DOI: 10.21858/msr.23.03

Wpływ nowych technologii na ryzyko utraty płynności sektora bankowego

Krzysztof Spirzewski

STRESZCZENIE

Obecnie wiemy, że kryzys finansowy z 2007 r. można było zażegnać, gdyby świadomość zagrożeń i ich przyszłych konsekwencji była pełniejsza. Dzisiejszemu rozwojowi technicznemu w sektorze bankowym towarzyszą tradycyjne zagrożenia w postaci paniki bankowej, gdy większość klientów banku jednocześnie zdecyduje się wypłacić zdeponowane pieniądze. W konsekwencji ryzyko utraty płynności gwałtownie rośnie. Wraz z rozwojem nowych technik IT upowszechniają się internetowe kanały dostępu do usług bankowych (mowa w szczególności o bankowości internetowej), stwarzając nowe, systemowe zagrożenie dla bezpieczeństwa. Wzrasta ryzyko upadku banku z powodu utraty płynności wskutek realizacji w krótkim przedziale czasowym bardzo wielu transferów pieniędzy z wielu rachunków w jednym banku do innych banków.

Opisywane w niniejszym artykule zagrożenie nie jest czysto teoretyczne. Kłopotów z nim związanych polski system płatniczy doświadczył w I połowie 2016 r. Doszło wówczas do incydentu związanego z bezpieczeństwem IT polegającego na ataku na infrastrukturę klienta banku za pomocą akcji phishingowej. W celu podniesienia skuteczności tej akcji rozpowszechniono w mediach społecznościowych plotkę o niewypłacalności owego banku, sugerując natychmiastową wypłatę pieniędzy.

Wstęp

Wiele dyskusji na temat kryzysu finansowego zapoczątkowanego w 2007r. kończy się konkluzją, że gdyby w okresie na krótko poprzedzającym ów rok świadomość przyszłych zagrożeń była większa, to odpowiednia reakcja zapobiegłaby bardzo poważnym następstwom, których skutki są odczuwane do dziś. Idąc tym tropem myślenia, warto rozważyć podobną sekwencję zdarzeń, związaną tym razem z ryzykiem wprowadzania nowoczesnych technologii do usług bankowych. Ewentualne ryzyko dla płynności banku może się zmaterializować w sytuacji, gdy większość jego klientów ma bezpośredni dostęp do rachunku bankowego realizowany za pośrednictwem bankowości internetowej[1]. Sytuacja taka występuje praktycznie we wszystkich bankach w Polsce. Obserwowane różnice dotyczą raczej procentowego udziału klientów posiadających dostęp zdalny, na tle pozostałych klientów banku. Ten nowy rodzaj ryzyka powinien być klasyfikowany jako ryzyko systemowe i zostać należycie rozpoznany przez Urząd Komisji Nadzoru Finansowego (KNF). Wynika to z konieczności przeciwdziałania wielu zagrożeniom, jakie mogą przynieść nowe technologie.

[1] W niniejszym artykule przyjmuje się, że sformułowania bankowość internetowa i elektroniczna są tożsame i używane wymiennie.

Nowe technologie przyczyniają się ponadto do opracowywania nowych regulacji prawnych, takich jak Dyrektywa PSD2[2] [EC, PSD2], stawiających banki w nowej roli. Perspektywicznie zaś trzeba mieć również świadomość, że technologia *blockchain*/*DLT* (*Distributed Ledger Technology*)[3] stwarza możliwość znacznej zmiany sposobu funkcjonowania systemu finansowego, a szczególnie systemu płatniczego. Rewolucyjność tego rozwiązania przejawia się przede wszystkim w dziedzinie bezpieczeństwa, w ten sposób, że każdy nowy zapis w rejestrze jest związany z poprzednim, a ów – z jeszcze wcześniejszym. Bezpieczeństwo raz wprowadzonego zapisu polega na braku możliwości jego zmiany bez korekty poprzednich zapisów [Król 2017].

Jednocześnie rozwój techniczny, nowe narzędzia informatyczne, a także coraz większa łatwość ich stosowania idą w parze z rosnącymi umiejętnościami i apetytami cyberprzestępców. Cyberzagrożenia ciągle ewoluują, trzeba zatem umieć je dostrzegać, analizować i podejmować skuteczne działania obronne.[4]

Niniejszy artykuł ma na celu wskazanie na rosnące ryzyko utraty płynności banku w wyniku rozwoju technicznego, którego osiągnięcia zastosowano na szeroką skalę w sektorze bankowym. Utrata płynności pojedynczego banku – nawet średniej wielkości – może poprzez efekt kaskadowy zagrozić płynności całego sektora. Niniejsze opracowanie wskazuje na konieczność wypracowania przez zarządy banków i instytucje nadzorcze odpowiednich metod postępowania mogących zminimalizować opisywane ryzyko.

Postęp techniczny i tradycyjne zagrożenia

W sektorze bankowym straty wynikające z działalności operacyjnej to problem o długoletniej historii, istniejący tak długo jak sama instytucja banku. Przez większą część tego okresu straty owe utożsamiane były ze zwykłymi napadami rabunkowymi czy stratami towarzyszącymi podstawowej działalności operacyjnej banku: przeliczaniu gotówki czy czynnościom księgowym. Obecnie katalog tego typu strat jest szerszy. Docenienie znaczenia ich ryzyka przez instytucje regulujące rynek bankowy nastąpiło w 1999 r., wraz z przyjęciem samoregulacji sektora bankowego znanej pod nazwą „Bazylea I" [Koterwas 2003]. W kontekście kryzysu z 2007 r. samoregulacja okazała się niewystarczająca. Instytucje nadzoru miały wówczas pełny wgląd w sytuację finansową banków, a mimo to nie zareagowały na alarmujące dane świadczące o zbliżającym się zagrożeniu [Zieliński 2014, s. 40].

---

[2] PSD2: nowa wersja dyrektywy w sprawie usług płatniczych w ramach rynku wewnętrznego. Przyjęta przez Parlament Europejski i Radę (UE) w dniu 25 listopada 2015 r. nr 2015/2366, w celu udoskonalenia obowiązujących przepisów i uwzględnienia nowych cyfrowych usług płatniczych. Dyrektywa wejdzie w życie w 2018 r.

[3] DLT (*Distributed Ledger Technology*): Technologia Rozproszonych Rejestrów to rodzaj rozproszonej księgi, w której można przechowywać informacje w układzie chronologicznym. Często określenia *blockchain*, rozproszone rejestry i współdzielone rejestry występują zamiennie.

[4] W 2015 r. UKNF zarejestrował 8 914 potwierdzonych przypadków naruszeń cyberbezpieczeństwa, wobec 7 498 takich zdarzeń w 2014 r. Mimo wzrostu świadomości zagrożenia wśród użytkowników internetu poziom zagrożenia nie maleje. http://www.knf.gov.pl/

Wraz z rozwojem techniki rośnie liczba usług bankowych opartych na nowoczesnych rozwiązaniach elektronicznych. Wśród tych usług najbardziej rozpowszechniona jest dyspozycja przelewu złożona za pomocą bankowości elektronicznej[5]. Mieści się ona w segmencie usługi zastępującej papierowy formularz dyspozycji przelewu z konta, w której kluczową rolę odgrywał własnoręcznie złożony podpis osoby upoważnionej do składania takiej dyspozycji. W bankowości elektronicznej rolę tę przejął system loginów i haseł.[6] W usługach elektronicznych największe ryzyko jest związane z bezpieczeństwem informatycznym. Z punktu widzenia banku niejako równolegle występuje również inne nowe zagrożenie. Wynika z samego faktu, iż w celu zadysponowania rachunkiem nie trzeba udawać się fizycznie do placówki banku, a dodatkowo z tego, że dyspozycja zostanie wykonana w krótkim czasie. Ten fakt powoduje, że rośnie ryzyko operacyjne w jego dawnych formach związanych z naturalną reakcją klientów banku na wieść o grożącym bankructwie. Ta reakcja to tzw. *run* na bank, czyli sytuacja gdy większość klientów banku chce jednocześnie wypłacić zdeponowane pieniądze.[7] Mamy zatem do czynienia ze starym zagrożeniem w nowej odsłonie.

Na takie zagrożenie zwraca uwagę A. Schaechter [2002], mówiąc, że „*bankowość elektroniczna ma wpływ na ryzyko utraty płynności*". Dodatkowo stwierdza on, że ryzyko utraty płynności będzie postrzegane jako znacznie wyższe dla banków wirtualnych, tj. nieposiadających tradycyjnych placówek bankowych niż w przypadku tradycyjnych banków.

W oddziałach operacyjnych banków czy też w firmach zewnętrznych obsługujących obrót gotówkowy, rezerwy gotówki pokrywają zaledwie niewielki odsetek sald rachunków klientów. Jednocześnie wielkość środków płynnych na rachunku w banku centralnym dostępnych natychmiast także jest ograniczona, do wielkości wynikających z zasad gospodarki pieniężnej działów skarbowych banku. Te zaś wynikają z historii przepływów i z polityki płynności. W obliczeniach nie uwzględnia się w tym przypadku sytuacji wybuchu paniki bankowej, co w konsekwencji prowadzi do ryzyka dotyczącego utrzymania płynności banku.

---

[5] Przedstawione rozważania dotyczą zjawiska transferu środków w ramach polskiego systemu bankowego. Transfery do innego banku za granicą, z braku posiadania przez klientów kont w innych krajach poza nielicznymi wyjątkami, nie są brane pod uwagę.

[6] W rzeczywistości występuje wiele rodzajów metod weryfikacji przez bank osoby składającej dyspozycje elektroniczne. W niektórych przypadkach metody odbiegają znacznie od pierwowzoru, jakim był własnoręczny podpis osoby upoważnionej do dysponowania kontem bankowym. Metody uwierzytelniania regulowane są w umowie banku z klientem.

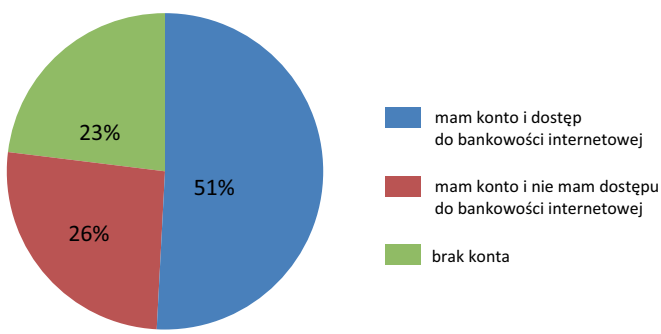
[7] Taka sytuacja nazywa się paniką bankową, w której znaczną rolę odgrywa zasada zachowania stadnego. Jeżeli z jakichś powodów niektórzy klienci zaczynają się zgłaszać do swojej placówki bankowej po wypłatę środków (np. w ramach protestu w zupełnie innej sprawie społecznej, jak miało to miejsce niedawno), to inni, obawiając się o własną gotówkę, również mogą podjąć taką decyzję. Dziś, w dobie komunikatorów społecznościowych, taka panika może wybuchnąć w ciągu godziny czy dwóch.

Dostęp do rachunku bankowego a ryzyko utraty płynności

W działalności bankowej ryzyko kredytowe jest najpoważniejszym z ryzyk, jakimi ta działalność jest obarczona. Stosunkowo od niedawna na pozycji numer dwa uplasowało się ryzyko operacyjne, w tym ryzyko związane z bezpieczeństwem środowiska IT. Wraz z rozwojem technicznym następuje bardzo dynamiczny rozwój internetowych kanałów dostępu do usług bankowych. Ten pakiet usług zwany bankowością internetową notuje w Polsce bardzo szybki wzrost, plasując tę dziedzinę na pozycji najbardziej innowacyjnej na świecie. W ramach strategii rozwoju systemu płatniczego i obrotu bezgotówkowego w Polsce Departament Systemu Płatniczego NBP prowadzi na bieżąco analizę sposobów płatności w Polsce. Dodatkowo Rada ds. Systemu Płatniczego zajęła się kwestią bezpieczeństwa środowiska teleinformatycznego w bankach, w kontekście usług bankowych, o czym informowała w sprawozdaniu ze swojej działalności.[8]

W niniejszym artykule autor zwraca uwagę na systemowe zagrożenie dla bezpieczeństwa wynikające z bezpośredniego dostępu klienta do rachunku bankowego za pośrednictwem środowiska informatycznego. Warto przy tym zwrócić uwagę, że ten aspekt zagrożenia o charakterze systemowym nie został należycie uwypuklony w dotychczasowym piśmiennictwie związanym z bezpieczeństwem w sektorze bankowym. W miarę upowszechnienia się internetowych kanałów dostępu do kont bankowych, w połączeniu z bardzo nowoczesnymi usługami oferowanymi przez sektor bankowy w Polsce, wzrasta ryzyko upadku banku z powodu braku płynności. W omawianym przypadku brak płynności następuje wskutek realizacji masowych, skupionych w krótkim przedziale czasowym, dyspozycji klienckich skutkujących transferem środków z kont bieżących do innego banku w kraju.

Ryc. 1. Dostęp dorosłych Polaków do bankowości internetowej



Źródło: T. Koźliński 2013, s. 94

W Polsce dostęp do rachunku bankowego za pośrednictwem środowiska informatycznego jest, na tle pozostałych państw Unii Europejskiej, bardzo rozpowszechniony. Badanie dzienniczkowe[9] sposobów płatności dla Polski dotyczące lat 2011–2012 wykazało, że 66% posiada-

[8] http://www.nbp.pl/home.aspx?f=/systemplatniczy/rada/rada.html

[9] Badanie dzienniczkowe przeprowadza się z użyciem dzienniczków płatności. Szczegółowe ich wypełnianie skutkuje wysoką dokładnością i precyzyjnością pozyskiwania danych, na tle dotychczas stosowanych metod.

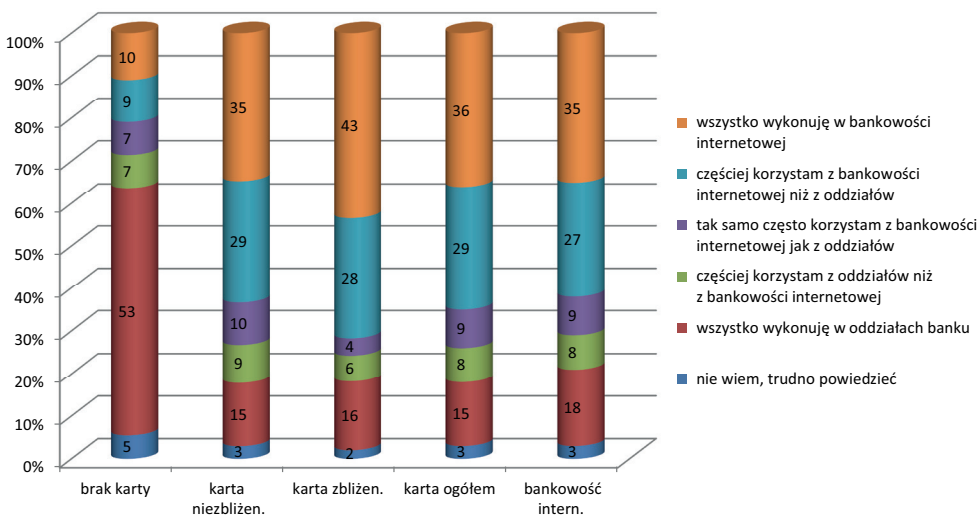
czy kont osobistych korzysta z systemów bankowości internetowej [Koźliński 2013]. Natomiast ogółem 51% dorosłych Polaków ma dostęp do bankowości internetowej, (ryc.1 i ryc. 2).

Badanie przeprowadzone przez Narodowy Bank Polski jest unikatowe, wpisuje się bowiem w nurt badań wykonywanych tylko przez kilka banków centralnych na świecie. Należą do nich banki: Austrii, Australii, Niemiec, Kanady, Holandii i Węgier.

Zagrożenie utratą płynności wskutek realizacji masowych, skupionych w krótkim przedziale czasowym dyspozycji klienckich może powstać nie tylko w wyniku transferu środków do innego banku. Klient może skorzystać z posiadanej karty płatniczej, dokonując zakupów lub wypłaty gotówki. Jednak w tych dwóch przypadkach istniejące limity wartości operacji dokonywanych przy użyciu karty znacznie ograniczają możliwość dysponowania środkami na rachunku bankowym w pełnym zakresie. Dodatkowo banki dysponują instrumentem zmiany przyznanych limitów czy wręcz zablokowaniem możliwości korzystania z karty. Jak widać, wykonywanie operacji w oddziałach bankowych zostało ostatnio zastąpione innymi możliwościami, które przyniosła nowoczesna technika.

Temat wpływu metody dostępu do kont bankowych na zagrożenie utratą płynności banku poruszono na Kongresie Gospodarki Elektronicznej[10], gdzie przedstawiciele wielu sektorów gospodarki wskazywali, jak nowe technologie i elektronizacja życia mają bezpośrednie

Ryc. 2. Częstotliwość korzystania z bankowości internetowej w porównaniu z częstotliwością korzystania z oddziałów banków



Źródło: T. Koźliński 2013, s. 100

[10] Kongres organizowany przez Związek Banków Polskich odbył się w dniu 28 czerwca 2016 r. w Warszawie.

przełożenie na codzienne funkcjonowanie instytucji z sektora finansowego i administracji publicznej. Ryzyko operacyjne (w tym IT) związane z nowymi technologiami należy oceniać również pod kątem tzw. *phishingu* (jest to metoda wyłudzania danych dostępowych do bankowości internetowej w celach przestępczych)[11]. Ostatnio odnotowano znaczący wzrost akcji *phishigowych*, co wzmacnia tezę, iż ryzyko IT jest drugim – po ryzyku kredytowym – ryzykiem, na jakie narażona jest działalność bankowa. W tym kontekście wspomniano, że w pierwszej połowie 2016 r. w Polsce odnotowano pierwszy przykład próby wywołania paniki wśród klientów banku. W mediach społecznościowych rozpowszechniano informację negatywną, o rzekomych kłopotach banku, co jakoby zagrażało wypłacalności banku. Celem akcji było wywołanie dużej liczby logowań za pośrednictwem bankowości internetowej, co zwiększało skuteczność akcji *phishigowej*. W tym kontekście ujawnia się nowe zagrożenie dla utraty płynności wynikające z dostępu elektronicznego większości klientów banku. Omówione zagrożenie systemowe wzrasta wraz ze wzrostem zakresu i powszechności nowoczesnych usług bankowych w zakresie płatności. W tym, w szczególności usług płatności natychmiastowych oferowanych w Polsce od 2013 r.[12]

Kwestia płynności banku, czy też ściślej płynności sektora bankowego, omawiana jest w większości przypadków w kontekście kryzysu na rynkach finansowych [Zajder 2013]. Zagadnienie to stało się szczególnie ważne w okresie po 2008 r., w którym doszło do bardzo głębokiego kryzysu finansowego wywołanego utrzymywaniem się przez dłuższy czas, co najmniej od 2005 r., wysokiego poziomu ryzyka systemowego [Balcerzak 2009] rozumianego jako występowanie takiej zależności między instytucjami, że wystąpienie perturbacji w jednej skutkuje perturbacjami w pozostałych. Utrata płynności finansowej w jednym banku rodzi poważne zaburzenia utrudniające utrzymanie płynności sektora bankowego w danym kraju. W przypadku zaburzenia w bieżącym funkcjonowaniu banku, wywołanego brakiem płynności, następuje wzrost niepewności uczestników rynku finansowego w sprawie możliwości regulowania nadchodzących zobowiązań tego banku w stosunku do nich. Jednocześnie spada zaufanie własnych klientów banku, co skutkuje decyzjami o wycofaniu środków pieniężnych z rachunków i depozytów. Zjawisko to określane jest zmianą od preferencji zysków do bezpieczeństwa i dotyczy zarówno osób indywidualnych, jak i przedsiębiorstw [Wiśniewski 2009].

Dostęp do kont bankowych za pośrednictwem bankowości elektronicznej nie jest związany tylko z zagrożeniem utraty płynności banku. Na inne aspekty tego zagadnienia zwracają uwagę tacy autorzy jak: A. Fredrick [2012], M. Malesky [2014] oraz M. Josefowicz

[11] *Phishing* można również zdefiniować następująco: jest to technika stosowana przez oszustów polegająca na przekonaniu ofiary, że zostaje skierowana do zaufanej strony trzeciej. Taka strona używana jest w celu uzyskania danych osobowych wykorzystywanych do popełnienia przestępstwa podszywania się (personifikacji) i oszustwa.

[12] Usługa oferowana pierwotnie przez sektor prywatny, została udostępniona przez KIR SA pod nazwą Express Elixir. Przelew natychmiastowy Express Elixir jest dostępny przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Jest wykonywany natychmiast, co w praktyce oznacza czas kilku sekund. Warto zwrócić uwagę, że bank przystępujący do oferowania tej usługi może zawęzić czas dostępu usługi, jak i określić daty niedostępności. Dodatkowo, w zależności od segmentu klienta, stosowana jest różna dostępność czasowa. Dla klientów korporacyjnych są to okresy znacznie krótsze niż dla klienta indywidualnego.

i M.M. Novarica [2011]. Szczególnie uwypukla się zagrożenie przejęcia danych lub nieuprawnionego dostępu do rachunku bankowego.

Podsumowanie

Podjęte przez KNF działania w sferze bezpieczeństwa IT są jednym z elementów aktywnego nadzoru nad sektorem bankowym w tym zakresie[13]. Problem z płynnością z powodu wystąpienia zjawiska zmiany preferencji z zysków na bezpieczeństwo nie zmaterializował się w Polsce. Jednak skala zjawiska, jakim jest rosnący odsetek klientów korzystających z bankowości internetowej, powinna spowodować dodatkową dociekliwość władz nadzorczych w zakresie ewentualnych skutków zachwiania płynnością banku, jak i wypracowaniem środków zaradczych [Gemzik-Salwach 2009].

Polski nadzór bankowy od wielu lat rozpoznaje to zagrożenie, stąd wydana w 2013 r. Rekomendacja D, nakazująca bankom m.in. uświadomienie klientom zagrożeń występujących w trakcie korzystania z bankowości internetowej. Ta rekomendacja w rzeczywistości zastępuje poprzednią, opracowaną ponad dekadę wcześniej, a wydaną w 2002 r. Postęp techniczny wpłynął na pojawienie się nowych rodzajów ryzyka operacyjnego, związanych z nowoczesnymi usługami bankowymi, co spowodowało konieczność wprowadzenia zmian dotychczasowych rozwiązań, w zakresie nowych regulacji nadzorczych, w celu ochrony przed ryzykiem związanym z procesami IT w sektorze bankowym.

Reasumując: nieprzewidywalny i gwałtowny spadek wielkości pasywów banku jest obecnie nieporównywalnie bardziej prawdopodobny niż dotychczas. Stosowanie nowoczesnej techniki w systemie bankowym wymusza nowe podejście do tego zagrożenia.

W niniejszym artykule autor przedstawił nowe spojrzenie na zagrożenie, jakie od zawsze towarzyszyło bankom, a nasilało się w okresach kryzysowych lub obniżonej stabilności systemu bankowego. Takie podejście do problemu ryzyka jest konsekwencją rozwoju nowych technologii i dynamicznego rozwoju nowych usług[14]. Wymusza konieczność monitorowania wynikających z tego zagrożeń dla danego banku, jak i dla stabilności sektora bankowego. Zagrożenia owe powinny być brane pod uwagę przez instytucje nadzorcze oraz przez władze zarządcze banku i mieć odzwierciedlenie w scenariuszu działań w obliczu sytuacji wynikłej z niekorzystnych zdarzeń rynkowych lub zdarzeń wywołanych celowo. Dotkliwe konsekwencje, jakie niesie za sobą plotka o możliwości utraty płynności – w szczególności w przypadku banków średnich i małych – oraz wywołane w ten sposób straty wizerunkowe dla sektora bankowego skłaniają do kompleksowego rozważenia omawianego nowego rodzaju ryzyka operacyjnego. Nowe technologie już przyniosły znaczne ułatwienia w dystrybucji usług bankowych – a wraz z nimi, nowe zagrożenia. Ponadto stoimy obecnie przed kolejnym wyzwaniem, wynikającym z przyszłościowej technologii *blockchain/DLT*,

[13] Przegląd literatury na temat wpływu bankowości elektronicznej na system bankowy przedstawił Bakare Sali [2015].
[14] Niniejszy artykuł skupia się na sektorze bankowym, ale z pewnością na podobne niebezpieczeństwa narażona jest pozostała część sektora finansowego. Rzecz warta rozpoznania i przeanalizowania ze względu na inną specyfikę niż poruszana w niniejszym artykule.

której możliwości mogą całkowicie zmienić model działalności sektora bankowego oraz przynieść nowe, zupełnie dziś nieznane ryzyko. Rozproszony rejestr (*blockchain/DLT)* jest w zasadzie bazą danych, która zapisuje informacje o właścicielu aktywów finansowych, fizycznych lub cyfrowych. Przykładem tych aktywów mogą być: jednostka waluty, diamenty czy zakupiony towar znajdujący się jeszcze w kontenerze, będący w trakcje spedycji. Co istotne, każdy uczestnik rejestru może przechowywać kopię łańcucha bloków, uaktualnianą automatycznie za każdym razem, gdy pojawia się nowy zapis o transakcji. Bezpieczeństwo i zgodność informacji są zapewnione dzięki kryptografii, dzięki czemu wszystkie kopie rejestru są identyczne. Prawie wszystko, co obecnie jest zapisane na papierze, może również istnieć we współdzielonym rejestrze [Government Office for Science 2016]. Technologia ta została już wykorzystana w skomplikowanych bankowych rozliczeniach dokumentowych, stosowanych w handlu międzynarodowym.

Bibliografia

Bakare S., 2015, *Varying Impacts of Electronic Banking on the Banking Industry,* "Journal of Internet Banking and Commerce", 20, 2, s. 1-9 [online].

Balcerzak A.P., 2009, *Przegląd i wstępna ocena teoretycznych stanowisk dotyczących źródeł globalnego kryzysu gospodarczego*, [w:] S. Antkiewicz, M. Pronobis (red.), *Gospodarka w warunkach kryzysu*, CeDeWu.pl, Warszawa, s. 261-264.

Fredrick A., 2012, *The impact of electronic banking transaction in the banking industry: The case of ADB, SG-SSB and Barclays Bank branches in the eastern region.*, CEMBA Thesis, Kwame Nkrumah University of Science and Technology, Ghana.

Gemzik-Salwach A., 2009, *Innowacje finansowe jako przyczyna kryzysu na rynkach międzynarodowych*, „eFinanse", 3, [online].

Government Office for Science, 2016, *Distributed ledger technology: beyond block chain*, [online], https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review [dostęp dnia: 19.07.2017].

Josefowicz M., Novarica M.M., 2011, *U.S. banking industry trends and IT impacts.*, [w:] *Bank System and Technology*, "Information week" [online].

Koterwas M., 2003, *Bazylejski Komitet ds. Nadzoru Bankowego i jego wpływ na kształt nadzoru bankowego na świecie*, „Bank i kredyt", 10, s. 56-66.

Koźliński T., 2013, *Zwyczaje płatnicze Polaków*, Narodowy Bank Polski, Departament Systemu Płatniczego, Warszawa.

Król A., 2017, *Czy blockchain zmieni świat?*, 3, „Bank", s. 80-81.

Malesky M., 2014, *Traditional banking vs. electronic banking system*., "eHow" [online].

Schaechter A., 2002, *Issues in Electronic Banking: An Overview*, IMF Policy Discussion Paper, International Monetary Fund, s. 1-27.

Unia Europejska, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en [dostęp dnia: 07.07.2017].

Unia Europejska, Revised Directive on Payment Services (PSD2), http://ec.europa.eu/finance/payments/framework/index_en.htm

Wiśniewski J., 2009, *Wpływ światowego kryzysu finansowego 2007-2008 na akcję kredytową w Polsce – wstępna ocena*, [w:] P. Karpuś, J. Węcławski (red.), *Rynek finansowy w erze zawirowań*, Wydawnictwo UMCS, Lublin.

Zajder M., 2013, *Kryzys na rynkach finansowych i jego skutki dla płynności polskiego sektora bankowego w latach 2007-2010*, „Bezpieczny Bank", 2-3, s. 26-50.

Zieliński T., 2014, *Niejednoznaczność wpływu regulacji bazylejskich na bank jako instytucje zaufania publicznego*, „Studia Ekonomiczne", 171, Uniwersytet Ekonomiczny w Katowicach, s. 31-49.

Impact of new technologies on the possible loss of liquidity of the banking sector

ABSTRACT

We now know that the financial crisis of 2007 could have been staved off, if awareness of the risks and their future consequences had been more complete. Today's technology development in the banking sector is accompanied by the old threat of a banking panic, when most clients of a bank decide to withdraw their money at the same time. As a result, liquidity risk is growing rapidly. With the development of new IT techniques, the prevalence of online access to banking services (especially to electronic banking) increases, causing a new, systemic threat. The risk of the collapse of the bank, due to the loss of liquidity caused by performing in a short period a large number of money transfers from multiple accounts in one bank to other banks, increases.

The threat described in this article is not purely theoretical. Polish payment system experienced such sort of troubles in the first half of 2016. An IT security incident consisting in a use of a phishing technique was recorded – it was an attack on the infrastructure of a bank's customer. In order to improve the effectiveness of said action, rumours about the insolvency of the bank were distributed via social media, suggesting an immediate payment of money.

This article has been written in order to indicate the subject and to encourage a deeper reflection on it.

dr Krzysztof Spirzewski, *adiunkt w Katedrze Bankowości, Finansów i Rachunkowości Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego; kontakt e-mail: kspirzewski@wne.uw.edu.pl*