrastruktury, edukację użytkowników oraz spójne regulacje. Skuteczna implementacja tych mechanizmów pozwala ograniczyć ryzyko cyberzagrożeń oraz zwiększa zaufanie do systemów cyfrowych i wspiera rozwój gospodarki cyfrowej w sposób bezpieczny i stabilny.

Wnioski

Analiza roli wirtualnego pieniądza w rozwoju gospodarki cyfrowej z perspektywy cyberbezpieczeństwa wskazuje na następujące kluczowe wnioski:

1. Wirtualny pieniądz jako katalizator gospodarki cyfrowej: kryptowaluty, stablecoiny oraz CBDC znacząco wspierają rozwój cyfrowych systemów płatniczych, zwiększają efektywność transakcji oraz

umożliwiają wdrażanie innowacyjnych modeli biznesowych, takich jak DeFi czy tokenizacja aktywów.

2. Wieloaspektowe zagrożenia cyberbezpieczeństwa: systemy wirtualnego pieniądza są narażone na ataki typu phishing, ransomware, kradzież kluczy kryptograficznych oraz manipulację transakcji (np. double-spending). Zagrożenia te podkreślają konieczność integracji mechanizmów ochrony z architekturą systemów finansowych.
3. Znaczenie technologii ochronnych: skuteczna obrona wymaga stosowania zaawansowanej kryptografii, monitorowania transakcji w czasie rzeczywistym, segmentacji infrastruktury i redundancji systemów, a także ciągłego testowania odporności systemów na ataki cybernetyczne.
4. Edukacja i świadomość użytkowników: czynniki ludzkie pozostają jednym z najsłabszych ogniw systemów bezpieczeństwa. Szkolenia, świadomość zagrożeń i praktyki bezpieczeństwa, takie jak uwierzytelnianie dwuskładnikowe i bezpieczne przechowywanie kluczy prywatnych, mają kluczowe znaczenie dla ograniczenia ryzyka.
5. Ramy regulacyjne i nadzór: globalne zróżnicowanie przepisów prawnych stwarza wyzwania dla bezpieczeństwa i stabilności systemów wirtualnego pieniądza. Spójne regulacje, takie jak MiCA w UE czy wytyczne FATF, stanowią podstawę zrównoważonego rozwoju i ochrony uczestników rynku.
6. Zintegrowane podejście do cyberbezpieczeństwa: aby wirtualny pieniądz mógł efektywnie wspierać rozwój gospodarki cyfrowej, niezbędna jest integracja technologii, procedur operacyjnych, edukacji i regulacji. Kompleksowe podejście zwiększa odporność systemów na ataki oraz wspiera zaufanie użytkowników i instytucji finansowych.

Literatura

1. Binance. (2022). *Security notice: Cryptocurrency theft incident report*. Binance. Pobrano z: https://www.binance.com/en/support/announcement/security-2022 (dostęp: 20.12.2025).

2. EBA. (2022). *Risk assessment of crypto-assets: EBA report*. European Banking Authority. Pobrano z: https://www.eba.europa.eu/crypto-assets (dostęp: 20.12.2025).
3. ENISA. (2023). *Threat landscape for cryptocurrencies and virtual assets*. European Union Agency for Cybersecurity. Pobrano z: https://www.enisa.europa.eu/publications/crypto-threats-2023 (dostęp: 20.12.2025).
4. ESET. (2022). *Ransomware attacks targeting cryptocurrency exchanges*. ESET Research. Pobrano z: https://www.eset.com/int/research (dostęp: 20.12.2025).
5. FATF. (2022). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Financial Action Task Force. Pobrano z: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/virtual-assets-guidance.html (dostęp: 20.12.2025).
6. Fed. (2022). *Security considerations for a central bank digital currency*. Federal Reserve. Pobrano z: https://www.federalreserve.gov/econres/notes/feds-notes/security-considerations-for-a-central-bank-digital-currency-20220203.html (dostęp: 20.12.2025).
7. Gasz, M. i Smalara, R. (2025). Cyfrowy pieniądz banku centralnego – analiza korzyści i ryzyk związanych z wprowadzeniem nowego instrumentu płatniczego. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 69*(3), 21-37. https://doi.org/10.15611/pn.2025.3.02
8. IMF. (2024). *Central bank digital currencies: Financial stability implications*. International Monetary Fund. Pobrano z: https://www.imf.org/en/Publications/WP/Issues/2024/01/01 (dostęp: 20.12.2025).
9. Karpiuk-Wawryszuk, N. (2023). Uwarunkowania prawne emisji cyfrowego pieniądza banku centralnego w świetle raportów banków centralnych europejskich państw stojących u progu jego wdrożenia. *Ius et Administratio, 51*(2), 75-93. https://doi.org/10.15584/iuseta.2023.2.6
10. Kshetri, N., Bhushal, C., Pandey, P. (2022). *Blockchain Technology Applications for Cyber Defense and Cybersecurity*. Pobrano z: https://thesai.org/Publications/ViewPaper?Code=IJACSA&Issue=11&SerialNo=40&Volume=13 (dostęp: 20.12.2025).
11. Sayeed, S., Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

12. OECD. (2024). *Tokenisation of assets and digital finance: Implications for financial stability*. OECD Publishing. Pobrano z: https://www.oecd.org/finance/tokenisation-assets (dostęp: 20.12.2025).
13. Ryś, D. (2023). Kryptowaluty oraz waluty cyfrowe w polskich i międzynarodowych uwarunkowaniach prawno-gospodarczych. *Studia Ekonomiczne. Gospodarka, Społeczeństwo, Środowisko, 12*(2), 112-124.
14. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153-174. https://doi.org/10.2139/ssrn.3571335
15. WEF. (2021). *Central bank digital currencies: Key cyber risks and mitigation strategies*. World Economic Forum. Pobrano z: https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies (dostęp: 20.12.2025).