Wyższa Szkoła Kultury Społecznej i Medialnej

w Toruniu

Studia podyplomowe

Kierunek: Polityka gospodarcza, finanse i bankowość

Adrianna Wiśniewska

Nr albumu: 1958 P

Rozwój pieniądza elektronicznego w Polsce

Praca dyplomowa

napisana pod kierunkiem

dr Doroty Żuchowskiej

Toruń 2020

Spis treści

Wstęp

Dawniej środkiem płatniczym były różnego rodzaju towary, potem metale szlachetne jak srebro czy złoto i w końcu papierowe banknoty i monety. Dzisiaj dostęp do gotówki uzyskujemy przy pomocy karty płatniczej czy telefonu komórkowego. Gotówka jest w ciągłym obiegu, ale obrót bezgotówkowy stał się naturalnym sposobem płatności. Nie dziwi, więc fakt próby opracowywania jak najprostszej, najszybszej, najwygodniejszej i najbezpieczniejszej formy takich płatności.

Nowe technologie to siła napędowa dla postępu i nieustannych przemian, które mają odzwierciedlenie również w bankowości. Należą do nich bankomaty, karty bankomatowe czy dostęp do finansów przez Internet. Z czasem jednak nadejdzie taki moment, kiedy w ogóle nie będziemy musieli mieć przy sobie portfela. Zmiany te są odpowiedzią na potrzeby rynku i konsumentów czyli klientów banków. Obrót bezgotówkowy to nie tylko dobrodziejstwo, ale także niebezpieczeństwo. Istotnym jest by banki zapewniały swoim klientom ochronę w tym zakresie. Klienci banków zanim podejmą decyzję o korzystaniu z elektronicznych kanałów dostępu w kontaktach z bankiem i składaniu tą drogą różnorodnych zleceń, bardzo szczegółowo analizują kwestię bezpieczeństwa. Opinie wśród różnych grup społecznych i zawodowych na temat usług elektronicznych są podzielone i w głównej mierze zależą od takich czynników jak wiek, zawód, wykształcenie, dochody, miejsce zamieszkania. Banki natomiast nieustannie poszukują nowych rozwiązań w dziedzinie bankowości elektronicznej, jak i jej bezpieczeństwa.

Celem pracy jest opisanie idei i historii pieniądza elektronicznego oraz charakterystyka bankowości elektronicznej w Polsce. W pracy wykorzystano metodę analizy opisowej.

Rozdział pierwszy definiuje pieniądz tradycyjny. Omawia zagadnienia związane z historią pieniądza oraz przedstawia jego funkcje.

Rozdział drugi opisuje e-pieniądz. Ukazuje jego funkcje oraz opisuje rolę pieniądza wirtualnego w gospodarce.

Rozdział trzeci przedstawia pojęcie bankowości elektronicznej oraz jej charakterystyki. Omówione zostały narzędzia e-bankowości oraz poruszone kwestie zagrożeń związanych z bankowością elektroniczną. Rozdział poświęcony jest również nowym technologiom w sektorze bankowym.

Do napisania pracy wykorzystano literaturę z zakresu bankowości, akty prawne, artykuły prasowe i informacje zawarte na stronach internetowych.

Rozdział I Rola pieniądza w gospodarce

1.1. Historia pieniądza

W literaturze ekonomicznej wielokrotnie podejmowano próby zdefiniowania pojęcia pieniądza. Jedna z definicji określa p*ieniądz jako serce systemu finansowego gospodarki. Jest on pierwszą formą i ostateczną podstawą roszczeń finansowych, ponieważ ma największą płynność. Oparty jest na zaufaniu*[1]. Dla ekonomistów pojęcie to jest znaczenie szersze, określa między innymi podaż pieniądza czyli *wszystko, co jest powszechnie akceptowane w formie zapłaty za dobra i usługi lub spłaty długu*[2]. Czym więc jest tak naprawdę pieniądz? Banknotami lub monetami w portfelu? Liczbą na rachunku bankowym? Czy może sumą limitów kart kredytowych czy indywidualnych linii kredytowych?

Najtrafniejszym terminem wydaje się określenie pieniądza jako środka wymiennego za otrzymane dobra. Taka forma płatności istnieje od początków ludzkości. Powstała po to aby ułatwić handel. Na przestrzeni wieków „pieniądz" zmieniał swoją formę w zależności od rozwoju danego społeczeństwa.

Według historyków „pieniądz" został wynaleziony przez Sumerów. Dzięki swojemu pismu klinowemu oraz nieskończonemu systemowi liczenia na podstawie liczby 12, stworzyli dział rachunkowy za pomocą którego można był określić wartość posiadanych dóbr. W kolejnych wiekach różne kultury wytwarzały swój własny „pieniądz" zwany płacidłem czy też pieniądzem towarowym. W Babilonii pieniądzem było ziarno, w Korei ryż, w Tybecie herbata, w Afryce czy Indiach muszle oraz perły, w Etiopii sól, a na ziemiach Słowiańskich skór wiewiórek oraz kun. Pieniądzem stawało się bogactwo danej kultury, które było produktem deficytowym innej kultury. Wyjątkowymi środkami płatności stały się także jasno sprecyzowane sztuki metalu oraz metali szlachetnych. Wyróżnić można sztuki żelaza, cyny, srebra (inaczej szekle), a także srebrne stateczki[3]. Warta uwagi jest tutaj Starożytna Grecja. Była uboga w dobre gleby, ale za to miała doskonałe położenie geograficzne. Dzięki linii brzegowej bogatej w zatoki, idealnej do wybudowania portów, Grecja była idealnym miejsce dla rozwoju handlu. Było potrzebne coś, co ten handel zoptymalizuje. Znaleziono w ten sposób

[1] T. Gruszecki, *Teoria pieniądza i polityka pieniężna,*Kraków 2004, s. 69.
[2] F. S. Mishkin, *Ekonomika pieniądza, bankowości i rynków finansowych*, Warszawa 2002, s. 85.
[3] P. Schaal, *Pieniądz i polityka pieniężna*, Warszawa 1996, s.17.

naturalne złoża srebra i złota, które posłużyły jako surowiec do wybijania monet. Nie tylko Grecja wybijała swoje monety, ale także państwa handlujące z nią. W VII wieku p.n.e. monetę metalową, inaczej zwaną kruszcową, wynaleźli Lidyjczycy. Tak rozwinięty pieniądz zaczął występować w formie wybijanych monet przez władców, a nie jak dotychczas w formie ważonej[4]. W tym czasie można też już zauważyć proceder „psucia pieniądza", zarówno handlarze, jak i władcy zmniejszali ilość metali szlachetnych w monetach czym obniżali ich wartość.

Następnym ważnym etapem w ewolucji pieniądza było wprowadzenie waluty papierowej czyli banknotów. Ich historia sięga Starożytnych Chin. W *czasach nowożytnych przejściowo wprowadzono go: w koloniach angielskich Ameryki Północnej (ok. 1690 i 1775), we Francji (ok. 1716 i 1782), w Rosji od 1796 roku. W czasie insurekcji Kościuszkowskiej w Polsce (1794), w Anglii 1797 roku. Na stałe wprowadzono walutę papierową po kryzysie światowym 1928-1933*[5]. Wydawanie banknotów było ściśle powiązane z przyjmowaniem złota kruszcowego, przez złotników, na przechowanie. W zamian za złoto otrzymywało się pokwitowanie, które upoważniało do wypłacenia powierzonego złota lub ustalonej ilości gotówki.

Oprócz banknotów istniały jeszcze weksle handlowe, rozpowszechnione w czasach renesansu, które również pełniły funkcję pieniądza. Handlarze dzięki wekslom udzielali sobie wzajemnie pożyczek. Weksle były obietnicą spłaty długu w konkretnym miejscu i czasie. Poważany kupiec mógł wekslami opłacić towar jak i spłacić kredyt[6].

Pierwszymi bankierami byli więc złotnicy. W XIX wieku, a nawet jeszcze w pierwszej połowie XX wieku, dochodziło do sytuacji w której różne banki wprowadzały do użytku swoje banknoty. Historia ukazuje upadki banków, które wydały za dużo weksli bankowych. W związku z tym oczekiwano, aby banknoty, którymi się posługują były zabezpieczone. Skutkiem tych oczekiwań było powstanie pierwszych banków centralnych już w XVIII wieku. Banki centralne były państwowym emitentem banknotów. Można w nich było nie tylko przechować swój depozyty ale także założyć konto, dzięki któremu w szybki sposób można było regulować należności poprzez przeksięgowania za pomocą czeków czy poleceń przelewów. Skutkiem takich przeksięgowań jest proces zanikania materialnego pieniądza. Zaczyna on już funkcjonować jako tylko zapisek na koncie posiadacza. Współcześnie zaczyna on już

[4] T. Gruszecki, *Teoria pieniądza i polityka pieniężna*, dz. cyt. s. 72.
[5] A. Kozak, *Znaczenie pieniądza. Norbertinum*, Lublin 2004, s. 11-12.
[6] T. Gruszecki, *Teoria pieniądza i polityka pieniężna*, Kraków 2004.

funkcjonować w większym stopniu jako zapisek na koncie posiadacza. Dzięki nowoczesnym systemom, które rejestrują przepływ pieniędzy, nie są potrzebne żadne dowody przeksięgowań.

W epoce dematerializacji pieniądza zaczęły powstać tak zwane kryptowaluty. Nie są one jednak uznawane jako oficjalne znaki pieniężne, pozostają tylko w sferze umownej jako środki wymienne. Waluty wirtualne w opinii Europejskiego Banku Centralnego, do projektu nowej dyrektywy, są określane cyfrowymi wyznacznikami wartości, nie emitowanymi przez żaden z banków centralnych ani organów publicznych. Nie musi opierać się na tradycyjnym pieniądzu fiducjarnym. Są akceptowane przez podmioty fizyczne oraz prawne jaki instrument płatniczy. Waluty wirtualne można przekazywać, przechowywać oraz sprzedawać drogą elektroniczną[7].

1.2. Funkcje pieniądza

Przez pokolenia pieniądz się zmieniał – od płacideł, poprzez kruszce szlachetne, metal, papier – aż po e-pieniądz. W obecnym czasie możemy wyróżnić dwie formy:

- Pieniądz gotówkowy – bilony oraz banknoty.
- Pieniądz bezgotówkowy – zwany również depozytowym, wkładowym czy żyrowym, a w dzisiejszych czasach funkcjonuje głównie jako e-pieniądz, czyli niematerialna forma gotówki istniejąca na podstawie zapisów na rachunkach bankowych.

Zamienniki pieniądza, czyli surogaty, nabierają również coraz większego znaczenia. Pełnią one funkcję „przechowalni" pieniądza, tak aby w łatwy sposób można było pozyskać z nich gotówkę. Mogą to być na przykład dzieła sztuki, nieruchomości, ziemie czy papiery wartościowe. Surogaty związane są wierzytelnością udokumentowaną i nieudokumentowaną, którą, w każdym momencie oraz po ustaniu terminu świadczenia, można zamienić w oba typy środków płatniczych – gotówkowych i bezgotówkowych[8].

Pomimo zmiennej formy fizycznej pieniądz w każdej gospodarce pełni cztery te same funkcje: cyrkulacyjną, obrachunkową, tezauracyjną, płatniczą. Przedstawia się to w następujący sposób:

---

[7] Europejski Bank Centralny, Opinia Europejskiego Banku centralnego z dnia 12 października 2016r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu i zmieniającą dyrektywę 2009/101/WE (CON/2016/49) (2016/c 459/05).
[8] P. Schaal, *Pieniądz i polityka pieniężna*, dz. cyt. s. 29-30.

- Wymienności – czyli jako środek płatniczy, jest to najbardziej podstawowa funkcja. Pieniądz umożliwia opłacenie wszelkich usług i towarów oraz ułatwia dokonywanie wszelakich operacji finansowych.
- Miernika wartości – jednostka do mierzenia cen za dobra oraz usługi, określona poprzez przypisanie wartości do pieniądza.
- Tezauryzacji – gromadzenie oraz przechowywanie dóbr.
- Dokonywania płatność – dzięki tej funkcji np. w Polsce nie można odmówić nikomu płatności złotówkami, co gwarantuje prawo[9].

Oprócz ekonomicznej funkcji pieniądza można również zaobsrewować jego społeczną rolę. Można wyróżnić pięć takich funkcji:

1. Behawioralna – pieniądz determinuje sposób zachowania, jest równowartością tego co człowiekowi jest niezbędne do życia. Odpowiada za sposób kształtowania się pragnień, sposobu myślenia, stylu życia czy konsumpcji. Jako wartość absolutna nie zawsze generuje w człowieku pozytywne zjawiska, może doprowadzić do chciwości, skąpstwa czy nawet przestępstwa.
2. Motywacyjna – człowiek podejmuje trud zdobycia pieniądza, może to robić uczciwie poprzez wynagradzaną pracę lub nieuczciwie na przykład poprzez korupcję lub inne przestępstwa.
3. Komunikacyjna – pieniądz informuje o stanie gospodarki danego państwa, również świadczy o tym sposób wykonania i jakość materiałów z których wykonane są banknoty i bilon.
4. Dezintegracyjna – bogacenie się oraz bankructwa powodują rozpad dotychczasowych grup społecznych oraz powstanie nowych. Ukazuje się to, jak bardzo rozwarstwione jest społeczeństwo pod kontem bogactwa, wpływów. Prowadzi to do wzrostu przestępstw na tle finansowym.
5. Integrująco-instytucjonalna – powstają i kształtują się na tym tle stosunki między ludzkie. Powstają na tej podstawie instytucje, które mają za zadanie zaspokoić ludzkie potrzeby (banki, ubezpieczenia itd.). Jednocześnie pieniądz kontroluje te instytucje[10].

[9] S. Miedziak, *Bankowość i podstawy rynku finansowego,* Lublin 2002.
[10] F. Bylok, J. Sikora, B. Sztumska, *Wybrane aspekty socjologii rynku,* Częstochowa 2001.

Rozdział II Idea i rodzaje pieniądza elektronicznego

2.1. Istota pieniądza elektornicznego

Po pieniądzu tradycyjnym w formie banknotów i monet, a następnie przepływach bezgotówkowych, pojawiły się nowe instrumenty płatnicze nazywane elektronicznymi środkami płatniczymi. Nowoczesność, szybkość oraz nieograniczony dostęp to synonimy pieniądza elektronicznego. Takie płatności zaczynają przeważać zarówno na świecie, jak i w Polsce.

Pieniądz elektroniczny dzięki rozwojowi komputerów oraz takich technologii, jak telekomunikacja i informatyka, okazał się innowacyjnym punktem w ewolucji światowych systemów płatniczych. Banki, wychodząc naprzeciw nowym potrzebom klientów, nieustannie poszukują nowych rozwiązań technologicznych. Efektem tego są kolejne bezgotówkowe formy płatności, które potrzebują usankcjonowania prawnego.

Unia Europejska zdefiniowała w drugim artykule dyrektywy 2009/110/WE w następujący sposób: pieniądz elektroniczny jest wartością pieniężną przechowywaną wirtualnie, również magnetycznie. Pozwala na żądanie od emitenta pokrycia dokonanych transakcji[11]. E-pieniądz jest także akceptowany przez podmioty fizyczne oraz prawne, które nie są emitentem pieniądza elektronicznego[12].

W polskim prawie pieniądz elektroniczny jest zdefiniowany jako ekwiwalent znaków pieniężnych, spełniający następujące warunki:

- jest przechowywany elektronicznie, w tym magnetycznie,
- jest wydawany do dyspozycji na podstawie umowy w zamian za środki pieniężne o nominalnej wartości nie mniejszej niż ta wartość,
- jest przyjmowany jako środek płatniczy przez przedsiębiorców innych niż wydający ją do dyspozycji,
- jest wyrażony w jednostkach pieniężnych[13].

Pieniądz elektroniczny może się różnić nośnikiem oraz zabezpieczeniami. Możemy rozróżnić dwie postacie e-pieniądza:

---

[11] Określonych w art. 4 pkt 5 dyrektywy 2007/64/WE.

[12] Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE.

[13] Ustawa z dnia 12 września 2002r. o elektronicznych systemach płatniczych. Dz.U. 2002r., nr 169, poz. 1385 z późn. zm.

- hardware – opierający się na technice kart procesowych
- software – opierający się na oprogramowaniach, czyli zdalnym dostępie do e-pieniądza – pieniądza sieciowego.

Pod technologią kart procesowych kryją się karty bankomatowe, debetowe, kredytowe oraz przedpłacowe inaczej zwanymi elektronicznymi portmonetkami. Mają one formę tradycyjnej karty, breloka lub naklejki na telefon. Rachunek takiej karty może zostać zasilony dowolną kwotą i dzięki niej można dokonywać wielokrotnego zakupu towarów i usług. Wyjątek tutaj stanowią karty przepłacowe, mogą one występować jako karty jednorazowe oraz jako karty wielokrotnego użytku. Jako że karty przedpłacone nie są związane z rachunkiem osobistym, transakcje takimi kartami są anonimowe.

E-pieniądz oparty na oprogramowaniu nie ma fizycznej postaci jak karty. Jest on w formie pliku, aplikacji z zdalnym dostępem, aby dokonywać transakcji pomiędzy rachunkami czy robieniu opłat za dobra i usługi poprzez Internet

W pierwotnej formie karty miały służyć do płatności bezpośrednich, a pieniądz sieciowy do płatności Internetowych. Obecnie różnice pomiędzy obiema forma są już mocno zatarte. Zarówno kartą można płacić w sieci, jak i aplikacją poprzez funkcję BLIK można zapłacić bezpośrednio.

2.2. Wirtualny pieniądz w gospodarce

E-pieniądz podlega ciągłej ewolucji, aby zaspokoić zmieniające się potrzeby konsumentów. Również postęp technologii powoduje pojawianie się nowych walut funkcjonujących tylko w wirtualnym świecie. Na początku waluty wirtualne istniały w grach internetowych. Gracze w czasie rozgrywki, trwającej nawet kilkanaście godzin, zdobywali artefakty, które następnie sprzedawali innym graczom na aukcjach. Powstały w ten sposób waluty, którymi można było operować aby zdobywać nowe przedmioty lub dokonywać zmian na koncie gracza. Waluty te jednak są ograniczone w swoich zasięgach, ponieważ dotyczą konkretnej gry, bez możliwości przeniesienia jej do innej, a także nie są samodzielnym oraz pospolitym środkiem płatniczym[14].

Najpopularniejszą wirtualną walutą jest Bitcoin stworzony w 2009 roku. Autor lub autorzy waluty ukrywa się pod pseudonimem Satoshi Nakamoto. *Bitcoin to innowacyjna waluta Internetu. Bitcoin to waluta zdecentralizowana czyli bez centralnej*

[14] M. Szymankiewicz*, Bitcoin. Wirtualna waluta internetu*, Gliwice 2014, s. 17.

instytucji emisyjnej, niezależna od banków, rządów i instytucji. To waluta nieznająca granic, dostępna wszędzie tam gdzie dostępny jest Internet (lub telefonia komórkowa)[15]. Jednostka ta jest niezależna od innych walut, anonimowa, niepowiązana z żadnymi instytucjami. Jej fundamentem jest korzystająca z niej społeczność, algorytmy kryptograficzne oraz model P2P. Na rynku pojawi się ograniczona liczba sztuk bitcoin'ó wydobytych przez użytkownikó, będzie to 21 mln bitcoinów[16].

Należy zwrócić uwagę na to, że bitcoin jest nazwą jednostki walutowej, w skrócie BTC. Natomiast Bitcoin to nazwa projektu/koncepcji w ujęciu całościowym. Aby dokonać transakcji tą walutą, potrzebny jest dostęp do komputera oraz internetu. Jako, że jest to cyfrowa waluta została stworzona w ten sposób aby być jak księga transakcyjna. Dzięki temu każda wykonana operacja jest w nim zapisywana z dokładnością do adresów odbiorcy i nadawcy, daty z godziną oraz kwotą transakcji. Wartość bitcoina określana jest w taki sam sposób jak innych walut poprzez wolny rynek oraz popyt z podażą[17].

Bitcoin jest pierwszą w historii walutą doskonałą. Zbudowany jest na prawach matematycznych, nikt go nie kontroluje oraz nie sprawuje nad nim władzy. Kryptowaluta ta nie ma właściciela lub zarządcy, którzy czerpali by z niej korzyści majątkowe. Bitcoin jako cyfrowa waluta jest kreowany oraz utrzymywany przez użytkowników dla użytkowników. Wszelkie zmiany są ustalane demokratycznie[18]. BTC jest podzielny do ósmego miejsca po przecinku, jego najmniejsza część nazywa się santoshi. BTC nie występuje pod postacią banknotów czy monet, jest dostępny dla każdego bez względu na narodowość, wiek czy wykształcenie. Konto jest anonimowe i jest w wyłącznym posiadaniu właściciela. Nie ma możliwości przejęcia takiego konta ani zablokowania go. Na adres właściciela składaj się numer i prywatny klucz, które autoryzują środki przypisywane do konta[19].

Bitcoinem na chwilę obecną można płacić za różne usługi i dobra, na przykład paliwo, bilety lotnicze czy zakupy spożywcze. Można również znaleźć informacje o zakupie auta czy domu. Waluta ta może być również traktowana jako inwestycja, należy jednak pamiętać o sporych wahaniach kursu co może spowodować utratę ulokowanego kapitału[20]. Bitcoiny można zdobyć na kilka sposobów: wymienić

[15] http://www.bitcoin.pl/o-bitcoinie/co-to-jest-bitcoin, (dostęp: 30.03.2020).
[16] M. Szymankiewicz*, Bitcoin. Wirtualna waluta internetu*, dz.cyt. s. 19.
[17] K. Kopańko, M. Kozłowski, *Bitcoin. Złoto XXI wieku*, Gliwice 2015, s. 15.
[18] http://www.bitcoin.pl/o-bitcoinie/co-to-jest-bitcoin, (dostęp: 30.03.2020).
[19] M. Szymankiewicz*, Bitcoin. Wirtualna waluta internetu*, dz.cyt. s. 23.
[20] M. Szymankiewicz*, Bitcoin. Wirtualna waluta internetu*, dz.cyt. s. 29-30.

w kantorze internetowym, podczas bezpośrednich transakcji z innymi posiadaczami lub jako nagrodę w zamian za użyczenie swojego komputera, a dokładniej jego mocy obliczeniowej, do procesu „wydobywania" bitcoinów. Wykopywanie Bitcoinów odbywa się poprzez obliczenie skomplikowanego równania matematycznego, które jest potrzebne do rozwiązania bloku. W blokach zawarte są transakcje, po rozwiązaniu następuje upublicznienie łańcucha. Łańcuchy są regularnie tworzone od wystartowania projektu[21].

Blockchain jest to nazwa sposobu przechowywania oraz przesyłania informacji związanych z transakcjami internetowymi skonstruowana jako łańcuch bloków. Ideą *blockchainów* jest zachowanie w jednym miejscu zapisu wszystkich dokonanych transakcji w wielu kopalniach. Kolejne transakcje układają się w następujące po sobie bloki danych. W każdym można znaleźć informacje o ilości dokonanych transakcji. Po zapełnieniu bloku informacjami, automatycznie tworzy się kolejny blok. W ten sposób tworzy się łańcuch, aktualizowany o nowy blok co 10 minut. W bloku można znaleźć informacje na temat takich transakcji jak: handlowe, stanach własności, udziałów, kupnach i sprzedażach walut, akcjach. *Blockchain* nie posiada centralnego serwera oraz nie ma kontroli nad transakcjami. Jest dostępny dla każdego przy jednoczesnym zabezpieczeniu dostępów przy pomocy narzędzi kryptograficznych. Użytkownik ma dostęp jedynie do swojej historii transakcji od początku do stanu obecnego.

Blockchainy są wykorzystywane podczas obsługi transakcji. Na chwilę obecną sprawdzane jest czy łańcuchy bloków mogą być wykorzystywane w bankowości w postaci ksiąg rachunkowych, a także system autoryzacyjny dokumentacji, podpisu cyfrowego czy zapis notarialny[22]. Transakcje te mogą odbyć się poza instytucjami zaufania publicznego, a jedynie pomiędzy zainteresowanymi stronami. W *blockchain* przechowywane są różne typy transakcji, które są nieodwracalne dzięki czemu nie da się ich zmieniać, podrabiać czy usuwać. Obecna technologia oraz moc obliczeniowa komputerów nie pozwala na podrobienie łańcuchów blokowych w formie księgi rachunkowej. Ocenia się, że aby złamać taki blok potrzebna by była zbliżona moc obliczeniowa połowy internetu.

Jako pierwsza potencjał „blockchain" rozpoznała branża finansowa. Powstaje nowa branża, nazwana od finansów i technologii branżą FinTech. W 2015 roku powołano konsorcjum banków i firm FinTech, którego celem jest rozwijanie blockchain.

---

[21] M. Szymankiewicz*, Bitcoin. Wirtualna waluta internetu*, dz.cyt. s. 39-40.
[22] http://businessinsider.com.pl/technologie/blockchain/blockchain-co-to-jest/vlfytn4, (dostęp: 03.05.2020).

W skład konsorcjum na wrzesień 2016 rok weszły m.in. Citi, Bank of America, Morgan Stanley, Societe Generale, Deutche Bank, HSBC, Barclays, Credit Suisse, Goldman Sachs, JP Morgan i ING. W lipcu 2016 roku Citi ogłosił, że wypracował własną krypto-walutę, którą nazwał Citicoin. FinTechowy start-up Chain.com, otrzymał w październiku 30 mln USD dofinansowania (od Nasdaq, Visa, CapitalOne, Orange i Citigroup) w celu zbudowania rozwiązania, które pozwoli na przesyłanie różnych wartościowych aktywów w sieci (punktów lojalnościowych, akcji, bonów i różnych instrumentów finansowych)[23]. Kolejną branżą dostrzegającą potencjał w łańcuchach bloków jest energetyka. *Blockchain* bardzo dobrze sprawdza się w rozliczaniu kupna-sprzedaży pomiędzy małym producentem a odbiorcami to jest gospodarstwami domowymi.

Blockchain stanowi zarówno szanse, jak i zagrożenie. Plusami tej technologii są: zmniejszenie kosztów, szybsze, bezpieczniejsze oraz bardziej przejrzyste transakcje. Największym minusem jest eliminacja pośredników jakimi są na przykład banki. W momencie ich wyeliminowania wiele osób zostanie bez pracy przez likwidację stanowisk.

[23] http://norbertbiedrzycki.pl/blockchain-trzeba-o-nim-wiedziec/, (dostęp: 03.05.2020).

Rozdział III Pieniądz elektroniczny w sektorze bankowym w Polsce

3.1. Charakterystyka bankowość elektronicznej w Polsce

Porównując bankowość sprzed kilkunastu lat ze stanem obecnym, od razu można zauważyć, jak bardzo kanały zdalne bankowości ewoluowały dając klientom kolejne możliwości poprzez coraz nowsze narzędzia do zarządzania swoimi finansami. Zauważalny jest ogromny postęp w e-bankingu. Banki, aby zdobyć większą ilość nowych klientów, zaczęły celować w młode pokolenie poprzez przenoszenie swoich produktów oraz usług do świata Internetu. Dzięki temu dzisiejszy e-bank jest zaawansowanym systemem umożliwiającym korzystanie ze swoich usług w dowolnym miejscu i czasie.

Bankowość elektroniczna czyli e-bankowość to zdalna możliwość obsługi klienta bankowego oraz zaopatrzenie go w usługi bankowe bez konieczności spotkania w placówce bankowej, dzięki technologii informacyjno-komunikacyjnej[24]. Natomiast według ustawy o świadczeniach usług kanałem elektronicznym bankowość elektroniczna określana jest jako *wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej*[25]. W najprostszym ujęciu bankowość elektroniczna daje klientowi możliwość skorzystania z usług bankowych bez konieczności odwiedzenia placówki bankowej lub partnerskiej. Za pomocą zdalnych kanałów, zarówno elektronicznych, jak i mobilnych, klient ma możliwość zlecenia przelewu, wypłaty z bankomatu, założenia konta czy wzięcia pożyczki gotówkowej.

Postępy gospodarcze, społeczne a także rozwój technologii spowodowały powstanie nowych rodzajów operacji bankowych. Klienci uzyskali dostęp do swoich kont bankowych przy pomocy urządzeń elektronicznych to jest komputerów, bankomatów, telefonów, terminali czy linii telekomunikacyjnych[26]. Elektroniczne instrumenty płatnicze dają możliwość z korzystania z tych urządzeń, znaczy to że *każdy instrument*

---

[24] A. Gospodarowicz, *Bankowość elektroniczna*, Warszawa 2005, s. 26.
[25] Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002r., nr 144, poz. 1204, art.2 pkt. 4.
[26] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych. Charakterystyka i zagrożenia,* Warszawa 2010, s. 5.

płatniczy, w tym z dostępem do środków pieniężnych na odległość, umożliwiający posiadaczowi dokonanie operacji przy użyciu informatycznych nośników danych lub elektroniczną identyfikację posiadacza niezbędną do dokonania operacji, w szczególności kartę płatniczą lub instrument pieniądza elektronicznego[27].

Przełom w polskiej bankowości elektronicznej nastąpił w drugiej połowie lat osiemdziesiątych. Bank Polska Kasa Opieki SA (dzisiejszy Bank Pekao) udostępnił dla swoich klientów pierwszy bankomat na ulicy Tadeusza Czackiego w Warszawie[28]. Karta płatnicza oznaczała ogromne ułatwienia dla klientów banku, ponieważ nie musieli oczekiwać w długich kolejkach w placówkach bankowych, aby podjąć środki dostępne na swoim koncie. Na przełomie lat 2000/2001 doszło do kolejnych zmian. Internet stacjonarny stał się powszechniejszy i dostępny w wielu polskich domach. Sektor bankowy od razu wykorzystał nowe możliwości tworząc pierwsze wirtualne banki mBank, Volkswagen Bank Direct i Inteligo Financial Services (PKO BP)[29]. Pierwsze konto z dostępem przez Internet zostało udostępnione przez Powszechny Bank Gospodarczy w Łodzi 18 października 1998 roku, który następnie został przejęty przez Bank Pekao. Szybko znaleźli się naśladowcy i w 2000 roku powstał bank wyłącznie internetowy – mBank, który do dziś jest w czołówce polskich banków pod względem aktywów[30].

Istotnym momentem dla polskiej bankowości internetowej było wykupienie Inteligo przez spółkę PKO BP. Zakup ten całkowicie zmienił realia rynku, a także wyznaczył kierunek rozwoju bankowości internetowej jako godny naśladowania lider w tej dziedzinie. W 2007 roku oraz 2010 roku Inteligo zostało wyróżnione mianem najlepszego konta internetowego w Polsce[31].

Nowe technologie informatyczne oraz telekomunikacyjne zdobywają dla bankowości elektronicznej coraz większy prestiż oraz uznanie klientów, chętnie korzystających z rozwiązań tych technologii jak bankomat, karta płatnicza czy Internet. Cechy odróżniające bankowość elektroniczną od tradycyjnej to:

---

[27] Ustawa z dnia 12 września 2002r. o elektronicznych systemach płatniczych. Dz.U. 2002r., nr 169, poz. 1385 z późn. zm.
[28] https://www.forbes.pl/technologie/historia-bankomatu/4yy2hn3#, (dostęp: 22.05.2020).
[29] https://www.forbes.pl/finanse/bankowosc-xxi-wieku-czym-jeszcze-moze-nas-zaskoczyc/0ceq7dj, (dostęp: 22.05.2020).
[30] https://www.bankier.pl/wiadomosc/Historia-bankowosci-internetowej-w-Polsce-7284848.html, (dostęp: 22.05.2020).
[31] https://prnews.pl/inteligo-najbardziej-przyjazna-bankowosc-mobilna-29564, (dostęp: 22.05.2020).

- Nieograniczony przez czas i miejsce dostęp do usług bankowych;
- Możliwość załatwienia spraw bez udziału pracownika banku;
- Zmniejszenie ilości dokumentów za usługi bankowe;
- Tańsza lub bezpłatna obsługa konta i usług z nim związanych;
- Obsługa większej ilości klientów;
- Większe bezpieczeństwo i poufność, pod warunkiem przestrzegania zasad bezpieczeństwa.

Bankowość elektroniczną możemy klasyfikować za pomocą różnych kryteriów, które zależą od:

- rodzaju klientów - detaliczna bankowość elektroniczną i korporacyjna bankowość elektroniczną,
- kanału komunikacji – internetowa, telefoniczna, przenośna, terminalowa, telewizyjna,
- trybu dostępu – online i offline,
- poziomu dostępu – poziom aktywny i poziom pasywny,
- typu modelu – model wielokanałowy, bank wirtualny, bank supermarketu finansowego, internetowy bank niszowy[32].

Możliwy jest również podział bankowości elektronicznej ze względu na sposób korzystania, w ten sposób wyróżniamy bankowość:

- terminalową,
- internetową,
- telefoniczną[33].

Dzięki bankowości terminalowej umożliwione zostały transakcje gotówkowe oraz bezgotówkowe, za pomocą kart płatniczych oraz urządzeń mobilnych w bankomatach i terminalach POS[34]. W bankomacie dzięki transakcji bezgotówkowej mamy możliwość sprawdzenia salda konta czy zmianę numeru PIN, natomiast transakcje gotówkowe to wypłaty oraz w niektórych dostosowanych bankomatach lub osobnych wpłatomatach wpłaty gotówkowe. Terminal POS daje możliwość bezgotówkowej

[32] M. Solarz, *Rozwój bankowości elektronicznej w Polsce*, Warszawa 2006, s. 46-48.
[33] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 6.
[34] POS to skrót z angielskiego point of sale.

zapłaty za towary i usługi lub dzięki usłudze *Cashback* wypłaty środków pieniężnych z konta. Najpopularniejsze w tym rodzaju bankowości są karty płatnicze inaczej nazywane plastikowym pieniądzem. Karta upoważnia do autoryzacji płatności lub wypłat z uwzględnieniem indywidulanych linii kredytowych (karta debetowa) oraz limitów kredytowych (karta kredytowa).

Biorąc pod uwagę sposób rozliczania, możemy karty podzielić na:

- debetowe – imienne, wydawane dla posiadacza rachunku oraz ewentualnie dla wyznaczonego pełnomocnika. Dzięki niej posiadacz ma stały dostęp do środków zgromadzonych na koncie oraz ewentualnej linii kredytowej, tak zwanego debetu spłacanego automatyczne podczas wpływów środków pieniężnych na konto. Możliwe jest ustalenie limitów dziennych i pojedynczych transakcji.
- Kredytowe – imienne, wydawane do odnawialnej linii kredytowej posiadaczowi jaki i ewentualnym pełnomocnikom. Do jej posiadania nie jest niezbędne konto bankowe. Spłaty można dokonywać całościowo lub w ratach – wysokość raty wyznaczana jest przez posiadacza, nie może być jednak niższa niż spłata minimalna, zazwyczaj 5% zadłużenia karty.
- Chargé – czyli obciążeniowe. Są powiązane z konkretnym rachunkiem bankowym, rozliczane raz w miesiącu. W zależności od wpływów na powiązane konto, bank udziela limitu do wykorzystania na taką kartę poza wolnymi środkami na koncie. Posiadacz takiej karty zobowiązany jest do posiadania środków na koncie dopiero podczas comiesięcznego rozliczenia.
- Przedpłacone – nie są imiennymi kartami, są powiązane z technicznym numerem bankowym który najpierw należy zasilić. Najczęstszą ich formą są karty prezentowe.

Dalej te karty możemy podzielić ze względu na fakturę, czyli karty wypukłe i płaskie. Na kartach płaskich dane są nadrukowywane. Tymi kartami można posługiwać się tylko za pomocą terminali elektronicznych. Na kartach wypukłych dane są wytłaczane i można się nimi posługiwać zarówno w terminalach elektronicznych, jak i podczas zakupów poprzez Internet.

Karty można sklasyfikować biorąc pod uwagę jej budowę oraz odczytywanie przez terminal, wyróżniamy[35]:

[35] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 17.

- pasek magnetyczny – są na nim zapisane dane do identyfikacji dzięki czemu można dokonać transakcji,
- układ elektroniczny – chipy lub mikroprocesory dane są zapisane na scalonym układzie posiadającym pamięć oraz mikroprocesor,
- system zbliżeniowy – inaczej bezstykowy, zawarty w nich układ elektroniczny pozwala na bezstykową finalizację transakcji, usługę tę oferuje Visa oraz MasterCard.

Z bankowości internetowej można korzystać w dwojaki sposób, za pomocą standardowego lub dedykowanego[36] programu przez sieć internetową. Serwisy internetowe podzielone są na dwie części: transakcyjną oraz informacyjną. Część informacyjna jest dostępna dla każdego użytkownika Internetu, bez konieczności posiadania jakichkolwiek produktów w danym banku. Część transakcyjna jest dostępna dla klientów banku, zarówno dla sektora detalicznego jak i małych i średnich przedsiębiorstw. W celu korzystania z bankowości elektronicznej klient musi założyć konto w danym banku, a następnie podpisać umowę o świadczenie tej usługi. Otrzymuje wtedy unikalny identyfikator/login oraz hasło jednorazowe, którego system przy pierwszym logowaniu wymusza zmianę. Po zalogowaniu się do swojego konta klient może między innymi sprawdzić stan swoich środków, blokady na rachunku, historię transakcji, utworzenie i zerwanie lokaty, otworzenie kolejnego rachunku również walutowego, zlecić przelew, doładować konto telefonu, zarządzać funduszami inwestycyjnymi, zlecić lub odwołać zlecenie stałe, zmienić PIN kart, zablokować i zamówić nową kartę, zmienić limity jednorazowe i dzienne, wziąć pożyczkę, kartę kredytową lub otworzyć indywidualną linię kredytową.

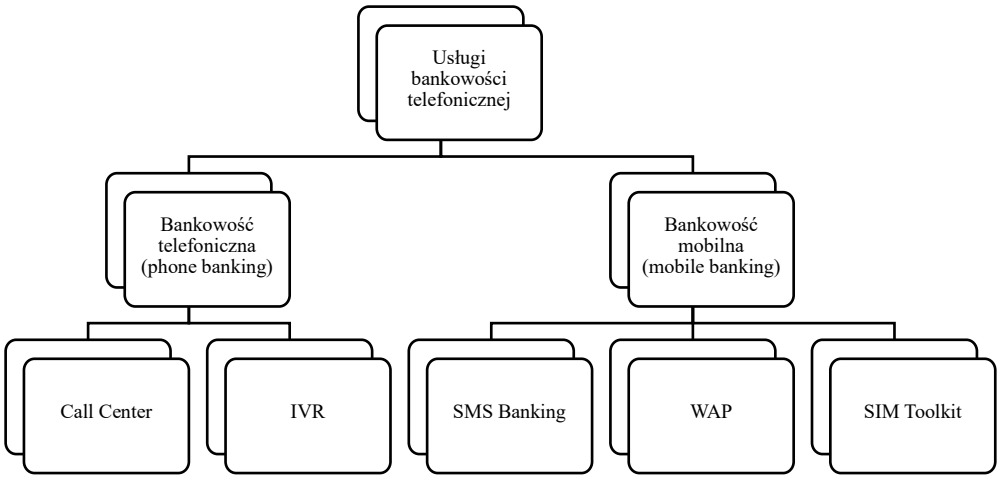
Bankowość telefoniczna pozawala klientowi na kontakt z bankiem przez telefon. Można wyróżnić dwa typy tej usługi. *Phone banking* polegający na kontakcie poprzez telefon stacjonarny, jest to najstarsza z form kontaktu zdalnego, oraz *mobile banking* opierający się na telefonach komórkowych oraz urządzeniach mobilnych (smartfon, tablet). Można wyróżnić pięć form dostępu do konta przez bankowość telefoniczną:

- rozmowę z pracownikiem call canter,
- polecenia w systemie IVR,
- SMS Banking,

[36] Home banking oraz corporate banking.

- protokół WAP,
- SIM Toolkit[37].

Rysunek 1. Klasyfikacja usług bankowości telefonicznej



Źródło: Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych. Charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa 2010, s. 38.

Zadaniem *phone bankingu* jest realizacja operacji na rachunku za pomocą teleserwisu, których można dokonać na dwa sposoby: call cenetr oraz IVR. Połącznie z call cenetr umożliwia klientowi realizację operacji z pomocą pracownika banku. Podczas takiego połączenia klient może sprawdzić stan konta, zlecić przelew lub zlecenie stałe, założyć lokatę, zapoznać się z ofertą banku czy zastrzec kartę. Serwis IVR jest połączeniem z „automatem". Za pomocą komend głosowych oraz tonowych wyborów klient ma dostęp do tych samych funkcji co podczas połączenia z call center dodatkowo może również połączyć się z konsulatem. Znaczącą różnica w tych serwisach jest to, że przy IVR klient nie może dokonać transakcji nietypowych lub wcześniej zdefiniowanych w automatycznym serwisie[38].

W *mobile banking* wykorzystywane są urządzenia przenośne z dostępem do Internetu. Największą zaletą jest to, że usługa ta dostępna jest w każdym miejscu i czasie. Najpopularniejsze formy bankowości mobilnej to: SMS Banking, WAP oraz SIM Toolkit.

[37] A. Gospodarowicz, *Bankowość elektroniczna,* dz.cyt. s. 106.
[38] K. Korzeń*, Bankowość elektroniczna jako kanał dystrybucji usług bakowych,* Warszawa 2006.

SMS Banking działa na podstawie krótkich wiadomości SMS, dzięki którym przekazywane są informacje na linii klient-bank. Można wyróżnić dwie formy takiej komunikacji:

- automatyczne powiadamianie (PUSH), klient otrzymuje informację o dokonanej operacji na rachunku, np. wpływ na konto lub zdebetowanie rachunku,
- zapytania do baz danych (PULL), klient wysyła wiadomość SMS, a następnie otrzymuje informację o stanie rachunku lub przypomnienie o nadchodzącej płatności[39].

Technologia WAP to dostosowanie witryn internetowych do możliwości oferowanych przez urządzenia przenośne. Dzięki dostępowi do Internetu w urządzeniach tych można otwierać uproszczone serwisy internetowe. Usługa ta jest tożsama z tym w jaki sposób obsługiwany jest rachunek przez serwis internetowy w komputerze.

Trzecią formą jest SIM Toolkit. Jest to najnowsza forma polegająca na dostępie do rachunku za pomocą dedykowanej aplikacji. Niezbędnym warunkiem korzystania z takiej aplikacji jest odpowiedni system Android, iOS lub Windows Phone, dla którego bank wydaje odpowiednią aplikację. Obsługa rachunku jest w zasadzie identyczna jak z poziomu WAP.

W 2013 roku sześć banków: Alior Bank, Bank Millenium, Bank Zachodni WBK, ING Bank Śląski, mBank oraz PKO BP, podjęło decyzję o współpracy, aby stworzyć nowe możliwości płatności mobilnych. Postanowiono aby poszerzyć możliwości, działającej od marca 2013 roku, systemu płatność mobilnych należącego do PKO BP. System miał zostać rozbudowany w taki sposób aby mogli do niego dołączyć nowi partnerzy. W ostatnim kwartale 2013 roku do programu dołączyła również Krajowa Izba Rozliczeniowa. Objęła ona pieczę nad systemem operacyjnym płatności mobilnych oraz technologią teleinformatyczną, dzięki której można było zrealizować projekt. 9 lutego 2015 roku ogłoszono nowy system płatności mobilnych – BLIK. 13 maja 2016 roku do projektu przystąpił Gettin Noble Bank[40].

Dzięki usłudze BLIK klienci banku mogą płacić za usługi, wypłacać pieniądze z bankomatów oraz płacić w Internecie. Płatność BLIK odbywa się za pomocą jednorazowego sześciocyfrowego kodu, ważnego przez tylko 2 minuty, podczas których należy wygenerować kod, wpisać go, a następnie zatwierdzić operację w terminalu oraz

[39] K. Korzeń*, Bankowość elektroniczna jako kanał dystrybucji usług bakowych,* Warszawa 2006, s. 33.
[40] http://www.polskistandardplatnosci.pl/o-nas, (dostęp: 25.05.2020).

na smartfonie. Metoda ta dała Polsce przepustkę do światowej czołówki nowinek oraz standardów technologicznych.

3.2. Bezpieczeństwo w bankowości elektronicznej

W związku z tym że bankowość elektroniczna polega przed wszystkim na zdalnym przetwarzaniu danych za pomocą komputerów, telefonów, itd., zachodzi podwyższone ryzyko przestępstw związanych z kradzieżą danych oraz wyłudzeń finansowych. Z tego powodu podstawową kwestią w rozwoju tej technologii jest bezpieczeństwo.

Dla bezpieczeństwa w sieci informatycznej niezbędne są charakterystyczne cechy do których można zaliczyć:

- poufność **–** gwarantuje ona, że do systemu operacyjnego mają dostęp tylko osoby uprawione;
- integralność – zapewnia, że dane przesyłane w systemie podczas transakcji nie są przez nic, ani nikogo modyfikowane;
- autentyczność – świadczy o tym, że osoba dokonująca transakcji jest osobą do tego uprawioną;
- niezaprzeczalność - uniemożliwia zaprzeczeniu faktu otrzymania lub nadania dyspozycji drogą elektroniczną;
- dostępność – pozwala na dostęp, bez względu na czas i miejsce, do systemu bankowości elektronicznej;
- niezawodność – gwarantuje pracę systemu w oczekiwany sposób[41].

System można nazwać bezpiecznym w momencie gdy wymienione cechy są na poziomie do zaakceptowania dla banku oraz jego klientów. Bezpieczeństwo staje się złożonym zagadnieniem, należy zapewnić ochronę klientowi, transferowi danych oraz bankowi i serwerowi, który przechowuje wszelki informacje związane z działaniami na rachunkach. Wszyscy uczestnicy zobowiązani są do przestrzegania zasad bezpieczeństwa transakcji aby wyeliminować jakiekolwiek zagrożenie. W poniższej tabeli przedstawione zostaną środki ochronne, które powinno się stosować[42].

[41] A. Gospodarowicz, *Bankowość elektroniczna,* dz.cyt. s. 55-56.
[42] A. Gospodarowicz, *Bankowość elektroniczna,* dz.cyt. s. 56.

Tabela 1. Środki ochrony bezpieczeństwa bankowości elektronicznej

Środki ochrony	Przykłady
Prawne	– Ustawa o elektronicznych instrumentach płatniczych – Ustawa o świadczeniu usług drogą elektroniczną – Ustawa o podpisie elektronicznym – Prawo bankowe – Kodeks Karny
Fizyczne	– urządzenia przeciwwłamaniowe – sejfy – alarmy – urządzenia ochrony przeciwpożarowej – pomieszczenia odpowiednio przystosowane do pracy komputerów – rozwiązania architektoniczne (np. lokalizacja centrum obliczeniowego w budynku banku
Techniczne	– urządzenia podtrzymujące zasilanie – karty magnetyczne i mikroprocesorowe – urządzenia do identyfikacji osób na podstawie linii papilarnych, głosu, siatkówki oka itp. (tzw. urządzenia biometryczne) – urządzenia do tworzenia kopii zapasowych wraz z metodami ich stosowania, – serwery Proxy – sprzętowe blokady dostępu do klawiatur, napędów dysku itp. – urządzenia i rozwiązania chroniące przed emisją ujawniającą – optymalizacja konfiguracji sprzętowej komputerów – dublowanie okablowania – dublowanie centrów obliczeniowych i baz danych
Programowe	– dzienniki systemowe (logi) - obowiązkowe w każdym systemie rozwiązania rejestrujące dane pozwalające na późniejszą identyfikację działalności użytkowników – programy śledzące- mechanizmy umożliwiające monitoring pracy użytkowników systemów w czasie rzeczywistym – mechanizmy rozliczania - rozwiązania pozwalające na identyfikację wykonawców określonych operacji w systemie – programy antywirusowe – zapory ogniowe (*firewall)* – programy wykrywające słabe hasła istniejące w systemie – mechanizmy zabezpieczenia statystycznych baz danych – wirtualne sieci prywatne (VPN)
Organizacyjne	– polityka bezpieczeństwa – analiza ryzyka – szkolenia użytkowników – monitoring systemu i wykrywanie anomalii
Kontroli dostępu	– hasła, numery identyfikacyjne (określają co użytkownik zna) – karty magnetyczne, tokeny, podpis elektroniczny, i in. (określają co użytkownik posiada) – metody biometryczne (określają kim użytkownik jest)
Kryptograficzne	– algorytmy – podpis elektroniczny – protokoły (SSL, SET)

Źródło: Opracowanie własne na podstawie: A. Gospodarowicz*, Bankowość elektroniczna,* Polskie Wydawnictwo Ekonomiczne S.A., Warszawa 2005, s. 65-95.

Szczególną uwagą należy zwrócić na kryptografię oraz kontrolę dostępu. Aby lepiej zobrazować te zagadnienia można posłużyć się przykładami kart płatniczych oraz bankowości internetowej i mobilnej.

Karty płatnicze od momentu wprowadzenia wciąż zyskują na popularności. Różnią się od siebie sposobem zabezpieczeń. W poniższej tabeli zostanie przedstawiony podział na ilość kart z danym typem zabezpieczeń na przestrzeni lat 2015-2017.

Tabela 2. Liczba wyemitowanych kart płatniczych wg technologii zapisu.

Liczba kart płatniczych (szt.)	2015 Q4	2016 Q4	2017 Q1
Karty wg technologii zapisu danych:	35 209 043	36 874 489	37 736 849
Karty wyposażone w pasek magnetyczny i mikroprocesor	33 395 976	34 519 493	35 331 147
Karty wyposażone tylko w pasek magnetyczny	1 345 338	1 686 457	1 683 779
Karty wyposażone tylko w mikroprocesor EMV	169 350	316 816	356 418
Karty wyposażone w mikroprocesor inny niż EMV	24 519	23 803	23 655
Karty wirtualne	273 860	327 920	341 850

Źródło: Narodowy Bank Polski, Liczba wyemitowanych kart płatniczych na przestrzeni kolejnych kwartałów od 1998r.

W Polsce wykorzystywane są przed wszystkim karty zabezpieczone paskiem magnetycznym oraz mikroprocesorem. Jak widać w powyższej tabeli, karty te stanowią prawie 94% wszystkich kart. Jak można również zauważyć, systematycznie wzrasta liczba kart, które nie posiadają paska magnetycznego, a są zabezpieczane tylko przez mikroprocesor EMV.

Ilość emitowanych kart z każdym rokiem się zwiększa, w związku z czym użytkownicy kart są zagrożeni przez działalność przestępczą z użyciem tych kart. Przestępczość w tym zakresie ma charakter międzynarodowy i zorganizowany. Banki cały czas odnotowują wzrost strat, co świadczy o dynamicznym rozwoju tego typu działań o charakterze przestępczym. Coraz częstszym zjawiskiem są nadużycia związane z posiadaniem numeru karty i wykorzystaniem go przez serwisy internetowe telefoniczne czy e-mailowe, a nie jak dotychczas z fizycznym użyciem karty. Najczęstszymi formami

takich nadużyć jest skimming, skopiowanie danych z karty wypukłej oraz zgubienie karty bezstykowej[43].

Karta może zostać skopiowana, jest to tak zwany skimming, w każdym miejscu w którym zostanie użyta: sklepy, restauracje, punkty usługowe. Jako, że w takich miejscach karta jest tylko krótki moment w posiadaniu ewentualnego przestępcy, który nie zawsze ma możliwość podejrzenia kodu PIN, kopiuje się w takim wypadku karty niewymagające potwierdzenia tym kodem. Do skopiowania danych z karty niezbędne jest urządzenie zamontowane w terminalu, które sczytuje dane z paska magnetycznego, zapisuje w pamięci. Następnie po podłączeniu do komputera można odczytać dane skopiowanych pasków magnetycznych.

Dużo groźniejszy jest natomiast skimming bankomatowy. W ten sposób pozyskuje się nie tylko dane z paska magnetycznego ale również kod PIN. Przestępca instaluje dwie specjalne nakładki – jedna w miejscu wkładania karty, druga imitująca oświetlenie a tak naprawdę zawierająca kamerę w górnej części bankomatu. W ten sposób przestępca uzyskuje niezbędne dane, aby podszyć się pod użytkownika karty[44]. Urządzenia takie są w zasadzie nierozpoznawalne dla przeciętnego klienta.

Bezpieczniejszym rozwiązaniem są karty zabezpieczone mikroprocesorem. Charakterystyczne jest dla nich bezpieczeństwo w kwestii kontroli dostępu, kodowanie i odkodowanie informacji oraz tworzenie i weryfikacja cyfrowych podpisów. Wdrożone obecnie systemy pozwalają na zabezpieczenie przed kopiowaniem technologii mikroprocesorowej. W takiej sytuacji i technologia przestępcza poszła na przód, obecnie skimming jest możliwy na kartach z mikroprocesorem, ale pod warunkiem, że posiada pasek magnetyczny, który umożliwia autoryzację transakcji na przykład w bankomacie nie obsługującym standardów EMV. Powodem dla, którego nadal emituje się karty z paskiem magnetycznym jest to, że nie każdy terminal POS oraz bankomat obsługują karty z mikroprocesorem.

Kolejnym zagrożeniem jest przejęcie danych z karty wypukłej, którą można płacić za dobra i usługi w Internecie. Aby dokonać takiej transakcji, należy podać numer karty, datę jej ważności oraz kod CVV2/CVC2. Podawanie takich danych w Internecie obciąża takie transakcje wysokim ryzkiem przestępstwa, ponieważ nie wymaga się podczas nich potwierdzenia kodem PIN. Aby podnieść bezpieczeństwo takich operacji,

---

[43] J. Wójcik, *Przeciwdziałanie przestępczości zorganizowanej,* Warszawa 2011, s. 52.
[44] http://www.zyjbezpiecznie.policja.pl/zb/finanse-i-dokumenty/47375,Skimming-i-phishing.html, (dostęp: 25.05.2020).

wydawca w celu autoryzacji może wysyłać do klienta na telefon kodu autoryzacyjnego. Dlatego ważne jest, aby karty nie fotografować oraz nie przekazywać jej danych osobom postronnym lub na podejrzanych stronach internetowych[45].

Rosnąca popularność bankowości elektronicznej spowodowała że jest ona obecnie podstawową funkcją w ofercie bankowej dla klientów. Wraz z rozwojem technologicznym i wzrostem popularności takiej metody pojawiły się nowe formy przestępstw związanych ze zdalnym dostępem do rachunków oraz kradzieży danych osobowych. Wpływ na przestępczość w zdalnych dostępach do usług bankowych mają sami klienci. Często nie zdają sobie oni sprawy z zagrożeń jakie na nich czekają, nie zachowują środków bezpieczeństwa poprzez ujawnianie loginów i haseł. Nie wiedzą również w jaki sposób chronić się przed cyber przestępstwami[46].

Posiadacze elektronicznego dostępu do rachunku bankowego muszą także dbać o bezpieczeństwo swoich dokumentów. W chwili przejęcia ich przez przestępcę ma on możliwość podszyć się pod klienta banku dokonać różnych zmian przy koncie, między innymi nadać nowe pełnomocnictwa, zmienić loginy, numery telefonów, a także metody autoryzacji. Zyskuje w takim momencie pełen dostęp do środków zgromadzonych na koncie. Przez takie próby wyłudzeń banki dały możliwość swoim klientom zastrzeżenia dokumentów telefonicznie na infolinii oraz w placówkach bankowych.

W bankowości elektronicznej dostępne są różne metody autoryzacyjne. Oprócz indywidualnego identyfikatora można użyć hasła stałego lub jednorazowego, certyfikatu cyfrowego połączonego z hasłem lub nadanym numerem PIN. Hasło jednorazowe klient może otrzymać jako listę takich haseł, kartę TAN[47], token sprzętowy lub jako aplikacja na smartfon lub jako wiadomość SMS[48].

Polskie banki zapewniają bezpieczeństwo w sieci swoim klientów poprzez protokół SSL, czyli bezpieczne połączenie. W celu weryfikacji, czy otwarta strona internetowa jest zabezpieczona tym protokołem, należy sprawdzić czy przed adresem strony znajduje się ikona zamkniętej kłódki oraz czy adres strony rozpoczyna się od *https://www....* . Protokół SSL jest certyfikatem autentyczności nadawanym bankom

---

[45] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 21.
[46] Komisja Nadzoru Finansowego, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną. Poradnik klienta usług finansowych,* Warszawa 2014, s. 5.
[47] Transaction Authorisation Number.
[48] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 30-31.

przez instytucje certyfikujące. Certyfikaty pozwalają na utożsamienie instytucji, która go otrzymała. Klikając na ikonę kłódki, która powinna być zamknięta, umożliwia sprawdzenie autentyczności banku z którym klient chce nawiązać łączność. Standardowy klucz kryptograficzny o długości 128 bitów zapobiega odszyfrowaniu chronionej transmisji danych. Dobrze zakodowana transmisja uniemożliwia włamanie na e-konto, oraz kradzież środków na nim zgromadzonych[49].

W większości przypadków system logowania się do bankowości elektronicznej jest dwuetapowy. W pierwszej kolejności klient podaje swój identyfikator, a następnie hasła statycznego – w całości lub losowo wybranych kolejnych znaków hasła. Rzadszą formą są tokeny sprzętowe lub powiadomienia na telefonie komórkowym autoryzacje jako silne uwierzytelnienie. Hasło statyczne powinno być „silne" kryptograficznie, osiąga się to za pomocą odpowiedniej ilości znaków, kombinacji małych i wielkich liter, cyfr oraz znaków specjalnych. Dodatkowo banki zabezpieczają swoich klientów poprzez blokowanie dostępu do konta po ustalonej ilości błędnych logowań, na przykład trzech.

Aby zakończyć operację na elektronicznym koncie bankowym, klient musi zautoryzować ją unikalnym kodem w zależności od wybranego typu autoryzacji. Może tego dokonać dzięki aplikacji na telefon, tokena sprzętowego, otrzymanego kodu za pomocą SMS lub karty kodów tak zwanej zdrapki. Zabezpieczenie haseł oraz przedmiotów generujących jednorazowe kody autoryzacyjne jest fundamentem bezpieczeństwa operacji internetowych na rachunku oraz obowiązkiem klienta banku. Częstym błędem użytkowników jest zapisywanie loginów wraz z hasłami w niezabezpieczonych miejscach, co daje możliwość wykorzystania tego przez przestępców. Klient w chwili odkrycia, że jego dane do logowania zostały odtajnione lub gdy utraci narzędzie do autoryzacji, powinien natychmiast skonstatować się ze swoim bankiem w celu zablokowania dostępu oraz zmiany danych do logowania i autoryzacji.

Kolejnym typem cyberprzestępstwa jest *phishing.* Metoda ta polega na próbie wyłudzenia danych prywatnych oraz uwierzytelniających. Przestępcy próbują je uzyskać podszywając się pod firmy czy instytucje, a nawet banki. Tworzą strony internetowe wyglądając niemal identycznie jak stron na przykład banku, wysyłają maile lub SMS które również mają przypominać te od prawdziwego dostawcy usługi. Najczęstszą formą są właśnie wiadomości e-mailowe, które mają wyglądać jak prawdziwa korespondencja

[49] Komisja Nadzoru Finansowego, Usługi Bankowości Elektronicznej dla Klientów Detalicznych, dz.cyt. s. 30.

z bankiem[50]. W takiej wiadomości zazwyczaj znajduje się informacja o zablokowaniu dostępu do konta, które należy jak najszybciej ponownie aktywować, przy pomocy podanego odnośnika do strony. Przez zachowanie tonu korespondencji tożsamej z tą którą stosuje bank oraz wyglądu strony z podanego linka ofiary przestępstwa udostępniają swoje dane do logowania: identyfikator, hasło, kody PIN. Niektórzy przestępcy w swoich wiadomościach wprost żądaj podania przez klientów danych do logowania, w celu potwierdzenia tożsamości klientów[51].

Realnym zagrożeniem dla bankowości elektronicznej jest używanie jej na komputerach w ogólnodostępnych miejscach, takich jak biblioteki, szkoły czy kafejki internetowe. W takich miejscach łatwo jest zainstalować programy szpiegowskie, które zapisują w pamięci kolejność zapisywanych znaków na klawiaturze, a także przechwytują zrzuty ekranu. W związku z takim zagrożeniem, banki rekomendują logowanie się do swojego rachunku na komputerach prywatnych. Również nie zalecane jest logowanie do systemu podczas połączenia z ogólnodostępnym, niezabezpieczonym hasłem Wi-Fi.

Kolejnym internetowym przestępstwem jest metoda *main in the browser.* Metoda ta opiera się na ataku przeglądarki internetowej. Podczas logowania się do rachunku bankowego następuje modyfikacja danych zawartych w wypełnianym formularzu. Dochodzi do zapisu danych na dysku twardym klienta przez „złośliwy" kod, a następnie dostosowuje się on do systemu konkretnego banku. Zabezpieczanie przed taki atakiem leży po stronie banku. Klient również może zminimalizować ryzyko poprzez użytkowanie aktualnej wersji przeglądarki internetowej, skonfigurowanej w sposób zalecany przez bank oraz instalację programu antywirusowego[52].

W dzisiejszych czasach telefon komórkowy jest nierozerwalną częścią życia zwłaszcza młodych ludzi. Jego funkcjonalność, uniwersalność oraz przejrzysty interfejs powoduje, że komórka coraz częściej zastępuje komputer. Dlatego usługi mobilne bankowości były nieuniknione. Rozwój technologiczny urządzeń mobilnych znacząco wpływa na ich bezpieczeństwo, a także wiąże się z różnymi zagrożeniami. Znaczący wpływ na bezpieczne korzystanie z usług bankowych ma odpowiednie zabezpieczenie

[50] http://www.zyjbezpiecznie.policja.pl/zb/finanse-i-dokumenty/47375,Skimming-i-phishing.html, (dostęp: 30.05.2020).
[51] http://www.zyjbezpiecznie.policja.pl/zb/komputer-i-internet/47343,Phishing.html, (dostęp: 30.05.2020).
[52] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 36.

telefonu oraz rozważne korzystanie z niego (między innymi unikanie wchodzenia na podejrzane strony WWW)[53].

Aby zachować środki bezpieczeństwa, należy pobierać aplikacje tylko z autoryzowanych sklepów na przykład Google Play czy Apple Store oraz sprawdzać telefon w kierunku szkodliwych programów za pomocą programów anty-malware'owych. Kolejnym punktem bezpieczeństwa jest blokada ekranu telefonu, kod PIN jest w tym wypadku bezpieczniejszą metodą niż rysowany wzór. Sam dostęp do aplikacji bankowej również powinien posiadać unikalny kod PIN, nie wykorzystywany w żadnym innym miejscu.

Kolejnym zagrożeniem dla smartfonów są wirusy, złośliwe oprogramowania czy tak zwane konie trojańskie, aczkolwiek nie jest to jeszcze tak powszechny problem jak dla komputerów. „Zarażony" telefon jest dla przestępcy źródłem wszelkich prywatnych danych zawartych na telefonie, haseł, loginów, numerów kart i tak dalej. Z tego powodu ważne jest aby również w telefonie posiadać ochronę antywirusową. Programy czasami posiadają wady, dlatego producenci cały czas pracują nad ich ulepszeniem wprowadzając aktualizacje, jednak aby działały one poprawnie należy ściągać oraz aktualizować aplikacje z zaufanych źródeł.

Technologia SIM Toolkit jest najbezpieczniejszym rozwiązaniem dla klienta łączącego się mobilnie z bankiem. Po otworzeniu aplikacji aby uzyskać dostęp do rachunku należy wpisać wcześniej ustalony przez siebie kod PIN. Analogicznie do bankowości elektronicznej, po kilkukrotnym błędnym wpisaniu PINu aplikacja zostaje zablokowana. W celu jej odblokowania należy udać się do placówki bankowej. Również podczas korzystania z aplikacji w celu potwierdzenia robionych operacji wymagany jest kolejny kod PIN utworzony przez użytkowania w celu autoryzacji transakcji. Do szyfrowania połączenia z bankiem używany jest algorytm symetryczny 3 DES. Oznacza to, że operator sieci komórkowej nie może w żaden sposób ingerować w transmisję danych. W momencie zaistnienia zagrożenia dla tej transmisji zarówno operator jak i bank może ją zablokować[54]. Bezpieczeństwo telefonu i wszelkich danych zapisanych na nim to przed wszystkim ochrona przed kradzieżą urządzenia lub zgubieniem.

Banki w szybkim tempie reagują na potrzeby konsumentów, często przejmując inicjatywę aby wyjść naprzeciw tym potrzebom. Tak więc rozwijają swoje usługi nie

[53] http://www.mobilnybank.pl/bezpieczenstwo, (dostęp: 30.05.2020).
[54] Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych*, dz.cyt. s. 47.

tylko w celu zaspokojenia potrzeb klientów, ale również w celu ich generowania, a tym samym przyciągnięcia większej liczby usługobiorców.

3.3. Sektor FinTech w rozwoju bankowości elektronicznej

Przez szybko zmieniający się świat, dzisiejsze społeczeństwo nie jest już w stanie wyobrazić sobie życia bez dostępu do Internetu oraz aplikacji mobilnych. Rynek bankowy jako część świata finansowego udostępnia coraz nowsze, lepsze i prostsze w obsłudze sposoby na korzystanie ze swoich usług w sposób zdalny. Ciągłe zmiany rynkowe, zwiększające się oczekiwania konsumentów oraz zapewnienie bezpieczeństwa wpływają na tworzenie kosztów tych instytucji. Ograniczenia w budżecie są czynnikiem, dla którego banki, aby móc się dalej rozwijać, rozpoczęły poszukiwania innych rozwiązań. W odpowiedzi na te potrzeby powstał FinTech. Są to instytucje działające w obszarze finansowym i technologicznym. W ich kompetencjach leży innowacyjność w branży finansowej w świecie wirtualnym.

Pierwsze wzmianki o FinTechu pojawiły się w latach osiemdziesiątych zeszłego wieku a amerykańskich pismach. Wspominano wtedy o masowej komputeryzacji oraz zastosowaniu telekomunikacji w świecie finansów. Początków FinTechu można również dostrzegać w pojawiających się w latach sześćdziesiątych bankomatów. Pierwszy rozkwit tej branży nastąpił w latach dziewięćdziesiątych wraz z rozwojem Internetu. Pierwszą z typowych, globalnych firm z sektora FinTech jest PayPal, powstały w 1999 roku, który odpowiadał za płatności powstałe podczas zakupów na portalach aukcyjnych. Drugim etapem był rok 2010, kiedy urządzenia typu smartfon zaczęły się upowszechniać[55].

Najnowsze technologie wykorzystywane są do coraz to nowszych rozwiązań, przyspieszenia, zabezpieczenia, ulepszenia, powszechności, a także do obniżenia kosztów danego podmiotu finansowego.

Branżę FinTech można podzielić na trzy działy:

- Bankowy i ubezpieczeniowy (mobile banking, e-banking, sprzedaż ubezpieczeń w modelu direct lub za pośrednictwem sieci afiliacyjnych),
- Rozwiązania obejmujące analizę danych i optymalizację procesów, doradztwo w zakresie podejmowania decyzji,

[55] https://fintek.pl/definicja-fintech-fintech/, (dostęp: 30.05.2020).

- Płatności online i ich zabezpieczenie[56].

Od 2016 roku dostępne online są również pożyczki czy wyceny. Kolejnymi rozwiązaniami sprzedaży oraz decyzyjności były te związane z blockchain, identyfikacją biometryczną lub głosową, sztuczną inteligencją.

W Polsce banki wraz z instytucjami finansowymi korzystające z usług FinTechu, swoje oferty przewidują w większej mierze dla klienta detalicznego. Koncentrują się na konkretnym produkcie, aby jak najlepiej dostosować się do wymagań i potrzeb konsumenta. W sektorze FinTechu można między innymi znaleźć:

- obsługę płatności online (PayU, PayPal, BLIK),
- e-bankowość i bankowość mobilna (BZ WBK, iPKO),
- pożyczki online (Vivus, Wonga)
- aplikacje wykorzystywane do optymalizacji budżetów domowych/ wydatków, płatności mobilne wykorzystujące HCE (ApplePay, AndroidPay)
- kantory internetowe (Cinkciarz, Walutomat),
- przedsiębiorstwa oferujące płatności z wykorzystaniem technologii blockchain (Bilion)[57].

FinTech jest dostępny zarówno dla „starych" firm jak i dla start-upów, testujących dopiero najnowsze rozwiązania. Dzięki bankom, które pomagają start-upom, mają one możliwość testowania swoich rozwiązań na tak zwanym „żywym organizmie" – czyli prawdziwych klientach.

W sierpniu 2016 roku portal fintek.pl przedstawił najbardziej innowacyjne i FinTechowe banki w Polsce (aktualizowane w czerwcu 2019):

- Idea Bank – darmowe konta dla firm, oprocentowanie depozytów nawet do 4%, kredyt „Na start", Inkubator Przedsiębiorczości, darmowy mobilny wpłatomat, usługa „Wirtualny oddział",
- mBank – „lekkie oddziały", szybkie kredyty gotówkowe dostępne również online, program dla niesłyszących, odznaczony nagrodami: w 2014 Bank Innovation Award, a w 2015 w kategorii „Innowacyjność" podczas konkursu „Gwiazdy Bankowości",

[56] https://fintek.pl/definicja-fintech-fintech/, (dostęp: 30.05.2020).
[57] Tamże.

- BZ WBK – od 2011 gdy wchodzi w skład Santadera rozpoczną się rozwój banku, w 2014 uruchomiony zostaje inkubator Santander InnoVentures oraz organizacja hackathon, w 2015 wspiera poznańskie „NeedApp", podwojenie inwestycji w innowacje, dzięki tym zabiegom aplikacja BZ WBK jest jedną z najlepszych a sam bank dynamicznie się rozwija,
- Bank Millenium – przeznaczył 500 milionów złotych na wspieranie innowacji, firma może od banku otrzymać do 6 milionów złotych na spłatę zadłużeń związanych z rozwoje technologicznej innowacyjności w firmie, posiada również jedną z lepszych aplikacji mobilnych,
- PKO BP – po wypuszczeniu najnowszej wersji aplikacji IKO osiągnął rekord pobrań wśród bankowych aplikacji mobilnych (ponad 1 milion pobrań, na rok 2020 jest to już ponad 5 milionów), w 2016 roku została podpisana umowa pomiędzy PKO BP a PKN ORLEN na mocy której klienci będą mogli połączyć korzyści płynące z posiadania rachunku bankowego oraz członkostwa w klubie VITAY – jest to pierwsze tego typu rozwiązanie w Europie[58].

Banki dzięki wprowadzanym innowacjom zdobywają nowe narzędzia oraz usługi które dotychczas były poza ich zasięgiem. Zapewni im to dynamiczną reakcję na zapotrzebowanie konsumentów. Te banki, które będę unikać wprowadzania takich zmian będą zmuszone zakończyć swoją działalność.

[58] https://fintek.pl/top5-fintechowych-bankow-polsce/, (dostęp: 30.05.2020).

Zakończenie

Pieniądz na przestrzeni wieków przybierał różne postaci. Na podstawie przeprowadzonej analizy można stwierdzić, że mamy współcześnie do czynienia ze zmniejszeniem się roli pieniądza tradycyjnego w gospodarce, za sprawą ciągłego rozwoju pieniądza elektronicznego. Być może obecne młode pokolenie jest już ostatnim, które będzie wykorzystywało pieniądz papierowy w rozliczeniach. Karta płatnicza, która jeszcze do niedawna była nieosiągalna dla wielu osób, dzisiaj jest standardem. Obecnie wielu klientów banków nie wyobraża sobie konta bankowego bez dostępu do niego przez internet czy telefon. Rosnące potrzeby klientów, w tym mobilnego pokolenia Y, coraz bardziej świadomych nowych technologii będą wyznacznikiem dla banków w rozwoju e-bankowości.

Jak pokazała analiza, wzrost popularności usług internetowych i mobilnych wiąże się nierozerwalnie z zapewnieniem bezpieczeństwa ich użytkowania. Przed bankami stoi ogromne wyzwanie. Z jednej strony ciągły rozwój i unowocześnianie bankowości elektronicznej, a z drugiej nieustanna praca nad poprawą systemów zabezpieczeń transakcji dokonywanych w Internecie. Być może w przyszłości potwierdzenie transakcji odbywać się będzie za pomocą odcisku palca, skanu siatkówki czy danych biometrycznych, najprawdopodobniej będzie to najbezpieczniejsza forma weryfikacji.

Rosnąca popularność elektronicznych sposobów zdalnego dostępu w przyszłości może spowodować zastąpienie banków tradycyjnych bankami wirtualnymi. Polskie banki posiadające sieci oddziałów mocno pracują nad promowaniem usług bankowości elektronicznej wśród swoich klientów. PKO Bank Polski jako pierwszy zaczął wdrażać nowoczesne technologie m. in. aplikacji mobilnej IKO, która stała się fundamentem międzybankowego standardu płatności mobilnych BLIK. W najbliższym czasie konkurujące ze sobą banki w Polsce będą musiały w rozpoczętym pędzie ku nowoczesności wykazać się innowacyjnością produktów i usług finansowych.

Bibliografia

1. Bylok F., Sikora J., Sztumska B., *Wybrane aspekty socjologii rynku,* Częstochowa 2001.
2. Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE.
3. Europejski Bank Centralny, Opinia Europejskiego Banku centralnego z dnia 12 października 2016r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu i zmieniającą dyrektywę 2009/101/WE (CON/2016/49) (2016/c 459/05).
4. Gospodarowicz A., *Bankowość elektroniczna*, Warszawa 2005.
5. Gruszecki T., *Teoria pieniądza i polityka pieniężna*, Kraków 2004.
6. Komisja Nadzoru Finansowego, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną. Poradnik klienta usług finansowych,* Warszawa 2014.
7. Komisja Nadzoru Finansowego, *Usługi Bankowości Elektronicznej dla Klientów Detalicznych. Charakterystyka i zagrożenia. Urząd Komisji Nadzoru Finansowego,* Warszawa 2010.
8. Kopańko K., Kozłowski M., *Bitcoin. Złoto XXI wieku,* Gliwice 2015.
9. Korzeń K., *Bankowość elektroniczna jako kanał dystrybucji usług bakowych*, Warszawa 2006.
10. Kozak A., *Znaczenie pieniądza*, Lublin 2004.
11. Koźliński T., *Bankowość elektroniczna,* Warszawa 2004.
12. Mishkin F.S., *Ekonomika pieniądza, bankowości i rynków finansowych*, Warszawa 2002.
13. Schaal P., *Pieniądz i polityka pieniężna*, Warszawa 1996.
14. Solarz M., *Rozwój bankowości elektronicznej w Polsce,* Warszawa 2006.
15. Szymankiewicz M., *Bitcoin. Wirtualna waluta internetu*, Gliwice 2014.

16. Ustawa z dnia 12 września 2002r. o elektronicznych systemach płatniczych. Dz.U. 2002r., nr 169, poz. 1385 z późn. zm.
17. Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002r., nr 144, poz. 1204, art.2 pkt. 4.
18. Wójcik J., Przeciwdziałanie przestępczości zorganizowanej. Wolters Kluwer Polska. Warszawa 2011.

Źródła internetowe

1. http://businessinsider.com.pl/technologie/blockchain/blockchain-co-to-jest/vlfytn4 (dostęp: 03.05.2020).
2. http://norbertbiedrzycki.pl/blockchain-trzeba-o-nim-wiedziec/ (dostęp: 03.05.2020).
3. http://www.bankier.pl/wiadomosc/Historia-bankowosci-internetowej-w-Polsce-7284848.html (dostęp: 22.05.2020).
4. http://www.bitcoin.pl/o-bitcoinie/co-to-jest-bitcoin (dostęp: 30.03.2020).
5. http://www.mobilnybank.pl/bezpieczenstwo (dostęp: 30.05.2020).
6. http://www.polskistandardplatnosci.pl/o-nas (dostęp: 25.05.2020).
7. http://www.zyjbezpiecznie.policja.pl/zb/finanse-i-dokumenty/47375,Skimming-i-phishing.html (dostęp: 30.05.2020).
8. http://www.zyjbezpiecznie.policja.pl/zb/komputer-i-internet/47343,Phishing.html (dostęp: 25.05.2020).
9. https://fintek.pl/definicja-fintech-fintech/ (dostęp: 30.05.2020).
10. https://fintek.pl/top5-fintechowych-bankow-polsce/ (dostęp: 30.05.2020).
11. https://www.forbes.pl/finanse/bankowosc-xxi-wieku-czym-jeszcze-moze-nas-zaskoczyc/0ceq7dj (dostęp: 22.05.2020).
12. https://www.forbes.pl/technologie/historia-bankomatu/4yy2hn3#, (dostęp: 22.05.2020).
13. https://prnews.pl/inteligo-najbardziej-przyjazna-bankowosc-mobilna-29564 (dostęp: 22.05.2020).

Spis rysunków

Spis tabel