CYFROWY ZŁOTY
BANK CYFROWEJ GOTÓWKI

Sygn. PAB/WIB 6/2023

Raport przygotowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM ANALITYCZNO BADAWCZY

Poznań, kwiecień 2023

O raporcie

Raport **Cyfrowy Złoty** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy

Raport został opracowany przez zespół w składzie:

Prof. dr hab. inż. Wojciech Cellary – jest informatykiem pracującym aktualnie w Uniwersytecie WSB Merito w Poznaniu, a poprzednio na trzech uczelniach w Polsce i sześciu za granicą: we Francji i Włoszech. Był kierownikiem 80 projektów badawczych, głównym organizatorem 60 konferencji naukowych, członkiem komitetów programowych 400 konferencji. Jest autorem 200 publikacji naukowych. Jego aktywność zawodowa obejmuje doradztwo oraz udział w pracach grup eksperckich, komitetów, rad i stowarzyszeń. Wypromował 18 doktorów, z których sześciu uzyskało habilitację, a dwóch tytuł profesora. Na jego wykłady w języku polskim, angielskim i francuskim uczęszczało około 20.000 studentów. Aktualna tematyka badawcza to: gospodarka i społeczeństwo cyfrowe oraz przemysł 4.0.

Dr hab. Paweł Marszałek – profesor Uniwersytetu Ekonomicznego w Poznaniu, kierownik Katedry Pieniądza i Bankowości oraz Dyrektor Studiów w zakresie finansów i rynków finansowych. Specjalizuje się w teorii pieniądza, polityce gospodarczej i historii myśli ekonomicznej, a także zajmuje się problematyką systemów bankowych i finansjalizacji. Autor ponad stu publikacji naukowych, w tym dwóch monografii: „Koordynacja polityki pieniężnej i polityki fiskalnej jako przesłanka stabilności poziomu cen" oraz „Systemy pieniężne wolnej bankowości. Koncepcje, cechy, zastosowanie", nagrodzonej w 2016 roku w II edycji Konkursu o Nagrodę Prezesa NBP za wybitne publikacje książkowe z dziedziny bankowości i finansów. Pełnił m.in. funkcję doradcy Generalnego Inspektora Nadzoru Bankowego, Prodziekana Wydziału Ekonomii UEP oraz Głównego Redaktora Wydawnictw Poznańskiego Towarzystwa Przyjaciół Nauk.

O programie

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

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

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

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

Kontakt

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

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

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

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

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

Spis treści

1. Wstęp

W październiku 2008 roku ukazał się w Internecie artykuł autorstwa tajemniczego Satoshi Nakamoto, który pozostaje nieznany do dzisiaj, pt. „Bitcoin: A Peer-to-Peer Electronic Cash System". Pozostałby on pewnie niezauważony, gdyby kilka miesięcy później, w styczniu 2009 roku, Satoshi Nakamoto nie udostępnił w internecie perfekcyjnie przemyślanego w każdym szczególe, niezwykle innowacyjnego oprogramowania Bitcoinu o otwartym kodzie, którego każdy mógł używać, a także sprawdzić, skopiować i wykorzystać do swoich celów. Tak narodziły się kryptowaluty – nowa, nieznana przedtem forma elektronicznego instrumentu płatniczego, z czasem aspirującego od bycia nową formą pieniądza.

Przekaz Satoshi Nakamoto był zuchwały: nie potrzebujemy banków, w szczególności centralnych, aby mieć pieniądze, w dodatku zabezpieczone przed inflacją, dostępne dla wszystkich na całym świecie, którzy mają dostęp do Internetu. Tymi pieniędzmi, czyli bitcoinami, możemy płacić w sposób pseudonimowy chroniąc swoją prywatność. Nie jesteśmy skazani na zaufanie do banków centralnych, które często nas zawodzą drukując „pusty" pieniądz i prowadząc nieodpowiedzialną politykę pieniężną, bo możemy zaufać algorytmom, które są bezstronne.

Początkowo ten przekaz nie miał żadnego istotnego znaczenia. Jednak powoli, ku zdumieniu banków centralnych, Bitcoin znalazł ludzi zainteresowanych, którzy zaczęli kupować tę kryptowalutę. A Bitcoin z kolei zaczął rosnąć w siłę. W szczytowym momencie, w listopadzie 2021 roku jeden bitcoin kosztował około 63 000 USD, co przy liczbie około 18 milionów wykopanych bitcoinów oznaczało kwotę 1,134 biliona USD ($1{,}134*10^{12}$). Jest to kwota niebagatelna, choć nie aż tak znacząca w gospodarce światowej. Rosło też zainteresowanie innymi kryptowalutami powstałymi na bazie Bitcoina, np. etherem z platformy Ethereum, który w szczytowym momencie był wyceniany na 4 600 USD co oznaczało kwotę około 0,5 biliona USD. Aktualnie cena bitcoina wynosi około 27 800 USD (44% ceny szczytowej), a cena ethera 1 740 USD (38% ceny szczytowej).

W sytuacji sukcesów kryptowalut banki centralne poczuły się niejako zagrożone i postanowiły odpowiedzieć na to zagrożenie podejmując prace – głównie analityczne – nad *cyfrową walutą banków centralnych – CBDC* (*Central Bank Digital Currency*). Wobec gwałtownie postępującej cyfryzacji gospodarek i społeczeństw niewątpliwie zasadne jest rozważenie odejścia od papierowej gotówki na rzecz rozwiązań cyfrowych. Pojawia się jednak pytanie, w jaki sposób to zrobić?

Banki centralne były w ewidentny sposób zafascynowane rozwiązaniem zaproponowanym przez Satoshi Nakamoto w Bitcoinie, w szczególności łańcuchem bloków (rozproszonym rejestrem). Dlatego postanowiły wykorzystać te same technologie do implementacji CBDC. Niestety – jak pokazujemy w tym raporcie – takie podejście nie prowadzi do sukcesu, dlatego że założenia, przy jakich opracowano Bitcoin i inne kryptowaluty są sprzeczne z celami, jakie stawiają sobie banki centralne przy tworzeniu CBDC.

W tym raporcie przedstawiamy najpierw genezę, uwarunkowania wprowadzenia i charakterystykę cyfrowych walut banków centralnych. Pokrótce omawiamy stan prac badawczo-wdrożeniowych w zakresie CBDC na świecie oraz przegląd dotychczasowych stanowisk i dyskusję zalet i wad CBDC. Stosunkowo dużo miejsca poświęcamy kwestiom technologicznym, które najczęściej w opracowaniach banków centralnych są albo pomijane, albo traktowane tak zdawkowo, że czytelnik nie jest w stanie wyrobić sobie własnej opinii na temat ich możliwości i ograniczeń. Po wykazaniu sprzeczności tych technologii z celami CBDC, proponujemy alternatywne rozwiązanie polegające na utworzeniu przez bank centralny wydzielonego i całkowici podporządkowanego mu *Banku Gotówki Cyfrowej – BCG*.

Raport kończą wnioski i odwołania do licznych pozycji literaturowych.

2. Cyfrowa waluta banku centralnego – geneza, uwarunkowania wprowadzenia, charakterystyka

2.1. Trendy w rozwoju form pieniądza

Całą historię pieniądza i systemów pieniężnych można rozważać w kategoriach rozwoju i zmian w zakresie najważniejszych elementów sfery monetarnej: samej jednostki pieniężnej, władzy monetarnej (od pewnego momentu utożsamianej z bankami centralnymi) i instytucji bankowych uczestniczących w procesie kreacji pieniądza. Zmiany następowały na przestrzeni wieków nierównomiernie, z różnym natężeniem i częstotliwością. Okresy swoistego zastoju czy nawet regresu w organizacji stosunków pieniężnych przeplatały się z dekadami bardzo szybkich i głębokich zmian. Zmieniały się przy tym formy i cechy samego pieniądza, sposoby jego pozyskiwania i tworzenia, regulacje sfery monetarnej i nadzór nad nią, sposób organizowania płatności detalicznych i hurtowych oraz kompetencje i mandat, w tym zakres niezależności, władz monetarnych. (zob. np. [43], [64], [85], [113].)

Zmiany w sferze monetarnej – w tym zmiany technologiczne – były i są nieuniknione. Można uznać za Goetzmannem [56], że pieniądz i sfera finansowa ewoluowały wraz z historią ludzkości. W szerokim ujęciu, przemiany pieniądza i instytucji go tworzących były napędzane przez ogólne przemiany społeczno-kulturowe, w tym rosnące zapotrzebowanie na płynność wraz z rozwojem gospodarczym, oraz zmieniające się potrzeby podmiotów gospodarujących i związane z nimi poszukiwania instrumentów możliwie najlepiej wypełniających tradycyjne funkcje pieniądza (środek wymiany, środek płatniczy, miernik wartości, środek skarbienia). W tym kontekście, przemiany sfery monetarnej wynikają niejako z przemian samej gospodarki i zachowań jej uczestników.

Niewątpliwie, bardzo istotnym katalizatorem zmian monetarnych były coraz większe możliwości technologiczne pozwalające na standaryzację jednostki pieniężnej i operacji z jej udziałem, wzrost skali transakcji, ich szybkości i efektywności, a także zasięgu geograficznego. Z czasem technologia umożliwiła fundamentalne wręcz zmiany w charakterze pieniądza i sposobach posługiwania się nim. Co ciekawe, pod obecną cyfrową „rewolucję" w tym zakresie grunt przygotowały, jak podkreśla Bordo [18] „historyczne transformacje".

Pierwsza z nich miała miejsce w XVIII i XIX wieku, kiedy to konieczność rosnących kosztów finansowania wojen we wczesnej epoce nowożytnej doprowadziła do emisji przez rządy poszczególnych państw niewymienialnego pieniądza fiducjarnego[1]. Ta nowa technologia finansowa doprowadziła przy tym do pojawienia się wymienialnych banknotów, co znacznie obniżyło koszt produkcji monet i bilonu.

Drugą fundamentalną zmianą była rządowa regulacja bankowości komercyjnej i wprowadzenie rządowego monopolu na emisję banknotów. Zakończyło to okres tzw. wolnej bankowości (*free banking*), postrzegany jako wysoce niestabilny [81]. Rządy, zawsze odgrywające kluczową rolę w dostarczaniu waluty (zewnętrznego pieniądza), będącej dobrem publicznym, z czasem uregulowały również w poszczególnych krajach pieniądz wewnętrzny dostarczany (kreowany) przez banki komercyjne[2]. Te ostatnie utraciły wówczas przywilej emisji banknotów, która stała się monopolem banków centralnych. Oprócz zwiększenia stabilności, pozwoliło to również ograniczyć bardzo dużą asymetrię informacyjną między uczestnikami rynków finansowych, przyczyniającą się do niskiej efektywności systemów płatniczych.

Trzecim wreszcie doniosłym przekształceniem w obrębie systemów pieniężnych była ewolucja banków centralnych, od instytucji wyłącznie emisyjnych w wyspecjalizowane podmioty, realizujące kluczowe cele makroekonomiczne: utrzymanie stabilnego poziomu cen, utrzymanie stabilności finansowej i dbałość o efektywny system płatności. W wyniku systematycznego procesu uczenia się i adaptacji, banki centralne zaczęły prowadzić politykę pieniężną i makroostrożnościową, budując jednocześnie swoją wiarygodność i doskonaląc strategię oraz instrumentarium.

Do tych trzech „transformacji" należy jeszcze dodać przejście od pieniądza towarowego do pieniądza w pełni fiducjarnego. Nastąpiło to w sposób formalny począwszy od 1 kwietnia 1978 roku, choć praktycznie pieniądz stracił powiązanie z towarem już w roku 1971, wraz z zawieszeniem wymienialności dolara amerykańskiego na złoto [68]. Stanowiło to przełom nie tylko techniczny, ale także koncepcyjny i symboliczny – po raz pierwszy w historii pieniądz nie miał już postaci fizycznej i powiązania z jakim-

1 Mowa tu o zachodnim obszarze kulturowym. Dużo wcześniej takie rozwiązania były znane w Azji.

2 Proces ten przebiegał różnie w poszczególnych krajach. Zasadniczo, zakończył się on na początku XX wieku.

kolwiek towarem, stając się czystą abstrakcją i pewną konwencją społeczną[3].

Wszystkie te procesy doprowadziły do wykształcenia się współczesnych systemów pieniężnych oraz ukształtowania się ich charakterystycznych cech. Należy podkreślić, że – zasadniczo – taki kierunek ewolucji oceniano raczej pozytywnie, podkreślając, że sprzyjał on ogólnemu dobrobytowi i procesom wzrostu gospodarczego.

Patrząc na tę ewolucję w sposób ciągły, od samych (niejasnych) początków pieniądza oraz jego pierwotnych form i zastosowań, przez historycznie pierwsze rodzaje systemów pieniężnych opartych na pieniądzu kruszcowym, a następnie systemy pieniądza kierowanego (*managed money*), aż po upowszechnienie się pieniądza w pełni fiducjarnego, w konstrukcji i funkcjonowaniu systemów pieniężnych można wyróżnić pewne swoiste trendy. Najważniejszymi spośród nich były **postępująca dematerializacja pieniądza i umacnianie państwowego (rządowego) monopolu monetarnego**. Obie tendencje stały się jeszcze wyraźniejsze w ostatnich trzech dekadach, wraz z wpływem na systemy pieniężne takich zjawisk, jak globalizacja, finansyzacja i postęp technologiczny. Dodatkowo, w ostatnich latach pojawiły się kolejne (a także nasiliły dotychczasowe) czynniki wpływające na jednostki pieniężne i władze monetarne, stanowiąc katalizator dalszych zmian w tych obszarach [14], [19], [21], [124], [125]. Rozwój pieniądza cyfrowego – najpierw prywatnego, a następnie państwowego – można postrzegać jako swoistą kontynuację tych właśnie trendów.

Kwestie cyfrowego pieniądza były przedmiotem badań już w końcu XX wieku. Dopiero jednak splot wielu czynników (praktycznych i teoretycznych) sprawił, że przestały one być przedmiotem zainteresowania tylko zwolenników nowoczesnych technologii i ekonomistów specjalizujących się w badaniach sfery pieniężnej, ale stanęły w centrum publicznej debaty nad organizacją i funkcjonowaniem gospodarki w warunkach procesów nazywanych niekiedy czwartą rewolucją przemysłową [112]. Bitcoin – pierwsza kryptowaluta, która przebiła się do świadomości społecznej – powstał w 2008 roku, a upowszechnił się i stał przedmiotem wielu debat i naśladownictwa w następnych latach. Zawładnął on wyobraźnią akademików, polityków, inwestorów i przedstawicieli praktyki do tego stopnia, że w świadomości opinii publicznej pieniądz cyfrowy wiązano głównie z kryptowalutami. Zainteresowanie nimi stanowiło wyraz postępującej dematerializacji i cyfryzacji pieniądza, co postrzegano – oprócz przypisywanej im funkcji aktywów inwestycyjnych – jako sposób na reformę i współczesnych systemów pieniężnych [83], [84].

Dopiero od kilku lat za pieniądz cyfrowy uważa się także waluty cyfrowe banków centralnych (*Central Bank Digital Currency* – CBDC). Postrzega się je jako jedną z najbardziej spektakularnych reprezentacji postępu technologicznego w sferze finansowej i element przyszłego – potencjalnego – ładu monetarnego. CBDC rozpatruje się w przy tym w rozmaitych kontekstach i aspektach – jako nową formę pieniądza, instrument wzmacniana pozycji geopolitycznej, środek zwiększenia efektywności płatności oraz metodę na zachowanie skuteczności polityki pieniężnej i, szerzej, pozycji banków centralnych w warunkach gospodarki 4.0 (*Economy 4.0*), cechującej się odmiennymi od dotychczas identyfikowanych mechanizmami transmisji impulsów monetarnych i strukturalnymi cechami poszczególnych rynków. Warto jednak zwrócić uwagę, że tak duża popularność, czy wręcz swoista moda (*hype*) na CBDC jest następstwem pewnych specyficznych uwarunkowań, które wystąpiły w ostatnich dwóch dekadach, kumulujących się niejako w okresie pandemii COVID-19.

2.2. Uwarunkowania i przesłanki wprowadzenia CBDC

Badania oraz dyskusje nad koncepcjami i rozmaitymi aspektami emisji pieniądza banku centralnego w formie cyfrowej trwają od 2014 roku, kiedy działania w tym zakresie rozpoczął Ludowy Bank Chin [129]. Natomiast od roku 2020 jest już widoczny bardzo wyraźny wzrost zaangażowania poszczególnych banków centralnych w badania nad możliwością emisji CBDC. Intensyfikacja prac analityczno-badawczych i pilotażowych (a w kilku przypadkach również wdrożeniowych) dotyczących CBDC postrzeganych jako instrument rozwiązania konkretnych problemów społeczno-gospodarczych poszczególnych państw, sprawia, że zainteresowanie tym instrumentem rośnie nie tylko wśród specjalistów, lecz zaczyna także docierać do coraz szerszego kręgu podmiotów.

3 Dopiero wtedy znalazły w pełni zastosowanie tzw. nominalistyczne teorie pieniądza ([64], [73], [144].

Można wskazać kilka głównych przesłanek intensyfikacji prac nad CBDC[4]:

1. pojawienie się i wzrost popularności kryptowalut;
2. utrudnione – wskutek splotu rozmaitych czynników – warunki realizacji polityki pieniężnej przez banki centralne;
3. ewolucja i swoista emancypacja instytucji finansowych oraz rozwój podmiotów z obszaru tzw. fintech, BigTech i niefinansowych instytucji płatniczych;
4. dostrzeżenie problemu wykluczenia finansowego;
5. spadek popytu na papierową gotówkę;
6. dyskusje dotyczące suwerenności monetarnej poszczególnych państw.

2.3. Kryptowaluty

Już od kilkunastu lat kryptowaluty – głównie bitcoin – stanowią ważny element rynków finansowych, będąc instrumentem szeroko wykorzystywanym przez doświadczonych, jak i przez mniej zaawansowanych inwestorów. Kryptowaluty cechuje przy tym zadziwiająca na pierwszy rzut oka dychotomia – są popularne zarówno wśród najbogatszych uczestników rynków i procesów finansowych, szukających coraz to nowszych i bardziej wyrafinowanych kierunków lokowania środków, jak i wśród mieszkańców krajów mniej rozwiniętych lub borykających się z poważnymi kryzysami gospodarczymi, w szczególności inflacją.

Mimo, że wbrew obiegowej opinii wielkość rynków kryptowalut i ich wykorzystanie w porównaniu z innymi instrumentami finansowymi nie są duże, to kryptowaluty w zasadzie od samego powstania znajdują się w centrum dyskusji dotyczącej wpływu nowoczesnych technologii na gospodarkę. Postrzega się je jako rozwiązanie komplementarne wobec innych czynników, zjawisk i procesów, składających się na gospodarkę 4.0, dopełniając je w sferze monetarnej. W tym kontekście, kryptowaluty stanowią nie tyle formę inwestycji czy spekulacji, ale pewne systemowe rozwiązanie, ułatwiające przejście do gospodarki bezgotówkowej (*cashless economy),* a także sprzyjające takim procesom, jak rozwój gospodarki współpracy (*collaborative economy*), tzw. postkapitalizm i dezintermediacja w sektorze finansowym.

W kontekście pieniądza i systemów pieniężnych kryptowaluty mieszczą się w nurcie badań nad tzw. najlepszym, „idealnym" pieniądzem. Problematyka ta, podnoszona chociażby przez słynnego Johna Nasha [93], od dawna stanowi przedmiot ożywionych dyskusji, zwłaszcza w kontekście (rzekomych) niedostatków współczesnych systemów pieniężnych[5]. Kryptowaluty – czy szerzej dążenie do postępującej dematerializacji i cyfryzacji pieniądza – postrzega się tu jako krok ku niezbędnej reformie współczesnych systemów pieniężnych. Rozpatruje się je przy tym w kontekście nowych, prywatnych jednostek pieniężnych, potencjalnie emitowanych przez globalne korporacje, grupy interesów lub nawet społeczności lokalne.

Warto zaznaczyć, że wbrew obiegowej, potocznej opinii, takie makroekonomiczne ujęcie kryptowalut jako pieniądza przyszłości nie pojawiło się od razu. W swoistym manifeście Nakomoto [92], od którego datuje się narodziny bitcoina i pochodnych kryptowalut, jest w zasadzie mowa tylko o problemie zaufania wobec rozliczeń i płatności elektronicznych oraz banków jako podmiotów organizujących i nadzorujących rozliczenia. Brak natomiast konkretnych nawiązań i rozważań odnoszących się do bardziej ogólnych kwestii pieniądza, banków centralnych i całego kontekstu instytucjonalnego.

Ponadto, jak wskazuje Popper [103], przez pierwsze dwa lata od wprowadzenia bitcoina w zasadzie nikt go nie używał. Zwolennicy bitcoina i szerzej, całej ideologii stojącej za kryptowalutami, próbowali wręcz – o czym świadczy analiza forów internetowych z tamtych czasów – zainteresować bitcoinem szarą strefę i świat przestępczy, w tych kręgach upatrując podatnego gruntu do jego popularyzacji. Szersze zainteresowanie kryptowalutami przyszło dopiero później, wraz z kolejnymi rekordami ich notowań, postępem „czwartej rewolucji przemysłowej" [77]) i swoistą modą (choć często raczej

4 Por. też przesłanki wprowadzenia CBDC wskazane w raporcie NBP [94].

5 W dyskusjach tych próbuje się zidentyfikować możliwie najbardziej efektywną, dostosowaną do współczesnych warunków instytucjonalnych formę pieniądza, a także wypracować takie zasady jego emisji i regulacji, które pozwalałyby na możliwie największy stopień zarówno stabilności monetarnej, jak i finansowej.

w obrębie pewnych „baniek" społecznościowych). Trudno przy tym uchwycić moment, w którym zaczęto upatrywać w tych jednostkach (lub samej technologii łańcucha bloków, którą wykorzystują) remedium na skuteczną przebudowę systemów pieniężnych[6].

Niemniej, w kolejnych latach kryptowaluty postrzegano często wręcz jako „pieniądz przyszłości" z uwagi na takie ich zalety, jak (rzekomy) brak presji inflacyjnej typowej dla fiducjarnych jednostek pieniężnych emitowanych przez współczesne banki centralne, lub przejrzystość i bezpieczeństwo transakcji tymi jednostkami (zob. np. [61], [102], [147]). Z drugiej strony, kryptowaluty wywołują też liczne kontrowersje, dotyczące przede wszystkim ich prawnego statusu, trudnego do zrozumienia dla przeciętnego odbiorcy procesu ich emisji i transferu (bazujących na zastosowaniu kryptografii) i bardzo częstych i znaczących fluktuacji ich wartości [20], [115], [116], [130].

Z jednej strony kontrowersje i wątpliwości dotyczące różnych aspektów funkcjonowania zróżnicowanych form kryptowalut (w tym m.in. zmienność, problem zaufania, wysoka emisyjność gazów cieplarnianych i koszty energetyczne), a z drugiej fakt, że postrzega się je jako zagrożenie dla państwowego monopolu pieniężnego (w kontekście potencjalnej emisji własnych kryptowalut przez globalne korporacje[7] lub grupy interesów), sprawiły, że kwestią tą zainteresowały się banki centralne. Instytucje te, dostrzegając zalety, jakie wiążą się z kryptowalutami i technologią, na której są one oparte, obserwując dynamiczny rozwój tych instrumentów i coraz większą ich popularność, a także próbując adaptować się do warunków nowej gospodarki, podjęły prace nad wprowadzeniem własnych walut cyfrowych. Wprowadzenie CBDC miałoby w tym kontekście stanowić swoisty „kontratak" banków centralnych.

2.4 Utrudnione prowadzenie polityki pieniężnej

Już w zasadzie od upowszechnienia doktryny monetarystycznej, przez nową szkołę klasyczną, aż po nową syntezę neoklasyczną i związaną z nią tzw. politykę pieniężną Nowego Konsensusu (*New Consensus Monetary Policy*), banki centralne są jednymi z najważniejszych podmiotów funkcjonujących we współczesnej gospodarce [119], [143]. Realizowana przez nie polityka pieniężna wysunęła się na pierwsze miejsce w hierarchii dziedzin polityki gospodarczej. Decyzje z jej zakresu stanowią główny parametr, uwzględniany w decyzjach podmiotów rynkowych, a prezesi banków centralnych są jednymi z najpilniej słuchanych osób w świecie finansowym.

Środowisko, w którym funkcjonują banki centralne ulega jednak szybkim zmianom. Zarówno w gospodarce światowej, jak i w poszczególnych państwach, uwidaczniały się i nadal uwidaczniają procesy oraz zjawiska wpływające na sposób i możliwości realizacji skutecznej polityki pieniężnej. Wśród najważniejszych z nich wymienia się [21], [27], [39], [42], [82]:

1. globalizację i zjawiska z nią związane (m.in. deregulacja, internacjonalizacja, wzrost skali przepływów kapitałowych);
2. sytuację tzw. nowej gospodarki (*new economy*);
3. finansyzację;
4. zmiany w podejściu oraz sposobie realizacji polityki fiskalnej i kursowej w poszczególnych krajach;
5. zmiany w cechach i charakterze współczesnego pieniądza oraz wiążące się z tym zmiany w popycie na pieniądz i podaży pieniądza;
6. kwestie klimatyczne.

Charakterystyczne jest przy tym, że czynniki te były i są ze sobą ściśle powiązane, wchodząc w liczne i głębokie interakcje. O ile przy tym niektóre z wymienionych zjawisk sprzyjały osiąganiu celów przez banki centralne (głównie globalizacja i upłynnienie kursów walutowych), to inne oddziaływały raczej negatywnie (zwłaszcza rosnące obciążenie finansów publicznych).

Ostatnie dwie dekady stanowiły wyjątkowo trudny czas dla banków centralnych. Złożyła się na to zarówno cała seria niekorzystnych szoków (wstrząsów) zewnętrznych, kontynuacja pewnych trendów komplikujących funkcjonowanie banków centralnych, jak i – z drugiej strony – osłabienie

6 Poglądy takie formułowali i szeroko propagowali np. przedstawiciele austriackiej szkoły ekonomii Milne [90], Peneder [100].

7 Vide np. program Libra/Diem przygotowywany przez Facebook, ostatecznie (?) zakończony.

lub wręcz wygaszenie pewnych tendencji, które ułatwiały realizację polityki pieniężnej (np. globalizacji). W zasadzie, począwszy od kryzysu dotcomów na początku tego stulecia, przez globalny kryzys finansowy lat 2007-2009 (rozpoczęty kryzysem na amerykańskim rynku kredytów subprime), będące jego następstwem, kryzys zadłużeniowy (szczególnie dotkliwy w państwach europejskich) i Wielką Recesję, tendencje deflacyjne w wielu krajach, pandemię COVID-19 i wreszcie wybuch wojny w Ukrainie i jej następstwa, banki centralne nieustannie zmagały się z różnego rodzaju problemami.

Nie bez znaczenia był również pewien kryzys teoretyczny i koncepcyjny, przed jakim stanęli bankierzy centralni, w obliczu niespotykanych dotychczas wyzwań i zagrożeń, takich jak sytuacja *zero bound* (zerowych nominalnych stóp procentowych), zakłócenia w funkcjonowaniu kanałów transmisji, nieskuteczność tradycyjnych instrumentów polityki pieniężnej, presja ze strony rządów poszczególnych państw stawiająca pod znakiem zapytania faktyczną niezależność banków centralnych, lub wreszcie konieczność wyboru między realizacją sprzecznych w danym momencie celów, jakie postawiono przed tymi instytucjami. Ponadto, nowe instrumenty użyte w celu przezwyciężenia tych negatywnych okoliczności, okazały się same w sobie źródłem problemów, czego najlepszym przykładem są programy QE (*Quantitative Easing*).

W rezultacie tych zjawisk, banki centralne zostały niejako „odczarowane". Mervyn King, były gubernator Banku Anglii pisał w tym kontekście wręcz o „końcu alchemii" [71]. W tej sytuacji pojawiły się próby szukania nowych – teoretycznych i praktycznych – sposobów na zwiększenie kontroli władz monetarnych nad sferą pieniężną i na wzrost możliwości osiągania poszczególnych celów polityki pieniężnej. Jako jeden z nich traktuje się właśnie CBDC, upatrując w nich nowego, efektywnego instrumentu polityki pieniężnej, co przedstawiono w podrozdziale 4.5.

2.5. Ewolucja instytucji finansowych

Zjawiska wymienione w podrozdziale 2.4 wywierały także wpływ na funkcjonowanie instytucji bankowych i – szerzej – całego systemu finansowego. Szczególnie zmieniły się warunki prowadzenia działalności bankowej. Swoboda przepływów kapitałowych, wzmożony popyt na instrumenty z zakresu rozliczeń międzynarodowych i zarządzania ryzykiem, możliwości ekspansji na nowe rynki i wzrost konkurencji sprawiły, że odmiennie zaczęły kształtować się warunki działania pojedynczych instytucji bankowych, jak i całych systemów bankowych. Co za tym idzie, zmieniały się również warunki działania nadzorców oraz decydentów w poszczególnych krajach. Znamienne było przy tym to, że w wielu przypadkach tracili oni część lub nawet całość wpływu na funkcjonowanie narodowego sektora bankowego.

Bilans zmian nie jest przy tym jednoznaczny. Oprócz wzrostu ryzyka i pojawienia się nowych jego rodzajów, a także zagrożeń dla stabilności banków, pojawiły się bowiem także szanse, wynikające z możliwości świadczenia nowych usług lub ekspansji na nowe rynki i tym samym rozwinięcia skali swojej działalności. Zmiany otoczenia spowodowały konieczność dostosowań ze strony banków, wzmacniając przy tym pewne tendencje już wcześniej występujące w systemach bankowych poszczególnych krajów.

Jako najważniejsze z tych tendencji uznaje się cztery procesy:

1. internacjonalizację banków;

2. deregulację działalności bankowej (i szerzej, finansowej);

3. zjawisko dezintermediacji oraz

4. postęp technologiczny.

Charakterystyczne, że ich wpływ nie był identyczny – część z nich wiązała się z szansami banków, tworząc środowisko korzystne dla ich dalszego rozwoju. Inne natomiast jeszcze bardziej utrudniały sprostanie presji konkurencyjnej. Wpływ poszczególnych procesów był też odmienny, jeżeli wziąć pod uwagę potencjał danego banku – zazwyczaj beneficjentami zmian były duże instytucje, dysponujące odpowiednim kapitałem ludzkim i finansowym.

Postęp technologiczny, oprócz wielu innych elementów, zmienił także natężenie i formy walki konkurencyjnej w systemie finansowym [70], [76]. W szczególności, pojawiły się nowe struktury rynkowe oraz nowe podmioty stanowiące konkurencję dla banków. W tym kontekście można wskazać dwie grupy. Pierwsza z nich obejmuje struktury wyrażające się w odmiennej, komplementarnej wobec tradycyjne-

go mechanizmu rynkowego, organizacji gospodarki i społeczeństwa (m.in. gospodarkę współdzielenia i tzw. współfinansowanie – *collaborative finance*), druga natomiast – nowych konkurentów, mieszczących się jednak w obrębie dotychczas obowiązującego modelu stosunków rynkowych.

Konkurenci banków ujęci w drugiej grupie stanowią bardzo zróżnicowaną kategorię. Zalicza się do niej nowego rodzaju instytucje finansowe – neobanki – które działają w innowacyjnych modelach biznesowych, często wyłącznie w formie cyfrowej. Neobanki (*challenger banks*, banki pretendujące, banki wirtualne) starają się wypełnić lukę spadku zaufania do tradycyjnych banków oraz wykorzystują nowoczesne rozwiązania finansowe (technologie i narzędzia) do ekspansji rynkowej, cechując się w wielu przypadkach bardzo konkurencyjnymi wobec "tradycyjnych" banków cenami. Przyjęte normy prawne w zakresie współpracy banków z podmiotami trzecimi (m.in. Dyrektywa PSD2) dają szansę neobankom na uzupełnienie bankowości klasycznej. W sytuacjach krytycznych podmioty te mogą nawet stanowić jej substytut [117].

Neobanki zalicza się do sektora FinTech. Są one, podobnie jak firmy tzw. BigTech, instytucjami szczególnie ważnymi z punktu widzenia funkcjonowania i osiągania przychodów przez „tradycyjne" (choć też w coraz większym stopniu zdigitalizowane) banki. Warto dodać, że neobanki w coraz większym stopniu wchodzą do segmentów usług finansowych (głównie płatności) tradycyjnie obsługiwanych przez banki. Funkcjonalność oraz modele biznesowe neobanków zmieniają się wraz ze zmianami oczekiwań konsumentów. Co istotne, neobanki mogą przybierać formę inicjatyw istniejących banków, w celu modyfikacji już funkcjonujących modeli biznesowych.

Kolejną grupę konkurencyjnych względem banków podmiotów stanowią instytucje zaliczane do tzw. sektora bankowości cienia (*shadow banking)*. Dokonują one operacji podobnych do realizowanych przez „klasyczne" banki, ale nie podlegają takim jak one regulacjom. Nie mogą również korzystać z refinansowania w banku centralnym ani, zasadniczo, nie pozyskują funduszy z depozytów. Działają więc niejako „w cieniu" tradycyjnych instytucji bankowych, choć realizują te same zadania [2], [91]. Z punktu widzenia płatności szczególne znaczenie mają podmioty zaliczane do tzw. drugiej generacji bankowości cienia. Obejmuje ona podmioty (również nie podlegające „klasycznym" regulacjom) stawiające w przeważającym stopniu na działalność w sferze cyfrowej. Sprowadza się ona do formuły P2P, B2B, C2C lub B2C. Z reguły są to różnorakie tzw. platformy finansowania społecznościowego (*crowdfunding*).

Osobnym rodzajem graczy są wspominane firmy z sektora BigTech[8]. Zasadniczo, ich podstawowa działalność dotyczy innych segmentów gospodarki, ale ze względu na jej masowość, bardzo szeroką bazę klientów tych firm oraz liczne powiązania, jakie łączą firmy BigTech z innymi obszarami gospodarki, coraz częstsze są przymiarki BigTech związane z ekspansją także na rynki finansowe, uruchomieniem własnych systemów płatności, czy nawet z planami emisji własnych środków płatniczych.

Konkurencja ze strony opisanych podmiotów występuje z różnym nasileniem w odniesieniu do poszczególnych sfer działalności bankowej [66], [72]. Wspólnym rysem jest to, że zwiększa ona wymogi stawiane „tradycyjnym" bankom przez ich klientów, zmuszając do poprawy jakości świadczonych usług i konieczności szybszego przetwarzania i zamykania zleceń klientów [60].

2.6. Spadek popytu na gotówkę i warunki gospodarki „bezgotówkowej"

Jedną z najczęściej wymienianych przesłanek wprowadzenia CBDC są kwestie związane ze spadkiem znaczenia papierowej gotówki i jej udziału w strukturze płatności, jak i agregatów pieniężnych. Tendencja ta jest manifestacją sygnalizowanej w podrozdziale 2.1 dematerializacji pieniądza, widocznej na przestrzeni całej historii monetarnej.

Najbardziej bezpośrednim symptomem spadku znaczenia papierowej gotówki jest widoczne w wielu krajach[9] (głównie skandynawskich) znaczące ograniczenie jej wykorzystania w transakcjach detalicznych. Jak ujęto to w raporcie NBP [94], implikuje to ograniczoną dostępność środka płatniczego, do tej pory powszechnie wyko-

8 Zazwyczaj w tym kontekście wymienia się tzw. GAFAM – Google, Apple, Facebook, Amazon i Microsoft [55]. Oczywiście nie są to jedyne firmy, które można określić mianem BigTech.

9 Należy tu jednak podkreślić, że proces zmniejszania się roli gotówki przebiega w poszczególnych krajach z różnym natężeniem. Oprócz czynników technologicznych i ekonomicznych, bardzo ważne są tu kwestie kulturowe i historyczne.

rzystywanego w dokonywaniu płatności i zwalnianiu ze zobowiązań, który był przy tym pozbawiony ryzyka kredytowego i miał charakter autonomiczny w stosunku do istniejących systemów płatności. Ponadto, co chyba najczęściej wskazuje się w dyskusjach na temat potencjalnych zagrożeń płynących z marginalizacji banknotów i bilonu, traci się anonimowy środek płatniczy.

Spadku znaczenia papierowej gotówki nie powinno się jednak utożsamiać tylko z jej rzadszym używaniem w transakcjach i ewentualnymi problemami z tego wynikającymi. Kwestia ma charakter bardziej fundamentalny. Mianowicie, w kontekście potencjalnej reformy systemów pieniężnych rozważa się – jako jeden ze scenariuszy – sytuację tzw. bezgotówkowej gospodarki (*cashless economy*). Pełne przejście na gospodarkę bezgotówkową niewątpliwie będzie miało określone – gospodarcze i społeczne – konsekwencje dla decydentów, systemów finansowych i całego społeczeństwa. Warto podkreślić, że taka sytuacja ma już niemal miejsce w niektórych gospodarkach (np. Szwecja, Wielka Brytania, Chiny), gdzie udział gotówki w obiegu pieniężnym jest znikomy, a granica między papierową gotówką a aktywami „quasi" pieniężnymi (tzw. *near money*) uległa zatarciu.

Gospodarka bezgotówkowa, postrzegana jako problem nieodłącznie związany z obserwowaną rewolucją technologiczną, nie jest zagadnieniem nowym. Dość paradoksalnie, dyskutowano to zagadnienie jeszcze przed powstaniem kryptowalut, rozmnożeniem wyrafinowanych produktów inżynierii finansowej czy postępem bezgotówkowych form płatności. Mimo to, termin ten nie jest jasno zdefiniowany ani rozumiany.

Po pierwsze, należy wyraźnie podkreślić, że gospodarka bezgotówkowa to nie to samo co gospodarka barterowa, choć ta druga jest oczywiście również „bezgotówkowa". Gospodarki bezgotówkowej nie należy – często błędnie – utożsamiać z sytuacją gospodarki bez pieniądza. Pieniądz nadal istnieje w tego typu gospodarce; lecz po prostu nie ma fizycznej formy. Innymi słowy, można powiedzieć, że gospodarka bezgotówkowa jest równoznaczna z sytuacją, w której nie ma fizycznych środków płatniczych, a waluta państwowa jest tylko jednostką rozliczeniową (*money of account*), a w gospodarce funkcjonują inne środki płatnicze.

W pracach dotyczących gospodarki bezgotówkowej problematykę tę definiowano i wyjaśniano na różne sposoby. Według Mauryi [86] gospodarka bezgotówkowa charakteryzuje się wymianą środków za pomocą czeków[10], kart debetowych lub kredytowych lub metodami elektronicznymi, a nie przy użyciu papierowej gotówki. Podobną definicję prezentują Ejiofor i Rasaki [44], którzy argumentują, że gospodarka bezgotówkowa to taka, w której zakupy i transakcje są dokonywane głównie drogą elektroniczną, rzadziej gotówką.

Co ciekawe, żaden z tych autorów nie zakłada całkowitego zniknięcia papierowej gotówki. Jest to zgodne z definicjami Achora i Roberta [1] oraz Yaquba i in. [146], również utrzymujących, że gospodarka bezgotówkowa nie polega na całkowitej eliminacji z systemu gospodarczego operacji papierową gotówką, ale jest raczej równoznaczna z sytuacją, w której operacje takie są ograniczone do minimum.

Ta grupa definicji ma wyraźny wydźwięk mikroekonomiczny. Są jednak i inne, które zajmują się tymi zagadnieniami z perspektywy makroekonomicznej. Jak się wydaje, w kontekście CBDC właśnie taka optyka jest szczególnie użyteczna. I tak, przykładowo, według Cochrane'a [31] gospodarkę bezgotówkową można zdefiniować jako sytuację, w której w danej gospodarce nie ma gotówki, a tradycyjne kategorie popytu na pieniądz i podaży pieniądza nie mają już zastosowania. Popyt na rządowy pieniądz fiducjarny zanikł, a co za tym idzie – zanikła również jego podaż. Cochrane argumentował, że sytuacja ta, z pewnym przybliżeniem, występuje w niektórych rozwiniętych gospodarkach od początku XXI wieku. Modelując te zagadnienia, Cochrane przedstawia gospodarkę, w której transakcje są finansowane przez wymianę zobowiązań, polegającą na dostarczeniu określonej ilości aktywów prywatnych[11]. Jednocześnie nie ma miejsca na politykę pieniężną, ponieważ nie ma prawie żadnych mechanizmów, za pomocą których mogłaby ona oddziaływać na gospodarkę. Bank centralny w zasadzie stracił wpływ na stan równowagi rynku pieniężnego i finansowego, ponieważ w takich nowych uwarunkowaniach, jest on zbyt małym graczem na rynku finansowym. Jego zobowiązania finansowe nie mają już żadnych szczególnych cech,

10 Nie zawsze zatem bezgotówkowa gospodarka musi wiązać się z postępem technologicznym i cyfryzacją.

11 Podkreśla, że takie transakcje mogą być denominowane np. w „dolarach", mimo że „dolary" dostarczane przez rząd jako nie istnieją już w formie fizycznej, ale cały czas występują jako miernik wartości (jednostka obrachunkowa).

które skłaniałyby agentów do ich nabywania i utrzymywania [30]. Ma to wpływ nie tylko na przebieg transakcji dokonywanych i rozliczanych w danej gospodarce, ale także na funkcjonowanie banków jako kreatorów pieniądza bezgotówkowego oraz innych instytucji odpowiedzialnych za płatności i tworzenie instrumentów płatniczych [87]. Zmieniałoby to też aktualną rolę banków centralnych jako emitentów banknotów, bilonu i monet, niejako unieważniając ich monopol na dostarczanie określonej kwoty prawnego środka płatniczego. Jednak pieniądz państwowy może nadal istnieć jako jednostka rozliczeniowa, a nawet – w bardzo niewielkim stopniu – jako środek wymiany.

Oczywiście scenariusz Cochrane'a nie potwierdził się do końca w praktyce, niemniej, pozwolił zrozumieć pewne wyzwania, przed jakim stały i stoją banki centralne w obliczu spadku znaczenia papierowej gotówki. Bez wątpienia problem nie jest tylko teoretyczną ciekawostką, gdyż pandemia COVID-19 wzmocniła popularność rozliczeń bezgotówkowych. Dodatkowo wydaje się, że niektóre trendy, takie jak masowy wzrost handlu elektronicznego, popularność sklepów internetowych, korzystanie przez Internet z wielu usług, które tradycyjnie były świadczone wyłącznie w formie stacjonarnej (jak np. pomoc medyczna), czy postępująca cyfryzacja usług administracji państwowej i samorządowej, są już nieodwracalne, otwierając kolejne pole do upowszechnienia płatności bezgotówkowych.

Ponadto, jak to opisano w podrozdziale 2.5, należy spodziewać się dalszej ewolucji banków, niebankowych pośredników finansowych, jak i podmiotów niefinansowych (w tym firm BigTech), coraz mocniej wchodzących na rynek płatności. Wszystkie te podmioty oferują społeczeństwu całą gamę bezgotówkowych instrumentów płatniczych i form rozliczeń, a to wymaga reakcji banków centralnych, próbujących utrzymać swój monopol emisyjny w zakresie prawnego środka płatniczego.

Trudno obecnie wyobrazić sobie całkowity zanik papierowej gotówki. Nadal ma ona wiele do zaoferowania gospodarstwom domowym i małym przedsiębiorstwom. Podobnie jak ci, którzy przepowiadali „śmierć" tradycyjnych banków wraz z pojawieniem się bankowości elektronicznej, tak i prognozy śmierci banknotów wydają się, parafrazując słynny cytat, mocno przesadzone. Gotówka prawdopodobnie przetrwa, dopóki jej zalety nie zostaną ograniczone lub dopóki tryby życia społeczno-gospodarczego, a także cechy kulturowe społeczeństw nie ulegną drastycznym zmianom pod wpływem cyfryzacji lub innych procesów różnej natury. Jednocześnie niektórych problemów gospodarki bezgotówkowej nie da się łatwo rozwiązać. Chodzi tu zwłaszcza o kwestie związane z wolnością osobistą i prywatnością obywateli oraz pewne kwestie psychologiczne związane z postrzeganiem pieniądza.

Jeszcze inną kwestią jest to, że w wielu krajach nadal systemy płatności bezgotówkowych są słabo rozwinięte i nieefektywne (albo wręcz słabo dostępne dla potencjalnych użytkowników), nie pozwalając na szybki i bezpieczny transfer środków. W takiej sytuacji, gotówka jest często jedynym dostępnym instrumentem.

Biorąc to wszystko pod uwagę, gospodarka bezgotówkowa z pewnością nie jest nieuniknionym scenariuszem, nawet jeśli w wielu krajach jest już mocno zaawansowana[12]. Można sobie jednak wyobrazić, że w obliczu kolejnych kryzysów, podobnych do tego wywołanego pandemią, rosnąca rola rządów i konkretne przyzwolenie na określone działania i decyzje mogą doprowadzić do wprowadzenia dalszych ograniczeń w posługiwaniu się papierową gotówką, a nawet wycofania się z niej. Wydaje się to racjonalnym założeniem, ponieważ kryzysy są zwykle wyzwalaczem (*trigger*) głębokich zmian, których nie da się wprowadzić w „zwykłych" czasach.

To rodzi pytania o sprawne funkcjonowanie gospodarki i zaufanie do istniejącego systemu monetarnego, utrzymanie dostępu do pieniądza banku centralnego, możliwość zachowania anonimowości w związku z realizowaną transakcją, możliwość uniknięcia pośrednictwa w dokonywaniu płatności, możliwość ograniczenia dostępu do danych osobowych oraz ryzyko wykluczenia finansowego osób nieznających się na nowoczesnych rozwiązaniach technologicznych. Jednocześnie zanik papierowej gotówki może powodować ryzyka związane z formowaniem się prywatnych monopoli w systemie płatniczym.

W tej sytuacji, wiele zależy od możliwości reakcji banków centralnych. Krokiem niejako wyprzeda-

12 Generalnie bardzo duże zróżnicowanie geograficzne jest tutaj ważnym aspektem, ponieważ niektóre kraje są wyraźnie „zakorzenione" w gotówce, podczas gdy inne raczej dążą do jej wyeliminowania.

jącym ze strony tych podmiotów, podobnie jak w przypadku reakcji na kryptowaluty (podrozdział 2.2), byłoby wprowadzenie CBDC, postrzegane tutaj jako sposób na zachowania instrumentu oddziaływania na system finansowy i płatniczy (oraz utrzymanie dochodów z renty menniczej – szerzej podrozdział 4.8). Z punktu widzenia obywateli CBDC byłyby cyfrowym środkiem płatniczym oferowanym nie przez prywatne podmioty, ale agencję państwową o dużym co do zasady autorytecie i poziomie zaufania, a więc – w teorii – bezpieczniejszym. Ponadto, zastąpienie papierowej gotówki przez CBDC mogłoby przynieść również dodatkowe korzyści władzom państwowych, stanowiąc element szerszych pakietu działań na rzecz ograniczania takich problemów jak pranie pieniędzy i finansowanie terroryzmu, funkcjonowanie szarej strefy czy korupcja. Innymi słowy, wprowadzanie CBDC mogłoby pomóc niwelować te niekorzystne (szkodliwe lub wręcz przestępcze) praktyki, dla których przebiegu czy samego zaistnienia kluczowe znaczenie ma funkcjonowanie w obiegu papierowej gotówki – anonimowego środka płatniczego.

2.7. Wykluczenie finansowe

Jedną z wad gospodarki bezgotówkowej jest problem tzw. wykluczenia (wyłączenia) finansowego i wynikających z niego nierówności. Jak informuje Warchlewska [137] problem wykluczenia finansowego pojawił się w analizach szerszego problemu, jakim jest wykluczenie społeczne (*social exclusion*) na początku XXI wieku. Mianowicie, wzmianki na ten temat można odszukać w Strategii Lizbońskiej UE oraz Raporcie Milenijnym ONZ.

Zjawisko wykluczenia finansowego, rozumiane jako wykluczenie jednostek lub gospodarstw domowych z korzystania z usług finansowych w sferze konsumpcji, produkcji i spójności społecznej [79], określa się mianem jednego z najważniejszych problemów ekonomicznych i społecznych obecnego świata. Nieco paradoksalnie[13], problem nasilił się wraz z procesami finansjalizacji i szybkim rozwojem sektorów finansowych na całym świecie. Znacząco wzrósł wtedy stopień komplikacji rynków i transakcji finansowych, lub, inaczej mówiąc, zwiększył się „próg wejścia" w sferę finansową. Wykluczenie finansowe nabrało również nowego wymiaru w związku ze zwiększonym wykorzystaniem przez sektor bankowy nowych technologii finansowych oraz wprowadzaniem przez banki nowych usług, produktów i kanałów dystrybucji [136]. Rosnąca złożoność usług finansowych przekłada się na zwiększone zapotrzebowanie na sprzęt technologiczny oraz kwalifikacje niezbędne do jego obsługi. W takich okolicznościach osoby odseparowane fizycznie i mentalnie od nowoczesnych technologii napotykają na barierę uniemożliwiającą dostęp do tych nowych rozwiązań i urządzeń technologicznych.

Dotyczy to również bezgotówkowych form płatności, które wymagają specjalistycznego sprzętu, wiedzy i znacznego poziomu zaufania. Jednak dla osób narażonych na wykluczenie finansowe spełnienie tych wymagań jest trudne. Jednocześnie podstawowym warunkiem wspierania rozwoju gospodarki bezgotówkowej jest zapewnienie wystarczającej i dostępnej infrastruktury płatniczej, co oczywiście wymaga zaangażowania banków i dostępu do nich zwykłych ludzi.

Wykluczenie finansowe można zatem sprowadzić do jeszcze bardziej pierwotnych czynników, a mianowicie do poziomu rozwoju danego kraju, wiedzy i zamożności jego obywateli, oraz poziomu zaawansowania i dostępności systemu bankowego – i to nie tylko w zakresie złożonych produktów inwestycyjnych, rozliczeniowych i depozytowych, ale usług zupełnie podstawowych. Warunek ten nie jest jednak spełniony w wielu krajach, gdyż typowy jest znaczny odsetek osób, które składają się na grupę tzw. „nieubankowionych". Tych ostatnich można określić jako osoby dorosłe lub rodziny, które w żaden sposób nie korzystają z banków lub instytucji bankowych lub – biorąc pod uwagę fakt, że taka sytuacja może nie być dobrowolna – jako osoby lub podmioty niemające dostępu do usług banków lub podobnych instytucji finansowych [99].

Liczba osób, które kwalifikują się jako nieposiadające rachunku bankowego, jest wysoka. Według Demirguc-Kunt i in. [33] w 2017 roku na całym świecie około 1,7 miliarda dorosłych nie posiadało konta w jakiejkolwiek instytucji finansowej ani u pośredników niebankowych. Zjawisko to nie występuje równomiernie[14], a problem jest najpoważ-

13 Paradoks jest tym większy, że jeszcze stosunkowo niedawno, w okresie przed globalnym kryzysem finansowym formułowano poglądy, zgodnie z którymi przeobrażenia rynków finansowych oraz postęp techniczny zbliżyły rynki finansowe do stanu bliskiego doskonałej konkurencji [128].

14 Wśród osób nieposiadających rachunku bankowego w większości gospodarek nadreprezentowane są kobiety.

niejszy w Azji i Afryce. Jak jednak wynika z raportu Federalnej Korporacji Ubezpieczeń Depozytów nawet w Stanach Zjednoczonych 6,5% gospodarstw domowych nie miało w 2017 roku konta bankowego [53].

Jednocześnie z danych wynika, że najbardziej narażone na brak konta bankowego są osoby o niskich dochodach i że 70% tej grupy używa gotówki do codziennych zakupów. W świecie bezgotówkowym miliony obywateli nieposiadających rachunku bankowego miałyby trudności z zakupem tego, czego potrzebują do codziennego życia. Osoby bez wiedzy, kont bankowych i nowoczesnych urządzeń technologicznych (takich jak smartfony) będą miały trudności z nadążaniem za szybko rozwijającą się technologią bezgotówkową. Tym samym, jeśli płatności cyfrowe staną się powszechną lub wręcz jedyną opcją, osobom, które nie mogą lub nie chcą (np. ze względu na prywatność) korzystać z takich usług, grozi wykluczenie z gospodarki.

Z drugiej strony gotówka jest „włączająca". Konieczne jest zapewnienie włączenia obywateli znajdujących się w trudnej sytuacji społecznej, którzy mogą nie mieć rachunków bankowych lub którym brakuje niezbędnych umiejętności cyfrowych. Z tych powodów z gotówki regularnie korzystają obywatele w każdym wieku, na wszystkich poziomach wykształcenia i we wszystkich grupach dochodowych, uwzględniając wszelkie różnice kulturowe i zwyczaje płatnicze w poszczególnych krajach. Utrzymanie sprawnego funkcjonowania obiegu papierowej gotówki, w tym łatwego do niej dostępu i szerokiej akceptacji tego instrumentu płatniczego w punktach sprzedaży, można w tym kontekście postrzegać jako coś, co mogłoby zapobiegać wykluczeniu finansowemu.

Inny sposób rozwiązania tego problemu wiąże się z technologią. Nawet w państwach rozwijających się, z ograniczoną siecią dostępności oddziałów instytucji i niskim ubankowieniem społeczeństwa, jeśli tylko odpowiednio szeroka jest skala posługiwania się smartfonami[15]. Nawet jeżeli podmioty prywatne nie byłyby, z różnych względów, w stanie (lub nie byłyby zainteresowane) oferować mobilnych usług finansowych, wówczas lukę tę mógłby wypełnić bank centralny danego państwa, proponując własną cyfrową gotówkę.

2.8. Suwerenność monetarna państw

Konstatacja, że narodowa waluta jest ważnym narzędziem budowania pozycji międzynarodowej danego państwa (oraz oczywiście instrumentem wpływania na koniunkturę krajową), jest w zasadzie tak stara jak sam pieniądz[16]. Ingerencję w dany narodowy system monetarny i płatniczy (np. fałszowanie pieniędzy i próby obniżania jego wartości) zawsze postrzegano jako próbę zdobycia kontroli lub co najmniej destabilizacji danego państwa[17]. Z drugiej strony, wzmacnianie pozycji własnej waluty, rozszerzanie przestrzeni monetarnej, na jakiej się nią posługiwano oraz zachęcanie do posługiwania się w rozmaitych transakcjach rzeczowych i finansowych były naturalnym i logicznym sposobem budowania własnej przewagi[18].

Dobitnie uwypukliło się to w okresie funkcjonowania w latach 1944–1971 systemu dewizowo-złotego, zwanego potocznie systemem z Bretton Woods. System ten, mający charakter asymetryczny, był jednym z instrumentów budowania gospodarczej przewagi USA, których waluta była w tym systemie uprzywilejowaną, jako jedyny narodowy pieniądz wymienialny na złoto [68].

W kolejnych dekadach typowym zjawiskiem stały się wojny walutowe [110]. Problem suwerenności waluty stoi również w centrum wszelkich dyskusji dotyczących (potencjalnego) członkostwa danego kraju w unii monetarnej, wyboru systemu kursowego, budowania pozycji konkurencyjnej danego kraju na arenie międzynarodowej oraz wyboru formy i waluty rozliczeń w transakcjach z innymi krajami.

W tym kontekście, skuteczne wprowadzenie przez dane państwo waluty cyfrowej mogłoby być instru-

15 W styczniu 2023 roku smartfony posiadało 5,44 mld ludzi [62]. Według danych IDC w samym 2022 roku, przy negatywnych trendach na rynku, sprzedano na świecie 1,21 mld nowych smartfonów.

16 Obecnie zyskują na popularności poglądy, że pieniądz nie wyłonił się w następstwie spontanicznych procesów rynkowych z barteru, ale że jego geneza nieodłącznie wiąże się kwestią stosunku władzy [63].

17 Jak przypomina Wilson [140], fałszerstwo monety w średniowieczu było wystarczającym *casus belli*.

18 W tym kontekście ukuto koncepcję tzw. „pieniężnego Machiavellego" (The monetary Machiavelli), zgodnie z którą wojna walutowa i szukanie przewagi pieniężnej jest jednym z elementów gry gospodarczej i szukania zdobycia przewagi konkurencyjnej na arenie międzynarodowej.

mentem wzmacniającym – w obliczu dyskutowanych w poprzednich podrozdziałach zjawisk i tendencji – pozycję danego banku centralnego, a tym samym całego państwa i jego waluty. Szczególne znaczenie miałoby to dla państwa o otwartej gospodarce, aktywnie uczestniczącego w procesach wymiany towarowej i finansowej.

Jak podkreślono w opracowaniu NBP [94], gdyby CBDC emitował bank centralny z kraju zajmującego poczesne miejsce w handlu międzynarodowym i którego pieniądz jest przy tym ważną walutą transakcyjną lub rezerwową, to z czasem ta waluta cyfrowa mogłaby znaleźć zastosowanie także w krajowych transakcjach płatniczych, zwłaszcza tam, gdzie waluta lokalna ma niską wiarygodność. Byłaby to zatem niejako cyfrowa „dolaryzacja", stanowiąca zagrożenie dla stabilności i bezpieczeństwa krajowych systemów płatności oraz dla efektywności krajowej polityki pieniężnej, nie wspominając już o względach prestiżowych i wizerunkowych.

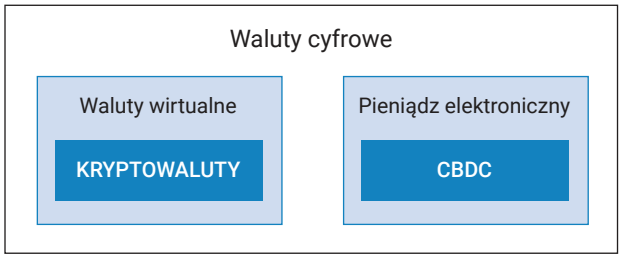
Jeszcze inną możliwą do wyobrażenia sytuacją jest wywołany czynnikami zewnętrznymi paraliż systemu płatności, skutkujący brakiem dostępu do pieniądza i możliwości dokonywania transakcji. Jak podkreśla Wilson [140], by uniknąć paraliżu całej gospodarki, władze nie mogą w tej sytuacji polegać tylko na prywatnych bankach komercyjnych, lecz muszą same zapewnić płynność i sprawny przebieg rozliczeń. Wyjściem z sytuacji byłaby właśnie cyfrowa gotówka, którą można by dostarczyć szybko i tanio na rynki.

Rozumienie tych zależności i mechanizmów może zatem wywołać swoisty wyścig do CBDC poszczególnych państw, dążących, jeśli nie do narzucenia swojej waluty innym, to przynajmniej do zachowania własnej suwerenności monetarnej. Innymi słowy, oferując efektywne CBDC, dany bank centralny może zmniejszyć ryzyko, że znajdzie się w danej wojnie walutowej po stronie przegranych.

2.9. Definicje CBDC

W literaturze zagadnienia występuje dość duży zamęt definicyjny, wynikający z istnienia wielu bliskoznacznych, ale nie będących synonimami terminów, takich jak waluta cyfrowa, waluta wirtualna czy kryptowaluta. Zależności między nimi przedstawiono na schemacie 1.

Schemat 1. Zależności między kategoriami definicyjnymi



Źródło: opracowanie własne.

Najbardziej ogólny charakter ma pojęcie waluty cyfrowej. Najogólniej mianem takim określa się dowolną walutę, pieniądze lub aktywa podobne do pieniędzy (*quasi money*), które są zarządzane, przechowywane i wymieniane za pomocą cyfrowych systemów, zwłaszcza przez Internet. Waluta cyfrowa może być zapisana w rozproszonym rejestrze (*distributed ledger*) dostępnym przez Internet, w scentralizowanej komputerowej bazie danych będącej własnością firmy lub w banku, w plikach cyfrowych lub na karcie ze zmagazynowaną wartością (przedpłaconej) [10].

Jeżeli dana waluta cyfrowa jest denominowana w jakiejś narodowej jednostce pieniężnej i emituje ją podmiot (władza monetarna) odpowiedzialny za wymianę pieniądza cyfrowego na gotówkę, można uznać, że w takim przypadku waluta cyfrowa reprezentuje pieniądz elektroniczny (*e-money*). Pieniądz elektroniczny, zgodnie z Dyrektywą 2009/110/WE oznacza wartość pieniężną przechowywaną elektronicznie, w tym magnetycznie, stanowiącą prawo do roszczenia wobec emitenta, która jest emitowana w zamian za środki pieniężne w celu dokonywania transakcji płatniczych określonych w art. 4 pkt 5 dyrektywy 2007/64/WE i akceptowana przez osoby fizyczne lub prawne inne niż emitent pieniądza elektronicznego

W kategorii pieniądza elektronicznego mieszczą się właśnie waluty cyfrowe banków centralnych. Natomiast waluta cyfrowa denominowana we własnych jednostkach wartości, cechująca się przy tym zdecentralizowaną lub automatyczną emisją traktuje się jako walutę wirtualną [10]. Swoistą odmianą walut wirtualnych są kryptowaluty [127]. Charakterystyczną ich cechą jest sposób tworzenia ściśle związany z kwestiami technologicznymi [37].

Chen i Wu [28], śledząc ewolucję pieniądza od pieniądza towarowego aż po waluty wirtualne uznali, że te ostatnie rozwijają się dzięki nowym technologiom cyfrowym, handlowi elektronicznemu oraz powstawania światów i społeczności wirtualnych. Waluty te nie służą zakupowi dóbr materialnych, a jedynie zakupowi dóbr i usług cyfrowych, w ramach ograniczonego wirtualnego świata (na przykład związanego z grą sieciową). Nie mają one zatem atrybutu powszechnego środka płatniczego. Stanowią natomiast swoisty środek wymiany wartości pomiędzy ich emitentem a danym użytkownikiem lub ich grupą.

Europejski Bank Centralny (EBC) przyjął w 2012 roku, że wirtualna waluta jest pewnym rodzajem nieuregulowanego, cyfrowego pieniądza emitowanego przez jego twórców, a wykorzystywanym i akceptowanym przez uczestników danej społeczności lub wirtualnego świata [40]. Z kolei Financial Action Task Force (FATF) oraz Europejski Urząd Nadzoru Bankowego przyjęły w 2014 roku, że waluta wirtualna jest cyfrową reprezentacją wartości, która może być przekazywana za pomocą technologii informatycznych i stosowana jako środek wymiany, jednostka rozrachunkowa lub środek przechowywania wartości, jednakże nie ma statusu oficjalnego środka płatniczego (*legal tender*) [51], [52]. Innymi słowy, jej wartość nie jest gwarantowana przez żaden rząd lub bank centralny, co nie wyklucza, że może ona podlegać regulacjom państwa.

FATF w [52] prezentuje różne podziały walut wirtualnych. Podkreślając odmienność spełnianych przez nie funkcji, zgodnie z zapotrzebowaniem użytkowników dokonuje w pierwszej kolejności rozróżnienia na wirtualne waluty wymienialne (otwarte), do których zalicza się kryptowaluty, oraz waluty niewymienialne (zamknięte), np. Project Entropia Dollars, Q Coins, World of Warcraft Gold. Drugą z klasyfikacji FATF jest podział na waluty scentralizowane (tj. kontrolowane przez administratora) i zdecentralizowane (tj. pozbawione takiej kontroli)[19].

W 2015 roku EBC zredefiniował walutę wirtualną, traktując ją jako cyfrową reprezentację wartości niewyemitowanej przez bank centralny, instytucję kredytową lub instytucję pieniądza elektronicznego, która w pewnych okolicznościach może być użyta jako alternatywa dla pieniędzy [41].

Parlament Europejski w rezolucji z 26 maja 2016 roku w sprawie walut wirtualnych uznał za wirtualną walutę cyfrową gotówkę, cyfrowe wyznaczniki wartości, które nie są emitowane przez bank centralny ani organ publiczny, nie są powiązane z walutą fiducjarną, a przy tym są przyjmowane przez osoby fizyczne lub prawne jako środek płatniczy. Jako taka, wirtualna waluta może być przekazywana, przechowywana lub sprzedawana i kupowana drogą elektroniczną.

Natomiast zgodnie z polską ustawą o przeciwdziałaniu brudnych pieniędzy, walutą wirtualną jest cyfrowe odwzorowanie wartości, które nie jest (Ustawa z 1 marca 2018 roku):

1. Prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej;

2. Międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub współpracujące z nią;

3. Pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 roku o usługach płatniczych;

4. Instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 roku o obrocie instrumentami finansowymi oraz

5. Wekslem lub czekiem.

Waluty wirtualne emituje się poza państwowym monopolem pieniądza, co oznacza, że można je traktować jako formę pieniądza prywatnego (*private money*). Przez pieniądz taki rozumie się jednostkę, która nie została wyemitowana ani nie jest gwarantowana przez jakikolwiek podmiot rządowy lub płynne zobowiązanie, utworzone świadomie przez źródła niepaństwowe (często lokalne), w celu wypełniania przezeń wypełniać standardowej funkcji pieniądza [32], [38], [57].

Wraz z rozwojem CBDC i wzrostem zainteresowania ich problematyką różnice między nimi a walutami wirtualnymi (w tym kryptowalutami) zaczęły być coraz powszechniej dostrzegane i rozumiane. Jednocześnie, zaczęły pojawiać się coraz bardziej specjalistyczne definicje.

I tak, w [75] zdefiniowano CBDC jako cyfrowy pieniądz emitowany przez bank centralny, denomino-

19 Do tych ostatnich Clayes et al. [29], opierając się na klasyfikacji typów pieniądza zaproponowanej przez Becha i Garrata [9] zaliczają kryptowaluty.

wany w narodowej jednostce obrachunkowej i stanowiący zobowiązanie banku centralnego.

Z kolei BIS oraz inne banki centralne [13] określiły CBDC jako cyfrowy instrument płatniczy, denominowany w narodowej jednostce obrachunkowej, stanowiący bezpośrednie zobowiązanie banku centralnego.

Inne ujęcie zastosowano w opracowaniu MFW [80]. Uznano tam, że **CBDC stanowi nową formę pieniądza, wydawaną w formie cyfrowej przez bank centralny, która ma służyć jako prawny środek płatniczy.**

W zasadzie zatem jedyne, co różni CBDC od „tradycyjnego" pieniądza, jest jego forma. W przeciwieństwie bowiem do np. kryptowalut zachowują one status oficjalnego środka płatniczego (*legal tender*), mogąc realizować wszystkie funkcje pieniądza i czerpiąc zaufanie oraz wartość z autorytetu stojącej za nimi władzy monetarnej.

Ich ścisły związek z bankiem centralnym podkreśla też w swojej definicji Bjerg [16]. Określa on mianowicie CBDC jako zobowiązanie z tytułu powszechnie dostępnych depozytów, które jest rejestrowane elektronicznie w bilansie banku centralnego.

Na potrzeby tego raportu przyjęto definicję MFW. W opinii jego autorów, oddaje ona najlepiej istotę i właściwości CBDC

2.10. Warianty i cechy CBDC

Iwańczuk-Kaliska [65] wyróżnia wiele opcji wprowadzenia CBDC uwzględniających rozmaite aspekty technologiczne, organizacyjne i regulacyjne. I tak, można rozważać tu następujące kwestie dotyczące zaprojektowania określonej CBDC jak: dostęp (bezpośredni lub pośredni), wykorzystywanie (lub nie) technologii łańcucha bloków, zaangażowanie (lub nie) zaufanych stron trzecich, oprocentowanie (lub nie) oraz stopień anonimowości posiadaczy i stron dokonujących transakcji z wykorzystaniem CBDC.

Opcje te stanowią jednocześnie (nierozłączne) kryteria podziału walut cyfrowych banków centralnych. W szczególności, można wyróżnić następujące antynomie w odniesieniu do CDBC [12], [25], [94], [105], [129]:

- bezpośredni – bank centralny dostarcza walutę do użytkownika vs pośredni – bank centralny korzysta z pośrednictwa banków;
- oparty na tokenach (cyfrowych odpowiednikach gotówki) vs oparty na kontach (dziś działa tak np. system Target 2; rozliczenia są w czasie rzeczywistym, jednak system bazuje na kontach, a nie na tokenach – zob. [66]);
- bazujący na łańcuchu bloków vs niebazujący na łańcuchu bloków (zob. podrozdział 6.4);
- oprocentowany vs nieoprocentowany (jak w gotówce papierowej);
- hurtowy (dla dużych odbiorców) vs detaliczny (dla pojedynczych podmiotów).

Wybór danej opcji wiąże się zawsze z określonym wpływem zarówno na rozwiązania w skali mikro, jak i na kwestie makroekonomiczne. Innymi słowy, wybór (zaprojektowanie) danego rozwiązania zależy od wyboru celu, jakim przede wszystkim ma służyć wprowadzenie CBDC. Ponadto podkreśla się, że CBDC – niezależnie od wybranej opcji – by móc efektywnie i sprawnie funkcjonować – powinny spełniać pewne określone cechy, odnoszące się nie tylko do samej jednostki lub systemu, lecz także do kwestii instytucjonalnych. W raporcie BIS [12] wymieniono 14 takich cech, ujętych w trzech grupach. Pierwsza z nich odnosi się do samego instrumentu, który powinien cechować się:

- wymienialnością (CBDC powinno być wymienialne bez żadnych kłopotów na gotówkę papierową i depozyty na żądanie);
- wygodą użytkowania (co najmniej taką samą jak gotówka papierowa lub instrumenty bezgotówkowe);
- akceptowalnością i dostępnością;
- niskimi kosztami.

Druga grupa cech dotyczy całego systemu. Powinien on cechować się bezpieczeństwem, ciągłością, odpornością na błędy i zakłócenia w funkcjonowaniu, dostępnością (tylko online lub online i offline; przez 24 godziny na dobę 7 dni w tygodniu lub w określonym czasie), przepustowością, skalowalnością, interoperacyjnością (możliwość interakcji systemu CBDC z prywatnymi systemami płatności i łatwego przepływu środków między systemami) oraz płynnością i adaptowalnością.

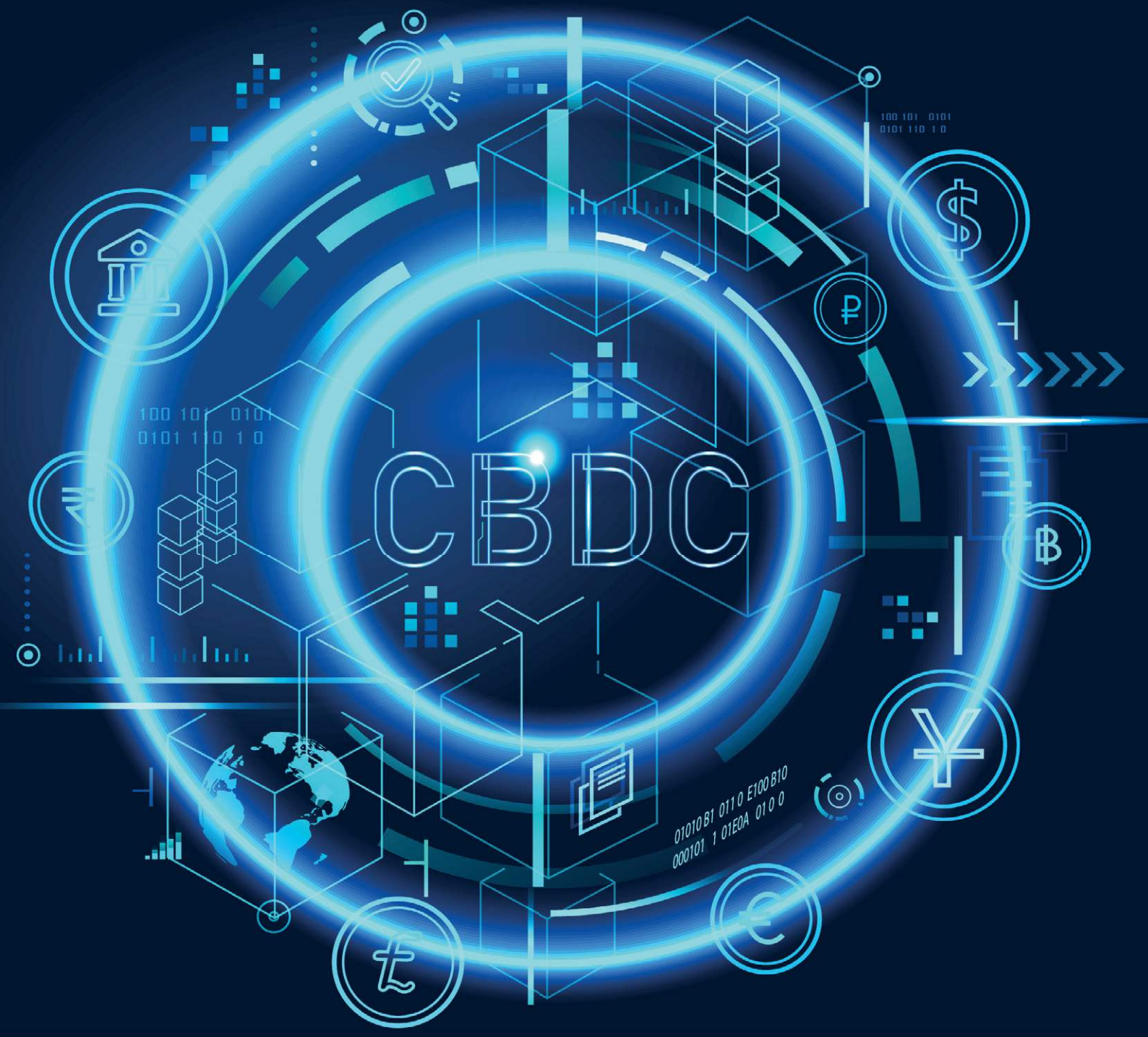
Dwie ostatnie cechy dotyczą uwarunkowań instytucjonalnych. Pierwszą stanowią solidne ramy prawne, jasno przyznające bankowi centralnemu prawo emisji CBDC. Drugą natomiast – ogólne standardy i normy regulacyjne i ostrożnościowe.

Opisane cechy pozwalają na wyraźne rozróżnienie CBDC i kryptowalut, mimo że obie kategorie są odmianami walut cyfrowych.

Niezależnie od tych cech warto zwrócić uwagę na jeszcze jedną, potencjalną właściwość, jaką mogłyby być obdarzone CBDC. Jest nią tzw. data ważności (*expiration date*) implikująca, że jednostki danej CBDC zgromadzonej na koncie klienta traciłyby z czasem (linearnie lub skokowo) pewną część swojej wartości. Niewątpliwie, cecha ta jest bardzo kontrowersyjna – pominąwszy już nawet kwestie praw obywatelskich, „czasowość" gotówki jest czynnikiem wykluczającym jakiekolwiek zaufanie do niej i posługiwanie się takim instrumentem[20].

20 Dyskusję tego zagadnienia zawarto w [69].

3. Stan dotychczasowych prac nad CBDC



Jak wspominano, pionierem w zakresie CBDC był Bank Ludowy Chin, który rozpoczął prace nad cyfrową gotówką już w 2014 roku. Niewiele później problemem zainteresowały się także Bank Anglii (w 2015 roku), banki centralne Kanady i Singapuru (w 2016 roku) oraz Bank Szwecji (w 2017 roku). W kolejnych latach ruszyła wręcz lawina prac (o różnym stopniu zaawansowania) nad CBDC podejmowanych przez banki centralne całego świata.

Na początku 2023 roku już ponad 100 banków centralnych na świecie pracowało nad emisją własnego cyfrowego pieniądza cyfrowego (głównie w wersji detalicznej). Również na 2023 rok Europejski Bank Centralny (EBC) zapowiedział rozpoczęcie testów nad wprowadzeniem cyfrowego euro, które miałoby funkcjonować już od roku 2026. Natomiast NBP opublikował swój raport w kwestii walut cyfrowych banków centralnych w maju 2021 roku[21].

Charakterystyczne jest, że liderami prac nad wprowadzeniem CBDC nie są bynajmniej banki centralne krajów o rozwiniętym systemie finansowym[22]. Nie powinno to jednak dziwić, jeżeli przywoła się scharakteryzowane w rozdziale 2 przesłanki prac nad CBDC – na najbardziej podstawowym poziomie, zainteresowane tym narzędziem powinny być właśnie kraje rozwijające się, z relatywnie słabiej rozwiniętym systemem płatniczym i finansowym oraz niskim ubankowieniem.

Właśnie taką strukturę prac nad CBC potwierdzają dane zgromadzone przez CBDC Tracker –projekt o otwartym dostępie (*open source*), utworzony w celu zapewnienia kompleksowego źródła informacji o światowych inicjatywach CBDC. Prace nad walutami cyfrowymi są tu klasyfikowane według kilku możliwych statusów [24]:

1. Anulowane: kraje, które anulowały lub zlikwidowały CBDC[23].

2. Badania: kraje, które przeprowadziły analizę implikacji (prawnych, ekonomicznych) emisji CBDC.

3. Prace koncepcyjne: kraje, które zbadały potencjalne możliwości technologiczne, opublikowały raporty badawcze w tym zakresie i zaczęły eksperymenty z CBDC.

4. Pilotaż: kraje, które prowadzą pilotażowy program CBDC, np. dla krajowych transakcji międzybankowych lub międzynarodowych, w rzeczywistym środowisku z ograniczoną liczbą uczestników.

5. Wdrożenie: kraje, które oficjalnie uruchomiły CBDC.

W marcu 2023 roku jako kraje, które uruchomiły CBDC (status 5), funkcjonowały tylko dwa: Wyspy Bahama (Sand Dollar) i Jamajka (waluta JAM-DEX). Pierwsze rozwiązanie jest oparte na tokenach i technologii rozproszonego rejestru DLT (zob. szerzej podrozdział 6.4), a wprowadzono je w celu sprawnego zarządzania opłatami handlowymi. Natomiast CBDC Jamajki wykorzystuje konta, nie korzysta z technologii DLT, a głównym motywem jego wprowadzenia były kwestie włączenia finansowego, usprawnienia procesów i kosztów zarządzania oraz wspieranie działań na rzecz przekształcenia Jamajki w gospodarkę cyfrową.

Wśród banków centralnych ze statusem 4. – „Pilotaż" znajduje się łącznie 15 CBDC. Są wśród nich instytucje i CBDC z krajów o dużo większym znaczeniu dla światowej gospodarki: chiński e-yuan[24], hurtowe i detaliczne CBDC Francji, e-Naira z Nigerii, kanadyjski Jasper, urugwajskie e-peso oraz Aber – wspólna inicjatywa Arabii Saudyjskiej i ZEA.

Dużo liczniejsze były grupy krajów, które podjęły prace koncepcyjne i badania. W tej ostatniej grupa znajduje się Polska. Trzeba jednak zaznaczyć, że od badań CBDC do ich wprowadzenia droga jest bardzo długa, a przed podjęciem tak ważnych decyzji warto dokładnie rozważyć zalety i wady, z jakimi wiąże się cyfrowa gotówka.

21 Zgodnie z konkluzją tego raportu, w Polsce nie występowała potrzeba wprowadzania CBDC. Kwestie te zostaną rozwinięte w rozdziale 4.

22 Bank centralny USA opublikował pierwszy dokument odnośnie do potencjalnego cyfrowego dolara dopiero w styczniu 2022 roku.

23 Taki status miały CBDC Ekwadoru, Singapuru, Danii, Finlandii, Haiti i Filipin.

24 Przykład Chin – ze względu na rosnącą pozycję gospodarczą i polityczną tego kraju, jego dynamiczny rozwój (a także ekspansję chińskich technologii) ogromną liczbę potencjalnych użytkowników e-yuana i szeroką salę programów pilotażowych – jest szczególnie często przywoływany w literaturze. Zob. np. [105], [145].

4. Zalety CBDC – przegląd stanowisk

4.1. Ogólna charakterystyka zalet i wad CBDC – ujęcie literaturowe

Przed przedstawieniem technologicznych aspektów CBDC i ich potencjalnego wprowadzenia, należy przybliżyć formułowane w literaturze naukowej, publicystyce i toczących się dyskusjach odnośnie do CBDC argumenty na rzecz takiego rozwiązania, jak i wskazywane jego potencjalne wady. W tym celu, w tym i następnym rozdziale najpierw przedstawiono, a następnie poddano krytycznej analizie, najczęściej wymieniane zalety i wady cyfrowych walut banków centralnych.

Jest to tym bardziej zasadne, że na wiele z nich wskazuje się dość automatycznie, bez głębszej refleksji lub próby zrozumienia faktycznych mechanizmów i zależności, jakie wiązałyby się z poszczególnymi atrybutami CBDC, w tym zwłaszcza faktycznych, możliwych do uzyskania korzyści. Często też – traktując CBDC jako instrument wysoce uniwersalny – abstrahuje się od kontekstu technicznego, gospodarczego i społecznego w różnych krajach. Kontekst ten jest tymczasem mocno zróżnicowany. Ponadto, w poszczególnych krajach w różnym stopniu i zakresie wystąpiły scharakteryzowane w rozdziale 2 przesłanki wprowadzenia CBDC. Obie kwestie w oczywisty sposób będą wpływały na ostateczny bilans (potencjalnego) wprowadzenia przez bank centralny danego kraju waluty cyfrowej.

Rozważając te kwestie, zestawiono tabelę 1, w której ujęto syntetycznie zalety i wady CBDC przedstawiane w literaturze zagadnienia i dokumentach, przygotowywanych przez instytucje zaangażowane w prace nad CBDC. Przed dokładniejszym scharakteryzowaniem plusów i minusów cyfrowych walut banków centralnych warto podkreślić pewną prawidłowość odnośnie do źródeł. Mianowicie, prezentacja poszczególnych zalet i wad w raportach opracowaniach poszczególnych narodowych banków centralnych jest dużo bardziej wyważona, niż poglądy formułowane przez ekonomistów czy finansistów. Jak się wydaje, ci ostatni prezentują podeście bardziej optymistyczne.

4.2. Usprawnienie funkcjonowania systemu płatniczego

Zaleta ta wydaje się być jedną z najbardziej podstawowych. To właśnie bowiem problemy z nieefektywnym, przestarzałym i niewydolnym systemem płatniczym (zarówno w zakresie systemów płatności wysokokwotowych, jak i detalicznych) są tym, co uwypukla potrzebę wprowadzenie nowych cyfrowych instrumentów płatniczych. Zwiększa się przy tym rozdźwięk między tradycyjnymi formami płatności i ich rozliczeń, a możliwościami oferowanymi przez postępującą cyfryzację gospodarki. Innym jeszcze problemem jest sygnalizowany spadek znaczenia papierowej gotówki, co znacznej części spo-

Tabela. 1. Zalety i wady CBDC identyfikowane w dotychczasowych pracach na temat CBDC

Zalety CBDC	Wady CBDC
• Usprawnienie systemu płatniczego. • Poprawa ściągalności podatków i zmniejszanie szarej strefy. • Włączenie finansowe. • Możliwość prowadzenia skuteczniejszej i bardziej elastycznej polityki pieniężnej. • Możliwość prowadzenia skuteczniejszej polityki fiskalne i społecznej. • Większa kontrola emisji pieniądza i zarządzania gotówką. • Kwestie renty menniczej. • Suwerenność monetarna.	• Zakłócenie modeli biznesowych banków. • Ryzyko spadku reputacji i utraty wiarygodności. • Ryzyko błyskawicznego odpływu pieniądza, mogącego oddziaływać kryzysogennie. • Problem z zapewnieniem stabilności (i w tym kontekście wpływem CBDC na płynność międzynarodową i dynamikę kursu walutowego). • Kwestia anonimowości, braku prywatności i szerokich możliwości kontroli ze strony państwa, jakie daje stosowanie CBDC.

Źródło: opracowanie własne na podstawie: [3], [7], [8], [11], [22], [65], [94], [104], [105], [113], [129].

łeczeństwa może utrudnić dokonywania transakcji i płatności, gdy, z jakichś względów nie mogą oni korzystać z prywatnych instrumentów płatniczych. Kwestia ta ściśle wiąże się z problemem wykluczenia finansowego i cyfrowego.

Wprowadzenie CBDC miałoby przynieść w tym zakresie znaczące korzyści, zarówno dla osób fizycznych, jak i podmiotów gospodarczych i instytucji. Korzyści te wiązałyby się przede wszystkim z obniżką kosztów transakcyjnych oraz skróceniem czasu realizacji transakcji płatniczych, a w odniesieniu do płatności międzynarodowych – także z przyspieszeniem rozrachunku i zwiększeniem jego dostępności czasowej (przy płatnościach realizowanych pomiędzy podmiotami z różnych stref czasowych). Jak to ujęto w opracowaniu FED [54], „CBDC mogłyby potencjalnie służyć jako nowa podstawa systemu płatniczego i most między tradycyjnymi i nowymi usługami płatniczymi". Byłby to również sposób na „skokowe" przeprowadzenie danego kraju do ery płatności cyfrowych, jak uczyniły to Chiny.

W tym kontekście rozważa się takie rozwiązania, jak [94]:

- zmiany w istniejących systemach płatności RTGS (*Real-Time Gross Settlement*), które umożliwią współdziałanie różnego typu prywatnych i publicznych systemów płatniczych (w tym opartych na łańcuchu bloków),
- zastosowanie CBDC w systemach płatności (oraz w systemach rozrachunku papierów wartościowych),
- wykorzystania CBDC do płatności detalicznych w stacjonarnych punktach handlowo-usługowych, w handlu elektronicznym i w płatnościach dokonywanych bezpośrednio (*peer-to-peer*) pomiędzy płatnikiem i odbiorcą płatności.

Pojawia się tu jednak kilka kwestii. Po pierwsze, nasuwa się pytanie, czy zamiast wprowadzać CBDC, a zatem nowe i niesprawdzone rozwiązanie, nie lepiej po prostu zmodernizować i dostosować istniejące systemy płatności elektronicznych. Nawet jeżeli konieczna byłaby nie tyle modernizacja, co wręcz budowa i wprowadzenie danego systemu od podstaw, to nadal wydaje się to posunięciem bezpieczniejszym, niż zmiana o charakterze wręcz rewolucyjnym.

Po drugie, nie ma w zasadzie przeszkód technicznych, by jeszcze bardziej usprawnić istniejące rozwiązania w zakresie płatności i rozliczeń, często bardzo innowacyjne w chwili ich wprowadzania, ale nie spełniające już obecnych wymogów cyfrowej gospodarki. Bez wątpienia przełożyłoby się to na skrócenie czasu płatności i rozliczeń oraz obniżkę związanych z tym kosztów. Niekoniecznie musiałyby z tym wiązać się duże wydatki. Przeszkodami są tu raczej inercja i kwestie osiągnięcia kompromisu w tej sprawie przez zainteresowane podmioty, które musiałyby dostrzec w tym korzyści dla siebie, uzasadniające wysiłek modernizacyjny.

Po trzecie, ta zaleta CBDC nie ma charakteru uniwersalnego. W krajach z efektywnym i bezpiecznym systemem płatniczym, charakteryzującym się niskimi kosztami funkcjonowania trudno dostrzec korzyści z wprowadzenia CBDC. Jak się wydaje, jest to właśnie casus Polski (zob. np. [67], [95]). Jak zresztą wynika z rozdziału 3., pierwsze wdrożenia i pilotażowe realizacje CBDC przebiegały właśnie w krajach o niskim poziomie rozwoju systemu płatniczego i finansowego.

4.3. Poprawa ściągalności podatków i zmniejszanie szarej strefy

Zaleta ta wiązałaby się głównie z wyeliminowaniem papierowej gotówki, wykorzystywanej powszechnie w transakcjach szarej strefy. Cyfrowa gotówka byłaby natomiast łatwa w monitorowaniu, uniemożliwiając działania naruszające prawo – w zasadzie każda transakcja mogłaby być łatwo prześledzona. Innymi słowy, nie byłoby możliwe wykorzystanie CBDC do prowadzenia działalności przestępczej ani do przeprowadzania transakcji poza oficjalnym obiegiem. W tej sytuacji, nastąpiłaby poprawa ściągalności podatków, gdyż nie zachodziłaby erozja bazy podatkowej, a sama szara strefa w zasadzie byłaby wyeliminowana (albo ograniczona do wymiany barterowej lub – ewentualnie – kryptowalut). Kwestię lepszej ściągalności podatków można dodatkowo rozpatrywać w kontekście przechowywania przez obywateli swojej cyfrowej gotówki na koncie w banku centralnym (bezpośredni wariant CBDC), skąd podatki mogłyby być ścigane niejako automatycznie.

Jak się wydaje, osiągnięcie tych korzyści nie wymaga wprowadzenia CBDC. Prostym sposobem byłoby ograniczenie (lub wyeliminowanie) papierowej gotówki. Proces ten zresztą już zachodzi – coraz niższa jest kwota, od której transakcje muszą być przeprowadzane za pośrednictwem kont banko-

wych. Sprzyjają temu liczne regulacje AML (*Anti Money Laundering*)[25]. Ponadto, chęć osiągnięcia faktycznych korzyści w zakresie redukcji szarej strefy wymagałoby przyjęcia wariantu, w którym CBDC całkowicie zastępuje papierową gotówkę, a nie jest wobec niej komplementarna.

4.4. Włączenie finansowe

CBDC niewątpliwie mogą być czynnikiem „włączającym", ułatwiając dostęp do podstawowych usług finansowych osobom, które – jak to opisano w podrozdziale 2.7 – są ich z rozmaitych względów pozbawione. Dotyczy to przede wszystkim państw o słabo rozwiniętym systemie finansowym, z ograniczoną siecią oddziałów bankowych i niewielkiej liczbie innych pośredników finansowych. Jeżeli jednocześnie w takich krajach – co na ogół rzeczywiście ma miejsce – jest powszechny dostęp do smartfonów, udostępnienie przez bank centralny cyfrowej gotówki staje się czynnikiem, który może znacząco poprawić sytuację społeczeństwa w zakresie dostępu do podstawowych usług finansowych[26]. Tym samym, zmniejszeniu może ulec poziom wykluczenia finansowego w tym kraju.

Drugą zaletą, jaką należy wskazać w kontekście wpływu CBDC na ograniczanie wykluczenia finansowego, jest to, że stanowiłaby ona państwowy, powszechnie akceptowany prawny środek płatniczy, który byłby w dyspozycji obywateli. Należy bowiem zwrócić uwagę na fakt, że spadek powszechności wykorzystania gotówki[27] może się wiązać z ograniczonym dostępem znacznej części społeczeństwa do pieniądza emitowanego przez bank centralny. Innymi słowy, część obywateli jest wówczas niejako „skazana" na prywatne instrumenty płatnicze, których używanie może być z różnych powodów utrudnione lub odbywać się na niekorzystnych warunkach, lub których po prostu nie darzy się zaufaniem. CBDC mogłyby (i powinny) niejako w naturalny sposób zastąpić papierową gotówkę.

Nieco podobną kwestią byłaby możliwość swobodnego dostępu obywateli do CBDC i możliwości wykorzystania tej formy prawnego środka płatniczego w transakcjach z wykorzystaniem nowoczesnych kanałów handlu elektronicznego. Kwestie te rozważa się między innymi w kontekście rozwoju tzw. Internetu Rzeczy. Jeżeli bowiem upowszechniłby się model, w którym towary lub usługi i wiążące się z tym płatności byłyby dokonywane bezpośrednio przez urządzenia domowe (np. lodówkę czy drukarkę) z wykorzystaniem środków udostępnionych przez ich właściciela, to mogłoby jednocześnie wystąpić ryzyko wprowadzania przez producentów tego typu urządzeń (we współpracy z dostawcami usług płatniczych) specyficznych rozwiązań płatniczych, do których dostęp byłby limitowany. Dość łatwo można wyobrazić sobie także zmonopolizowanie tego typu działalności przez jednego dostawcę konkretnych usług i instrumentów płatniczych. W takiej sytuacji – ponownie – CBDC byłoby instrumentem niwelujące takie dyskryminujące praktyki.

Nie negując zalet CBDC związanych z ograniczaniem wykluczenia finansowego, należy jednak wskazać na kilka kwestii. Po pierwsze, by te zalety mogły się ujawnić, konieczny jest brak wykluczenia cyfrowego, co samo w sobie może stanowić pewien problem. Po drugie, wykluczenie finansowe może mieć różne przyczyny i nie wszystkie z nich wiążą się tylko z rozwojem systemu finansowego czy (wysokimi) kosztami usług finansowych – ważne jest tu również zaufanie do instytucji bankowych (również do banku centralnego), zasób wiedzy finansowej czy chęć zachowania prywatności. Stąd, zmniejszanie skali „nieubankowienia", oprócz samego wprowadzenia CBDC wymaga dodatkowo szeroko zakrojonej działalności informacyjnej i edukacyjnej. Po trzecie, rozważając kompensacyjny charakter CBDC w kontekście spadku roli gotówki, należy zaznaczyć, że trend taki nie jest bynajmniej oczywisty. Pomimo dynamicznego rozwoju płatności bezgotówkowych na świecie, wartość gotówki w obiegu w relacji do PKB w większości krajów zarówno rozwiniętych, jak i wschodzących nie obniża się, a nawet rośnie[28].

W przypadku gospodarki polskiej poziom włączenia finansowego jest relatywnie wysoki. również gotówka pozostaje ciągle ważnym elementem w polskiej

25 Warto zaznaczyć, że wszelkie działania w tym zakresie budzą kontrowersje, niezależnie od zaangażowania CBDC – chodzi tu o zakres prywatności transakcji i anonimowości uczestników (zob. szerzej podrozdział 5.4).

26 Usługi te są oczywiście oferowane już przez firmy prywatne. Dostęp do nich może jednak być z jakichś względów ograniczony. Można również popatrzeć na CBDC jako próbę utrzymania przez państwo kontroli nad systemem płatności.

27 To, na ile faktycznie spada wykorzystanie gotówki jest oczywiście rzeczą dyskusyjną i zależy także, jak to sygnalizowano w podrozdziale 2.6, od konkretnego państwa.

28 Oczywiście, ostatnie lata z uwagi na nieprzewidziane i niekorzystne wydarzeń (pandemia, wojna w Ukrainie, drastycznie zwiększających stopień niepewności, nie są reprezentatywne w ocenie popularności gotówki. Z drugiej strony, natężenie wstrząsów jest tak duże i trwa już tak długo, że można oswajać się z myślą, iż stanowią one nową „normalność".

gospodarce[29]. W tej sytuacji, motywy wprowadzenia CBDC również w tym aspekcie nie są przekonujące.

4.5. Możliwość prowadzenia skuteczniejszej i bardziej elastycznej polityki pieniężnej

W literaturze podkreśla się, że jedną z większych zalet prowadzenia CBDC byłyby większe możliwości realizacji polityki pieniężnej przez banki centralne [17]. Wiązałoby się to z kilkoma kwestiami; większość z nich dotyczy sytuacji, w której CBDC jest oprocentowane.

Po pierwsze, bank centralny mógłby – zmieniając oprocentowanie CBDC – bezpośrednio i natychmiast wpływać na oprocentowanie środków podmiotów posiadających CBDC, a tym samym na ich skłonność do oszczędzania i/lub inwestycji. Ponadto, zmiany oprocentowania CBDC wpływałyby oczywiście na oprocentowanie depozytów bankowych, dla których CBDC byłby bezpośrednią konkurencją. Tym samym, wzrosłaby efektywność mechanizmu transmisji stóp procentowych banku centralnego do gospodarki.

Po drugie, wprowadzenie CBDC pozwoliłoby bankom centralnym ograniczyć lub nawet wyeliminować problem wynikający z (efektywnego) dolnego ograniczenia dla nominalnych stóp procentowych (*effective lower bound*). Mianowicie, banki centralne nie są w stanie obniżyć stóp procentowych wyraźnie poniżej zera. Deponenci zawsze mogą bowiem zamienić depozyty na (papierową) gotówkę, której oprocentowanie wynosi zero – a zatem korzystniej, niż depozytów.

Po trzecie, możliwa byłaby potencjalna realizacja programów QE (*Quantitative Easing*) w sposób bezpośredni, przez nabywanie za jednostki cyfrowej gotówki papierów wartościowych bez udziału banków. Oprócz wyeliminowania pośredników, zwiększyłoby to również znacząco liczbę podmiotów, które mogłyby łatwo być stronami tego typu transakcji.

Po czwarte, sygnalizowana potencjalna data ważności CBDC mogłaby stanowić dodatkowy instrument stymulowania zagregowanego popytu w sytuacji zagrożenia recesją. Skrócenie „terminu przydatności" CBDC zwiększałoby zapewne skłonność do wydatków, dając gospodarce impuls wzrostowy[30]. Tego typu rozwiązanie jest jednak bardzo kontrowersyjne.

Zalety te jednak nie są oczywiste. Przede wszystkim, oprocentowanie CBDC budzi wiele wątpliwości jako czynnik naruszający warunki rynkowej konkurencji[31]. To samo dotyczy daty ważności CBDC jako czynnika podważającego zaufanie do cyfrowej gotówki i pozbawiającego jej nieodzownej cechy, jaką powinien mieć każdy pieniądz – pewności przyszłej wartości. Oczywiście, inflacja może pozbawić tej cechy każdy pieniądz, tu jednak chodzi o działanie władz monetarnych z premedytacją. Szukając analogii historycznych, można wskazać na wszelkie sytuacje nieekwiwalentnej reformy monetarnej, w wyniku której obywatele tracili swoje oszczędności (jak np. w roku 1950 w Polsce).

Z kolei wyeliminowanie problemu dolnego ograniczenia dla nominalnych stóp procentowych wymagałoby całkowitego zaniku gotówki papierowej, co w praktyce wymagałoby zapewne prawnego zakazu jej używania. Bez takiego posunięcia ciągle byłaby bowiem możliwa zamiana ujemnie oprocentowanych depozytów lub CBDC na gotówkę papierową. Dyskusyjne jest również, na ile wprowadzenie CBDC stanowiłoby wartość dodaną w stosunku do obecnych rozwiązań. Podkreśla się bowiem – również w odniesieniu do warunków polskich – że obecny mechanizm transmisji polityki pieniężnej jest efektywny, a zmiany stóp procentowych banków centralnych są dość szybko przenoszone na oprocentowanie depozytów i kredytów w sektorze bankowym.

4.6. Możliwość prowadzenia skuteczniejszej polityki fiskalnej i społecznej

Posiadanie przez obywateli danego państwa kont, przez które mieliby oni dostęp do CBDC, dawałoby władzom danego kraju bardzo wygodną opcję pro-

29 Rok 2022, a zwłaszcza jego końcówka, przyniósł pewien odwrót od gotówki. Po pierwsze, trudno jednak ocenić, czy jest to tendencja trwała (choć płynności bezgotówkowe rosną bardzo dynamicznie). Po drugie, niewątpliwy wpływ na to ma wysoka inflacja. Po trzecie, znaczenie miał też wzrost stóp procentowych, zmieniający strukturę oszczędności Polaków.

30 Lub też mogłoby skłonić deponentów do zmiany struktury oszczędności w stronę odejścia od cyfrowej gotówki banku centralnego.

31 Warto tu przypomnieć doświadczenia Polski z lat 90. ubiegłego wieku i reakcje na program przyjmowania lokat od ludności przez NBP.

wadzenia polityki fiskalnej (ale i społecznej). Mianowicie, możliwe byłyby szybkie transfery środków budżetowych do określonych grup społecznych (lub nawet indywidualnych jednostek), zgodnie z przyjętym kształtem polityki fiskalnej. Wprawdzie większym problemem dla polityki fiskalnej są jej opóźnienia (*time lags*) wewnętrzne, a nie zewnętrzne [77], niemniej tego typu sposobność „dedykowanego", punktowego zasilania w fundusze określonych grup obywateli, lub całego społeczeństwa niewątpliwie podniosłaby skuteczność instrumentów fiskalnych – zwłaszcza tych o charakterze ekspansywnym.

Inną kwestią byłaby możliwość realizacji polityki społecznej państwa przez kierowanie jej bezpośrednio do potrzebujących. Ponadto, CBDC, połączone z systemem potwierdzania tożsamości cyfrowej klientów, mogłaby zapewnić sprawną dystrybucję środków z pomocy publicznej w sytuacjach wyższej konieczności (pandemia, klęski żywiołowe). Problemy w te dziedzinie wyraźnie uwidoczniły się podczas pandemii COVID-19.

Powyższe potencjalne zalety cyfrowej gotówki banku centralnego wymagają jednak założenia, że każdy obywatel będzie miał konto CBDC. Polityka fiskalna nie powinna bowiem działać selektywnie tylko na tych, którzy są częścią CBDC, ale powinna obejmować swoim zakresem wszystkich uprawnionych do danego świadczenia/pomocy. Należy również pamiętać, że osoby korzystające z transferów socjalnych relatywnie często są wykluczone cyfrowo.

4.7. Suwerenność monetarna

Zaletą, która nie ma wymiaru wyłącznie ekonomicznego, jest wprowadzenie CBDC jako instrumentu utrzymywania suwerenności monetarnej w sytuacji, gdy cyfrowe waluty innych krajów zaczną być z jakichś względów postrzegane jako atrakcyjne. Dotyczyłoby to zwłaszcza sytuacji, gdyby CBDC wprowadził jako formę swojego pieniądza kraj o silnej, szeroko stosowanej w wymianie międzynarodowej walucie[32].

Jak wspomniano w podrozdziale 2.8, takie CBDC mogłoby stanowić poważną konkurencję dla walut innych krajów, zwłaszcza o słabszym systemie monetarnym i niskiej wiarygodności. Z czasem taki środek płatniczy mógłby być wykorzystany także w krajowych transakcjach płatniczych, co byłoby ryzykowne dla stabilności i bezpieczeństwa funkcjonowania krajowych systemów płatności. Innymi słowy, CBDC silnego kraju przyspieszyłoby proces tzw. „dolaryzacji" kraju o słabszej walucie.

Na względy gospodarcze nakładają się zatem (a czasem wręcz dominują) również kwestie geopolityczne, związane z grą o dominację i wojnami walutowymi (por. podrozdział 2.8). Jak to przykładowo, ujęto w raporcie EBC [40], „cyfrowe euro wsparłoby proinnowacyjne dążenia Europy. Pomogłoby też chronić jej suwerenność finansową i wzmocniło międzynarodową rolę euro". Przyjęcie (lub nie) CBDC byłoby postrzegane jako pewien krok wizerunkowy, wyraz aspiracji danego państwa.

Zbliżoną kwestią jest zachowanie kontroli nad krajowym pieniądzem i jego stosowaniem w obliczu potencjalnego wzrostu znaczenia prywatnych walut cyfrowych i tzw. stabilnych kryptowalut (*stablecoin*)[33], w tym ewentualności rozpoczęcia ich emisji przez korporacje (w tym z obszaru BigTech).

Uznając zasadność tych argumentów, należy jednak zaznaczyć, że występuje tu ryzyko swoistego instynktu stadnego, skutkujące przyjmowaniem CBDC nawet przez kraje, w odniesieniu do których nie byłoby one znaczącym skokiem jakościowym. Podobnie jak w przypadku innych przedstawianych tu zalet CBDC, tutaj również nie ma zatem mowy o uniwersalności. Historia jest pełna przykładów reform i posunięć monetarnych, mających przyczyniać się do wzrostu potęgi danego państwa, których efekt był dokładnie odwrotny, jak choćby kurczowe trzymanie się reliktów systemu waluty złotej w dwudziestoleciu międzywojennym.

4.8. Większa kontrola emisji pieniądza i kwestie renty menniczej

Za zaopatrzeniem w papierową gotówkę wiążą się rozliczne trudności kosztowo-logistyczne. Dotyczy

32 Takie zastosowanie – jako instrumentu wspierania międzynarodowej pozycji – przewiduje się np. dla dolara amerykańskiego w pierwszym opracowaniu Systemu Rezerwy Federalnej, dotyczącym walut cyfrowych [54].

33 Warto tu dodać, że deklarowana stabilność „stabilnych kryptowalut" okazała się dość wątpliwa, czego dowodem mogą być choćby spektakularna utrata wartości kryptowaluty Luna w maju 2022 roku i USDC w marcu 2023 roku (w powiązaniu z upadkiem Sillicon Valley Bank).

to zarówno, krajów rozwijających się, które borykają się z brakiem gotówki papierowej w obliczu takich czynników, jak szybki wzrost gospodarczy, często duży geograficznie obszar do zaopatrzenia w banknoty i bilon oraz słaba sieć instytucji finansowych[34], jak i rozwiniętych, gdzie masa papierowej gotówki w obiegu jest znacząco większa. W obu przypadkach czas i koszty produkcji, dystrybucji, weryfikacji autentyczności znaków pieniężnych i sprawna wymiana zużytych banknotów stanowi bardzo duże wyzwanie dla władz monetarnych[35]. CBDC, po początkowych nakładach nie generujących zasadniczo kosztów, jest tu naturalnym usprawnieniem. Jak wynika z raportu MFW [89], przejście na waluty cyfrowe mogłoby zmniejszyć koszty emisji i obsługi papierowej gotówki nawet o 0,5% do 1,0% PKB.

Ponadto, gdyby udało się wykreować popyt na cyfrową gotówkę mógłby on zrównoważyć spadek popytu na gotówkę papierową, a tym samym zrównoważyć, lub nawet odbudować przychody banków centralnych z renty menniczej (senioratu).

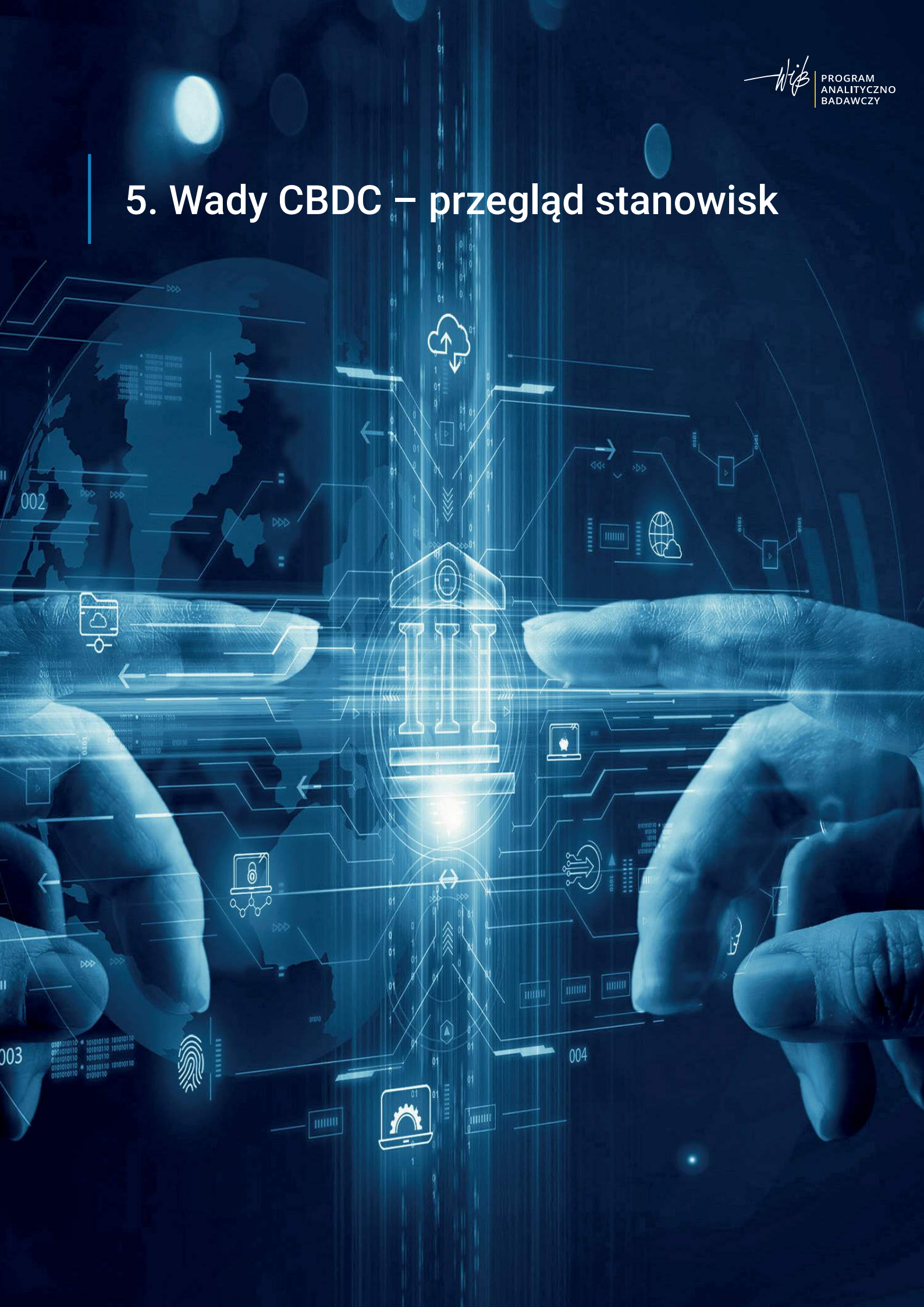
Podsumowując rozważania w tym rozdziale, należy uznać, że zalety CBDC są dość niejednoznaczne. Przede wszystkim warto zwrócić uwagę, że ze względu na heterogeniczność warunków w poszczególnych krajach, jak i mnogość wariantów CBDC (zależnych od doboru i zaprojektowania konkretnych cech), rozwiązanie to zdecydowanie nie jest uniwersalne. Należy także podkreślić dość fundamentalny problem. Mianowicie, między poszczególnymi zaletami i sposobami wykorzystania CBDC pojawiają się sprzeczności. Przykładowo, nie można mieć jednocześnie CBDC jako efektywnego środka płatniczego, podnoszącego sprawność rozliczeń oraz służącego płynnemu obrotowi gospodarczemu, i jako instrumentu polityki pieniężnej. Podobnie, nie da się mieć instrumentu do walki z wykluczeniem finansowymi, któremu obywatele ufają, będącego jednocześnie CBDC z datą ważności, służącego do stymulacji gospodarki lub realizacji innych celów państwa. Ponadto, wielu zalet CBDC nie da się osiągnąć bez odgórnego zakazu stosowania papierowej gotówki, a to nie jest ani celowe, ani zasadne ze społecznego punktu widzenia.

Niemniej, wprowadzenie CBDC może jednak nastąpić z powodów wizerunkowych (chęć tworzenia wizerunku danego państwa jako nowoczesnego i aktywnego w sferze finansowej) lub politycznych, a nie czysto gospodarczych. Takie działanie i motywacje byłyby jednak obarczone dość dużym ryzykiem.

34 Co ciekawe, sytuację np. w państwach afrykańskich ratuje swoisty „import" banknotów drobnych nominałów euro i dolarów, wykorzystywanych następnie w krajowych transakcjach.

35 Osobną kwestią są problemy fałszerstw papierowej gotówki lub nawet kwestie zdrowia i higieny, co dobitnie uwidoczniała pandemia COVID-19.

5. Wady CBDC – przegląd stanowisk



5.1. Zakłócenie modeli biznesowych banków i tendencje dezintermediacyjne

Wśród potencjalnych problemów związanych z wprowadzeniem CBDC warto w pierwszej kolejności zwrócić uwagę na konsekwencje, jakie rodziłoby to dla pozostałych banków. Niewątpliwie wpływ ten będzie różnił się w zależności od przyjętego modelu CBDC. Największe wątpliwości budziłaby opcja CBDC eliminująca instytucje bankowe, a także kwestia oprocentowania cyfrowej waluty banku centralnego.

Rozważając to pierwsze zagadnienie, warto zauważyć, że gdyby wprowadzony system CBDC oferował obywatelom pieniądz cyfrowy, możliwości wygodnego i bezkosztowego posługiwania się nim oraz przechowywania dowolnej kwoty na całkowicie bezpiecznym rachunku w banku centralnym[36], to sytuacja taka stanowiłaby trudną do sprostania konkurencję dla pozostałych banków. Można by wtedy oczekiwać odpływu depozytów bankowych na rzecz rachunków CBDC, gdyż te pierwsze staną się relatywnie mniej atrakcyjne.

W takiej sytuacji banki stoją przed dwoma wyborami. Muszą albo poszukać nowych (droższych i/lub bardziej ryzykownych) form operacji pasywnych, by zrekompensować odpływ środków z rachunków klientów, albo podwyższyć oprocentowanie, by skłonić w ten sposób klientów do pozostawienia depozytów w danym banku. Obie opcje pogarszają sytuację tych instytucji. Można nawet założyć, że zwiększyłoby się wówczas ryzyko wzrostu oprocentowania kredytów bankowych. Przy wyższych stopach procentowych od wkładów zmniejszyłaby się bowiem marża odsetkowa. By utrzymać ją na niezmienionym poziomie, kredyty musiałyby stać się dla klientów bankowych droższe.

Mechanizm ten może wystąpić nawet wtedy, gdy CBDC w banku centralnym nie będą oprocentowane. Ciągle bowiem cyfrowa gotówka przechowywana w ten sposób dysponuje walorem w postaci większego bezpieczeństwa[37] oraz – potencjalnie – szerokiego wykorzystania w płatnościach. Jeżeli jednak CBDC byłoby oprocentowane, opisane zależności wystąpią na znacznie większą skalę, stawiając banki w jeszcze gorszym położeniu.

Rozumowanie to można rozszerzyć. Mianowicie, przy bezpośrednim, oprocentowanym modelu CBDC, cały system finansowy mógłby zmierzać w stronę tzw. monobanku. Jeśli bowiem banki nie byłyby w stanie uzupełnić depozytów, które odpłynęły do kont CBDC w drodze rynkowych operacji pasywnych (pożyczki międzybankowe, emisja papierów wartościowych itp.), musiałyby ostatecznie refinansować się w banku centralnym. Zabezpieczeniem kredytu refinansowego byłyby aktywa posiadane przez banki – głównie kredyty dla prywatnego sektora niefinansowego. W rezultacie, nastąpiłoby przeniesienie na bank centralny ryzyka kredytowego, a tym samym ten ostatni mógłby być zmuszony do interwencji w proces kredytowania. Zacząłby więc wkraczać na kolejny obszar niejako zarezerwowany dla banków. Ponadto, bank centralny cały czas mógłby umacniać swoją pozycję i rolę w obszarze płatności i rozliczeń. Coraz mniej byłoby zatem obszarów, w których banki nie napotykałyby na konkurencję (nierynkową) ze strony banku centralnego.

Pojawiłoby się zatem zjawisko tzw. dezinteremediacji, czyli zmniejszania udziału banków w aktywach systemu finansowego[38]. Znaczenie tych tradycyjnych pośredników finansowych, i tak już nadwątlone opisanymi w podrozdziale 2.5. procesami i konkurencją podmiotów niefinansowych, jeszcze bardziej by zmalało.

Trudno sobie wyobrazić, żeby struktura monobanku była skuteczna w warunkach gospodarki rynkowej. Oczywisty byłby tu konflikt różnych ról i celów banków centralnych, prowadzący – między innymi – do zanikania potencjalnych korzyści z wprowadzenia CBDC. Niewątpliwie, prowadziłoby to również do przeciążenia banków centralnych, już obecnie borykających się z rozmaitymi zadaniami. CBDC, nowy instrument w gestii władz monetarnych, przyniósłby zatem, nieco paradoksalnie, nowe obowiązki i zagrożenia dla banków centralnych.

Jednocześnie mogłaby rosnąć rola podmiotów z sektora tzw. bankowości równoległej (*shadow*

36 Innymi słowy, cyfrowa gotówka pełniłaby zarówno funkcję środka płatniczego, jak i środka skarbienia. Jednocześnie, będąc denominowaną w walucie krajowej, cały czas pozostawałaby przy tym jednostką obrachunkową.

37 Jest to argument niebagatelny w sytuacji rysujących się napięć w systemach bankowych poszczególnych krajów w końcu pierwszego kwartału 2023 roku

38 Jak się wydaje, proces ten byłby bardziej wyraźny, a jednocześnie bardziej dotkliwy, w systemach finansowych typu uniwersalnego (europejskiego), opartych głównie na bankach.

banking, paralel banking) [104]. To jednak zwiększyłoby, jak się wydaje, poziom ryzyka i niepewności w systemie finansowym i całej gospodarce, z uwagi na nie do końca jasny status prawny takich instytucji oraz niewystarczające regulacje ich funkcjonowania. „Tradycyjne" banki, mimo całej krytyki, z jaką spotykają się od kryzysu lat 2007–2009, są jednak dalece bardziej przewidywalne, a realizowany przez nie zdecentralizowany proces kredytowy jest zasadniczo efektywny.

Rozumiejąc te problemy, banki centralne w swoich opracowaniach na temat CBDC deklarują raczej pośredni model cyfrowej gotówki i dość ostrożnie wypowiadają się w kwestii jej potencjalnego oprocentowania. Jak się jednak wydaje, sama możliwość wykorzystania tego narzędzia sprawiałaby, że, prędzej czy później, sięgnięto by po nie, z wszystkimi opisanymi tutaj konsekwencjami.

5.2. Problemy z zapewnieniem stabilności finansowej

Z problemem opisanym w podrozdziale 5.1. bezpośrednio wiąże się kwestia potencjalnych trudności z zapewnieniem stabilności finansowej, a tym samym – tworzeniem warunków, minimalizujących ryzyko wystąpienia kryzysu finansowego (bankowego lub walutowego). Mianowicie, bank centralny mógłby, wskutek opisanego mechanizmu zamiany depozytów bankowych na CBDC, doprowadzić do destabilizacji systemu finansowego.

Zważywszy, że pieniądz banku centralnego jest najbezpieczniejszą dostępną formą pieniądza, CBDC byłyby szczególnie atrakcyjne dla użytkowników unikających ryzyka i szukających pewnych, bezpiecznych inwestycji. W sytuacji napięć na rynkach finansowych mogliby oni łatwo zamienić swoje oszczędności w bankach na CBDC w banku centralnym[39]. Te ostatnie stanowiłyby swoistą „bezpieczną przystań" (*safe haven*), ułatwiając klientom bankowym zagwarantowanie bezpieczeństwa swoim środkom – zwłaszcza tym przewyższającym kwotę wypłaty gwarantowanej przez instytucje sieci bezpieczeństwa.

Zrozumiałe jest, że tego typu działania byłyby najbardziej zintensyfikowane w okresach zagrożeń (rzeczywistych lub antycypowanych) dla sektora bankowego, a więc wtedy, gdy stabilność i brak nieoczekiwanych wypłat z banków byłyby najbardziej pożądane. CBDC może zatem zwiększyć prawdopodobieństwo (a także skalę) runu na banki. Tradycyjne środki, takie jak nadzór ostrożnościowy, ubezpieczenie depozytów rządowych i dostęp do płynności banku centralnego mogą w takiej sytuacji nie wystarczyć, aby powstrzymać masowy odpływ depozytów bankowych do CBDC[40]. W przekonaniu klientów bankowych, CBDC będą po prostu zawsze lepszą opcją w sytuacji zagrożeń dla stabilności finansowej.

Co przy tym paradoksalne, im większy byłby sukces i popularność CBDC, tym silniejszy byłby mechanizm potencjalnego poszukiwania „bezpiecznej przystani" CBDC, a co za tym idzie – większa destabilizacja.

5.3. Ryzyko spadku reputacji i utraty wiarygodności

Tak poważna reforma i zmiana systemu monetarnego, jaką byłoby wprowadzenie CBDC wymaga wiarygodności instytucji państwowych (głównie banku centralnego), odpowiedniej przejrzystości całego procesu, wyboru rozwiązań technicznych i organizacyjnych najbardziej adekwatnych dla danego państwa, i wreszcie odpowiedniej polityki informacyjnej ze strony władz państwowych. Konieczne jest również przemyślenie całej gamy rozwiązań ogólnych, jak i bardzo wielu szczegółów operacyjnych, z których każdy może decydować o powodzeniu całego przedsięwzięcia.

Każda zmiana ustroju pieniężnego zawsze budziła kontrowersje, niepewność czy wręcz obawy ze strony tych, którzy w takiej sytuacji mieli najwięcej do stracenia, a więc posiadaczy środków pieniężnych. Ilekroć reforma była źle zaprojektowana, wprowadzona zbyt nagle i bez odpowiedniego przygotowania, pociągało to za sobą znaczące napięcia społeczne i perturbacje gospodarcze[41].

39 Oczywiście mógłby też wystąpić tu mechanizm blokowania wypłat przez banki. Zważywszy jednak na charakter i cechy CBDC oraz ich powiązania z bankiem centralnym, raczej nie byłby on skuteczny.

40 Niekontrolowanemu przepływowi środków do banku centralnego można by przeciwdziałać ustanawiając limity kwotowe odnośnie do realizowanych transakcji lub wysokości salda rachunków CBDC odpowiednio dla osób fizycznych i podmiotów gospodarczych. Inną opcja byłoby ograniczenie możliwości zamiany wkładów bankowych na CBDC lub nakładanie opłat z tego tytułu. To jednak w oczywisty sposób zniechęcałoby do CBDC, czego jego emitenci chcieliby zapewne uniknąć.

41 Jako jeden z najnowszych przykładów można podać denominację przeprowadzoną w Indiach w 2016 roku.

Jak się wydaje, przejście z gotówki papierowej na cyfrową, w dodatku opartą na – jak się na ogół postuluje – technologiach dość trudnych do zrozumienia dla przeciętnego odbiorcy (często kojarzonych z niestabilnymi kryptowalutami), byłoby operacją szczególnie wrażliwą. Co za tym idzie, potencjalne niepowodzenie (czy nawet przejściowe problemy) we wprowadzeniu CBDC może całkowicie zdestabilizować sferę monetarną danego kraju. Nie chodzi tu nawet o niepowodzenie samej cyfrowej gotówki, ale o ogólną utratę wiarygodności przez władze monetarna co za tym idzie – odwrót od danej waluty.

5.4. Kwestia anonimowości, braku prywatności i możliwości kontroli ze strony państwa

Jak to ujęto w raporcie Systemu Rezerwy Federalnej [54], każda CBDC musiałaby zachować odpowiednią równowagę między ochroną prywatności obywateli, przy jednoczesnym zapewnieniu przejrzystości niezbędnej do powstrzymania działalności przestępczej. Jak się wydaje, właśnie kwestia praw obywatelskich, prywatności i anonimowości jest najczęściej postrzegana jako wada CBDC.

W powszechnej dyskusji, zwłaszcza między laikami, CBDC postrzega się jako instrument niejako „domykający" system nadzoru nad obywatelami[42]. Pozwala on bowiem, w przekonaniu przeciwników CBDC, na monitorowanie każdej transakcji oraz zmuszanie (przez ewentualną datę ważności CBDC) do wydatkowania środków pieniężnych[43]. Rzeczywiście, przykładowo, w opracowaniach Riskbanku [120], [121] przyznaje się, że wszystkie transakcje e-kroną byłyby możliwe do wyśledzenia.

Niewątpliwie, stopień anonimowości i prywatności CBDC byłby żaden. Z drugiej jednak strony, również istniejące obecnie rozwiązania w zakresie płatności bezgotówkowych nie pozwalają na ukrywanie transakcji. Ponadto, ważne są tu kwestie ustrojowe – można by optymistycznie założyć, że w państwie demokratycznym agendy rządowe nie będą nadużywały możliwości inwigilacji obywateli. Stąd, zarzuty pod adresem CBDC można uznać, za Prasadem [105], za nieco przesadzone[44].

Inaczej oczywiście mogą mieć się sprawy w krajach autorytarnych. Tutaj można wskazać przede wszystkim na przypadek Chin i łatwe do wyobrażenia wykorzystywanie cyfrowego yuana nie tylko do celów gospodarczych, ale i do skuteczniejszej kontroli obywateli. W szczególności, bardzo groźnym rozwiązaniem byłoby połącznie chińskiego CBDC z funkcjonującym w tym kraju systemem „zaufania społecznego" (*social credit)*[45].

42 Prasad [105] zauważa, że problem ma tu w dużej mierze charakter generacyjny – największe obawy względem CBDC wyrażają tzw. millenialsi oraz reprezentanci pokolenia „Z".

43 Oczywiście, na najbardziej podstawowym poziomie CBDC jest krytykowane jako wręcz „grabarz" papierowej gotówki, z którą tradycyjnie utożsamiają się osoby o wolnościowych poglądach.

44 Z drugiej strony, autor ten zauważa trzeźwo, że w zasadzie nie ma powodów, dla których banki centralne miałyby się troszczyć o prywatność i anonimowość swoich instrumentów. Nigdzie nie jest to bowiem ich celem ani częścią ich mandatu [105].

45 Zwrot ten często tłumaczy się na język polski jako „kredyt społeczny".

PROGRAM ANALITYCZNO BADAWCZY

6. Podstawowe rozwiązania techniczne kryptowalut

6.1. Wstęp

CBDC są inspirowane kryptowalutami [58], które były przełomową innowacją, choć nie odgrywają tak wielkiej roli gospodarczej jak to się marzyło ich twórcom. Dlatego dla dyskusji o CBDC tak ważne jest zrozumienie podstawowych rozwiązań technicznych, które leżą u podstaw kryptowalut. W tym rozdziale przedstawiono najpierw dwie podstawowe techniki, które są szeroko stosowane w kryptowalutach, ale które powstały znacznie wcześniej i mają uniwersalny charakter – funkcję skrótu i cyfrowy podpis.

Następnie przedstawiono techniki stosowane w Bitcoinie[46]: konstrukcję łańcucha bloków, kopanie umożliwiające przestawienie dowodu pracy, rolę transakcji i portfeli, zasady emisji bitcoinów, konstrukcję rozproszonego rejestru i sposób osiągania globalnego konsensusu bez centralnego serwera. Szczególną uwagę poświęcono problemowi podwójnego wydatkowania pieniędzy, ponieważ od niego zależy, co można, a czego nie można osiągnąć implementując dowolny cyfrowy pieniądz.

W dalszej części tego rozdziału przedstawiono rozwiązania zastosowane w Ethereum, rozpoczynając od jego koncepcji jako rozproszonego światowego komputera, inteligentnych kontraktów, kont i transakcji. Omówiono tokeny w Ethereum, których koncepcja może być przydatna do implementacji CBDC, oraz przedstawiono dowód stawki stosowany od niedawna w Ethereum Merge, jako mniej energochłonny i szybszy sposób osiągania globalnego konsensusu bez centralnego serwera niż dowód pracy.

W końcowej części tego rozdziału przedstawiono porównawcze dane dotyczące przepustowości kryptowalut oraz przeanalizowano problem prywatności.

6.2. Funkcja skrótu

Funkcja skrótu SHA3 (*hash function*) [97] zamienia dokument cyfrowy o dowolnej długości na 256-bitową liczbę binarną zwaną „skrótem", „odciskiem" lub „haszem" (*hash*). Dla funkcji skrótu nie istnieje funkcja odwrotna, zatem z dokumentu można utworzyć skrót, ale ze skrótu nie można odtworzyć dokumentu. Funkcja skrótu taką właściwość, że zmiana choćby jednego bitu w dokumencie wpływa na każdy bit skrótu – z około 50-procentowym prawdopodobieństwem każdy bit skrótu ulegnie zmianie. Zatem po zmianie choćby jednego bitu w dokumencie statystycznie połowa jedynek w skrócie zmieni się na zera, a połowa pozostanie jedynkami; analogicznie połowa zer zmieni się na jedynki, a połowa pozostanie zerami. Te zmienione zera i jedynki będą rozrzucone po całym skrócie. Dlatego cały skrót będzie z bardzo dużym prawdopodobieństwem inną liczbą binarną. Z praktycznego punktu widzenia można przyjąć, że funkcja skrótu zastosowana do dwóch różnych dokumentów wygeneruje dwa różne skróty. Funkcja skrótu jest funkcją deterministyczną, co oznacza, że zastosowana wielokrotnie do tego samego dokumentu zawsze wygeneruje taki sam skrót.

Dla pełności obrazu należy wyjaśnić, że z matematycznego punktu widzenia z faktu, że na wejście funkcji skrótu można podać nieskończoną liczbę dokumentów, a skrótów jest 2^{256}, to na każdy skrót przypada nieskończenie wiele dokumentów. Jednak prawdopodobieństwo, że dwa bliskoznaczne, sensowne dokumenty wygenerują ten sam skrót jest bliskie zeru. Dlatego funkcja skrótu może być zastosowana do wykrywania fałszerstw, co zostanie opisane w podrozdziale 6.3.

6.3. Cyfrowy podpis

U podstaw cyfrowego podpisu leży kryptografia z parą kluczy: prywatnym i publicznym. Jej twórcami są trzej amerykańscy naukowcy Ronald Rivest, Adi Shamir i Leonard Adleman, którzy opracowali system RSA [111].

Jak sama nazwa wskazuje, klucz prywatny jest objęty tajemnicą – jego właściciel (człowiek lub komputer) nie może go nikomu udostępnić. Musi on pozostawać tylko do jego wiadomości pod groźbą złamania szyfrowania lub podszycia się pod niego. Natomiast klucz publiczny może być przekazany dowolnej osobie lub dowolnemu komputerowi.

Cechą charakterystyczną tej kryptografii jest to, że plik z tekstem zaszyfrowany za pomocą klucza prywatnego nie może być odszyfrowany tym samym kluczem. Do jego odszyfrowania trzeba użyć klucza publicznego od pary. Podobnie plik z tekstem zaszyfrowany za pomocą klucza publicznego nie może być odszyfrowany tym samym klu-

46 Bitcoin pisany z wielkiej litery oznacza system, a z małej – kryptowalutę.

czem. Do jego odszyfrowania trzeba użyć klucza prywatnego od pary.

Kryptografii z parą kluczy: prywatnym i publicznym używa się w dwóch celach: utajnienia informacji i autentykacji, czyli podpisu cyfrowego.

Jeśli mamy dwie komunikujące się strony: nadawcę A i odbiorcę B, to jeśli A chce wysłać tajną wiadomość do B, szyfruje plik ze swoim tekstem za pomocą klucza publicznego odbiorcy B. Wówczas tylko B, jako posiadacz klucza prywatnego od pary, będzie w stanie go odszyfrować.

Autentykacja wymaga potwierdzenia dwóch rzeczy: po pierwsze, że wiadomość pochodzi od danego nadawcy oraz po drugie, że wiadomość nie została zmieniona w trakcie transmisji. W tym celu nadawca A tworzy skrót swojej wiadomości za pomocą funkcji skrótu i szyfruje go za pomocą swojego klucza prywatnego. Odbiorca B po otrzymaniu niezaszyfrowanej wiadomości i zaszyfrowanego skrótu, najpierw tworzy własny skrót z tej wiadomości za pomocą tej samej funkcji skrótu, potem odszyfrowuje przesłany mu skrót za pomocą publicznego klucza nadawcy A i porównuje oba skróty. Jeśli są identyczne, to wiadomość jest autentyczna, a ponieważ do odszyfrowania użył publicznego klucza nadawcy A, to wie, że do zaszyfrowania musiał być użyty klucz prywatny nadawcy A, który zna tylko on.

Zatem cyfrowym podpisem pod dokumentem jest skrót z niego zaszyfrowany za pomocą klucza prywatnego osoby podpisującej.

Oczywiście utajnianie i autentykację wiadomości można łączyć. Warto natomiast zauważyć, że autentykacja nie musi oznacza identyfikacji osoby podpisującej, choć w sytuacji podpisu fizycznego na papierze tak jest, bo osoba podpisuje się swoim imieniem i nazwiskiem. W [27] zaproponowano ślepy podpis cyfrowy, który zastosowany do cyfrowych płatności [35] uniemożliwia bankom wykrycie związku między płatnikiem a odbiorcą płatności.

Dla dopełnienia obrazu przedstawimy jeszcze rolę certyfikatu cyfrowego, którego zadaniem jest uniemożliwienie ataku polegającego na podszyciu się pod inną osobę. Cyfrowe certyfikaty są wydawane przez tzw. Zaufane Strony Trzecie (*Trusted Third Parties*), które muszą spełniać szereg kryteriów określonych w ustawie o usługach zaufania oraz identyfikacji elektronicznej [134]. Cyfrowy certyfikat potwierdza związek między daną osobą fizyczną lub prawną a jej kluczem publicznym. Jest on podpisany cyfrowo przez Zaufaną Stronę Trzecią. W celu uniemożliwienia podszycia się pod nadawcę A przez inną osobę, dołącza on cyfrowy certyfikat do przesyłanej wiadomości i skrótu zaszyfrowanego swoim kluczem prywatnym. Odbiorca B do odszyfrowania przesłanego skrótu używa klucza publicznego nadawcy A pobranego z certyfikatu, który stanowi dowód, że ten klucz należy do A.

6.4. Łańcuch bloków

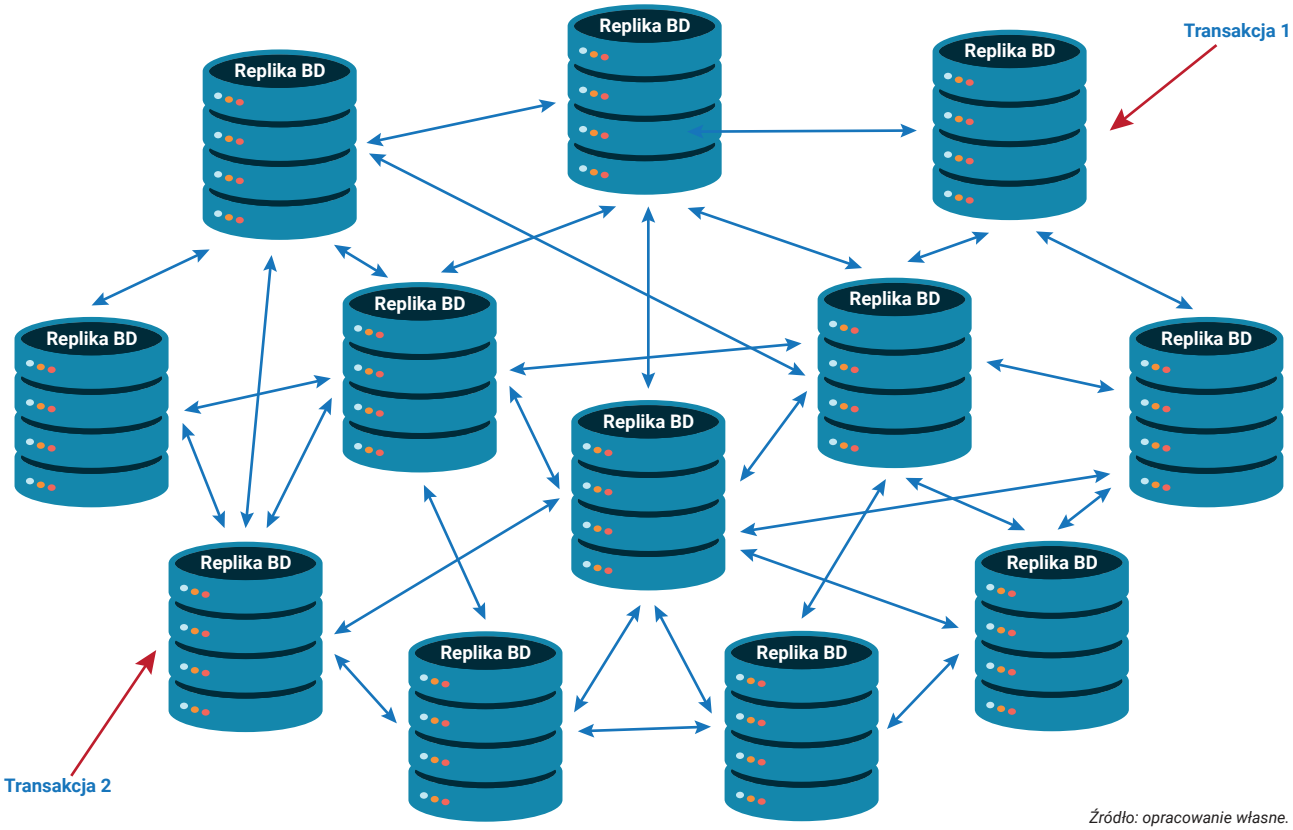
Łańcuch bloków był wymyślony i po raz pierwszy użyty przez dwóch kryptologów: Stuarta Habera i Scotta Stornetta'ę [59], którzy zastosowali go w dzienniku *New York Times* do artykułów [98] w celu bezspornego określania kolejności ich pojawiania się, co miało znaczenie dla ustalenia praw autorskich. Ten łańcuch bloków stał się inspiracją dla Satoshi Nakamoto – twórcy Bitcoina [92]. Z kolei łańcuch bloków Bitcoina stał się inspiracją dla jego licznych modyfikacji dla różnych zastosowań. Takie adaptacje ułatwia fakt, że oprogramowanie Bitcoina ma otwarty kod, który można bezpłatnie pobrać i dostosować do dowolnych celów.

Na gruncie teorii baz danych łańcuch bloków jest złożeniem dwóch koncepcji:

- rozproszonej, w pełni replikowanej bazy danych oraz
- historycznej bazy danych.

Przykład rozproszonej, w pełni replikowanej bazy danych jest przestawiony na Rysunku 1. Warto zauważyć, że baza danych jest rozproszona, ale informacja zawarta w niej jest scentralizowana. W stanie ustalonym każda lokalna baza danych zawiera dokładnie taką samą, pełną informację. W trakcie działania rozproszonej bazy danych lokalne bazy kontaktują się ze sobą w celu spójnego uaktualnienia. Trudność w zarządzeniu taką bazą danych polega na konieczności rozwiązywaniu konfliktów, jakie mogą wyniknąć z faktu, że w prawie takim samym czasie zostaną wykonane dwie transakcje zaadresowane do różnych lokalnych baz danych. Pomimo nieuniknionych opóźnień w uaktualnianiu kolejnych lokalnych baz danych, wynikających z czasów propagacji, wszystkie one muszą docelowo wykonać transakcje w tej samej kolejności, aby zachować spójność rozproszonej bazy danych. Ten

Rysunek 1. Rozproszona, w pełni replikowana baza danych



Źródło: opracowanie własne.

problem pod nazwą „zarządzenie współbieżnością w rozproszonych bazach danych" był przedmiotem badań od końca lat osiemdziesiątych dwudziestego wieku [26]. Sposób rozwiązania tego problemu w Bitcoinie przedstawiono w podrozdziale 6.9.

W historycznych bazach danych żadna dana nie jest nigdy uaktualniana (zmieniana) ani usuwana. Jeśli jakaś transakcja chce zmienić wartość danej, to nowa wartość jest zapisywana obok starej jako jej nowa wersja. W historycznej bazie danych jest przechowywana pełna historia zmian każdej danej.

Dysponując tymi dwoma pojęciami można zdefiniować łańcuch bloków jako rozproszoną, w pełni replikowaną, historyczną bazą danych.

Blok, o którym mowa w tym raporcie, zawiera zbiór cyfrowych dokumentów. W przypadku Bitcoina tymi dokumentami są transakcje finansowe bitcoinami; w innych przypadkach mogą to być różne dokumenty w zależności od konkretnego zastosowania.

Poniżej przestawiono organizację łańcucha bloków w Bitcoinie traktując je jako wzorcowe.

Rysunek 2. Struktura bloku w Bitcoinie

Rozmiar	Pole	Opis
4 bajty	Rozmiar bloku	Rozmiar bloku w bajtach następujących po tym polu
80 bajtów	Nagłówek bloku	Pola składające się na nagłówek bloku
1–9 bajtów	Licznik transakcji	Liczba transakcji w tym bloku
Zmienna	Transakcje	Transakcje zapisane w tym bloku

Rysunek 3. Struktura nagłówka bloku w Bitcoinie

Rozmiar	Pole	Opis
4 bajty	Wersja	Numer wersji oprogramowania/ protokołu
32 bajty	Skrót nagłówka poprzedniego bloku	Odwołanie do identyfikatora (skrótu nagłówka) rodzica w łańcuchu bloków
32 bajty	Korzeń drzewa Merkle'a	Skrót korzenia drzewa Merkle'a transakcji w tym bloku
4 bajty	Znacznik czasowy	Przybliżony czas utworzenia tego bloku (sekundy z Unix Epoch)
4 bajty	Stopień trudności	Stopień trudności algorytmu „Dowód Pracy" dla tego bloku
4 bajty	Niuans (*nonce*)	Liczba używana w algorytmie „Dowód pracy"

Strukturę bloku w Bitcoinie przedstawiono na Rysunku 2 [4].

Warto zwrócić uwagę na fakt, że zarówno liczba transakcji w bloku, jak i rozmiar transakcji, są zmienne. Każdy blok ma nagłówek, którego strukturę w Bitcoinie przedstawiono na Rysunku 3 [4].

Łańcuch bloków (*blockchain*) jest listą bloków powiązanych wstecznie – por. Rysunek 4.

Łańcuch bloków jest często obrazowany jako pionowy stos z blokami leżącymi jeden na drugim, gdzie pierwszy blok nazywany „blokiem genezy" (*Genesis*) jest podstawą całego stosu, a ostatni jest nazywany „koniuszkiem" (*tip*).

Każdy blok jest identyfikowany w łańcuchu bloków nie przez sekwencyjną liczbę, tylko przez skrót wygenerowany za pomocą algorytmu SHA-3 zastosowanego do nagłówka bloku.

Każdy blok odwołuje się do poprzedniego bloku, nazywanego „rodzicem", w polu swojego nagłówka o nazwie „skrót nagłówka poprzedniego bloku" – por. Rysunek 4.

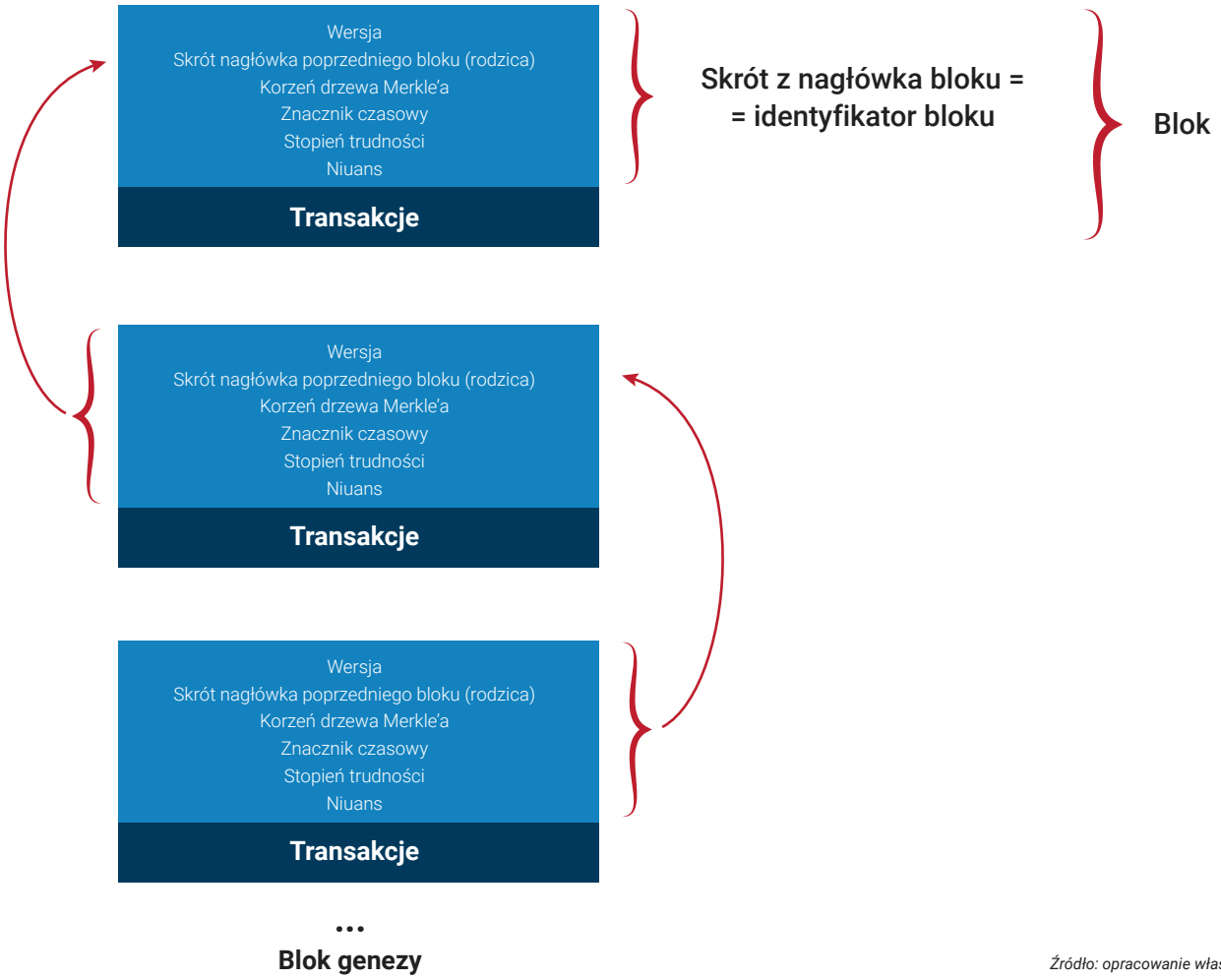
Sekwencja skrótów łączących każdy blok ze swoim rodzicem tworzy łańcuch aż do bloku genezy.

Pole „Skrót nagłówka poprzedniego bloku" znajduje się wewnątrz nagłówka bloku, a zatem wpływa na skrót nagłówka bieżącego bloku. Jak wynika z właściwości funkcji skrótu (por. podrozdział 6.2) skrót nagłówka dziecka musiałby się zmienić, gdyby zmienił się skrót nagłówka rodzica, a to miałoby miejsce w przypadku jakiejkolwiek zmiany w bloku rodzica, gdyż spowodowałaby ona zmianę jego nagłówka. Z kolei zmiana nagłówka dziecka wymagałaby zmiany nagłówka wnuka itd. Ten efekt kaskadowy sprawia, że gdy blok ma wielu następców, to nie można go zmienić bez konieczności ponownego obliczenia skrótów nagłówków wszystkich następnych bloków. W Bitcoinie i innych zastosowaniach łańcucha bloków opartych na dowodzie pracy (por. podrozdział 6.5) takie ponowne obliczenie wymagałaby ogromnej mocy obliczeniowej (a zatem zużycia bardzo dużej energii), zatem istnienie długiego łańcucha bloków po danym bloku zapewnia jego niezmienność.

Wymienione na Rysunku 3 drzewo Merkle'a [88] jest binarnym drzewem[47] skrótów z transakcji zawartych w bloku. Zapewnia ono niezmienność transakcji, ponieważ korzeń drzewa Merkle'a znajduje się

47 Drzewo binarne jest acyklicznym, spójnym grafem, w którym każdy wierzchołek ma co najwyżej dwa następniki [142].

Rysunek 4. Łańcuch bloków w Bitcoinie



Źródło: opracowanie własne.

w jednym z pól nagłówka bloku. Zatem jakakolwiek zmiana transakcji spowodowałaby zmianę jej skrótu, a w konsekwencji zmianę drzewa Merkle'a, w tym jego korzenia. Zmiana korzenia drzewa Merkle'a wpłynęłaby na zmianę nagłówka bloku i jego skrótu z konsekwencjami opisanymi powyżej. Ponadto drzewa Merkle'a umożliwiają efektywne sprawdzanie, czy dana transakcja jest zawarta w bloku.

6.5. Dowód pracy – kopanie

Do zabezpieczenia łańcucha bloków przed zmianami służy proces nazywany „kopaniem" (*mining*) wykonywany przez osoby zwane „kopaczami" (*miners*). Ich celem jest znalezienie takiego niuansu będącego polem w nagłówku bloku (por. Rysunek 3), aby skrót z nagłówka był mniejszy od stopnia trudności. Stopień trudności jest 256-bitową liczbą binarną, czyli ma taką samą długość jak skróty generowane przez funkcję SHA-3. Stopień trudności ma określoną liczbę zerowych bitów na początku – na przykład 60. Zatem celem kopaczy jest znalezienie takiego niuansu, aby skrót z nagłówka bloku miał więcej zer na początku niż stopień trudności. Jedyną znaną metodą znalezienia takiego niuansu jest przyjęcie pewnej wartości niuansu, obliczenie skrótu z nagłówka bloku z tym niuansem i sprawdzenie, czy ma wymaganą liczbę zer na początku. Jeśli nie, to przyjęcie innej wartości niuansu i powtórzenie obliczenia.

Znalezienie właściwego niuansu, które jest nazywane dowodem pracy (*Proof of Work*), wymaga ogromnej mocy obliczeniowej, a zatem też kosztownej energii elektrycznej[48]. Przy poziomie trudności

48 Przykładowo, z raportu Polskiego Instytutu Ekonomicznego [101] wynika, że w 2021 roku roczne zużycie energii przez dwie najpopularniejsze kryptowaluty, czyli bitcoin i ether, wyniosło łącznie ponad 175 TWh, przekraczając łączne zapotrzebowanie energetyczne Polski (ok. 165 TWh).

60 zerowych bitów, pojedynczy kopacz wykonujący 1 bilion haszy (10^{12}) na sekundę za pomocą komputera wyspecjalizowanego tylko do liczenia skrótów, tzw. „koparki" (*bitcoin rig*), jest w stanie znaleźć rozwiązanie średnio co 59 dni. Średnio potrzeba więcej niż 1,8 petahaszy (10^{15}) na sekundę, aby sieć Bitcoin wykopała następny blok. To wydaje się graniczyć z niemożliwością, ale na szczęście sieć bitcoin dysponuje mocą obliczeniową 3 exahaszy (10^{18}) na sekundę, dzięki czemu można wykopać blok średnio w około 10 minut.

Te 10 minut jest parametrem w systemie Bitcoin. Oznacza to, że jeśli bloki są średnio kopane szybciej niż co 10 minut, to poziom trudności automatycznie wzrasta, a jeśli wolniej – to się obniża.

6.6. Transakcje i portfele

Każdy bitcoin lub jego część (bitcoin dzieli się na 100 milionów satoshi, które są najmniejszą podjednostką bitcoina) ma swojego właściciela. Właściciel jest identyfikowany za pomocą pseudonimu zawierającego jego klucz publiczny. Para kluczy prywatny–publiczny jest samodzielnie generowana przez właściciela, więc nie korzysta on z Zaufanej Strony Trzeciej (por. podrozdział 6.3) i nie wymaga certyfikatu.

Transakcja jest zapisem o charakterze księgowym z kogo na kogo przeszła własność bitcoina lub jego części. Każda transakcja jest podpisana cyfrowym podpisem płatnika, który potwierdza nim przekazanie własności odbiorcy płatności.

Każda transakcja jest identyfikowana skrótem z niej. Transakcja zawiera listę wejść i wyjść. Wejścia są skrótami transakcji, w których płatnik nabył bitcoiny. Wyjścia są pseudonimami odbiorców płatności. Wśród odbiorców płatności może też być sam płatnik w celu wypłacenia sobie reszty, jeśli z transakcji podanych na wejściu wynika, że jest właścicielem większej liczby bitcoinów niż chce przekazać odbiorcom płatności. Konieczność wydawania reszty wynika z braku kont w Bitcoinie – model UTXO (*Unspent Transaction Output*) [135].

Transakcja zawiera też opłatę transakcyjną w bitcoinach, która trafi do tego kopacza, który wykopie blok zawierający tę transakcję, i dołączy go do łańcucha bloków.

Transakcje są formowane w „portfelach", które są oprogramowaniem przeznaczonym do przechowywania kluczy i operowania na bitcoinach [4]. Jednym z głównych zadań portfela danego właściciela jest poszukanie w łańcuchu bloków transakcji, w których przekazano temu właścicielowi bitcoiny włącznie z UTXO w liczbie co najmniej równej zaplanowanej płatności wraz z opłatą transakcyjną.

6.7. Emisja bitcoinów

Nowe bitcoiny są emitowane w każdym nowo wykopanym bloku dołączonym do łańcucha bloków. Ich właścicielem staje się kopacz, który tego dokonał. Otrzymuje on też opłaty transakcyjne ze wszystkich transakcji zawartych w bloku.

Początkowo liczba nowych bitcoinów w bloku wynosiła 50. Co 210 tysięcy wykopanych bloków, czyli co około cztery lata, liczba ta jest zmniejszana o połowę. Obecnie wynosi 6,25 bitcoina. Maksymalna liczba bitcoinów wynosi 21 milionów i będzie wykopana około roku 2140. Po tej dacie nagrodą za kopanie bitcoinów będą tylko opłaty transakcyjne. Aktualnie wykopano już 19 milionów bitcoinów [126].

6.8. Problem podwójnego wydatkowania pieniędzy

Jednym z fundamentalnych problemów, który musi być rozwiązany w każdym przypadku płatności pieniędzmi, jest problem podwójnego wydatkowania pieniędzy. Chodzi o to, aby ktoś nieuczciwy nie mógł skopiować banknotu i zapłacić nim dwa razy – raz oryginałem, a drugi raz kopią. W świecie fizycznym banknoty, szczególnie wyższych nominałów, są zabezpieczone skomplikowanym wzorem, znakami wodnymi, znakami widocznymi w świetle ultrafioletowym, paskiem metalowym itp. Dlatego podrobienie banknotu jest trudne. Natomiast w świecie cyfrowym kopia pliku jest w 100% zgodna z oryginałem, dlatego że w procesie kopiowania każda jedynka pozostanie jedynką, a każde zero zerem. Stanowi to problem w przypadku próby zastosowania plików cyfrowych jako pieniędzy i wymaga innych podejść.

Poniżej pokażemy, w jaki sposób rozwiązano ten problem w przypadku, gdy cyfrowymi pieniędzmi są odpowiednio zaszyfrowane pliki, a jak – w bardzo innowacyjny sposób –rozwiązano ten problem w Bitcoinie.

Jedną z wczesnych prób wprowadzenia pieniędzy cyfrowych był system DigiCash utworzony w 1989

roku [35], który nie przetrwał próby czasu i został zamknięty w 1998 roku. Zaproponowane rozwiązanie zapewniało anonimowość w tym sensie, że banki uczestniczące w procesie płatności nie mogły powiązać płatnika z odbiorcą płatności [27].

W systemie DigiCash odpowiednikiem papierowego banknotu był banknot cyfrowy, czyli plik zawierający odpowiednio zaszyfrowany tekst obejmujący unikalny identyfikator banknotu. Płatnik zwracał się do banku o wyemitowanie takiego cyfrowego banknotu płacąc za niego tradycyjnym przelewem ze swojego konta. Banknot ten mógł być następnie wydatkowany, czyli przekazany od płatnika do odbiorcy płatności. Odbiorca płatności nie mógł jednak zapłacić nim komuś innemu; mógł tylko przekazać go do swojego banku w celu otrzymania przelewu na swoje konto. Bank odbiorcy płatności przed dokonaniem przelewu sprawdzał, czy identyfikator banknotu nie znajduje się na liście skasowanych banknotów prowadzonej przez bank, który ten banknot wydał płatnikowi. Jeśli tak, to traktował przedłożony cyfrowy banknot jako sfałszowany (skopiowany) i odmawiał dokonania przelewu. Jeśli nie, dokonywał przelewu i dopisywał identyfikator tego cyfrowego banknotu do listy. Zatem jeśli nieuczciwy płatnik skopiował cyfrowy banknot i zapłacił dwóm odbiorcom płatności, to przelew na konto dostał ten, który przedłożył ten banknot bankowi jako pierwszy. Decydujący był zatem chronologiczny porządek przekazania cyfrowego banknotu do banku w celu dokonania przelewu i dopisania identyfikatora tego banknotu do listy skasowanych banknotów. Warto zauważyć, że nie jest to sprawiedliwe w powszechnym rozumieniu tego słowa – przelewu nie dostanie ten, któremu pierwszemu zapłacono cyfrowym banknotem, tylko ten, który pierwszy przedłoży go bankowi.

Rozwiązanie z centralną listą skasowanych cyfrowych banknotów było o tyle niebezpieczne, że system był bardzo wrażliwy na możliwy atak na tę listę. Usunięcie wpisów z tej listy pozwalałoby na powtórne wydawanie wydanych wcześniej pieniędzy. Natomiast zablokowanie dostępu do tej listy unieruchamiałoby cały system płatności.

W Bitcoinie podejście do problemu podwójnego wydatkowania pieniędzy jest zupełnie inne. Nie ma w nim bowiem cyfrowego odpowiednika papierowego banknotu, który byłby przekazywany między płatnikiem a odbiorcą płatności. Jest tylko rejestr – implementowany w formie łańcucha bloków – w którym są zapisane transakcje przekazania własności bitcoinów z płatnika na odbiorcę (odbiorców) płatności (por. podrozdział 6.6). Ten rejestr zawiera scentralizowaną informację o wszystkich transakcjach wykonanych w systemie Bitcoin, choć sam rejestr jest rozproszony (*Distributed Ledger Technology – DLT*), a dokładnie rzecz biorąc zreplikowany w wielu węzłach. Aktualnie sieć Bitcoin liczy ponad 13 tysięcy pełnych węzłów [15], co oznacza, że łańcuch bloków jest tyle razy powielony. Warto też zauważyć, że łańcuch bloków nieustannie rozrasta się w miarę wykonywania kolejnych transakcji i rejestrowania kolejnych bloków, a cały musi pozostawać dostępny online.

Rozwiązanie problemu podwójnego wydatkowania pieniędzy oparte na łańcuchu bloków wyklucza możliwość płacenia offline. Każda transakcja musi być bowiem najpierw sprawdzona, a potem zarejestrowana w łańcuchu bloków, a w tym celu jest konieczny zdalny dostęp do węzłów, w których jest on przechowywany.

6.9. Rozproszony rejestr i globalny konsensus

Replikacja łańcucha bloków w wielu węzłach ma na celu podniesienie niezawodności systemu i jego odporności na ataki. Rozproszenie rejestru powoduje jednak problem, w jaki sposób zapewnić spójność całego systemu, czyli spowodować, aby w stanie ustalonym łańcuchy bloków we wszystkich węzłach były identyczne. W Bitcoinie wprowadzono rozwiązanie tego problemu niewymagające centralnego serwera, który byłby bardzo wrażliwym punktem systemu, narażonym na ataki. Rozwiązanie to łączy się z kopaniem bloków (por. podrozdział 6.5) równocześnie przez wielu kopaczy, którzy konkurują ze sobą o to, kto pierwszy wykopie nowy blok (czyli znajdzie odpowiedni niuans). Zwycięzca dołącza nowy blok do łańcucha bloków, który staje się jego koniuszkiem (por. podrozdział 6.4) i informuje o tym przez sieć wszystkich kopaczy, który niezależnie od siebie sprawdzają, czy blok został poprawnie wykopany. Zwycięstwo oznacza, że kopacz otrzymuje w nagrodę nowo wyemitowane w tym bloku bitcoiny i wszystkie opłaty transakcyjne. Gdyby okazało się, że blok nie został poprawnie wykopany, to kopacz, który go sprawdza, nie dołączy tego bloku do swojej kopii łańcucha bloków i będzie kopał dalej w nadziei na otrzymanie nagrody. Podobnie postąpią wszyscy inni kopacze pracujący niezależnie od siebie, zatem tylko poprawnie wykopane bloki mają szansę na dołączenie do łańcucha bloków zaakceptowanego przez wszystkich kopaczy.

W trakcie kopania bloku każdy kopacz zbiera nowo zawarte transakcje przesyłane przez sieć. Jeśli dowie się, że przegrał rywalizację o bieżący blok, to z zebranych transakcji tworzy następny blok wskazując aktualny koniuszek jako jego rodzica i rozpoczyna kopanie go. W ten sposób krok po kroku jest tworzony przez niezależnych kopaczy jeden łańcuch bloków powielony w wielu węzłach.

Problem ze spójnością łańcucha bloków pojawia się wówczas, gdy dwóch kopaczy wykopie ten sam blok w prawie tym samym czasie i rozpocznie rozsyłanie go przez sieć z dwóch różnych węzłów położonych w różnych częściach świata, co oznacza, że ze względu na opóźnienia transmisji bloki te będą docierać do różnych węzłów w różnej kolejności.

Oznaczmy aktualny koniuszek łańcucha bloków przez B_K, a dwa bloki nowo wykopane w różnych węzłach przez B_1 i B_2. Zarówno B_1, jak i B_2, wskazują B_K jako swojego rodzica. Chociaż oba bloki B_1 i B_2 są poprawnie wykopane, to tylko jeden z nich może być docelowo dzieckiem B_K. Chwilowo mamy do czynienia z rozgałęzieniem łańcucha i koniecznością zlikwidowania go przez wszystkich kopaczy w taki sam sposób bez centralnego serwera.

Jeśli do danego kopacza pierwszy dotrze blok B_1 to, tak jak to opisano powyżej, dołączy on B_1 do B_K i rozpocznie kopanie B_3 wskazując B_1 jako jego rodzica. Tworzy się zatem łańcuch B_K, B_1, B_3.

Jeśli następnie dotrze do niego B_2 również wskazujący na B_K jako jego rodzica, czyli rozpoczynający gałąź boczną łańcucha, to zachowa go, ale będzie dalej kopał B_3 wskazujący B_1 jako jego rodzica.

W innym węźle sieci sytuacja może być odwrotna – najpierw do kopacza w tym węźle dotrze blok B_2, więc w nowym bloku kopanym przez niego wskaże on B_2 jako rodzica. Rozpoczyna się wyścig dwóch gałęzi sieci. Po pewnym czasie okaże się, czy więcej nowych bloków jest dołączonych do gałęzi B_K, B_1 czy do gałęzi B_K, B_2. Dłuższy łańcuch wygrywa, ponieważ skumulował więcej pracy. Każdy kopacz, który stwierdzi, że jedna gałąź jest dłuższa, do niej będzie dołączał nowe bloki kopane przez siebie. Natomiast gałąź boczną zlikwiduje, to znaczy sprawdzi, które transakcje z gałęzi bocznej nie są zawarte w blokach gałęzi głównej (większość będzie w obu) i doda je do nowo kopanego bloku. Jedyną konsekwencją dla tych transakcji będzie późniejsze umieszczenie ich w łańcuchu bloków. Każdy kopacz wybiera łańcuch dłuższy we własnym interesie – dostanie nagrodę tylko jeśli nowo wykopany przez niego blok będzie ostatecznie dołączony do gałęzi głównej.

Dzięki powyższemu rozwiązaniu 13 tysięcy pełnych węzłów Bitcoina osiąga globalny konsensus, czyli spójność łańcucha bloków, bez centralnego serwera.

6.10. Koncepcja Ethereum

Platforma Ethereum powstała pięć lat po Bitcoinie i jest jego rozszerzeniem [5]. W przeciwieństwie do Bitcoina, który pretenduje do roli światowego pieniądza, Ethereum jest „światowym komputerem", rozproszonym i dobrze zabezpieczonym, zdolnym do wykonywania dowolnie złożonych programów nazywanych *inteligentnymi kontraktami* (*smart contracts*), w skrócie *i-kontraktami*.

Ethereum zawsze znajduje się w pewnym stanie, który jest zapisany w łańcuchu bloków – rozproszonym i zreplikowanym w równorzędnych węzłach, których aktualnie jest 10 tysięcy [48]. Jednak w przeciwieństwie do Bitcoina, w którego blokach są zapisywane tylko transakcje płatności bitcoinami, w blokach Ethereum są zapisywane dowolne dane, o różnym przeznaczeniu, a w łańcuchu bloków – cała historia ich zmian.

W Ethereum jest używana kryptowaluta o nazwie „ether", która służy do uiszczania opłat za korzystanie z platformy. Podobnie jak bitcoin, ether jest emitowany w blokach dołączanych do łańcucha. Również, podobnie jak bitcoin, ether jest notowany na giełdach i może być obiektem spekulacji.

I-kontrakty są podobne do kontraktów prawnych, ale są napisane w języku programowania i dlatego mogą być wykonane przez komputer. Są one zapisane w łańcuchu bloków Ethereum, więc nie można ich modyfikować; można co najwyżej tworzyć ich nowe wersje i zapisywać w łańcuchu bloków.

Kontrakty prawne stosowane w świecie fizycznym mogą być niejednoznaczne w zależności od użytych wyrażeń, natomiast i-kontrakty są zawsze jednoznacznie interpretowane, co jednak nie oznacza, że zawsze w pełni oddają intencję kontraktora. I-kontrakty mogą obejść się bez prawników, sądów i komorników – jeśli warunki i-kontraktu są spełnione, to na pewno będzie on zrealizowany, a jeśli nie – to automatycznie będą zrealizowane zapisane w nim

konsekwencje ich niespełnienia, które mogą obejmować wypłatę odszkodowania.

Wyobraźmy sobie i-kontrakt między dłużnikiem a wierzycielem. Zabezpieczeniem długu w etherach może być np. własność samochodu dłużnika. Jeżeli przed wyznaczonym terminem nie wpłynie do i-kontraktu kwota długu (warto zauważyć – do i-kontraktu, a nie bezpośrednio do wierzyciela), to przeniesie on własność samochodu na wierzyciela. Jeśli kwota długu wpłynie do i-kontraktu, to przekaże on ethery wierzycielowi, a dłużnik pozostanie właścicielem samochodu. Jeśli w terminie wpłynie część długu, to można w i-kontrakcie zapisać dowolne warunki, jak wówczas postąpić – np. przedłużyć termin spłaty, ale naliczyć kary umowne.

I-kontrakty są pisane w specjalistycznych językach programowania, takich jak Solidity [118], a następnie tłumaczone na tak zwany *kod bajtowy* (*bytecode*), który jest wykonywany przez *wirtualną maszynę Ethereum* [5]. Jest to oprogramowanie, które dostosowuje dowolny komputer do platformy Ethereum.

6.11. Konta i transakcje w Ethereum

W Bitcoinie użytkownicy nie mają kont. Na podstawie transakcji zapisanych w łańcuchu bloków można jedynie obliczyć, ile bitcoinów jest przypisanych do każdego pseudonimu. W Ethereum są dwa rodzaje kont:

- *konta zewnętrzne* przypisane do użytkowników i kontrolowane za pomocą ich kluczy prywatnych oraz
- *konta i-kontraktowe* kontrolowane przez oprogramowanie i-kontraktów.

Konto zewnętrzne nie zawiera żadnego programu. Na tym koncie są natomiast przechowywane ethery jego właściciela, które mogą być przelewane na inne konta. Ethery można kupić na giełdach kryptowalut.

Właściciel konta zewnętrznego może wysyłać z niego wiadomości tworząc *transakcje* i podpisując je swoim kluczem prywatnym. Transakcje mogą zawierać ether oraz dane wskazujące, którą specyficzną funkcję w i-kontrakcie wykonać, oraz jakie parametry przekazać tej funkcji.

Za każdym razem, gdy konto i-kontraktowe dostanie wiadomość, uaktywnia swój program, co umożliwia pobranie danych z łańcucha bloków, przetworzenie danych przy wykorzystaniu pamięci chwilowej i wewnętrznego stosu, zapisanie ich w łańcuchu bloków, wysyłanie innych wiadomości, a nawet tworzenie innych i-kontraktów.

Platforma Ethereum nie działa w tle, to znaczy niczego nie robi z własnej inicjatywy, a jedynie pod wpływem transakcji – tylko one mogą zmienić stan platformy i spowodować wykonanie i-kontraktu przez wirtualną maszynę Ethereum przekazując mu ethery i/lub niezbędne parametry. Jeśli jednak transakcja zostanie zaadresowana do nieistniejącego konta, to „spali" przekazywane ethery, które będą nie do odzyskania.

Podobnie jak w Bitcoinie transakcje w Ethereum są formowane w portfelach (por. podrozdział 6.6).

6.12. Tokeny w Ethereum

Token jest cyfrowym odpowiednikiem żetonu. Żeton jest prywatnie wyemitowanym przedmiotem przypominającym monetę, który ma niewielką wartość, do wykorzystania w określonych działach: myjniach, pralniach, kasynach itp.

W Ethereum tokeny są abstrakcjami (a nie plikami) bazującymi na łańcuchu bloków, mającymi właścicieli, które reprezentują [5]:

- Jednostkę pieniężną – token może służyć jako forma pieniądza.
- Zasób – token może reprezentować zasób uzyskany lub wytworzony w gospodarce współdzielenia, np. pamięć lub procesor, które można współdzielić w sieci.
- Aktywa – token może reprezentować prawo własności materialnej lub niematerialnej, np. złoto, nieruchomości, samochód, ropę naftową, energię itp.
- Prawo dostępu – token może umożliwiać dostęp do cyfrowej lub fizycznej własności, takiej jak forum dyskusyjne, ekskluzywna strona internetowa, pokój hotelowy, wynajęty samochód itp.
- Udział – token może reprezentować kapitał udziałowy w organizacji cyfrowej lub prawnej.
- Prawo głosowania – token może reprezentować prawo głosu w systemie cyfrowym lub prawnym.

- Obiekt kolekcjonerski – token niezamienny (*Non-Fungible Token – NFT*) może reprezentować cyfrowy obiekt kolekcjonerski.
- Tożsamość – token może reprezentować tożsamość cyfrową (np. awatar) lub prawną (np. PESEL).
- Zaświadczenie – token może reprezentować zaświadczenie wydane przez formalny organ lub zdecentralizowany system reputacji (np. akt urodzenia, akt małżeństwa, dyplom ukończenia studiów itp.).

Należy rozróżnić tokeny zamienne i niezamienne. Zamienne są tokeny, których jednostki są nierozróżnialne – w świecie fizycznym analogicznymi przykładami są waluty – każdy banknot o wartości jednego dolara (euro, złotego) jest taki sam i może być zamieniony na inny banknot jednodolarowy. Natomiast token niezamienny jest unikalny. Jeśli token reprezentuje czyjąś tożsamość (PESEL), to nie może być zamieniony na inny reprezentujący inną tożsamość. Tokeny niezamienne upowszechniły się w odniesieniu do obiektów kolekcjonerskich [141].

6.13. Implementacja tokenów w Ethereum

Tokeny są w Ethereum implementowane za pomocą i-kontraktów. Każdy token danego rodzaju jest implementowany za pomocą osobnego i-kontraktu, w którym są zapisane jego specyficzne cechy. Taki i-kontrakt przechowuje stan własności tokenów tego rodzaju i prawa dostępu oraz realizuje ich transfer.

Ponieważ i-kontrakty mogą być dowolnie złożonymi programami, to również i-kontrakty implementujące tokeny mogą być napisane w dowolny sposób. Jednak najczęściej stosuje się do ich implementacji standard ERC20 [45] opracowany w 2015 roku dla tokenów wymiennych lub jego późniejsze rozszerzenia ERC223 [34], ERC777 [46].

Zgodnie ze standardem ERC20 i-kontrakt implementujący zamienny token co najmniej:

- Informuje o łącznej liczbie tokenów. Tokeny ERC20 mogą mieć stałą lub zmienną liczbę wyemitowanych jednostek.
- Informuje o liczbie tokenów przypisanych do danego adresu.
- Transferuje podaną liczbę tokenów z bieżącego adresu na adres docelowy.
- Udziela zgody na dokonanie kilku transferów do podanej liczby tokenów z bieżącego adresu na adres docelowy.
- Wykonuje transfer po podaniu adresu nadawcy, odbiorcy i liczby tokenów.
- Informuje o dostępnej liczbie tokenów do wydania z podanego adresu.
- Informuje o dokonanym transferze.
- Informuje o udzieleniu zgody na transfery.

Warto zauważyć, że adresy właścicieli tokenów oraz liczby przypisanych do nich tokenów zamiennych są implementowane wewnątrz i-kontraktu w jego długoterminowej pamięci, która jest zapisywana w łańcuchu bloków w celu zapewnienia jej trwałości. Tokeny mogą być transferowane z jednego adresu do drugiego, co oznacza umniejszenie liczby tokenów przypisanych do adresu nadawcy (np. płatnika, jeśli token reprezentuje walutę), a zwiększenie – odbiorcy (odbiorcy płatności). Transfer odbywa się przez wykonanie transakcji w Ethereum skierowanej na adres i-kontraktu implementującego tokeny, w której są podane odpowiednie parametry: wywołanie funkcji transferu tokenów, adresy właścicieli tokenów i liczba przesyłanych tokenów. Tokeny mogą być też kupowane za ethery.

Warto podkreślić, że tokeny nie są plikami tylko abstrakcjami, których liczba jest przypisana do adresów ich właścicieli zaimplementowanych w i-kontrakcie.

Warto też zauważyć, że do i-kontraktu implementującego tokeny można teoretycznie wpisać dowolne warunki ich wydawania. Zatem osoba kontrolująca i-kontrakt może uniemożliwić ich wydawanie z wybranych adresów. Potencjalnie stanowi to istotne zagrożenie dla wolności obracania własnymi pieniędzmi reprezentowanymi przez tokeny.

6.14. Dowód stawki jako alternatywa dla dowodu pracy

We wrześniu 2022 roku w Ethereum zaczęto stosować dowód stawki (*Proof of Stake*) [106] o nazwie Casper [23] zamiast dowodu pracy (por. podrozdział 6.5) co do zasady takiego, jak w Bitcoinie, choć

z pewnymi modyfikacjami (algorytm osiągania konsensusu EThash [47]).

W przypadku dowodu stawki bloki do łańcucha dołączają nie kopacze tylko *walidatorzy,* którzy oddali w zastaw każdy 32 ethery (przy kursie 1600 ETH/USD równe około 51 tysięcy USD, czyli przy kursie 4,3 PLN/USD – około 220 tysięcy zł.).

Walidatorzy działają w 12-sekundowych szczelinach czasowych; 32 szczeliny tworzą epokę. W każdej szczelinie spośród aktualnie około pół miliona walidatorów jest wybierany losowo jeden atestator, który tworzy nowy blok i rozsyła go do węzłów w sieci. Również w każdej szczelinie jest losowo wybierany komitet co najmniej 128 walidatorów, którzy głosują za lub przeciw atestowaniu proponowanego bloku. Co najmniej dwie trzecie walidatorów musi zagłosować za atestacją bloku, aby był on dołączony do łańcucha. Zarówno atestator, jak i walidatorzy, otrzymują wynagrodzenie w etherach za dołączenie bloku do łańcucha.

Walidator, który nie jest obecny w sieci w czasie, gdy został wybrany do atestacji bloków, traci możliwość otrzymania wynagrodzenia w etherach za atestację. Jeśli jest obecny w sieci, ale nie wziął udziału w atestacji, to ponosi małą karę pobieraną z jego zastawu. Jednak, gdy zachowuje się nieuczciwie, to traci część lub nawet całość etherów oddanych w zastaw i może stracić status walidatora. Za nieuczciwe zachowanie uznaje się zaproponowanie wielu bloków w jednej szczelinie i składanie sprzecznych atestacji.

Przejście w Ethereum z dowodu pracy na dowód stawki spowodowało obniżenie konsumpcji energii elektrycznej o 99,99% [50], co było głównym argumentem przeciwko zabezpieczaniu łańcucha bloków dowodem pracy. Dowód stawki promuje decentralizację, ponieważ walidacja może być prowadzona na zwykłych laptopach, a posiadanie drogich specjalizowanych koparek zbudowanych z układów scalonych ASIC (*Application-Specific Integrated Circuit – ASIC*) [6] nie daje korzyści, bo walidatorzy są losowani i nie konkurują ze sobą mocą obliczeniową.

6.15. Przepustowość

Aktualna przepustowość Bitcoina, Ethereum i kart kredytowych wynosi:

- Bitcoin – 0,3 miliony transakcji dziennie [14];
- Ethereum – 1 milion transakcji dziennie [49];
- Karty płatnicze łącznie – 1.000,0 milionów transakcji dziennie [123], w tym:
- Visa – 500,00 milionów transakcji dziennie [123].

Jak widać przepustowość Bitcoina i Ethereum, które są oparte na łańcuchu bloków, jest o trzy rzędy niższa niż przepustowość kart płatniczych.

6.16. Prywatność

Prywatność obywateli jest chroniona konstytucyjnie. Artykuł 76 Konstytucji Rzeczypospolitej Polskiej [74] stanowi:

*Władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, **prywatności** i bezpieczeństwu oraz przed nieuczciwymi praktykami rynkowymi. Zakres tej ochrony określa ustawa.*

Z artykułu tego wynika konieczność ochrony prywatności przez Narodowy Bank Polski, który zalicza się do władz publicznych. Ustawa o Narodowym Banku Polskim [131] nie odwołuje się bezpośrednio do ochrony prywatności. Jest natomiast takie odwołanie nie wprost w Prawie Bankowym [133], którego artykuł 104 ustanawia tajemnicę bankową:

*Bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować **tajemnicę bankową**, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.*

W tym prawie jest jednak długa lista innych władz publicznych, które w określonych okolicznościach mają prawo dostępu do tajemnicy bankowej dotyczącej obywateli, czyli naruszenia ich prywatności:

- Agencja Bezpieczeństwa Wewnętrznego,
- Agencja Wywiadu,
- Centralne Biuro Antykorupcyjne,
- Służba Ochrony Państwa,
- Sądy,

- Minister Sprawiedliwości,
- Prokuratura,
- Policja,
- Inspektor Nadzoru Wewnętrznego ministra właściwego do spraw wewnętrznych,
- Inspektorat Wewnętrzny Służby Więziennej,
- Służba Więzienna,
- Służba Wywiadu Wojskowego,
- Służba Kontrwywiadu Wojskowego,
- Żandarmeria Wojskowa,
- Straż Graniczna,
- Urząd Ochrony Danych Osobowych,
- Urząd Ochrony Konkurencji i Konsumentów,
- Zakład Ubezpieczeń Społecznych,
- Komisja Nadzoru Finansowego,
- Najwyższa Izba Kontroli,
- Rzecznik Finansowy,
- Krajowa Administracja Skarbowa.

Należy podkreślić, że bank, w którym dany obywatel ma konto, na które wpływają jego należności i z którego dokonuje płatności, ma pełną wiedzę o jego przepływach finansowych realizowanych w nim. Na potrzeby własne, np. marketingu własnych produktów i usług bankowych, może też je dowolnie przetwarzać. Jeśli obywatel płaci kartą płatniczą, to informacje o jego płatnościach ma również operator kart płatniczych. Jeśli kartę płatniczą obywatel ma zapisaną w swoim telefonie komórkowym na pewnej platformie cyfrowej, np. w Google Pay, to informacje te otrzymuje także operator tej platformy.

Popularnym i do pewnego stopnia efektywnym zabezpieczeniem prywatności jest posiadanie rachunków w kilku bankach i korzystanie z kart płatniczych różnych operatorów. Wówczas, co do zasady, jeden bank nie wie o płatnościach dokonywanych do/z rachunków w innych bankach, ani jeden operator o transakcjach dokonywanych nie jego kartami. Jeśli jednak kilka kart od różnych operatorów z kilku banków jest zapisanych na jednej platformie cyfrowej, to operator tej platformy może zintegrować informacje o płatnościach (choć nie o wpływach). Natomiast płatność kartą w terminalu płatniczym (*Point of Sale – POS*) daje dostęp do danych karty właścicielowi terminalu, a płatność kartą przez internet w sklepie internetowym bezpośrednio lub przez pośrednika płatności – dane karty wraz z kodem zabezpieczającym CVV/CVC (*Card Verification Value/Code*) podmiotowi realizującemu płatność.

W celu zwiększenia konkurencji na rynku płatności cyfrowych, a w konsekwencji poprawienia wygody i obniżenia kosztów, dyrektywa unijna PSD2 [36] umożliwiła udzielanie przez właściciela konta w banku zgody na dostęp innych podmiotów do następujących informacji i czynności:

- Potwierdzenia dostępności pieniędzy na koncie – CAF (*Confirmation of the Availability of Funds*).
- Informacji o koncie, w tym saldzie i historii transakcji – AIS (*Account Information Service*).
- Inicjowania płatności z konta – PIS (*Payment Initiation Service*).

Z tej możliwości korzystają nie tylko niezależni dostawcy usług płatniczych, ale też banki, aby dla wygody swoich klientów i za ich zgodą pokazywać salda i historię transakcji z ich kont w innych bankach i umożliwiać inicjowanie z nich płatności. Oczywiście odbywa się to kosztem obniżenia ochrony prywatności klientów.

Warto też zauważyć, że jeśli płatnik (osoba fizyczna lub prawna) – klient banku – dokonuje przelewu na konto odbiorcy płatności, to poznaje on dane płatnika, w szczególności numer konta i nazwę banku oraz w przypadku osoby fizycznej – jej imię i nazwisko – lub w przypadku osoby prawnej – jej nazwę.

Jak widać z powyższego, ochrona prywatności w obecnym systemie płatności za pośrednictwem banków jest dość iluzoryczna.

W przypadku papierowej gotówki ujawnienie swojej tożsamości nie jest warunkiem dokonania płatności – płatnik papierową gotówką może pozostać anonimowy. Jednak Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [132] w artykule 35.1 punkt 3 stanowi:

Art. 35. 1. Instytucje obowiązane stosują środki bezpieczeństwa finansowego w przypadku:

3) przeprowadzania gotówkowej transakcji okazjonalnej o równowartości 10 000 euro lub większej, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane – w przypadku instytucji obowiązanych, o których mowa w art. 2 ust. 1 pkt 21–23.

Ustawa ta istotnie ogranicza anonimowość w obrocie gotówkowym, a tym samym dopuszcza naruszanie prywatności stron transakcji, ponieważ środki bezpieczeństwa finansowego obejmują odkrycie ich tożsamości.

Ograniczenie prywatności w przypadku płatności zarówno bankowych, jak i gotówkowych, jest uzasadnione koniecznością ochrony obywateli przez państwo przed zagrożeniami, takimi jak ataki terrorystyczne i kryminalne oraz malwersacje finansowe. Pozostaje jednak kwestia zaufania do państwa, czyli obaw obywateli przed naruszeniem ich prywatności przez funkcjonariuszy państwowych w celach innych niż ich ochrona. Często podnoszony przez polityków argument, że uczciwy obywatel nie ma nic do ukrycia, jest demagogiczny. Uczciwość obywatela nie chroni go bowiem przed wytypowaniem go do ataku kryminalnego, politycznego lub osobistego na podstawie ujawnionych informacji prywatnych.

Systemy Bitcoin i Ethereum stosują pseudonimy oparte na kluczach publicznych do identyfikacji swoich użytkowników. Pary kluczy prywatny–publiczny są samodzielnie generowane przez użytkowników, więc nie ma potrzeby korzystania z Zaufanych Stron Trzecich oferujących certyfikaty kluczy i potwierdzających tożsamość użytkowników.

W łańcuchu bloków Bitcoina nie są przechowywane żadne dane identyfikujące użytkowników poza ich kluczami publicznymi. Jednak łańcuch bloków jest publicznie dostępny, zatem każdy zainteresowany może poznać wszystkie transakcje zachodzące pomiędzy konkretnymi pseudonimami.

Jak wspomniano w podrozdziale 6.6, pary kluczy są przechowywane w portfelach użytkowników [4], zatem jeśli ktoś uzyska dostęp do portfela, np. na skutek włamania, i powiąże klucze z tożsamością użytkownika, to będzie mógł w łańcuchu bloków prześledzić wszystkie jego transakcje, podszyć się pod niego i wykonać nieuprawnione transakcje, które będą nieodwracalne. Dlatego użytkownicy często używają różnych par kluczy i przechowują je dla bezpieczeństwa w różnych portfelach.

Warto zauważyć, że również strony transakcji w bitcoinach pozostają dla siebie pseudonimowe. To znaczy, że osoba, która otrzymała bitcoiny w pewnej transakcji, wie jedynie, że otrzymała je od danego pseudonimu, ale na jego podstawie nie może odkryć kto się pod nim kryje.

Podobnie kwestia pseudonimowości wygląda w Ethereum, z tym, że w Ethereum użytkownicy mają konta zewnętrzne (por. podrozdział 6.11) identyfikowane – podobnie jak w Bitcoinie – pseudonimami opartymi na kluczach publicznych. I-kontrakty w Ethereum mogą być i najczęściej są wykonywane pseudonimowo. Jednak, ponieważ mogą być napisane w dowolny sposób zależnie od woli programisty, to można sobie wyobrazić, że i-kontrakty szczególnego rodzaju zawierają informacje o prawdziwej tożsamości użytkowników.

7. Alternatywne rozwiązania techniczno-organizacyjne e-złotego

7.1. Wstęp

Dwie podstawowe cechy papierowej gotówki różniące je od płatności przelewami bankowymi i kartami płatniczymi to:

- anonimowość,
- niezależność od dostępu do internetu.

W tym raporcie przez „internet" rozumiemy wszelkie sieci telekomunikacyjne do przesyłania danych cyfrowych. Obecnie prywatne sieci telekomunikacyjne dla pojedynczych celów są bardzo rzadkie ze względu na koszty inwestycji i utrzymania, dlatego najczęściej stosuje się sieci VPN (*Virtual Private Network*) [138], czyli szyfrowane kanały w ogólnodostępnym internecie.

Poniżej, w podrozdziałach 7.2 i 7.3 wyjaśniamy, dlaczego obie wyżej wymienione cechy nie mogą być w pełni osiągnięte w przypadku CBDC.

W kolejnych podrozdziałach analizujemy problemy związane z cyfrowymi portfelami, wyborem kont lub tokenów, implementacją CBDC z lub bez łańcucha bloków, w banku centralnym lub w bankach komercyjnych oraz z oprocentowaniem.

7.2. Anonimowość

Ze względu na bezpieczeństwo państw (por. podrozdział 6.16), banki centralne na pewno nie zdecydują się na wprowadzenie anonimowej cyfrowej gotówki. Z tego samego względu również rozwiązania pseudoanonimowe (por. podrozdziały 6.6 i 6.16) nie będą zastosowane. Anonimowość jako cecha papierowej gotówki nie zostanie zatem odwzorowana w cyfrowej gotówce, bo państwa nie będą chciały pozbawić się kontroli nad przepływami pieniężnymi.

Jedyne co można zaakceptować, to jawne odkrywanie lub zasłanianie swojej tożsamości przez płatników przed odbiorcami płatności, ale nie przed bankiem. Oznacza to, że płatnik będzie mógł dokonać płatności anonimowo lub nie. Jeśli będzie kupować produkt w fizycznym sklepie bez faktury, to będzie mógł zasłonić swoją tożsamość. Jednak, gdy będzie kupować fizyczny produkt w sklepie internetowym, to i tak musi podać swoje dane, w szczególności imię, nazwisko i adres, w celu dostawy, więc zasłanianie swojej tożsamości w tym przypadku byłoby bez sensu. Ujawnienie tożsamości jest konieczne w przypadku, gdy na nazwisko kupującego trzeba wystawić fakturę, licencję, gwarancję itp.

7.3. Niezależność od dostępu do internetu

Również niezależność od dostępu do internetu nie może być zagwarantowana w przypadku cyfrowej gotówki ze względu na problem podwójnego wydatkowania pieniędzy. Jak wspomniano w podrozdziale 6.8, można skopiować papierową gotówkę, ale kopia będzie różnić się od oryginału ze względu na fizyczne zabezpieczenia, więc można wykryć oszustwo polegające na wydatkowaniu oryginału i kopii tego samego banknotu. Po wykryciu oszustwa honorowany będzie jedynie oryginał.

W przypadku cyfrowego banknotu w formie pliku, nie ma możliwości odróżnienia oryginału od jego kopii, ponieważ są identyczne. Dlatego do rozwiązania problemu podwójnego wydatkowania pieniędzy jest konieczna baza danych, w której są rejestrowane wszystkie transakcje. Taką bazą danych jest na przykład łańcuch bloków (por. podrozdział 6.4), ale może ona być implementowana również w inny, tradycyjny sposób. W celu zarejestrowania transakcji jest konieczny dostęp portfeli, w których są formowane transakcje (por. podrozdziały 6.6 i 6.11), do tej bazy danych przez internet. Zatem również druga cecha wyróżniająca papierową gotówkę, a mianowicie niezależność od dostępu do internetu, nie może być spełniona w przypadku gotówki cyfrowej.

Jedyne co można zaakceptować, to czasowe opóźnienie zarejestrowania transakcji przez portfel w bazie danych. Jeśli portfele miałyby taką możliwość, to mogłyby wykonywać transakcje bezpośrednio między sobą bez dostępu do Internetu komunikując się np. przez NFC [96]. Portfel musiałby mieć kopię informacji z bazy danych o tym, ile cyfrowej gotówki posiada jego właściciel i dopuszczać transakcje tylko do jej wysokości. Wszystkie wykonane transakcje portfel musiałby lokalnie zapamiętywać. Po odzyskaniu dostępu do internetu musiałyby zarejestrować wykonane transakcje w bazie danych. Poprawność transakcji musiałby być ponownie zweryfikowana przed zapisem w bazie danych.

Niestety możliwość wykonywania transakcji bez dostępu do bazy danych przez internet umożliwia-

łaby podwójne wydatkowanie pieniędzy. Miałoby to miejsce wówczas, gdyby portfel lub cały telefon komórkowy, na którym był zainstalowany, został sklonowany. Wówczas byłaby możliwość równoległego wydawania pieniędzy z oryginału i z klonu, co wyszłoby na jaw dopiero po podłączeniu do internetu i próbie zarejestrowania transakcji w bazie danych. Jak wspomniano w podrozdziale 6.8, zarejestrowane byłyby te transakcje, które zostałyby zgłoszone jako pierwsze, niezależnie czy byłyby to transakcje wykonane oryginalnym portfelem, czy jego klonem, co kłóci się z pojęciem sprawiedliwości i ochroną płatników przed nadużyciami.

7.4. Cyfrowe portfele z e-złotym

Operowanie e-złotym będzie wymagać posiadania cyfrowego portfela służącego do dokonywania płatności, który może być zaimplementowany:

- w telefonie komórkowym wraz z jego odmianami takimi jak inteligentne zegarki, opaski itp.;
- na komputerze stacjonarnym, przenośnym, tablecie, komputerze pokładowym w samochodzie itp.;
- na karcie mikroprocesorowej podobnej do karty płatniczej.

Portfel na telefonie komórkowym będzie najczęstszym przypadkiem, ponieważ płatnicy mają go najczęściej przy sobie w trakcie zakupów i płatności za nie. Portfel na komputerach będzie miał uzupełniające znaczenie – w przypadku zakupów produktów i usług dokonywanych z komputera będzie wygodnie płacić za nie bezpośrednio z niego. Karty mikroprocesorowe z portfelami e-złotego raczej nie upowszechnią się w Polsce ze względu na prawie pełne pokrycie kraju dostępem do internetu mobilnego [107]. Nie będzie uzasadnienia ekonomicznego do inwestowania w takie portfele, skoro będą dostępne tańsze programowe portfele na telefonach komórkowych, z których będzie można korzystać na terenie całego kraju. Ponadto nie ma możliwości płatności z karty na kartę, bo karty nie mają własnego zasilania.

7.5. Konta lub tokeny

W [129] wskazano na możliwość implementowania CBDC przy użyciu kont bankowych lub tokenów (por. podrozdział 6.12 i 6.13).

W przypadku implementowania CBDC przy użyciu kont bankowych, w warunkach dobrze działającego systemu rozliczeniowego, w szczególności takiego„ jak działający w Polsce System Przelewów Natychmiastowych Express Eliksir [108] i korzystający z niego system Blik [109], trudno dopatrzeć się zalet CBDC z punktu widzenia płatnika. Blik umożliwia w szczególności płatności na numer telefonu komórkowego odbiorcy płatności nawet jeśli nie ma on konta bankowego w tym samym banku co płatnik. Innymi słowy Blik oferuje funkcję analogiczną do natychmiastowych płatności bezpośrednich za pomocą gotówki.

Również w przypadku implementowania CBDC przy użyciu tokenów trudno dopatrzeć się zalet z punktu widzenia płatnika. Ma on bowiem możliwość dokonania płatności cyfrowej ze swojego telefonu komórkowego lub komputera w sposób nieróżniący się zasadniczo od płatności Blikiem. Skoro, jak wspomniano w podrozdziale 2.13, tokeny są abstrakcjami, a nie plikami, to nie ma zasadniczej różnicy między kontami w bankach z uaktualnianymi na bieżąco saldami, a adresami w pamięci i-kontraktu z liczbami przypisanych do nich tokenów, również na bieżąco uaktualnianymi. W jednym i drugim przypadku jest przechowywana historia zawartych transakcji płatności.

Różnica występuje, jeśli chodzi o płatności między płatnikiem a odbiorcą płatności z różnych krajów. W przypadku implementacji CBDC za pomocą tokenów wystarczyłoby, aby zarówno płatnik, jak i odbiorca płatności, mieli przypisane sobie adresy w i-kontrakcie, aby mogli przelewać sobie tokeny odpowiadające CBDC. Zbyteczne byłoby korzystanie ze skomplikowanych, wolnych i kosztownych systemów płatności i rozliczeń międzynarodowych, takich jak SWIFT [122] lub SEPA [114].

Warto podkreślić, że jest to, jak opisywaliśmy to w podrozdziale 4.2, jedna z głównych motywacji prowadzenia zaawansowanych prac nad cyfrowym yuanem w Chinach [129]. Chinom zależy, aby każdy człowiek na świecie, w szczególności w krajach, w których nie ma zaawansowanych systemów bankowych, mógł rozliczać się w cyfrowych juanach za chińskie produkty i usługi bez konieczności posiadania konta w chińskim banku i bez pośrednictwa międzynarodowych systemów płatniczych, takich jak SWIFT, które nie są przez Chiny kontrolowane. Dla Polski ta motywacja nie ma istotnego znaczenia.

7.6. Implementacja CBDC z lub bez łańcucha bloków

CBDC może być zaimplementowana przy wykorzystaniu łańcucha bloków lub nie.

W Bitcoinie i Ethereum przyjęto radykalne założenie odejścia od konieczności zaufania do jakiejkolwiek instytucji – zaufanie wynika tylko z przyjętych rozwiązań informatycznych, w szczególności konstrukcji łańcucha bloków i dochodzenia do globalnego konsensusu. Ma to jednak swoją cenę wynikającą z rozproszenia systemu na bardzo wielu węzłach rozsianych po całym świecie – 13 tysięcy węzłów Bitcoina (por. podrozdział 6.8) i 10 tysięcy węzłów Ethereum (por. podrozdział 6.10), które są własnością niezależnych podmiotów. Ich liczba i niezależność są gwarantem bardzo małego prawdopodobieństwa przeprowadzenia ataku 51% polegającego na zmowie węzłów dysponujących ponad 51% mocy obliczeniowej w celu sfałszowania łańcucha bloków.

W przypadku Bitcoina kosztem zastosowanego rozwiązania jest ogromna konsumpcja energii elektrycznej potrzebnej do dowodu pracy (por. podrozdział 6.5), a w przypadku Ethereum (aktualna wersja Merge) utrzymywanie pół miliona walidatorów potrzebnych do dowodu stawki (por. podrozdział 6.14) również niezależnych i rozsianych po całym świecie. W odniesieniu do CBDC takie założenia są nieuzasadnione. Banki centralne cieszą się zaufaniem społecznym, które należy wykorzystać w CBDC i nie ponosić zbytecznych kosztów.

Dlatego nie jest uzasadnione przyjęcie mechanizmu kopania bloków, tak jak w Bitcoinie. Konieczna jest walidacja przesyłanych transakcji w szczególności ze względu na problem podwójnego wydatkowania pieniędzy w przypadku dokonywania transakcji bez dostępu do internetu (por. podrozdział 7.3), ale może ją przeprowadzać stosunkowo mała liczba zaufanych walidatorów.

Dlatego łańcuch bloków w przypadku CBDC mógłby pozostać taki, jak w Bitcoinie (por. podrozdział 6.4), ale z tak obniżonym poziomem trudności, że kopanie byłoby bardzo łatwe, albo wręcz pozbawione niuansu. Możliwe jest też zastosowanie *dowodu autorytetu* – rozwiązania, w którym walidacji bloków dokonują zaufani i jawni walidatorzy ryzykujący swoją reputację [139].

Nie ma również uzasadnienia zastosowanie tak skomplikowanego i ogólnego rozwiązania, jak Ethereum do implementacji CBDC. Platforma Ethereum może służyć dowolnym celom – wystarczy oprogramować odpowiedni i-kontrakt na platformie obok dowolnej liczby innych i-kontraktów. W przypadku CBDC mamy do czynienia z jednym celem – cyfrową walutą – dlatego nie jest potrzebna dwuwarstwowa architektura: pierwsza – obsługująca konta Ethereum (por. podrozdział 6.11) – i druga – obsługująca i-kontrakt implementujący CBDC z adresami, do których są przypisane tokeny odpowiadające CBDC. Wystarczy ta druga zaimplementowana od podstaw.

Otwartym pytaniem jest też, czy historię wykonywania transakcji trzeba trzymać w tak uproszczonym łańcuchu bloków, jak to przedstawiono powyżej. Oczywiście gromadzenie transakcji w blokach i łączenie ich w łańcuch za pomocą odwołań do skrótów z ich nagłówków podnosi bezpieczeństwo. Jednak w sytuacji rezygnacji z kopania do zmiany łańcucha bloków nie jest już potrzebna tak duża energia elektryczna, więc bank centralny, w którego posiadaniu byłby łańcuch bloków, mógłby go dość łatwo zmienić, co oczywiście oznaczałoby nadużycie zaufania społecznego. Jeśli zakładamy duże zaufanie społeczne do banku centralnego, to zabezpieczanie historii transakcji przed nim samym staje się zbyteczne. Historia transakcji mogłaby zatem być przechowywana w klasycznej bazie danych ze standardowymi zabezpieczeniami.

7.7. Implementacja CBDC w banku centralnym lub w bankach komercyjnych

W [129] wskazano na teoretyczną możliwość implementowania CBDC albo bezpośrednio w banku centralnym, albo w bankach komercyjnych.

W tym pierwszym przypadku każdy obywatel państwa miałby konto lub adres z tokenami w banku centralnym. Przelewy byłyby prawie natychmiastowe, tak jak obecnie prawie natychmiastowe są przelewy w ramach tego samego banku komercyjnego. Pozostaje problem efektywnego dostępu i przetwarzania, który przy obecnym stanie rozwoju informatyki nie byłby aż taki trudny do rozwiązania, oraz problem takiej reorganizacji banku centralnego, aby był zdolny do masowej obsługi klientów deta-

licznych, co niewątpliwie byłoby dla niego dużym wyzwaniem. Takie rozwiązanie ma jednak głównie hipotetyczny charakter, ponieważ oznaczałoby de facto nacjonalizację i centralizację znacznej części systemu bankowego, co nie byłoby z korzyścią dla gospodarki.

Dlatego o wiele bardziej realistyczna jest architektura pośrednia – bank centralny zasilałby w CBDC banki komercyjne, które z kolei zasilałyby portfele płatników. Takie rozwiązanie wymagałoby istnienia efektywnej izby rozrachunkowej, aby płatnicy mogli dokonywać w prawie czasie rzeczywistym przelewów do innych banków. Funkcję takiej izby rozrachunkowej mógłby teoretycznie pełnić bank centralny lub wyspecjalizowana instytucja. W Polsce taka instytucja istnieje – Krajowa Izba Rozrachunkowa (KIR) [78]. Dlatego trudno jest podać zalety przejścia na CBDC.

7.8. CBDC z oprocentowaniem

Do i-kontraktu implementującego CBDC można łatwo wbudować naliczanie oprocentowania (por. podrozdział 2.10), co byłoby istotną różnicą w porównaniu z papierową gotówką. W przypadku braku anonimowości CBDC i zgody na dostęp banków do danych osobowych ich posiadaczy (por. podrozdział 7.2) to oprocentowanie mogłoby być zróżnicowane w zależności od ich kategorii – np. mogłoby być inne dla studentów, a inne dla emerytów, albo różne dla przedsiębiorców działających w różnych branżach. W pewnych sytuacjach oprocentowanie to (i jego różnicowanie) mogłoby stanowić wręcz instrument polityki gospodarczej i społecznej państwa (zob. podrozdziały 4.5–4.6).

Warto podkreślić, że naliczanie oprocentowania jest związane z rezygnacją z papierowej gotówki, a nie formy pieniędzy cyfrowych – CBDC lub klasycznych form bezgotówkowych pieniędzy na kontach w bankach.

PROGRAM ANALITYCZNO BADAWCZY

8. Wnioski wynikające z analizy technicznej

Jak wynika z analizy przeprowadzonej w rozdziałach 6 i 7 techniki i rozwiązania zastosowane w kryptowalutach są nieprzydane do implementacji CBDC.

Banki centralne są instytucjami zaufania publicznego, więc techniki i rozwiązania wypracowane specjalnie po to, aby wyeliminować zaufane strony trzecie, takie jak łańcuch bloków, kopanie, nagrody kopaczy i osiąganie globalnego konsensusu motywowane chęcią zdobycia nagrody przez kopaczy, są niepotrzebne w przypadku CBDC.

Banki centralne są i chcą pozostać jedynym emitentami swoich walut i chcą mieć możność prowadzenia odpowiedniej polityki emisji pieniądza w zależności od sytuacji gospodarczej, więc automatyczne emitowanie CBDC w blokach w miarę ich wykopywania lub weryfikacji jest nieodpowiednie.

Banki centralne nie chcą anonimowości ani nawet pseudonimowości CBDC ze względu na konieczność walki z finansowaniem terroryzmu, narkotyków i innych działań kryminalnych, praniem brudnych pieniędzy, omijaniem sankcji, unikaniem opodatkowania i tym podobnych nielegalnych działań. Anonimowość jako jedna z dwóch podstawowych cech papierowej gotówki nie jest do zaakceptowania w przypadku CBDC.

Również druga podstawowa cecha papierowej gotówki – możliwość bezpośredniego zapłacenia nią odbiorcy płatności przez płatnika – nie jest możliwa do zapewnienia w przypadku CBDC ze względu na problem podwójnego wydatkowania pieniędzy.

CBDC nie daje żadnych widocznych korzyści ani płatnikom, ani odbiorcom płatności w porównaniu z płatnościami mobilnymi polegającymi na szybkich przelewach.

Jeśli intencją banków centralnych jest silne konkurowanie z operatorami kart płatniczych i korporacjami internetowymi, to rozwiązania typu Blik są korzystniejsze niż wprowadzanie CBDC.

Generalny wniosek wynikający z analizy technicznej jest taki, że banki centralne w krajach takich, jak Polska, w których jest powszechnie dostępny internet, powinny skupić się na zapewnieniu płatności mobilnych i realizowanych za pomocą stacjonarnego internetu, które są szybkie, tanie i nieograniczone co do wysokości przelewów, chyba, że płatnik sam sobie nałoży ograniczenia. Propozycją opartą na tych założeniach jest Bank Cyfrowej Gotówki, którego koncepcję przedstawiono poniżej w rozdziale 9.

PROGRAM ANALITYCZNO BADAWCZY

9. Bank Cyfrowej Gotówki BCG

9.1. Założenia BCG

1. Narodowy Bank Polski emituje własną cyfrową gotówkę (e-złoty). E-złoty byłby komplementarny wobec gotówki papierowej i – poza formą – posiadał wszystkie inne cechy gotówki „tradycyjnej", będąc prawnym środkiem płatniczym (*legal tender*) i mogąc służyć – potencjalnie – jako środek przechowywania wartości (*store of value*).

2. E-złoty, tak jak gotówka papierowa, nie byłby oprocentowany.

3. NBP tworzy specjalny podmiot – Bank Cyfrowej Gotówki (BCG). Posiadanie konta w tym banku byłoby jedyną opcją dla osób fizycznych i niefinansowych podmiotów gospodarczych wejścia w posiadanie e-złotego i posługiwania się tą formą pieniądza.

   Konto to byłoby dla klientów tej instytucji bezpłatne. Wszelkie koszty funkcjonowania BCG ponosiłby NBP w ramach wypełniania swojej funkcji emisyjnej.

4. BCG działałby w oparciu o dobrze rozpoznane, tradycyjne technologie informatyczne, stosowane powszechnie w bankach[49], a zatem w oparciu o scentralizowaną bazę danych z odpowiednimi zabezpieczeniami.

5. Bezpieczeństwo informatyczne e-złotych zgromadzanych w BCG byłoby co do zasady takie samo, jak w innych bankach, przy wykorzystaniu tych samych metod zabezpieczeń.

6. Struktura agregatu M0 zmieniłaby się, obejmując teraz papierową gotówkę w obiegu i kasach banków, cyfrową gotówkę oraz środki banków na rachunkach w NBP. Zmieniłby się również agregat M1, obejmując papierową gotówkę w obiegu, cyfrową gotówkę w BCG oraz depozyty na żądanie (a vista).

7. BCG we współpracy z NBP na każde żądanie posiadaczy kont w BCG wymieniałby papierową gotówkę na e-złoty i odwrotnie w stosunku 1:1. Wymienialność ta byłaby ustawowo zagwarantowana. Łączny wolumen gotówki w obiegu nie zmieniałby się w przypadku zamiany gotówki papierowej na cyfrową i odwrotnie.

8. Możliwe byłoby dokonanie przelewu z konta w innym banku na konto w BCG, co byłoby równoznaczne z zamianą bankowego pieniądza bezgotówkowego na cyfrową gotówkę. Zmieniałaby się wówczas struktura agregatu M1, bez zmiany jego wolumenu. Podobnie, byłoby możliwe dokonanie przelewu z konta w BCG na konto w innym banku, co byłoby równoznaczne z zamianą cyfrowej gotówki na bankowy pieniądz bezgotówkowy.

9. E-złoty byłby powszechnie akceptowanym instrumentem płatniczym, zwalniającym z zobowiązań w każdym rodzaju transakcji. Posiadacze kont w BCG mogliby swobodnie dokonywać płatności cyfrową gotówką (także regulując zobowiązania publiczno-prawne); mogliby również utrzymać go jako swoje płynne rezerwy. W sytuacji braku oprocentowania mogłoby być to wątpliwe w warunkach wysokiej inflacji, ale zasadne przy inflacji umiarkowanej, a bardzo zasadne w sytuacjach kryzysowych – czynnikiem przemawiającym za tym byłoby całkowite bezpieczeństwo e-złotego przechowywanego w BCG w porównaniu ze środkami w bankach (nawet wziąwszy pod uwagę gwarancje BFG).

10. Płatności i rozliczenia wynikające z posługiwania się e-złotym przebiegałyby za pośrednictwem KIR.

11. Skala emisji e-złotego byłaby wyznaczana przez zgłaszany nań popyt i zasób papierowej gotówki oraz stanów depozytów bankowych na żądanie w posiadaniu osób fizycznych i niefinansowych podmiotów gospodarczych. Nie byłoby możliwości samodzielnej („pustej") kreacji e-złotego przez BCG. Byłoby to wykluczone na mocy odpowiednich przepisów prawnych.

12. Korzyści dla posiadaczy e-złotego:

- dodatkowy instrument płatniczy, umożliwiający natychmiastowe płatności między posiadaczami kont w BCG;
- możliwość bezpiecznego przechowywania środków;
- dostęp do podstawowych płatniczych i depozytowych usług finansowych nawet przy braku możliwości/chęci skorzystania z usług banków

49 Przez banki rozumie się tu zarówno banki komercyjne, jak i spółdzielcze.

– ważne w przypadku braku/utraty zaufania do banków na przykład w przypadku kryzysów w sektorze bankowym;

- tańszy dostęp – brak kosztów transakcyjnych występujących w bankach.

13. Korzyści dla banku centralnego:

- mniejsza emisja papierowej gotówki, a zatem niższe koszty;
- instrument zwiększający sprawność systemu płatniczego;
- możliwość kreacji popytu na e-złoty;
- względy prestiżowe i wizerunkowe.

14. Korzyści dla banków:

- mimo funkcjonowania cyfrowej gotówki banki nie są eliminowane z rynku finansowego;
- zachowują możliwość realizacji wszystkich operacji bankowych;
- niezmienione pozostają procesy kredytowania.

9.2. Analiza wad CBDC w przypadku e-złotego z BCG

Zagrożenie 1: Zakłócenie modeli biznesowych banków, wynikające z ich malejącego znaczenia w warunkach funkcjonowania CBDC.

Nie znajduje zastosowania (por. punkt 13*), gdyż banki pozostają znaczącym aktorem w systemie finansowym, oferując wszystkie tradycyjne usługi; mogą ewentualnie odnotować zmniejszenie depozytów na żądanie i wzrost kosztów operacji pasywnych.*

Zagrożenie 2: Ryzyko spadku reputacji i utraty wiarygodności (gdy emisja CBDC będzie zawierała błędy, bank centralny może nie mieć drugiej szansy po porażce wizerunkowej).

BCG będzie implementowany przy wykorzystaniu tradycyjnych technologii informatycznych dobrze rozpoznanych i szeroko stosowanych w bankach. Nie występuje zatem ryzyko związane z eksperymentowaniem z nowymi, skomplikowanymi, a mało sprawdzonymi technologiami cyfrowymi.

Zagrożenie 3: Ryzyko błyskawicznego odpływu pieniądza z banków, które może oddziaływać kryzysogennie.

Zależnie od regulacji banków w tym zakresie, odpływ pieniądza z nich może być ograniczany lub nawet powstrzymany; co więcej e-złoty i BCG mogą oddziaływać stabilizująco.

Zagrożenie 4: Problem z zapewnieniem stabilności i w tym kontekście wpływem CBDC na płynność międzynarodową i dynamikę kursu walutowego.

Rozwiązanie raczej stabilizujące; kwestie międzynarodowe wymagają głębszej analizy, gdyż wymaganie byłyby odpowiednie umowy międzynarodowe między bankami centralnymi, ale raczej można się tu doszukiwać pozytywów.

Zagrożenie 5: Kwestia naruszania prywatności (braku anonimowości) i szerokich możliwości kontroli ze strony państwa, jakie daje stosowanie CBDC.

Bezpośrednia kontrola NBP nad przelewami z/do kont w BCG. Informacja o tych przelewach może być udostępniana innym organom państwa tylko na podstawie odpowiednich przepisów prawa. Kontrola ta jest większa niż w przypadku papierowej gotówki; jednak ta ostatnia pozostaje w obiegu – posiadane e-złotego jest dobrowolne i komplementarne wobec gotówki papierowej.

9.3. Analiza sygnalizowanych w literaturze zalet CBDC w przypadku e-złotego z BCG

Zaleta 1: Poprawa ściągalności podatków i zmniejszenie szarej strefy.

Brak większego wpływu, nadal możliwe transakcje papierową gotówką.

Zaleta 2: Włączenie finansowe.

Możliwe, e-złoty może przekonać do utrzymywania środków w BCG i posługiwania się nimi osoby nie korzystające z usług bankowych z powodu niskiego zaufania do banków lub ewentualnych kosztów korzystania ich usług.

Zaleta 3: Dezintermediacja.

Podobnie jak „klasyczne" CBDC w modelu pośrednim – rola banków ulega tylko nieznacznemu umniejsze-

niu wynikającemu z możliwości trzymania zasobów finansowych w formie e-złotego.

Zaleta 4: Większe bezpieczeństwo systemowe.

Tak, dzięki podwyższonemu poziomowi zaufania do e-złotego i BCG.

Zaleta 5: Możliwość prowadzenia skuteczniejszej i bardziej elastycznej polityki pieniężnej.

Możliwe w przypadku „awaryjnego" wprowadzenia oprocentowania e-złotego i wykorzystania BCG jako instrumentu ścigającego nadmierną płynność.

Zaleta 6: Możliwość prowadzenia skuteczniejszej polityki fiskalnej.

Nie, zważywszy na dobrowolność posiadania konta w BCG równolegle z kontami w bankach.

Zaleta 7: Większa kontrola emisji pieniądza.

Bez zmian – emisja e-złotego byłaby endogeniczna, odbywając się w takim zakresie, w jakim chciałby tego rynek.

Zaleta 8: Kwestie renty menniczej.

Wraz ze wzrostem popularności e-złotego wzrost renty menniczej (wyższa różnica między wartością e-złotych a (zerowym) kosztem ich wytworzenia)

Zaleta 9: Suwerenność monetarna.

Bez zmian, e-złoty jest nową formą gotówki, ale cały czas w ramach standardu (jednostki obrachunkowej), jaką jest polski złoty; ewentualne korzyści wizerunkowe, przy rozszerzeniu opcji płatności na sferę międzynarodową możliwość większej popularności waluty polskiej w ogóle.

9.4. Kwestia oprocentowania e-złotego

Można rozważyć sytuację, gdy zasoby e-złotego zgromadzone na kontach w BCG są oprocentowane – podobnie jak w pewnych scenariuszach dotyczących CBDC (por. podrozdział 2.10 i 7.8). Oprocentowanie to wypłacałby posiadaczom e-złotego NBP za pośrednictwem BCG. W naszym przekonaniu, rozwiązanie to, z wielu względów, **nie powinno być wprowadzone**.

1. Najgorszym scenariuszem byłoby przyjęcie rozwiązania, że odsetki wypłacane od e-złotego są rozwiązaniem trwałym. Tworzyłoby to trwałą alternatywę dla depozytów w bankach, stanowiąc instrument nierynkowej, trudnej do sprostania konkurencji dla banków. Ponadto, e-złoty zamiast być instrumentem zwiększającym efektywność płatności i rozliczeń, stałby się wówczas jeszcze jednym instrumentem polityki pieniężnej, a jego oprocentowanie – kolejną z oficjalnych stóp procentowych NBP. Taka sytuacja stałaby w sprzeczności z samą koncepcją i celem wprowadzenia cyfrowej gotówki.

2. Mniej wątpliwości budzi przejściowe (czasowe) wprowadzenie oprocentowania kont w BCG w nadzwyczajnych sytuacjach (np. nadmiernej płynności). Oznaczałoby to bowiem pewną doraźną interwencję NBP, w sytuacji uzasadnionej względami stabilności systemu finansowego lub stabilności monetarnej. Niemniej, takie rozwiązanie również byłoby naruszeniem konkurencji rynkowej. Ponadto, istnieje niewątpliwe ryzyko utrwalenia się takiego przejściowego oprocentowania e-złotego, gdyż NBP, zachęcony skutecznością takiego działania, mógłby odczuwać pokusę jego stosowania nawet bez wyraźnej potrzeby (choć oczywiście oznaczałoby ono dla niego także koszty). Z drugiej strony, posiadacze e-złotego mogliby niejako przyzwyczaić się do tego, że ich środki w BCG są oprocentowane i wycofanie się z takiego rozwiązania mogłoby nastręczać problemy.

60

10. Wnioski

Banki centralne powinny dążyć do wprowadzenia swojej cyfrowej gotówki, oferując obywatelom nową, dostosowaną do bieżących uwarunkowań technologicznych, ekonomicznych i kulturowych formę pieniądza. Może to wiązać się z licznymi korzyściami, natury nie tylko czysto gospodarczej, ale i politycznej oraz społecznej. Zawsze powinno to odbywać się jednak z uwzględnieniem warunków i sytuacji danego kraju. Władze gospodarcze powinny także odpowiedzieć sobie na pytanie, jakim celom miałaby służyć cyfrowa gotówka i jaka będzie hierarchia tych celów. Jak bowiem wskazano w raporcie, może wystąpić między nimi konflikt.

Jak wynika z tego raportu banki centralne, wdrażając cyfrową walutę ani nie muszą, ani nie powinny stosować w tym celu technologii opracowanych dla kryptowalut. Głównym założeniem tych technologii, w szczególności łańcucha bloków, jest brak zaufania do wszelkich instytucji, na rzecz algorytmów, rozwiązań rozproszonych i obdarzenia mocą decyzyjną społeczności niezależnych użytkowników, a banki centralne chcą pozostać instytucjami zaufania publicznego i zachować swoją władzę w systemach finansowych państw.

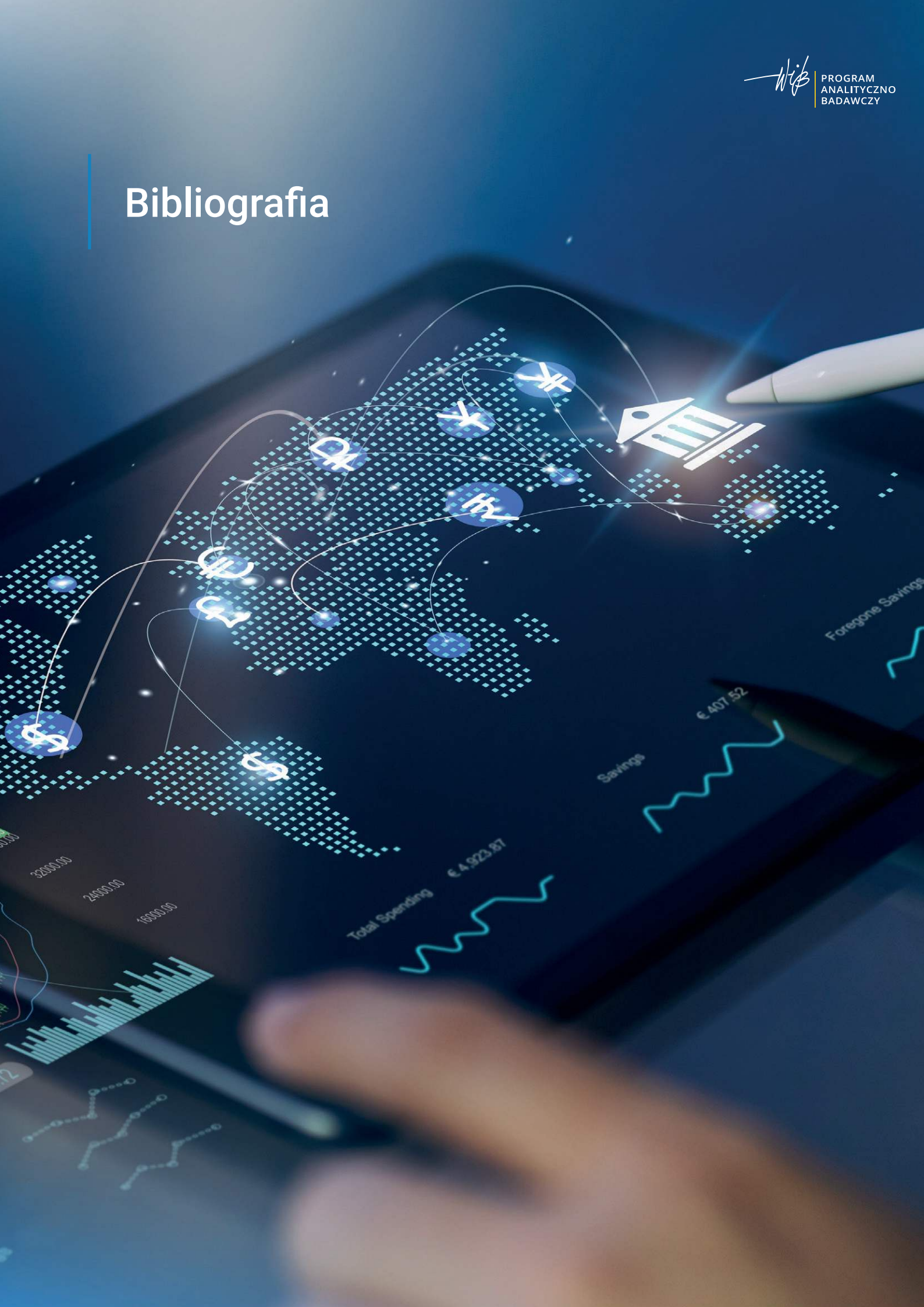
Banki centralne muszą odpowiedzieć sobie na pytanie czy ich celem jest zastosowanie technologii kryptowalut w swoim obszarze działalności, czy też ich celem jest wprowadzenie cyfrowej waluty na swoich zasadach. Te dwa cele nie są tożsame, co wykazujemy w tym raporcie.

Zastosowanie technologii kryptowalut do implementacji cyfrowych walut banków centralnych wymaga tak głębokich ich modyfikacji, że tracą one swoje unikalne właściwości.

Dlatego w tym raporcie proponujemy eleganckie rozwiązanie polegające na utworzeniu Banku Cyfrowej Gotówki. Pozwala ono zachować zalety płynące z cyfrowej gotówki, eliminując jednocześnie wady będące konsekwencją traktowania CBDC jako „kryptowalut banków centralnych". Propozycja utworzeniu Banku Cyfrowej Gotówki jest dobrze dostosowana do poziomu rozwoju płatności cyfrowych, w tym mobilnych, w Polsce, więc mogłaby być podstawą do wprowadzenia e-złotego.

PROGRAM ANALITYCZNO BADAWCZY

Bibliografia



[1] Achor, P.N., Robert, A. (2012). Shifting policy paradigm from cash-based economy to cashless economy: the Nigeria experience. Afro Asian Journal of Social Sciences, 4, 1–16, Dostęp: 2023-03-31; http://www.onlineresearchjournals.com/aajoss/art/124.pdf

[2] Adrian T., Shin H. (2019). The Shadow Banking System: Implications for Financial Regulation. Banque de France Financial Stability Review, No. 13.

[3] Adrian, T., Mancini-Griffoli, T. (2019). The Rise of Digital Money. IMF Fintech Note, 19/01.

[4] Antonopoulos, A. (2017). Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków, Wydanie II, Helion.

[5] Antonopoulos, A., Wood, G. (2019). Ethereum dla zaawansowanych. Tworzenie inteligentnych kontraktów i aplikacji zdecentralizowanych. Helion.

[6] Application-Specific Integrated Circuit (ASIC) Miner, Dostęp: 2023-02-04; https://www.investopedia.com/terms/a/asic.asp

[7] Bank of England (2023). The digital pound: Technology Working Paper. Dostęp: 2023-03-31; https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf?la=en&hash=A97A5C2056FF5CD4D494B1E6A2EED7B8271ACA54

[8] Bank of England and HM Treasury (2023), The digital pound: A new form of money for households and businesses? Consultation Paper. Dostęp: 2023-03-31; https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound--consultation-working-paper.pdf?la=en&hash=5CC053D3820DCE2F40656E772D9105FA10C654EC

[9] Bech, M., Garratt, R. (2017). Central Bank Cryptocurrencies. BIS Quarterly Review, 55–70.

[10] BIS (2015). Digital Currencies. Committee on Payments and Market Infrastructures, November.

[11] BIS (2018). Central Bank Digital Currencies. Committee on Payments and Market Infrastructures, Markets Committee, March.

[12] BIS (2020). Central bank digital currencies: foundational principles and core features. Report no 1 in a series of collaborations from a group of central banks. Basel.

[13] BIS, Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements[2021). Central bank digital currencies. Executive summary 1. Basel.

[14] Bitcoin Transactions Per Day, Dostęp: 2023-02-04; https://ycharts.com/indicators/bitcoin_transactions_per_day

[15] Bitnodes, Dostęp: 2023-01-12; https://bitnodes.io/

[16] Bjerg, O. (2017). Designing New Money. The Policy Trilemma of Central Bank Digital Currency. Copenhagen Business School (CBS), June.

[17] Bordo, M., Levin, A. (2017). Central Bank Digital Currency and the Future of Monetary Policy. NBER Working Paper, 23711.

[18] Bordo, M.D. (2022). Central Bank Digital Currency in Historical Perspective: Another Crossroad in Monetary History. Capitalism: A Journal of History and Economics, 3(2), 421–442. doi:10.1353/cap.2022.0015.

[19] Brunnermeier, M, James, H., Landau, J.P. (2019). The Digitalization of Money. NBER Working Papers, 26300.

[20] Budish, E. (2018). The Economic Limits of Bitcoin and the Blockchain. NBER Working Papers, 24717, National Bureau of Economic Research, Inc.

[21] Carney, M. (2015). Breaking the Tragedy of the Horizon. Climate Change and Financial Stability. Bank of England.

[22] Carstens, A. (2021). Digital currencies ant the future of the monetary system, Hoover Institution policy seminar.

[23] Casper protocol: What is it? Ethereum upgrade 101, Dostęp: 2023-02-03; https://www.cryptopolitan.com/casper-protocol-the-new-ethereum-upgrade-101/

[24] CBDC Tracker (2021). White paper. Dostęp: 2023-03-31; https://cbdctracker.org/cbdc-tracker--whitepaper.pdf

[25] CBDCs in emerging market economies (2022). BIS Papers, No 123 April.

[26] Cellary, W., E. Gelenbe, T. Morzy (1988). Concurrency Control in Distributed Database Systems. Elsevier Science Publishers, North-Holland, Amsterdam, New York, Tokyo.

[27] Chaum, D. (1983). „Blind signatures for untraceable payments". Advances in Cryptology Proceedings, 82 (3): 199–203. 1983, Dostęp: 2023-03-03; http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

[28] Chen L., Wu H. (2009). The Influence of Virtual Money to Real Currency: A Case-based Study, Beijing University of Posts and Telecommunications. International Symposium on Information Engineering and Electronic Commerce.

[29] Claeys G., Demertzis M., Esthatiou K. (2018). Cryptocurrencies and Monetary Policy. Policy Contribution, no. 10.

[30] Cochrane, J. (1998). A Frictionless View of US Inflation. In: Bernanke, B., Rotemberg, J. (eds.) NBER Macroeconomics Annual, vol. 13, MIT Press, Massachusetts.

[31] Cochrane. J. (2001). Money as Stock: Price Level Determination with no Money Demand. NBER Working Papers 7498, National Bureau of Economic Research, Inc.

[32] Cohen, B. J. (2004). The Future of Money, Princeton University Press.

[33] Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S. & Hess, J. (2018). Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. World Bank Group.

[34] Dexaran/ERC223-token-standard, Dostęp: 2023-02-02; https://github.com/Dexaran/ERC-223-token-standard

[35] DigiCash, Dostęp: 2023-01-12; https://en.wikipedia.org/wiki/DigiCash

[36] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), vol. OJ L, 23 December 2015, Dostęp: 2023-02-06; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L2366-20151223

[37] Dodd, N. (2018). The Social Life of Bitcoin. Theory, Culture and Society, 35(3), 35–56. https://doi.org/10.1177/0263276417746464.

[38] Dowd, K. (1998). Private Money: The Path to Monetary Stability. Institute of Economic Affairs.

[39] Dyson, B., Hodgson, G. (2016). Digital Cash: Why Central Banks Should Start Issuing Electronic Money. https://positivemoney.org/publications/digital-cash/

[40] ECB (2012). Virtual Currency Schemes, Frankfurt am Main.

[41] ECB (2015). Virtual Currency Schemes – a further analysis. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[42] ECB (2021). Climate-Related Risk and Financial Stability. ECB/ESRB Project Team on Climate Risk Monitoring.

[43] Eichengreen, B. (2019). From commodity to fiat and now to crypto: what does history tell us? NBER Working Paper, no. 25426.

[44] Ejiofor, V.E. & Rasaki, J.O. (2012). Realising the benefits and challenges of cashless economy in Nigeria: its perspective. International Journal of Advances in Computer Science and Technology, 1, 7–13.

[45] ERC-20: Token Standard, Dostęp: 2023-02-02; https://eips.ethereum.org/EIPS/eip-20

[46] ERC-777 Token Standard, Dostęp: 2023-02-02; https://ethereum.org/en/developers/docs/standards/tokens/erc-777/

[47] Ethash, Dostęp: 2023-02-03; https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/mining-algorithms/ethash/#top

[48] Ethereum Node Tracker, Dostęp: 2023-02-01; https://etherscan.io/nodetracker

[49] Ethereum Transactions Per Day, Dostęp: 2023-02-04; https://ycharts.com/indicators/ethereum_transactions_per_day

[50] Ethereum's energy expenditure, Dostęp: 2023-02-04; https://ethereum.org/en/energy-consumption/

[51] Europejski Urząd Nadzoru Bankowego (2014). EBA Opinion on „virtual currencies", Dostęp: 2023-03-31; 04https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1

[52] FATF (2014). FATF Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks. Paris.

[53] Federal Deposit Insurance Corporation (FDIC). (2020) How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey (October 2020). Retrieved from: https://www.fdic.gov/analysis/household-survey/2019report.pdf

[54] Federal Reserve System (2022). Money and Payments: The U.S.Dollar in the Age of Digital Transformation. Board of governors, Waszyngton.

[55] Galloway, S. (2018). Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook I Google. Rebis.

[56] Goetzman, W.N. (2016). Money changes everything. How finance made civilization possible. Princeton University Press.

[57] Good, B.A. (1998). Private Money: Everything Old is New Again. Federal Reserve Bank of Cleveland Economic Commentary.

[58] Grzybkowski, M., Bentyn, S. (2021). Kryptowaluty. Wydanie drugie, Crypto-logic.

[59] Haber, S., Stornetta, W.S. (1991). „How to time stamp a digital document", Journal of Cryptology, 3(2), 99–111.

[60] Harasim, J. (2021). FinTechs, BigTechs and Banks – When Cooperation and When Competition?, Journal of Risk and Financial Management, vol. 14, 2

[61] Hazlett, P., Luther, W. (2020). Is Bitcoin Money? And What That Means. The Quarterly Review of Economics and Finance, 77, 144–149. https://doi.org/10.1016/j.qref.2019.10.003.

[62] Kemp, S., Digital 2023: Global Overview Report. Dostęp 2023-03-31; https://datareportal.com/reports/digital-2023-global-overview-report

[63] Ingham, G. (2000). Nature of money. Polity.

64] Ingham, G. (2020). Money. Polity.

[65] Iwańczuk-Kaliska, A. (2018). Pieniądz cyfrowy banków centralnych – wnioski z analizy wybranych koncepcji. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, 531, 180–189.

[66] Iwańczuk-Kaliska, A. (2022). Bezgotówkowe płatności detaliczne w Polsce – rola banków i perspektywy rozwoju sektora paytech. W: K. Waliszewski (red.) Finanse osobiste. PAN.

[67] Iwańczuk-Kaliska, A., Schmidt-Jessa, K., Warchlewska, A., Marszałek, P. (2021). Ocena zmian na rynku płatności w Polsce. WIB PAB 10/2021.

[68] Jurek, M. (2011). Międzynarodowy system walutowy i systemy kursowe w warunkach integracji finansowej. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

[69] Kahn, Charles M. Van Oordt, Maarten R. C.Zhu, Yu (2021). Best before? Expiring central bank digital currency and loss recovery. Bank of Canada Staff Working Paper, No. 2021-67

[70] King, B. (2018). Bank 4.0: Banking everywhere, never at a bank. Marshall Cavendish International (Asia) Pte Ltd.

[71] King, M. (2017). The end of alchemy. W. W. Norton & Company.

[72] Kliber A., Będowska-Sojka, B., Rutkowska, A., Świerczynska K., Zdunkiewicz, W. (2020) FinTechs in Poland: Insights, Trends and Perspectives. Technical Report. DOI: 10.13140/RG.2.2.31841.53605/2

[73] Knakiewicz, Z. (2011). Nominalistyczne teorie pieniądza. W: M. Jurek, Z. Knakiewicz, P. Marszałek (red.). Teorie pieniądza i ich wykorzystanie. Od pieniądza kruszcowego do fiducjarnego. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

[74] Konstytucja Rzeczypospolitej Polskiej, Dziennik Ustaw 1997 nr 78 poz. 483, Dostęp: 2023-02-06; https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970780483/U/D19970483Lj.pdf

[75] Kosse, A., Mattei, I. (2022). Gaining Mmomentum. Results of the 2021 BIS Survey on Central Bank Digital Currencies. BIS Papers, 125.

[76] Kotliński, G., Marszałek, P., Waliszewski, K., Warchlewska, A. (2022). Wpływ nowoczesnych technologii na zmianę modeli biznesowych banków. WIB PAB 1/2022.

[77] Kowalski, T. (2001). Proces formułowania oczekiwań a teoria cyklu wyborczego. Implikacje dla polityki gospodarczej. Wydawnictwo Akademii Ekonomicznej w Poznaniu.

[78] Krajowa Izba Rozrachunkowa, Dostęp: 2023-02-12; https://www.kir.pl/

[79] Leyshon, A., & Thrift, N. (1995). Geographies of financial exclusion: financial abandonment in Britain and the United States. Transactions of the Institute of British Geographers, New Series, 20(3), 312–341.

[80] Mancini-Griffoli, T., Martinez Peria, M.S., Agur, I., Anil, A., Kiff, J., Popescu, A., Rochon, C. (2018). Casting Light on Central Bank Digital Currency. IMF Staff Discussion Note, 18/08.

[81] Marszałek, P. (2014). Systemy pieniężne wolnej bankowości. Koncepcje, cechy, zastosowanie. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

[82] Marszalek, P. (2015). Wybrane procesy wpływające na współczesne systemy bankowe. Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 401, 285–295.

[83] Marszałek, P. (2019). Kryptowaluty – pojęcie, cechy, kontrowersje. Studia BAS, 1(57), 105–125.

[84] Marszałek, P. (2021). Kryptowaluty jako element systemu pieniężnego. W: Innowacje finansowe w gospodarce 4.0 (s. 28–50). W: K. Perez (red.). Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

[85] Martin, F. (2013). Money. The Unauthorised biography. Vintage books.

[86] Maurya, P. (2019). Cashless Economy and Digitalization. Proceedings of 10th International Conference on Digital Strategies for Organizational Success. Retrieved from: https://ssrn.com/abstract=3309307 or http://dx.doi.org/10.2139/ssrn.3309307

[87] McCallum, B.T. (2004). Monetary policy in economies with little or no money. Pacific Economic Review, 9, 81-92. doi: 10.1111/j.1468-0106.2004.00213.x

[88] Merkle, R.C., „Protocols for public key cryptosystems”, Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, 122–133.

[89] MFW (2020) A Survey of Research on Retail Central Bank Digital Currency.

[90] Milne, A. (2018). Cryptocurrencies from an Austrian Perspective. In: Banking and Monetary Policy from the Perspective of Austrian Economics, DOI: 10.1007/978-3-319-75817-6_12.

[91] Moreira, A., Savov, A. (2017). The Macroeconomics of Shadow Banking. The Journal of Finance, 72(6), 2381–2431.

[92] Nakamoto, S. (2008). Bitcoin: A Peer to Peer Electronic Cash System. Dostęp: 2023-01-12; https://cryptocurrencyworks.com/.res/doc/BitcoinSNakamoto Oct 2008.pdf

[93] Nash, J. F. (2002). Ideal Money. Southern Economic Journal, 69(1), 4–11. https://doi.org/10.2307/1061553

[94] NBP (2021). Pieniądz cyfrowy banku centralnego. Warszawa: Narodowy Bank Polski.

[95] NBP (2022). Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2022 r. Warszawa

[96] Near Field Communication Technology Standards, Dostęp: 2023-02-06; http://nearfieldcommunication.org/technology.html

[97] NIST, SHA 3 Standard: Permiutation Based Hash and Extendable Output Functions, sierpień 2015, doi:10.6028/NIST.FIPS.202. S2CID 64734386. Dostęp: 2023-01-07; https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

[98] Oberhaus,D. (2018). „The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995", sierpień 2018, Dostęp: 2023-01-12; https://www.vice.com/en/article/j5nzx4/what was the first blockchain

[99] Oxford Dictionary (2021). Financial exclusion. Oxford University Press.

[100] Peneder, (2022). Austrian conceptions of money and the rise of digital currency. SUERF Policy Note, No 265.

[101] PIE (2021). Tygodnik Gospodarczy, nr 25, 24 czerwca 2021.

[102] Polański, Z. (2019). O polityce pieniężnej doby kryzysu, innowacjach i dwoistej naturze pieniądza. W: W. Przybylska-Kapuścińska, K. Perez (red.) Polityka pieniężna i rynki finansowe wobec wyzwań gospodarki 4.0. CeDeWu.

[103] Popper., N. (2012). Digital Gold. The Untold Story of Bitcoin. London.

[104] Pozsar, Z., Adrian, T., Ashcraft, A., Boesky, H. (2010). Shadow banking. Staff Report, Federal Reserve Bank of New York, No. 458.

[105] Prasad E.S. (2021). The Future of Money. How the Digital Revolution is Transforming Currencies and Finance. Harvard University Press.

[106] Proof-of-Stake (POS), Dostęp: 2023-02-03; https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[107] Raport o stanie rynku telekomunikacyjnego w Polsce w 2021 r., Urząd Komunikacji Elektronicznej, Warszawa 2022; https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/431/13/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2021_r..pdf

[108] Regulamin systemu Express Elixir, Wersja 1.6, Krajowa Izba Rozliczeniowa S.A. Obowiązuje od dnia 1 lipca 2018 r., Dostęp: 2023-02-11; https://www.expresselixir.pl/download/gfx/expresselixir/pl/defaultstronaopisowa/34/1/1/regulamin_express_elixir_wersja_1.6.pdf

[109] Regulamin Systemu Płatności Mobilnych BLIK, Wydanie dziewiąte z dnia 23.07.2021 r., Dostęp: 2023-02-11; https://blik.com/download/pobierz/regulamin

[110] Rickards, J. (2012). Wojny walutowe. Nadejście kolejnego globalnego kryzysu. Helion.

[111] Rivest, R.; Shamir, A.; Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM. 21 (2), 120–126, Dostęp: 2023-01-08; https://dl.acm.org/doi/10.1145/359340.359342

[112] Schwab, K. (2016). The Fourth Industrial Revolution. Penguin.

[113] Serval, J.F., Tranie, J.P. (2015). Monetary system. Analysis and New Approaches to Regulation. Wiley.

[114] Single Euro Payments Area – SEPA, Dostęp: 2023-02-11; https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.html

[115] Sławiński, A. (2019a). Could Cryptocurrencies or CBDCs Replace the Recent Monetary Systems? Ekonomista, 5, 636–646.

[116] Sławiński, A. (2019b). Kryptowaluty – zapowiedzi i rzeczywistości. W: W. Przybylska-Kapuścińska, K. Perez, Polityka pieniężna i rynki finansowe wobec wyzwań gospodarki 4.0. Warszawa: CeDeWu.

[117] Solarz J.K. (2014), Shadow banking: systemowa innowacja finansowa. SAN, Studia i Monografie, Łódź-Warszawa 2014, nr 52.

[118] Solidity, Dostęp: 2023-02-01 https://soliditylang.org/

[119] Sumner, S. (2021). The Money Illusion: Market Monetarism, the Great Recession, and the Future of Monetary Policy. University of Chicago Press.

[120] Sveriges Riksbank (2018), The Riksbank's e-krona project. Report 2.

[121] Sveriges Riksbank (2021), On the possibility of a cash-like CBDC. Staff Memo.

[122] SWIFT Dostęp: 2023-02-06; https://www.swift.com/

[123] The Average Number of Credit Card Transactions Per Day & Year, Dostęp: 2023-02-04; https://www.cardrates.com/advice/number-of-credit-card-transactions-per-day-year/

[124] Tooze, A. (2022a). Welcome to the world of the polycrisis. Financial Times, October, 28.

[125] Tooze, A. (2022b). Nie jesteśmy ani w 1939, ani w 1914 roku. Historia się nie powtarza. Rozmowa z Cezarym Morawskim. Puls Biznesu, opublikowano: 2023-01-05.

[126] Total Circulating Bitcoin, Dostęp: 2023-01-12; https://www.blockchain.com/explorer/charts/total bitcoins

[127] Trautman, L. J. (2018). Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace. Marquette Law Review, 447, Available at SSRN: https://ssrn.com/abstract=3182867 or http://dx.doi.org/10.2139/ssrn.3182867

[128] Trichet, J. C. (2000). World-wide tendencies in financial system. Deutsche Bundesbank Auszüge aus Presseartikeln, no. 49.

[129] Turrin, R (2022). Rewolucja finansowa w Chinach. Koniec gotówki. Cyfrowy Juan. Nowy globalny system walutowy? Zona Zero, sp. z o.o.

[130] Urquhart, A. (2016). The inefficiency of Bitcoin. Economics Letters, Volume 148, 80–82.

[131] Ustawa o Narodowym Banku Polskim, Dziennik Ustaw 2022 r. poz. 2025, Dostęp: 2023-02-06; https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19971400938

[132] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dziennik Ustaw 2018 poz. 723, Dostęp: 2023-02-06; https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000723/U/D20180723Lj.pdf

[133] Ustawa Prawo bankowe, Dziennik Ustaw 2022 r. poz. 2324, 2339, 2640, 2707, Dostęp: 2023-02-06; https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19971400939/U/D19970939Lj.pdf

[134] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz.U. 2016 poz. 1579

[135] UTXO Model: Definition, How It Works, and Goals, Dostęp: 2023-02-15; https://www.investopedia.com/terms/u/utxo.asp

[136] Warchlewska, A. (2020). Wokół istoty wykluczenia finansowego. Ujęcie przeglądowe, Finanse i Prawo Finansowe, vol. 1(25).

[137] Warchlewska, A. (2022). Wykluczenie finansowe. Od finansów tradycyjnych do finansów cyfrowych. Wydawnictwo UEP.

[139] What Is Proof-of-Authority? Dostęp: 2023-03-06; https://www.coindesk.com/learn/what-is-proof-of-authority/

[140] Wilson, P. (2019). Hostile money. Currencies in conflict. The History Press, Stroud.

[141] Wojciech Cellary, Token niezamienny, Gazeta Wyborcza, magazyn Wolna , 2022-01-15, Dostęp: 2023-02-02; https://wyborcza.pl/magazyn/7,124059,28003186,wojciech-cellary-czy-za-zeton-mozna-zaplacic-69-mln-dol-w.html

[142] Wolfram MathWorld, Binary tree, Dostęp: 2023-03-03; https://mathworld.wolfram.com/BinaryTree.html

[143] Woodford M. (2003). Interest and Prices. Princeton University Press.

[144] Wray, R.L. (2000). Modern money. In J. Smithin (Ed.). What is money? (42–66). Routledge.

[145] Xia, H., Gao, Y. & Zhang, J.Z. (2023). Understanding the adoption context of China's digital currency electronic payment. Financial Innovations 9(63). https://doi.org/10.1186/s40854-023-00467-5.

[146] Yaqub, J.O., Bell, H.T., Adenuga, I.A. & Ogundeji, M.O. (2013). The cashless policy in Nigeria: prospects and challenges. International Journal of Humanities and Social Science, 3(3), 200–212.

[147] Yermack, D. (2016). Is Bitcoin a Real Currency? An Economic Appraisal. In: D.L.K. Chuen (ed.) Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Elsevier.

PROGRAM
ANALITYCZNO
BADAWCZY

Central Bank Digital Currency

Raport przygotowany na zlecenie
Fundacji Warszawski Instytut Bankowości