Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-36 | strony: 371–378

Halina Świeboda
Akademia Sztuki Wojennej
Wydział Bezpieczeństwa Narodowego
Instytut Studiów Strategicznych
Katedra Bezpieczeństwa Informacyjnego i Komunikacji
h.swieboda@akademia.mil.pl

Ekonomiczne aspekty kryptowalut

Kod JEL: 033
Słowa kluczowe: cyberprzestępczość, kryptowaluty (waluty wirtualne), bitcoin
Streszczenie. Katalog współczesnych zagrożeń ekonomiczno-gospodarczych ewoluuje pod wpływem nowych zjawisk, jako skutek dynamicznego rozwoju technologii informacyjno-komunikacyjnych i poszerza się czyniąc go nieskończonym. Technologie wzbogaciły instrumentarium działań przestępczych i umożliwiły dokonywanie czynów zabronionych w cyberprzestrzeni. W kontekście zagrożeń postrzegane są wirtualne waluty. Artykuł poświęcono analizie zjawiska wirtualnych walut, by na tej podstawie sformułować przypuszczalne konsekwencje i najbardziej realne cele dla Polski, póki jest jeszcze czas, aby podjęte działania były skuteczne i zabezpieczały interesy państwa.

Wprowadzenie

Z uwagi na cechy cyberprzestrzeni, popełnianie w niej cyberprzestępstw jest zdecydowanie atrakcyjniejsze od popełniania przestępstw w środowisku rzeczywistym, realnym. Środowisko bowiem w wysokim stopniu zapewnia anonimowość, a brak odpowiednich regulacji prawnych zarówno krajowych, jak i międzynarodowych, nienadążających za dynamicznie rozwijającym się rynkiem usług cyberprzestępczych, pozwala na ich bezkarne podejmowanie.

Dotychczas ataki w cyberprzestrzeni miały charakter ataków masowych, natomiast w roku 2016 i 2017 pojawiły się bardzo zaawansowane i elitarne grupy przestępcze wykorzystujące techniki typowe dla zaawansowanych ukierunkowanych ataków na wewnętrzne funkcjonowanie międzynarodowego systemu finansowego. Wiele z zagrożeń przenika z sieci niekontrolowanych przez państwo, w których „kwitnie czarny ry-

nek" usług cybergospodarki. Na ogólnodostępnych „podziemnych forach" i „ciemnych" stronach internetowych sieci Tor, wśród oferowanych usług znalazły się również karty podarunkowe do restauracji, rezerwacje hotelowe i linie lotnicze obsługujące loty z częstymi przelotami. Rachunki bankowości online były również na sprzedaż, obok kont PayPal i kont detalicznych, do sklepów Amazon i Walmart. Jeśli chodzi o złośliwe oprogramowanie, zestawy narzędzi ransomware kosztuje 1800 USD i często są sprzedawane jako Crimeware-as-a-Service (CaaS), a trojany bankowe z Androidem są sprzedawane za 200 USD. Firma Symantec zaobserwowała wzrost ofert usług transferu pieniędzy, które były sprzedawane za około 10% ich wartości, np. „zapłać 100 $ w bitcoinach za przelew w wysokości 1000 $". Oznacza to, że proces wypłaty skradzionych pieniędzy jest nadal najtrudniejszym krokiem w łańcuchu cyberprzestępców (Raport ISTR, 2017), ale oznacza również, że kryptowaluty są instrumentami prania „brudnych", czyli pochodzących z przestępstwa pieniędzy.

Motywy podejmowania działań przestępczych są bardzo różne – od chęci osiągnięcia korzyści materialnych, nieuczciwej konkurencji biznesowej, działań ideologicznych, po zorganizowaną działalność państwową w ramach komórek służb specjalnych do zadań cybernetycznych (Charatynowicz, 2017, s. 157–158). Zagadnieniem, które nie doczekało się wyczerpujących opracowań ze względu na nowość zjawiska, jest rynek kryptowalut i sieci tzw. Shadow Interentu, które są niekontrolowane przez państwo. W przestrzeni publicznej, za sprawą wydarzeń z 2014 roku: upadek giełdy Mt.Gox (Raport WizSec), znaczące fluktuacje kursu Bitcoina oraz liczne oszustwa – nadwerężyło reputację wirtualnej waluty jako stabilnej cyfrowej waluty oraz bezpiecznego systemu płatności. Uznaje się, że kryptowaluty są zagrożeniem dla systemów bankowych państw i ułatwiają pranie brudnych pieniędzy, unikanie opodatkowania, finasowanie terroryzmu. Sieci niekontrolowane przez państwo stają się podstawą czarnego rynku i stanowić będą główne źródło dostępu do nielegalnych towarów, zasilają także rynek kryptowalut.

1. Wirtualne waluty

Zjawisko wirtualnych walut jest nowe, bowiem pierwsza wirtualna waluta bitcoin powołana została na rynku amerykańskim w 2009 roku, jako efekt złagodzenia ograniczeń w stosowaniu kryptografii (kontrolowanej wcześniej restrykcyjnie przez służby bezpieczeństwa większości państw świata), gwałtownego wzrostu znaczenia serwisów społecznościowych i rozproszonych systemów zarządzania sieciami (Raport *Wirtualne waluty*, 2014). Początki kryptowalut sięgają zaawansowanych koncepcji systemów płatności elektronicznych, bazujących na współczesnej kryptografii, które pojawiły się w latach dziewięćdziesiątych XX wieku. Chodziło o sieciowe oprzyrządowanie projektów w nurcie tradycyjnym – związane z rozwojem kart płatniczych, zdalnym doładowywaniem konta czy bezpiecznym transferem płatności. Jest to innowacja, dla której nie do końca poznane są skutki, jakie może wywołać na rynkach.

Pojęcie waluty wiązane jest z wymianą międzynarodową. Waluta jest miernikiem wartości, bo jest środkiem rozliczeniowym oraz środkiem regulowania płatności (należności i zobowiązań) w rozliczeniach międzynarodowych. Wyrażenie „pieniądz" kojarzymy z walutą kreowaną i kontrolowaną przez państwo. System finansowy państw jest umocowany ustawowo i nie ma konkurencji. W przypadku walut wirtualnych brak ograniczeń wynikających z regulacji prawnych, ograniczeniem jest sama technologia. Definicyjnie, w międzynarodowych dokumentach, waluty wirtualne ujmuje się jako cyfrowe reprezentacje wartości, które mogą być przedmiotem obrotu cyfrowego i działają jako środek wymiany i/lub środek przechowywania wartości, ale nie mają statusu środka płatniczego w jakiejkolwiek jurysdykcji (raport EBC 2012, 2015). Kryptowaluta to cyfrowa waluta, która jest tworzona i zarządzana przy użyciu zaawansowanych technik szyfrowania, znanych jako kryptografia. Obecnie na rynku wirtualnych walut funkcjonuje ponad 1000 ich rodzajów i ilość ta ciągle się zwiększa[1] (tab. 1).

Tabela 1. Wybrane, najpopularniejsze rodzaje wirtualnych walut w 2016 i 2017 roku

NAZWA	CHARAKTERYSTYKA
Litecoin (LTC)	Litecoin, uruchomiony w 2011 roku, był jednym z pierwszych kryptowalut po bitcoinie. Został stworzony przez Charliego Lee, absolwenta MIT i byłego inżyniera Google. Litecoin opiera się na globalnej sieci płatniczej o otwartym kodzie źródłowym, która nie jest kontrolowana przez żaden organ centralny. Używa „scryptu", jako dowodu pracy, który można dekodować za pomocą procesorów klasy konsumenckiej. Ma szybszą generację bloku niż bitcoin, a zatem oferuje szybsze potwierdzenie transakcji
Ethereum (ETH)	„Emisja" w 2015 r. Ethereum to zdecentralizowana platforma oprogramowania, która umożliwia tworzenie inteligentnych kontraktów i aplikacji rozproszonych (DApps) bez żadnego przestoju, oszustwa, kontroli lub ingerencji strony trzeciej. Według Ethereum można go wykorzystać do „kodyfikowania, decentralizacji, zabezpieczania i wymiany prawie wszystkiego". Po ataku na DAO w 2016 r. Ethereum zostało podzielone na Ethereum (ETH) i Ethereum Classic (ETC). Ethereum (ETH) ma wysoką tuż po bitcoinie*
Zcash (ZEC)	ZCash, zdecentralizowana kryptowaluta open-source, uruchomiona w 2016 r. Oferuje prywatność i selektywną przejrzystość transakcji. Według Zcash, zapewnia dodatkowe bezpieczeństwo lub prywatność, wszystkie transakcje są rejestrowane i publikowane w blockchain, ale szczegóły takie jak nadawca, odbiorca i kwota pozostają prywatne. Oferuje użytkownikom wybór „ekranowanych" transakcji, które pozwalają na szyfrowanie zawartości przy użyciu zaawansowanej techniki kryptograficznej lub konstrukcji o zerowej wiedzy, zwanej zk- SNARK opracowanej przez jego zespół
Dash (pierwotnie znany jako darkcoin)	Dash oferuje więcej anonimowości od bitcoina, ponieważ działa na zdecentralizowanej sieci kodu źródłowego, która sprawia, że transakcje są prawie niewykrywalne. Rozpoczęty w styczniu 2014 r. Został stworzony i opracowany przez Evana Duffielda i może być wydobywany za pomocą procesora lub GPU. W marcu 2015 r. „darkcoin" został przemianowany na Dash, co oznacza Digital Cash działa pod szyldem – DASH. Rebranding nie zmienił żadnej z jego funkcji technologicznych, takich jak Darksend, InstantX
Ripple (XRP)	Ripple to globalna sieć rozliczeniowa czasu rzeczywistego, która oferuje natychmiastowe, pewne i tanie międzynarodowe płatności. Umożliwia bankom rozliczanie płatności transgranicznych w czasie rzeczywistym, z pełną przejrzystością i niższymi kosztami. Wydana w 2012 r., ma kapitalizację rynkową na poziomie 1,26 mld USD. Konflikt konsensusowy Ripple'a – jego metoda konformacji – nie wymaga wydobycia, jest to cecha, która różni go od bitcoinów i altcoinów. Ponieważ struktura Ripple'a nie wymaga wyszukiwania, zmniejsza wykorzystanie mocy obliczeniowej i minimalizuje opóźnienia sieci

[1] W trakcie dokonywanych badań i porównań w ciągu kilku tygodni ilość notowanych rodzajów z 840 wzrosła do 1150.

Monero (XMR)	Monero jest bezpieczną, prywatną i niemożliwą do wykrycia walutą o otwartym kodzie źródłowym, uruchomiona w kwietniu 2014 r. Jej rozwój jest całkowicie oparty na darowiznach i na społeczności. Monero został uruchomiony z silnym naciskiem na decentralizację i skalowalność oraz zapewnienie pełnej prywatności dzięki specjalnej technice, zwanej „sygnaturą pierścieniową". Dzięki tej technice pojawia się grupa podpisów kryptograficznych, w tym co najmniej jeden prawdziwy uczestnik – ale ponieważ wszystkie wyglądają na prawdziwe, rzeczywistych nie da się wyizolować

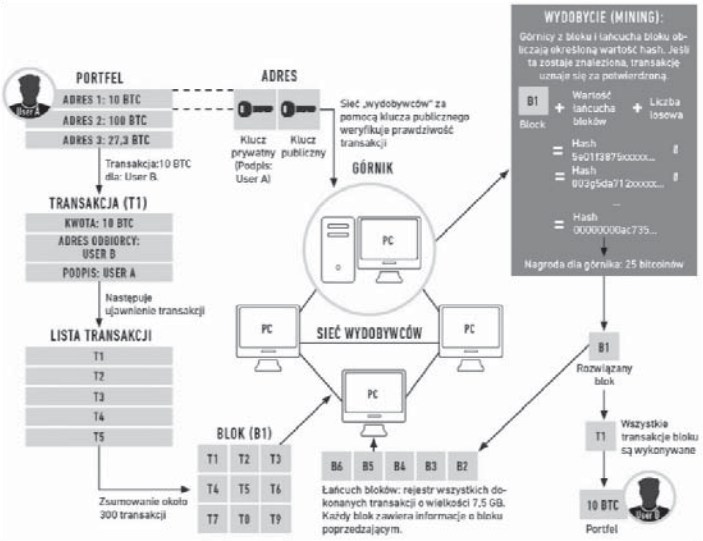
* The First-Ever Ethereum IRA jest Game-Changer, https://www.investopedia.com/news/make-way-here-comes-ethereum-ira.

Źródło: opracowanie własne na podstawie *The 6 Most Important Cryptocurrencies Other Than Bitcoin?* Investopedia. Pobrano z: https://www.investopedia.com/tech/6-most-important-cryptocurrencies-other-bitcoin/#ixzz52dWgLSQd (28.12.2017).

Bitcoin jako pierwszy nie tylko wyznaczał trendy, wprowadzając falę kryptowalut opartych na zdecentralizowanej sieci *peer-to-peer*, ale stał się ich standardem. Umożliwia zbiorową realizację wszystkich funkcji wydawania waluty, przetwarzania transakcji oraz zabezpiecza weryfikację w sieci. Waluty inspirowane bitcoinem są zbiorczo nazywane altcoinami i próbują przedstawić się jako zmodyfikowane lub ulepszone wersje bitcoina. Moneta ma ograniczoną podaż – na rynek trafi zaledwie 21 mln sztuk. Jak dotąd, „wykopano" blisko 80% całego zbioru. Obliczono, że wszystkie bitmonety trafią do obiegu do 2140 roku (finase.wp.pl). Bitcoiny można nabyć na dwa sposoby: 1) nabycie bitconów w internetowym kantorze (tak jak każdej innej waluty), 2) użycie własnego komputera do tzw. procesu „wydobywania" bitcoinów.

2. „Wydobywanie" kryptowalut

Kreowanie waluty cyfrowej odbywa się w procesie tzw. „wydobywania" lub „kopania" (*mining*) za pomocą tzw. Koparek, czyli zaawansowanych komputerów, których zadaniem jest rozwiązywanie złożonych algorytmów i liczb. Technologia, na której opiera się proces „kopania", to aplikacja blockchain (łańcuch bloków) i jest rodzajem matematyczno-kryptograficznego algorytmu, którego „paliwem" jest moc obliczeniowa uczestniczących w nim komputerów. Dlatego „kopanie" bitcoinów wymaga sprzętu o gigantycznej mocy obliczeniowej. W łańcuchu bloków transakcją jest każdy zapis informacji. Łańcuch nie służy do płacenia, ale może integrować się z innymi systemami informatycznymi – np. osobną platformą do dokonania płatności. „Kopanie" kryptowalut polega na użyczaniu mocy obliczeniowej komputera, który (razem z innymi w blockchain) weryfikuje poprawność transakcji zapisywanych w tym rejestrze. Kryptowaluta to w pewnym sensie nagroda za pracę komputera (Majdan, 2016). Nakład pracy mierzonej mocą obliczeniową wykorzystaną do ustalenia bloku obliczeniowego, w którym zawiązywane są transakcje przeprowadzane w systemie bitcoin, wyraża wartość kryptowaluty (Musiał, 2013, s. 61).



Rysunek 1. Minning – proces wydobywania kryptowaluty

Źródło: J. Gozdek, *Szum wokół bitcoina*. Pobrano z: https://www.chip.pl/2013/11/szum-wokol-bitcoina (30.12.2017).

Dla użytkowników bitcoina „wydobywanie" rozpoczęło się od programu bitcoin-Qt, który dokonuje transakcji i zarządza pieniędzmi. Bitcoina można podzielić na dowolnie małe ułamki. Najmniejszą możliwą jednostką jest jedna stumilionowa, nazywana satoshi, od najprawdopodobniej kryjącego się pod pseudonimem, twórcy – Satoshi Nakamoto. Aby wytwarzana samodzielnie waluta nie zalała rynku, ma wbudowany hamulec inflacyjny. Z czasem wzrasta stopień trudności obliczeń, a równocześnie nagroda spada o połowę co cztery lata. Oprócz tego jeden „górnik" może rozwiązywać jedno zadanie tylko co dziesięć minut. To wszystko skutkuje krzywą wzrostu, która zbliża się do zera – przypuszczalnie do roku 2040 (Satishi.pl). Te cechy sprawiają, że bitcoin zasadniczo różni się od waluty pieniądza, która jest poparta pełnym zaufaniem i wiarygodnością rządu. Emisja walutowa jest wysoce scentralizowaną działalnością nadzorowaną przez krajowy bank centralny. Chociaż bank reguluje ilość wydanych walut zgodnie z celami polityki pieniężnej, teoretycznie nie istnieje górny limit kwoty takiej emisji w walucie. Ponadto depozyty w walucie lokalnej są zazwyczaj ubezpieczane przez instytucje rządowe przed bankructwami. Waluty wirtualne nie mają takich mechanizmów wsparcia. Wartość bitcoina jest całkowicie zależna od tego, co inwestorzy są skłonni zapłacić za to w danym momencie. Jeśli giełda bitcoinów „się zwinie", klienci z saldami bitcoinowymi nie będą mieli możliwości odzyskania ich.

Wzrost znaczenia kryptowalut powoduje implikacje w różnych dziedzinach. Zrozumienie tego zjawiska wymaga podejścia multidyscyplinarnego. Oznacza to, że w analizie należy uwzględnić: problemy technologiczne, kryptograficzne, bezpieczeństwo systemu i podatność na atak.

3. Zagrożenia w obrocie wirtualnymi walutami

W Polsce brak jest definicji i uregulowań w zakresie obrotu kryptowalutami. Były one przedmiotem ostrzeżeń Generalnego Inspektora Informacji Finansowej w sprawie niebezpieczeństw związanych z walutami wirtualnymi, wykorzystania obrotu nimi do działań w procederze prania pieniędzy (KNF, 2000), przekaz został wzmocniony poprzez wydanie Komunikatu w tej samej sprawie w 2014 roku.

Wirtualne waluty nie mają oparcia w twardej ekonomii, a to oznacza, że są podatne na ryzyka związane z manipulowaniem jego wartością oraz ryzykami kursowymi – mogą być wykorzystywane jako piramida finansowa (Roubini, 2016). Zagrożeniem jest brak nadzoru KNF i Narodowego Banku Polskiego, co powoduje wątpliwości co do bezpieczeństwa realizowanych konwersji wirtualnych walut i gwarancji do przekazywanych wartości majątkowych, a brak gwarancji Bankowego Funduszu Gwarancyjnego dla transakcji i konwersji nie zapewnia bezpieczeństwa ich oraz zgromadzonych aktywów. Wartość wirtualnej waluty jest uzależniona od popytu i podaży i w żaden sposób nie jest odzwierciedleniem wartości gospodarki i kondycji finansowej emitenta. Na rynku nie ma stabilizujących narzędzi, dlatego zmienność w jedną lub drugą stronę jest praktycznie nieograniczona. Aspekt finansowy w cyberprzestrzeni realizowany jest w postaci transakcji bankowych, finansowych z udziałem autoryzowanych podmiotów PayPal, Western Union oraz wirtualnych walut. Podmioty realizujące transakcje wirtualnymi walutami narażone są na ryzyko prania pieniędzy, ukrywania majątku, unikania opodatkowania czy finansowania terroryzmu. Wymienione uwarunkowania skłaniają do wniosku, że najpoważniejszym zagrożeniem, według autorki, jest brak nadzoru instytucji systemu przeciwdziałania praniu pieniędzy bądź finansowaniu terroryzmu, których zadaniem jest rejestrowanie transakcji i dokonywanie analiz pod względem zagrożeń. Dla inwestorów indywidualnych, oprócz utraty wartości zgromadzonych kryptośrodków, w trakcie dokonywania transakcji istnieje możliwość jej „zatrucia", czyli umieszczenia dodatkowych informacji (plików, obrazów, danych tekstowych) niezgodnych z prawem. Przelew środków finansowych może zawierać pliki np. z pornografią, wtedy kontrahentowi grozi odpowiedzialność karna. Na niestabilność kryptowalut mogą mieć wpływ decyzje polityczne i prawne innych krajów świata. Przykładem jest sytuacja, gdy chiński rząd podjął decyzję o zamknięciu trzech największych giełd bitcoinowych (wrzesień 2017 r.) w Chinach, cena tej waluty spadała o kilkadziesiąt procent (Wrona, 2017), a JP Morgan, stwierdził, że „bitcoin to oszustwo" (Bankier.pl). Zagrożeniem dla użytkowników Internetu jest wykorzystywanie ich komputerów do „kopania" kryptowaluty. Z informacji udostępnionych przez Kasperski Lab wynika, że w sieci dostępne jest oprogramowanie dystrybuowane za pośrednictwem torrentów, które umożliwia włączenie w sieć bootnetów i bez zgody właściciela korzystanie z poboru prądu i mocy obliczeniowej komputera[2], co oczywiście naraża na straty właściciela zainfekowanego komputera.

[2] Program do „kopania" „pożera" ok. 90% pamięci RAM.

Podsumowanie

Sytuacja dojrzała do momentu, w którym konieczna jest interwencja państwa. Kwestią do rozwiązania jest sprawowanie kontroli nad emisją pieniądza wirtualnego, jego obiegiem (wirtualny *vs* rzeczywisty) i podjęcie badań określających jego rzeczywisty wpływ na gospodarkę. Prognozy (wirtualnemedia.pl) wskazują, że rynek dóbr i usług wirtualnych będzie się dynamicznie rozwijał, dlatego konieczne jest zdynamizowanie pracy nad wdrożeniami rozwiązań, które korzystnie wpłyną na rozwój rynku kryptowalut i zapewnią korzyści dla gospodarki (podatki) lub na tyle uregulują rynek, że dokonywanie cyberprzestępstw będzie kontrolowane i nieopłacalne. W aktualnym stanie rzeczy wydaje się niezasadnym zakazywanie „czegokolwiek", natomiast jak najbardziej wskazana jest regulacja, tym bardziej, że rządy wielu krajów zainteresowane są kryptowalutami, ale własnymi, np. Chiny, Rosja, kraje skandynawskie. Niemcy już uczyniły bitcoiny oficjalnym środkiem płatniczym. W Japonii rząd powołał grupę, która ma zająć się ustaleniem działania giełd bitcoinowych na zasadzie samoregulacji społeczności. W 2014 roku unormowano kwestie opodatkowania dochodów osobistych z bitcoinów w USA. Podejmowane działania podporządkowane są zdobyciu prymatu w świecie i czerpanie z tego korzyści, a także chęć podporządkowania wszystkich innych cyberrynków. W Unii Europejskiej sytuacja jest niejasna pod względem VAT-u na bitcoina, np. Finlandia zapewnia zwolnienie z podatku VAT, a reszta krajów czeka na wspólne stanowisko. Brak jasnych wytycznych to ryzyko prawne dla indywidualnych biznesów. W Polsce, ponieważ nie ma zainteresowania regulacjami ze strony podmiotów państwowych, prace nad regulacją inicjowane są oddolnie przez podmioty zainteresowane (prywatne) rozwojem działalności tego cybersektora. Konieczne jest stworzenie standardów bezpieczeństwa giełd bitcoinowych.

Literatura

Bankier.pl.

Charatynowicz, J. (2017). Ekonomiczne aspekty cyberprzestępczości. Zagrożenia związane z konwersją i transferem wirtualnych walut. W: J. Kosiński (red.). *Przestępczość teleinformatyczna 2016*. Szczytno: Wyższa Szkoła Policji w Szczytnie.

http://www.wirtualnemedia.pl.

https://satoshi.pl.

Majdan, K. (2016). *Komputer-niewolnik. Zesłany do pracy w kopalni wydobywa kryptowalutę, bez wiedzy właściciela*. Pobrano z: https://businessinsider.com.pl.

Musiał, M. (2013). *Technologiczne uwarunkowania korzystania z pieniądza wirtualnego*. W: E. Bogacka-Kisiel (red.), *Pieniądz wirtualny i determinanty jego rozwoju w sferze ekonomii i finansów i prawa*. Opole.

Raport EBC (2012, 2015). *Wirtualne systemy walut*.

Raport Internet Security Threat ISTR (2017).

Raport NCR. *Norton Cybercrime Report.*

Raport *Wirutalne waluty* (2014). Warszawa: Wardyński i wspólnicy.

Raport WizSec.

Roubini, N. (2016). The Mother Of All Asset Bubbles Will Burst In 2016. *Economic Outlook*. Pobrano z: http://www.businessinsider.com.

Sprawozdanie z działalności KNF z realizacji ustawy o przeciwdziałaniu praniu pieniędzy oraz finasowaniu terroryzmu z 16 listopada 2000 r.

The Future Of Cryptocurrency. Investopedia Staff. Pobrano z: https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp#ixzz52dXzqYu2.

Wrona J. (2017). *Bitcoin – jakie są korzyści i zagrożenia prawne wirtualnej waluty?* Pobrano z: http://di.com.pl/bitcoin---jakie-sa-korzysci-i-zagrozenia-prawne-wirtualnej-waluty-58389.

ECONOMIC ASPECTS OF CRYPTOCURRENCIES

Keywords: cybercrime, cryptocurrencies (virtual currencies), bitcoin

Summary. The catalog of contemporary economic threats evolves under the influence of new threats as a result of the dynamic development of information and communication technologies and expands making it infinite. Technologies enriched the instrumentation of criminal activities and made it possible to perform criminal acts in cyberspace. Virtual currencies are seen in the context of threats. The article is devoted to the analysis of the phenomenon of virtual currencies to formulate the supposed consequences and the most real goals for Poland while there is still time for the actions taken to be effective and secure the interests of the state.

Translated by Halina Świeboda

Cytowanie

Świeboda, H.. (2018). Ekonomiczne aspekty kryptowalut. *Ekonomiczne Problemy Usług*, *2* (131/1), 371–378. DOI: 10.18276/epu.2018.131/1-36.