Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/2-11 | strony: 105–113

Jerzy Kubasik
Politechnika Poznańska
Wydział Elektroniki i Telekomunikacji
Katedra Sieci Telekomunikacyjnych i Komputerowych
e-mail: jerzy.kubasik@put.poznan.pl

Bitcoin i inne kryptowaluty – dokąd zmierzają?

Kod JEL: E42
Słowa kluczowe: waluty cyfrowe, kryptowaluty, efekty sieciowe
Streszczenie. W artykule przedstawiono współczesne zagadnienia w dziedzinie walut cyfrowych. Przeanalizowano czynniki ekonomiczne, które doprowadziły do powstania walut cyfrowych wskazując, że jest to naturalny krok w rozwoju środków płatniczych. Dokonano przeglądu głównych typów walut cyfrowych i omówiono wpływ ich konstrukcji na popularność poszczególnych walut. Opisano zwięźle konkurencję na rynku kryptowalut.

Wprowadzenie

W ostatnich latach, waluty cyfrowe stały się jednym z najszerzej omawianych zagadnień z pogranicza technologii i ekonomii. Niewątpliwie waluty cyfrowe mają duży potencjał i mogą znacząco zmienić przebieg transakcji i sposób funkcjonowania rynków. Mogą być postrzegane jako naturalny etap rozwoju realizacji wymiany gospodarczej oraz sposobu funkcjonowania rynków. Początkowo, waluty cyfrowe były uważane za próbę stworzenia środka płatniczego dla rynku cyfrowego zastępującego bardziej nieporęczne metody, takie jak płatności kartami kredytowymi. Obecnie potencjał walut cyfrowych jest znacznie większy dzięki ich możliwemu zastosowaniu w organizacji infrastruktury płatności, realizacji transakcji.

W artykule opisano pokrótce potrzeby ekonomiczne zaspokajane przez środki płatnicze oraz ich rozwój od najstarszych do dzisiejszej gotówki i walut cyfrowych. Rozwój jest nieunikniony i zwykle związany jest z postępem technologicznym. Przełomowe badania, które doprowadziły do powstania **Bitcoina** oraz typu baz danych określanych jako ***blockchain*** (łańcuch bloków) rozwiązały istniejący od dawna problem informatyczny. Wykorzystanie przez Bitcoin narzędzi kryptograficznych dało początek

określeniu „kryptowaluta", używanego obecnie w kontekście setek walut cyfrowych wykorzystujących podobne techniki. Omówiono zagadnienia popularyzacji techniki *blockchain*, szybkiego rozwoju innych kryptowalut oraz potrzeby ekonomiczne zaspokajane przez te nowe waluty.

Zaprezentowany krótki przegląd, ze względu na ograniczony rozmiar artykułu, jest jedynie wstępem do tych interesujących i jakże współczesnych zagadnień. Omówienie technicznych innowacji leżących u podstaw walut cyfrowych ograniczone jest do minimum, Nacisk został położony na ich aspekty ekonomiczne, potrzeby ekonomiczne, determinujące ich tworzenie i realizację oraz przyszłość[1].

1. Waluty cyfrowe jako etap rozwoju pieniądza

Pieniądz został wprowadzony, zastępując handel wymienny (barter) jako główny system wymiany dóbr. Bezpośrednia wymiana dóbr lub usług na inne dobra lub usługi zależy w bardzo dużym stopniu od podwójnej zbieżności zapotrzebowania – transakcja dochodzi do skutku w wyniku „spotkania" jednej strony, oferującego dobro pożądane przez drugą stronę i odwrotnie. Kluczowym problemem w handlu wymiennym jest to, że podwójna zbieżność zapotrzebowania nie zawsze występuje w tym samym czasie. Brak tej zbieżności może w praktyce zniweczyć transakcję albo rozdzielić w czasie oba kierunki przepływu dóbr na tyle, że oczekiwanie na odwdzięczenie się drugiej strony może narazić pierwszego kupca na ograniczenie lub nawet całkowitą utratę korzyści z takiej transakcji.

W grupach zbieracko-łowieckich problemom tego typu zaradzono wykorzystując zbiorową pamięć grupy. Pamięć zbiorowa służyła za handlową księgę główną (*ledger*), w której zapisywano wkład każdego członka, umożliwiając skorzystanie z oferty w bliżej nieokreślonym czasie. Mówiąc współczesnym językiem, stosowano wydłużony termin płatności.

Taki system sprawdzał się w małych grupach. Przy większej liczbie członków społeczności trudno śledzić wkład każdej jednostki i wykorzystanie zasobów grupy przez nią. Poza tym, w większych grupach partnerzy handlowi nie znają się, co utrudnia wyegzekwowanie zapłaty w przyszłości. Z tego powodu system pamięci zbiorowej nie sprawdza się także w przypadku wymiany handlowej pomiędzy odrębnymi grupami.

Z czasem pamięć zbiorowa została zastąpiona instytucją **pieniądza**. W celu ułatwienia handlu wspomniana księga główna, w której zapisywany jest wkład każdej ze stron (dotąd księga wirtualna, rejestr przechowywany w pamięci grupy) może zostać zmaterializowana i zdecentralizowana. Zaspokajając potrzeby innych, bilans sprzedawcy jest powiększany i reprezentowany przez obiekty przechodzące w posiadanie sprze-

[1] W celu zgłębienia zagadnień poruszanych w tym artykule warto skorzystać z książki *Beyond Bitcoin* (Halaburda, Sarvay, 2016), gdzie zostały one potraktowane szczegółowo.

dawcy, np. muszle, zastępowane później kawałkami metalu, które dziś znamy jako monety.

Na podstawie przedstawionych powyżej powszechnie znanych faktów można określić potrzeby ekonomiczne zaspokajane przez waluty cyfrowe i główne problemy techniczne z nimi związane. Potrzeba jest oczywista: realizacja transakcji na rynku cyfrowym. Zanim pojawiły się waluty cyfrowe, płatności przez internet można było dokonywać za pomocą kart kredytowych lub bardziej czasochłonnych i droższych, tradycyjnych metod, np. czeków lub przelewów bankowych. Wiąże się to jednak z ujawnieniem danych osobowych kupującego.

Idea wykorzystania cyfrowego odpowiednika gotówki była konsekwencją rozwoju rynku cyfrowego. Podstawowym problemem do rozwiązania były zagadnienia fałszerstwa albo inaczej kopiowania czy wielokrotnego wydatkowania. Możliwość utworzenia idealnych kopii cyfrowych oznacza, że waluty cyfrowe muszą polegać na czymś w rodzaju księgi głównej, w której zapisywana jest każda jednostka waluty oraz czy dany fakt jej zużycia (lub nie) przez danego posiadacza. Koncepcja ta została zastosowana na dwa sposoby:

1. Można polegać na instytucji zewnętrznej, która będzie prowadzić księgę główną, pilnując jej zapisów pod kątem zgodności z transakcjami i stanami kont użytkowników. Z biegiem czasu platformy internetowe – organizacje, które łączą dwie strony na rynku (sprzedających i kupujących) – wyemitowały sporo takich walut cyfrowych.
2. Można prowadzić księgę, nad którą żadna ze stron nie ma całkowitej kontroli, co na pierwszy rzut oka wydaje się niemożliwe. Problem ten stanowi wyzwanie dla kryptografów (Halaburda, Sarvay, 2016). Drugie rozwiązanie jest trudniejsze pod względem technicznym, ale współcześnie bardziej popularne, a przynajmniej lepiej znane.

2. Bitcoin i jego środowisko

Sytuacja uległa istotnej zmianie po publikacjach anonimowego autora występującego pod pseudonimem Satori Nakamoto (2008; 2009), który zaproponował rozwiązanie problemu podwójnego wydatkowania i opisał potrzebny do tego algorytm. Rozwiązanie to oparte było na idei rozproszonej bazy danych tworzącej łańcuch bloków (*blockchain*). W rozwiązaniu tym zdecentralizowana księga główna, oparta na narzędziach kryptograficznych, może być przekazywana pomiędzy stronami, pozwalając uczestnikom na sprawdzanie jej zawartości a jednocześnie uniemożliwiając wprowadzanie jednostronnych zmian. *Blockchain* zapisuje transakcje dokonane przy użyciu danej waluty i pozwala uczestnikom na weryfikację źródła każdej jej jednostki oraz uprawnień użytkownika do jej użycia. Jak już wspomniano, wykorzystanie narzędzi kryptograficznych w algorytmie walut cyfrowych spowodowało, że zarówno Bitcoin,

jak i kolejne, podobne, zdecentralizowane waluty cyfrowe są określane jako **kryptowaluty**.

Co ciekawe, motywacją do stworzenia tego algorytmu były argumenty ekonomiczne przedstawione wcześniej w artykule. Nakamoto (2008) potwierdza wysoki koszt wykorzystania tradycyjnych metod płatności (np. kart kredytowych) w transakcjach zawieranych przez internet i argumentuje, że są one przyczyną ograniczenia zakresu transakcji gospodarczych, które mogłyby być zawierane w sieci, np. mikropłatności (o wartości pojedynczych czy ułamków centów). Ponadto, algorytm umożliwia przeprowadzenie transakcji, które są rozliczane relatywnie szybko, aczkolwiek nie natychmiast.

Inną potrzebą ekonomiczną wspomnianą przez Nakamoto (2008) jest potrzeba prywatności. Była to bez wątpienia ważna kwestia dla pierwszych użytkowników Bitcoina. Pierwsze szerokie zastosowanie Bitcoina wykorzystano w szarej strefie – anonimowość, szybkość i niski koszt transakcji przyciągnęły użytkowników, którzy handlowali nielegalnymi substancjami przez internet[2]. W niektórych kręgach motywacją wykorzystania tej waluty nadal było to, że działa ona poza systemem rządowym. Na przykład, Bitcoin był używany w projekcie Wikileaks i w okresie kryzysów (np. w reakcji na referendum dotyczące Brexitu w 2016 r.), a także w przypadku obaw lub problemów użytkowników związanych z wykorzystaniem ich narodowych walut (np. w Argentynie lub Chinach), a ostatnio w związku z wycofaniem z obiegu niektórych banknotów w Indiach.

Dla niektórych użytkowników atrakcyjność Bitcoina polega na tym, że funkcjnuje on poza systemem bankowym i nie podlega nadzorowi banku centralnego, stanowiąc aktywo nieskorelowane. Podaż Bitcoina jest podyktowana przez algorytm, więc użytkownicy wiedzą dokładnie, ile obecnie wystawiono Bitcoinów i jak sytuacja zmieni się w przyszłości. Całkowita podaż Bitcoina podlega ograniczeniom – całkowita liczba bitmonet dąży do 21 mln a jego limit ma zostać osiągnięty około 2140 roku. Odzwierciedla to ideę zakładającą, że w momencie, kiedy kryptowaluta będzie w powszechnym użyciu, jej całkowita podaż będzie stała, żeby wykluczyć inflację czy jakiekolwiek ingerencję w walutę.

Konstrukcja waluty odpowiadała na niektóre potrzeby ekonomiczne wymienione w publikacji Nakamoto (2008), równocześnie proponując wiele zachęt, które ostatecznie stały się słabością tej kryptowaluty. Zachęty te mają związek z tzw. wydobywaniem (*mining*), czyli sposobem, w jaki algorytm Bitcoina zarządza zmianami w jego łańcuchu bloków.

W celu zapewnienia niezmienności łańcucha bloków, każdej nowej transakcji dodanej do łańcucha musi towarzyszyć dowód wykonanej pracy (*proof of work*), czyli weryfikowalne rozwiązanie problemu zgłoszonego przez system, ale wymagającego

[2] Przykładem może być Silk Road, internetowa platforma aukcyjna działająca w sieci Tor, zamknięta w 2013 r. przez organa ścigania USA.

dużej mocy obliczeniowej. Użytkownicy rozwiązujący ten problem określani są mianem „górników" i są opłacani nowo wygenerowanymi bitcoinami.

Czynnikami, zarówno technologicznymi, jak i związanymi z gospodarką, które można uznać za słabości systemu Bitcoina i które zaczęły sprzyjać powstawaniu i rozwojowi innych kryptowalut są:

1. Wydobywanie wymaga sporych nakładów energetycznych, zapewniających funkcjonowanie systemu Bitcoin, ale inspiruje do szukania bardziej energooszczędnych rozwiązań.
2. Wydobywanie jest działalnością konkurencyjną, opartą na zasadzie, że zwycięzca bierze wszystko – „górnik", który pierwszy rozwiąże dany problem, otrzymuje całą zapłatę przewidzianą dla tego problemu, natomiast inni „górnicy" nie dostają nic. Prowadzi to do, często niezdrowej, konkurencji wśród „górników", którzy muszą nieustannie inwestować w swoje systemy (najczęściej specjalny sprzęt dedykowany „górnikom" Bitcoina). Ten wyścig może być nieekonomiczny, a także zniekształcać skład społeczności „górniczej" w kierunku elit z najbardziej wydajnym sprzętem. Jedną z odpowiedzi „górników" na ten problem jest połączenie sił i utworzenie kolektywów określanych mianem „*mining pools*", które współpracują przy rozwiązaniu problemu a ewentualne wynagrodzenie dzielą pomiędzy swoich członków. Prowadzi to jednak do utraty decentralizacji i stwarza ryzyko, że w końcu dany „górnik" albo kolektyw stanie się na tyle potężny, żeby zagrozić integralności łańcucha bloków (co może nastąpić, jeżeli pojedynczy „górnik" skupi ponad połowę mocy obliczeniowej sieci).
3. Duża zmienność ceny bitcoinów (kursu wymiany z tradycyjnymi walutami) będąca konsekwencją ograniczonej podaży kryptowaluty nierównoważącej zmian w popycie, ale mogąca także wynikać ze spekulacji. Zniechęca to do stosowania bitcoina jako codziennej waluty wbrew intencji twórcy systemu.

3. Kryptowaluty inne niż Bitcoin

Wraz ze wzrostem popularności Bitcoina, jego słabości stały się bardziej widoczne. Otwarty algorytm Bitcoina został wykorzystany w kryptowalutach, które miały być pozbawione jego wad. Nowe monety (*altcoiny*) pojawiały się masowo, w transakcjach internetowych – ponad 700 kryptowalut[3] wymienialnych jedna na drugą (lub na tradycyjne waluty). Spora część z nich powstała na drodze kosmetycznych zmian wprowadzonych do algorytmu Bitcoina.

Jednym z pierwszych konkurentów Bitcoina był **Litecoin**, stworzony w październiku 2011 roku. W tym altcoinie uproszczono narzędzia kryptograficzne, co zmniejszy-

[3] Prawdopodobnie powstało ich więcej, ale nie zyskały wystarczającej popularności, żeby odegrać znaczącą rolę w handlu.

ło wymagania sprzętowe i pozwalało na przetwarzanie bloków co 2,5 minuty, wobec 10 minut w Bitcoinie. Wstrzymało to wyścig technologiczny wśród „górników", ale tylko na pewien czas. Niezmienione zostały zachęty dla „górników" i konkurencyjna natura wydobycia. Czterokrotnie zwiększono całkowitą podaż kryptowaluty, do 84 mln, co jednak nadal może nie zrównoważyć presji deflacyjnej, wynikającej z ograniczonej podaży.

Inne altcoiny, **Peercoin** i **Novacoin**, utworzone odpowiednio w 2012 i 2013 roku, proponują inne rozwiązanie problemu wydobywania. Zamiast polegać na dowodzie wykonanej pracy i wynikającej z niego konkurencyjności, waluty te stosują system *proof-of-stake*, w którym „górnicy" nagradzani są proporcjonalnie do ich udziału w walucie. Algorytm losowo wybiera „górnika" obecnego w sieci do pracy w kolejnym bloku w łańcuchu[4]. „Górnicy" nadal rozwiązują problemy obliczeniowe, mogą być znacznie łatwiejsze, wymagające mniejszej mocy obliczeniowej niż w przypadku Bitcoina. Co więcej, Peercoin i Novacoin uwzględniają możliwość stopniowego wzrostu podaży, co odróżnia je od Bitcoina lub Litecoina.

Niektóre altcoiny oferują większą anonimowość niż Bitcoin. Łańcuch bloków Bitcoina ujawnia stan posiadania i zawierane transakcje, aczkolwiek przypisanie ich do rzeczywistych użytkowników może być trudne. Na przykład **Darkcoin** (obecnie znany jako **Dash**), rozwiązał ten problem oddzielając transakcje od źródeł pochodzenia pieniędzy.

W Tabeli 1 przestawiono ranking kryptowalut o największej kapitalizacji rynkowej według stanu na koniec stycznia 2017 roku na podstawie danych publikowanych online w czasie rzeczywistym przez serwis Crypto-Currency Market Capitalizations (2017). Kapitalizacja całego rynku kryptowalut monitorowanego przez ten serwis sięga 18 mld USD, z czego około 85% przypada na Bitcoin, a kapitalizacja kolejnej na liście (Ethereum) jest ponad szesnastokrotnie niższa. Jedynie 24 kryptowaluty osiągnęły kapitalizację przekraczającą 10 mln USD każda.

[4] Stan posiadania monet przez „górników" wpływa na szanse ich wyboru.

Tabela 1. Lista kryptowalut (styczeń 2017)

Miejsce	Waluta	Symbol	Rok powstania	Kapitalizacja w mln USD
1	Bitcoin	BTC	2009	15 849
2	Ethereum	ETH	2015	953
3	Ripple	XRP	2013	243
4	Litecoin	LTC	2011	202
5	Monero	XMR	2014	185
6	Ethereum Classic	ETC	2015	119
7	Dash (d. Darkcoin)	DASH	2014	114
8	MaidSafeCoin	MAID	2014	60
9	NEM	XEM	2015	49
10	Augur	REP	2015	47
11	Steem	STEEM	2016	38
12	Iconomi	ICN	2016	37
13	Factom	FCT	2014	31
14	Tether	USDT		25
15	Waves	WAVES	2016	23
16	Dogecoin	DOGE	2013	23
17	Zcash	ZEC	2016	23
18	Golem	GNT	2016	21
19	DigixDAO	DGD	2016	20
20	Ardor	ARDR	2016	19
21	Lisk	LSK	2016	16
22	Stellar Lumens	XLM	2014	16
23	GameCredits	GAME	2014	16
24	BitShares	BTS	2014	10

Źródło: Crypto-Currency Market Capitalizations (2017).

4. Konkurencja wśród kryptowalut

Liczba obecnie istniejących kryptowalut skłania do postawienia pytań:

- czy wszystkie kryptowaluty przetrwają?
- czy jedna (lub zaledwie kilka) z nich zdominuje inne?

Liczba kryptowalut oraz fakt, że każda kolejna miała być lepsza niż poprzednie sprawia, że konkurencja jest bardzo silna. Na wielu rynkach wyższa jakość produktów czy usług daje szanse na powiększenie udziału lub przejęcie rynku od prekursorów oferujących niższą jakość. Niekoniecznie sprawdza się to w przypadku kryptowalut, ponieważ jest to rynek z efektem sieciowym.

Efekt sieciowy powstaje, kiedy produkt lub usługa stają się atrakcyjniejsze wraz ze wzrostem liczby ich użytkowników. Klasycznym przykładem efektu sieciowego jest sieć telefonii – od całkowitej bezużyteczności dla jedynego użytkownika do intensyw-

nego wzrostu wartości ze wzrostem liczby telefonów w sieci[5]. Podobnie jest z kryptowalutami. Początkowo twórca kryptowaluty jest jedyną stroną, która ją uznaje i akceptuje. Wraz z pojawianiem się kolejnych użytkowników, kryptowaluta staje się coraz bardziej atrakcyjna, a maksymalizacja zysków następuje, kiedy wszyscy używają tej samej kryptowaluty. Tym samym, nowy gracz na rynku kryptowalut może nie mieć „siły przebicia", jeśli jego sieć jest mniejsza niż sieci innych graczy. Znaczna różnica w jakości pomiędzy graczem nowym a starym może zrównoważyć rozbieżność w skali efektu sieciowego.

Problem ten empirycznie rozwiązują Gandal i Halaburda (2016), analizując kursy wymiany pomiędzy kryptowalutami jako oznaki konkurencji. Bitcoin, najstarsza i najszerzej uznawana kryptowaluta, weszła w tę konkurencję z silnym efektem sieciowym. Istniała opinia, że każda następna kryptowaluta jest skazana na porażkę. W próbie przebadanej w latach 2013–2014 widać okresy, w których Bitcoin rzeczywiście zyskiwał kosztem innych kryptowalut, ale także okresy, w których zachodziła sytuacja odwrotna. Wcześniej badania wykazywały, że różne kryptowaluty rozwijają się w podobnym tempie, co wynikało z ogólnego wzrostu zainteresowania kryptowalutami, windującym ich ceny.

Po kwietniu 2014 roku, autorzy zaobserwowali okres czystej konkurencji pomiędzy Bitcoinem a altcoinami. Pod koniec badania Bitcoin pozostawał dominującą kryptowalutą. Altcoiny, które zostały ulepszone w stosunku do prekursora, nie zdobyły znacznego udziału rynkowego. Peercoin i Novacoin, dwa altcoiny oparte na systemie *proof-of-stake*, którego nie ma Bitcoin, pozostają stosunkowo mało znane. Litecoin stał się w miarę popularny, chociaż w jego przypadku poprawa jakości w porównaniu z Bitcoinem była mniejsza niż w przypadku Peercoina czy Novacoina. Wprowadzony wcześniej Litecoin miał pewną przewagę oraz możliwość zbudowania większej sieci przed pojawieniem się kolejnych graczy. Zdaniem autorów tego badania, popularność każdej kryptowaluty odzwierciedla w większym stopniu jej wiek niż jakość.

Podsumowanie

W artykule skupiono się na potrzebach ekonomicznych zaspokajanych przez waluty cyfrowe i ich roli na rynku, co pozwala na lepsze zrozumienie ich znaczenia oraz trafniejsze prognozy co do ich przyszłości.

Warto zwrócić uwagę na ciągły rozwój walut cyfrowych oraz technologii, na których są oparte. Pokazano jak słabości algorytmu Bitcoina (faktyczne bądź pozorne) stymulowały innowacyjność i konkurencyjność na rynku kryptowalut. Technika łańcucha bloków jest wykorzystywana w obszarach spoza walut. Na przykład, token znany

[5] W drugiej połowie XX w., w niektórych krajach (np. Belgia, Francja) stanowiło to podstawę do zróżnicowania wysokości abonamentu telefonicznego w zależności od liczby użytkowników w danej sieci lokalnej.

jako **Ripple**, uznawany niekiedy jako kryptowaluta, jest w rzeczywistości wykorzystywany wyłącznie jako system płatności i rozliczeń sieci Ripple. Inną ciekawą innowacją jest, ciągle rozwijająca się, platforma **Ethereum**, która wykorzystuje podobną technologię, żeby umożliwić pisanie inteligentnych kontraktów. Zgodnie z takim kontraktem, płatność może być zależna od aktywności lub jakości oferowanego produktu czy usługi. Jest to ciekawy obszar do obserwowania w przyszłości.

Bibliografia

Crypto-Currency Market Capitalizations (2017). Pobrano z: http://coinmarket cap.com/ (31.01.2017).

Gandal, N., Halaburda, H. (2016). Can we predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games*, *7* (3), 16. DOI:10.3390/g7030016.

Halaburda, H., Sarvary, M. (2016). *Beyond Bitcoin. The Economics of Digital Currencies*. Palgrave Macmillan US.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Pobrano z: bitcoin.org/bitcoin.pdf (10.01.2017).

Nakamoto, S. (2008). *Bitcoin P2P e-cash paper*. The Cryptography Mailing list at metzdowd.com, 31.10.2008.

BITCOIN AND OTHER CRYPTOCURRENCIES
WHERE ARE THEYGOING?

Keywords: digital currencies, cryptocurrencies, network effects

Summary. The article presents contemporary issues in the field of digital currency. It analyzes the economic factors that led to the exchange of digital indicating that it is a natural step in the development of means of payment. A review of the main types of digital currencies discusses the impact of their design on the popularity of individual currencies. It outlines the competition in the market of cryptocurrencies.

Translated by Jerzy Kubasik

Cytowanie

Kubasik, J. (2017). Bitcoin i inne kryptowaluty – dokąd zmierzają? *Ekonomiczne Problemy Usług, 1* (126/2), 105–113. DOI: 10.18276/epu.2017.126/2-11.