PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS nr 527 • 2018

ISSN 1899-3192
e-ISSN 2392-0041

Emil Ślązak
Szkoła Głowna Handlowa w Warszawie
e-mail: slazak@sgh.waw.pl

INNOWACYJNOŚĆ *BLOCKCHAIN* JAKO ROZPROSZONEGO REJESTRU DANYCH (DLT)

BLOCKCHAIN INNOVATION AS A DISTRIBUTED LEDGER TECHNOLOGY (DLT)

DOI: 10.15611/pn.2018.527.22
JEL Classification: G21, G23, G28

Streszczenie: Niniejszy artykuł ma na celu wykazanie przesłanek innowacyjności *blockchain* jako rodzaju rozproszonego rejestru danych, scharakteryzowanego poprzez pryzmat zasad jego funkcjonowania na rynku kryptowalut. Szczególne znaczenie w funkcjonowaniu *blockchain* przypisano wyeliminowaniu czasochłonnych procedur rozliczenia i rozrachunku polegających na rejestrowaniu zmian własności i transferze pieniądza poprzez dedykowane tym celom instytucje centralne. Tym samym w artykule wykazano, iż praktyczne zastosowanie *blockchain* na rynku kryptowalut pozwoliło na uzyskanie trwałej stabilności funkcjonowania systemu płatności i bezpieczeństwa transakcji dla anonimowanych uczestników przy znaczącej redukcji kosztów transakcyjnych. Wykazano także, iż innowacyjność *blockchain* wynika z szeregu przesłanek, które znacząco usprawniają elektroniczny obieg aktywów, z atutem bezspornego uwiarygodnienia praw własności na czele. Gwarantem bezpieczeństwa stron transakcji staje się rozproszony rejestr danych z wykorzystaniem technik kryptograficznych, a nie nadzór pośrednika i jakość stosowanych przez niego systemów zabezpieczeń centralnych rejestrów danych.

Słowa kluczowe: rejestr rozproszony, *blockchain*, innowacje finansowe.

Summary: The paper aims to demonstrate the premises of blockchain innovation as a kind of distributed data register. The special importance was attributed to the elimination of time-consuming settlement procedures involving multiple records of data and long transfer of money through dedicated central institutions. Thus, the article points out that the use of blockchain enables the lasting stability of direct payments system for anonymous participants with a significant reduction of transaction costs. The high level of security arises from distributed data register based on the cryptographic techniques to protect the data integration. As a consequence, the stable activity of the intermediary with central data register is due to be undermined.

Keywords: ditributed ledger technology, blockchain, financial innovation.

1. Wstęp

Wykorzystanie *blockchain* oznacza stworzenie zdecentralizowanego systemu wymiany danych opartego na powszechnym zaufaniu, chociaż żaden z uczestników systemu nie jest zobowiązany do dodatkowego poświadczania swojej wiarygodności. Innowacyjność *blockchain* opiera się na połączeniu kryptografii i zachęt do partycypacji w systemie zgodnie z założeniami teorii gier, w której uczestnicy transakcji wymiany aktywów i tzw. górnicy weryfikują prawdziwość i kompletność transakcji poprzez działania indywidualne, lecz wpływające na wzrost użyteczności całego systemu.

W odróżnieniu do aktualnych systemów transakcji z zaufaną stroną trzecią, która jako instytucja centralna (np. bank) poświadcza każdorazową zmianę praw własności i przechowuje aktualny rejestr danych, *blockchain* jest formą rozproszonego rejestru danych, który udostępnia dane o transakcjach każdemu użytkownikowi w danej sieci. Podstawowym wyróżnikiem *blockchain*, na tle innych rozproszonych baz danych, jest atrybut spójnego i wiarygodnego uwierzytelniania każdej transakcji poprzez zmianę praw własności pomiędzy anonimowymi użytkownikami, którzy kierują się odmiennymi motywacjami.

Celem niniejszego artykułu jest wykazanie przesłanek innowacyjności *blockchain* scharakteryzowanego poprzez pryzmat zasad jego funkcjonowania na rynku kryptowalut. Szczególne znaczenie w *blockchain* przypisano wyeliminowaniu czasochłonnych procedur rozliczenia i rozrachunku polegających na rejestrowaniu zmian wartości i transferze pieniądza poprzez dedykowane instytucje centralne.

Jako tezę główną przyjęto stwierdzenie, iż innowacyjność *blockchain* wynika z przesłanek radykalnego obniżenia kosztów transakcyjnych w dobie rozwoju gospodarki elektronicznej z atutem szybkiego i bezspornego uwiarygodnienia zmian praw własności nawet anonimowanych stron transakcji, przy pełnym zabezpieczeniu integralności danych.

2. *Blockchain* jako rozproszony rejestr danych (ang. *distributed ledger technology* – DLT)

Jako szczególny rodzaj technologii rejestru rozproszonego (DLT) *blockchain* umożliwia bezpieczną transakcję pomiędzy stronami z całkowitym wyłączeniem pośrednika, bez obciążania jednej ze stron transakcji pełnym ryzykiem rozliczenia i rozrachunku. Dodatkowo *blockchain* pozwala zweryfikować dane w sposób uniemożliwiający zakwestionowanie transakcji przez strony w warunku braku zaufanej strony trzeciej.

W konsekwencji rolę pośrednika z centralną bazą danych przejmuje rozproszony (tj. współdzielony) rejestr, w którym dane są w pełni replikowane pomiędzy użytkownikami. Poprawność danych jest uwierzytelniana przez społeczność użyt-

kowników danej sieci poprzez weryfikację zmian, a równocześnie dane te są w pełni dostępne dla każdego podmiotu. Innymi słowy, aktualny stan danych „widziany" przez każdego uczestnika współdzielonej bazy danych jest zgodny ze stanem danych „widzianych" przez wszystkich pozostałych uczestników. Ten atrybut *blockchain* gwarantuje, że wszyscy uczestnicy mają jednolity i spójny widok aktualnego stanu rozproszonej bazy danych. W takiej sytuacji każda manipulacja danymi przez pojedynczego lub grupę użytkowników (np. zmiana stanu własności) jest natychmiast wykrywana i odrzucona przez wszystkich uczestników. Oszust musi zmodyfikować dane na rachunku każdego użytkownika sieci rozproszonej, co jest procesem bardzo złożonym i wymagającym ogromnej mocy obliczeniowej [Huberman, Leshno, Moallemi 2017].

Zdolność uczestników sieci *blockchain* do samodzielnej i niezależnej weryfikacji integralności danych w ramach współużytkowanej bazy bez zaufanej stronie trzeciej jest jednym z głównych atutów innowacji *blockchain*. Uczestnicy systemu mogą zawierać transakcje w bezpośrednich transakcjach oraz uzyskiwać bieżący dostęp do aktualnych danych o transakcjach, których nikt nie może zakwestionować. Ponadto każdy uczestnik może dysponować prawem własności i indywidualnym dostępem do swoich pieniędzy, aktywów lub innych danych, które są chronione kryptograficznie. W systemie zabezpieczeń *blockchain* nie jest wykorzystany standardowy login i hasło, lecz uwierzytelnienie silne, tj. algorytm asymetryczny na wzór organizacji podpisu elektronicznego. Oznacza to, że właściciel ma pełną kontrolę nad własnymi aktywami czy danymi, których nie może sam przenieść czy modyfikować bez autoryzacji społeczności, tj. podejmowania szeregu świadomych działań zapisanych w systemie [Nakamoto 2008].

Rozproszony rejestr danych w ramach *blockchain* tworzy nową jakość w zakresie standardów bezpieczeństwa transakcji. Ataki hakerskie są zazwyczaj wymierzone w dane przechowywane w bazach centralnych pośredników, którzy pełnią rolę instytucji zaufania publicznego (takich jak banki). W przypadku *blockchain* dla najmniejszej zmiany danych wymagana jest równoczesna zmiana w ich kopiach zlokalizowanych we wszystkich węzłach sieci (tzw. nody). Ze względu na dużą liczbę węzłów (liczoną w milionach) i niezbędną szybkość realizacji takiej manipulacji działanie takie aktualnie pozostaje poza możliwościami mocy procesorów[1].

Dzięki rozproszonemu uwierzytelnieniu transferowanych aktywów *blockchain* ma potencjał radykalnego obniżenia kosztów transakcyjnych w dobie społeczeństwa informacyjnego przy zagwarantowaniu pełnych praw własności. Gwarantem bezpieczeństwa staje się zabezpieczenie kryptograficzne, a nie stabilność pośrednika i jakość zabezpieczania przechowanych przez niego danych zlokalizowanych w centralnym rejestrze danych.

[1] Stan ten może się zmienić w przypadku urzeczywistnienia się koncepcji komputerów kwantowych.

3. Zasady funkcjonowania *blockchain*

Poszczególni użytkownicy *blockchain* wykorzystują indywidualny adres (portfel) o zweryfikowanej lub niezweryfikowanej tożsamości (w zależności od rodzaju *blockchain*), gdzie są przechowywane społecznościowo zweryfikowane aktywa lub/i dane. Każda zamiana stanu aktywów lub danych w wyniku transakcji (np. płatniczej, sprzedaży, kupna aktywów) jest odzwierciedlana w chronionym kryptograficznie bloku danych, który po autoryzacji jest rozsyłany do wszystkich adresów (portfeli) i tam jest równocześnie archiwizowany. W konsekwencji wszystkie transakcje z udziałem danego adresu (portfela) są odzwierciedlone w blokach, które są zapisywane na adresach (portfelach) u każdego z użytkowników. W przypadku obrotu kryptowalutami jak bitcoin, typowy blok zawiera dane o dwustu – trzystu transakcjach.

Każdy z użytkowników systemu *blockchain* ma przypisanych do adresu (portfela) parę komplementarnych kluczy, które służą do przekształcenia kryptograficznego danych, opisanego unikalnym i ściśle określonym schematem (algorytmem). Para przypisanych do adresu (portfela) kluczy obejmuje [Hileman, Rauchs 2017]:

- klucz prywatny,
- klucz publiczny.

Klucz prywatny stanowi narzędzie do bezsprzecznego potwierdzenia własności do danego adresu (portfela) i służy do inicjonowania transferu danych/aktywów przechowywanych na danym adresie (portfelu). Klucz ten ma ściśle poufny charakter i musi być wykorzystywany wyłącznie przez właściciela adresu (portfela). Tym samym ujawnienie klucza prywatnego grozi utratą własności adresu (portfela), co umożliwia kradzież tożsamości, a więc inicjowanie transakcji z danego adresu (portfela) w imieniu właściciela, lecz bez jego wiedzy. Natomiast klucz publiczny służy wyłącznie do potwierdzania własności danego adresu (portfela) i jest ogólnie dostępny dla każdego uczestnika systemu. Jednakże za pomocą klucza publicznego nie można inicjować transferu z danego adresu (portfela).

Aby zrealizować transakcje pomiędzy stronami (np. sprzedawca bitcoina X na rzecz kupującego Y), podmiot X wykorzystuje przekształcenie kryptograficzne danych transakcyjnych zawarte na swoim kluczu prywatnym (klucz prywatny X) z pobraniem klucza publicznego beneficjenta transakcji (tj. klucz publiczny Y). Klucz prywatny X służy do inicjowania transakcji na rzecz ściśle określonego podmiotu zidentyfikowanego przez klucz publiczny Y. Przekształcenie z wykorzystaniem kluczy nie obejmuje wszystkich danych zawartych w bloku, lecz dla przyspieszenia procesu wykorzystywany jest reprezentatywny znacznik bloku, tzw. funkcja skrótu (ang. *hash*).

Funkcja skrótu (ang. *hash algorithm*) ma kilka charakterystycznych atrybutów:

- ma charakter jednokierunkowy – na podstawie skrótu nie można odtworzyć danych w bloku, które reprezentuje skrót, a więc stosunkowo łatwo jest wygenerować skrót na podstawie danych wejściowych, ale odgadnięcie danych wejścio-

wych bloku na podstawie znajomości tylko skrótu jest zadaniem praktycznie niemożliwym ze względu na ogromną liczbę możliwych kombinacji;
- zamienia dowolnie duży zbiór danych w bloku w quasi-losową wartość o stałej długości (np. w przypadku algorytmu SHA 256 skrót stanowi ciąg 256-bitowy);
- wartość skrótu zależy od całego zbioru danych wejściowych – najmniejsza zmiana oryginalnych danych wymaga wygenerowania nowego skrótu, co oznacza brak praktycznej możliwości wygenerowania dwóch takich samych skrótów na różnych zbiorach danych wejściowych.

Skrót bloku dla danej transakcji (ang. *block hash*) jest generowany z uwzględnieniem trzech elementów, na które składa się:

1) tzw. korzeń skrótów (ang. *root hash*) bieżącego bloku, tj. skrót wyliczony na podstawie drzewa skrótów wszystkich transakcji w bieżącym bloku,
2) *hash* poprzedniego bloku,
3) unikalny 32-bitowy znacznik zmienny w czasie (ang. *nounce*) o określonej liczbie zer na początku.

Wyliczenie poprawnej wartości skrótu bloku dla danej transakcji z uwzględnieniem ściśle określonego *nounce* jest elementem uwierzytelniania transakcji przez innych użytkowników sieci dysponujących odpowiednią mocą obliczeniową (tzw. górników). Zadanie kryptograficzne, tj. określenie *nounce* dla skrótu bloku danej transakcji, jest rozsyłane do wszystkich węzłów sieci (tzw. nodów). Górnicy, po samodzielnym zweryfikowaniu, czy podmiot X rzeczywiście posiada odpowiednią ilość aktywów niezbędną do realizacji transakcji (tj. poprzez pobranie klucza publicznego podmiotu X i weryfikacji danych zapisanych w historycznych blokach transakcji – średnio 20 razy w przypadku bitcoin), zaczynają konkurować między sobą, tak aby jako pierwszy obliczyć poprawną wartość *nounce* (tj. unikalną z wielu możliwych wartości), która jako jedyna pasuje do skrótu bloku [Hileman, Rauchs 2017].

W praktyce oznacza to proces generowania wielu różnych wersji *nounce* i dopasowywanie ich do skrótu dla sprawdzenia, czy można uzyskać zgodną całość. Dla osiągnięcia sukcesu i rozwiązania zadania kryptograficznego należy zaangażować jak największą moc obliczeniową komputerów. Z tego względu, o ile kiedyś każdy posiadacz bitcoina mógł być górnikiem, o tyle obecnie w praktyce występuje zaawansowana specjalizacja górników, którzy wykorzystują nieraz tysiące urządzeń z kilkoma płytami głównymi wyposażonych w kilkanaście procesorów ASCI, tzw. koparek.

Pierwszy górnik, który zidentyfikuje poprawny *nounce* i dopasuje go do skrótu bloku danej transakcji (czynność ta określona jest jako *proof of work*), otrzymuje nagrodę w postaci nowej liczby danej kryptowaluty doliczonej do jego stanu posiadania (np. bitcoiny). Każdy z górników w węźle sieci może szybko sprawdzić, czy w rzeczywistości wyliczony *nounce* jest zgodny z wymaganiami systemu, co kończy autoryzację, a tym samym finalizuje transfer aktywów od podmiotu X do podmiotu Y. Dodatkowo zwycięski węzeł sieci, tj. górnik, otrzymuje prowizję, którą płaci podmiot X za autoryzowanie transakcji. Im wyższa prowizja, tym szybciej transakcja

może być zautoryzowana, gdyż górnicy nadają jej większy priorytet w poszukiwaniu *nounce* (tzw. proces kopania).

Protokół *blockchain* może regulować szybkość rozwiązywania kryptograficznych zagadek przez górników. Przykładowo w przypadku *blockchain* w systemie bitcoin transakcja weryfikacji zajmuje do 10 min. Opóźnienie jest celowe, gdyż uniemożliwia bardzo szybkie wykorzystanie aktywów (czyli kryptowalut) w różnych transakcjach równocześnie (tzw. *double spending*) i pozwala na wielokrotne sprawdzenie stanu posiadania przez społeczność.

Poprzez skrót bloku danej transakcji bieżący blok transakcji jest automatycznie powiązany z poprzednim blokiem, a ten ze swoim poprzednikiem. Całość tworzy łańcuch bloków (ang. *blockchain*), które w sumie obrazują historię transakcji na danym adresie (portfelu). Łańcuch jest stale aktualizowany w procesie dodawania nowych bloków, a dane są rozesłane i przechowywane na adresach wszystkich uczestników sieci. Stanowi to podstawę dla publicznego potwierdzenia (i udowodnienia), ile jednostek danego aktywa (kryptowaluty) jest przypisanych do danego adresu (portfela).

Ze względu na zasady dostępu do systemu i przypisane funkcje można wyróżnić różne rodzaje *blockchain*, który może przyjąć status rejestru [Kisiel 2017]:

- otwartego (ang. *permissionless public ledgers*), który umożliwia dostęp do rozproszonej sieci danych dowolnemu (niezweryfikowanemu) użytkownikowi, przy czym każdy z użytkowników może zawierać transakcje lub/i weryfikować nowe zestawy danych. Systemy publiczne mają wielu anonimowanych walidatorów transakcji (tj. górników). Przykład: kryptowaluty bitcoin, ethereum;
- zamkniętego (ang. *permissioned private ledgers*), wykorzystywany przez społeczność użytkowników, którzy uprzednio przejdą proces dopuszczenia do sieci (tj. identyfikacji), a więc muszą charakteryzować się ściśle określonymi atrybutami (np. instytucje finansowe, agendy rządowe) i którzy zachowują kontrolę nad akceptacją nowych użytkowników i autoryzują walidatorów transakcji (jednego lub kilka). Przykład: bankchain;
- mieszanego (ang. *permissioned public ledgers*), który funkcjonuje w oparciu o rozróżnienie kompetencji użytkowników w zakresie pełnionych funkcji z zastrzeżeniem funkcji weryfikowania transakcji (tj. górników) dla ściśle określonego kręgu podmiotów. Przykład: kryptowaluta ripple.

W przypadku sieci otwartych adres nie jest zidentyfikowany poprzez dane osobowe użytkownika, co zapewnia pełną anonimowość. W każdym rodzaju *blockchain* strony danej transakcji (zidentyfikowanej lub nie) nie mogą się jej wyprzeć, gdyż zarówno obecna, jak i poprzednie transakcje są widoczne publicznie w postaci zabezpieczonych kryptograficznie bloków zawierających transakcje w łańcuchu bloków (ang. *chain of block*). Zmiana zawartości bloku wymagałaby zmiany wszystkich zapisów w sieci w bloku danej transakcji, jak i w integralnie powiązanych blokach wcześniejszych transakcji. W innym przypadku nie ma możliwości wyliczenia skrótu, a więc autoryzacji nowej transakcji.

4. Innowacyjność *blockchain*

Blockchain ma potencjał radykalnego obniżenia kosztów transakcyjnych w dobie rozwoju gospodarki opartej na elektronicznym obiegu dokumentów z niewątpliwym atutem natychmiastowego uwierzytelniania praw własności. Gwarantem bezpieczeństwa staje się rozproszony rejestr danych z wykorzystaniem kryptograficznych technik ochrony kompletności danych, a nie stabilność pośrednika i jakość stosowanych przez niego systemów zabezpieczeń centralnego rejestru danych. Nie jest to jednak jedyna przesłanka wskazująca, że *blockchain* należy do rodzaju radykalnej innowacji (tab. 1).

Tabela 1. Przesłanki innowacyjności *blockchain*

Przesłanka	Charakterystyka
Decentralizacja	System wykorzystuje w pełni zdecentralizowany system serwerów połączonych poprzez węzły (*nods*) bez centralnej jednostki zarządzającej (dezintermediacja)
Swobodny dostęp	W modelu otwartym *blockchain* każdy uczestnik może dodawać bloki i weryfikować nowe transakcje
Brak licencji	Technologia *blockchain* nie jest chroniona prawem patentowym – bezpłatna dla każdego uczestnika systemu z uniwersalnym zastosowaniem
Zaufanie stron	Automatyczny system tworzenia wzajemnego zaufania w transferze danych w oparciu o unikalne adresy użytkowników
Redundancja danych	Rejestr danych *blockchain* jest duplikowany na serwerach na całym świecie, co oznacza wysoką odporność na ryzyko stabilności i bezpieczeństwa centralnej bazy danych
Brak pośredników	Brak zaufanej strony trzeciej do przetwarzania transakcji i kosztów transakcyjnych związanych z ich obecnością
Zarządzanie anonimowością	*Blockchain* pozwala wymieniać zdematerializowane aktywa i dane na różnych poziomach anonimowości w zależności od rodzaju
Działanie on-line	Bloki z transakcjami są dodawane i weryfikowane z max. 10 min opóźnieniem – ograniczenie ryzyka arbitrażu danych i braku aktualności
Bezpieczeństwo	Wykorzystanie algorytmu asymetrycznego, który zapewnia silne uwierzytelnienie danych
E-rejestr	*Blockchain* utrzymuje pełne atrybuty własności aktywów, umów i danych w postaci całkowicie zdematerializowanej

Źródło: opracowanie własne.

Decentralizacja, jako atrybut *blockchain*, oznacza diametralną zmianę organizacji transferu danych w kierunku w pełni rozproszonych serwerów połączonych poprzez węzły (*nods*) bez wyróżnienia centralnej jednostki zarządzającej (dezintermediacja). Dzięki temu nowa technologia może znacząco przyspieszyć procesy zawierania transakcji na rynkach finansowych i zdynamizować procesy gospodarcze. Tym bardziej, że transakcje w *blockchain* mają charakter zbliżony do natych-

miastowego – bez znaczących opóźnień znamiennych dla aktualnych standardów procesów rozliczenia i rozrachunku.

Ważną przesłanką innowacyjności *blockchain* jest automatyczny system tworzenia środowiska wzajemnego zaufania stron w transferze danych i aktywów poprzez możliwość zdefiniowania określonych warunków niezbędnych do zautoryzowania danych, tzw. inteligentne kontrakty (ang. *smart contracts*). Kontrakty te pozwalają zapisać w danych bloku transakcji wymagania określone przez strony transakcji, które w ten sposób zabezpieczają swoje interesy, a tym samym ograniczają ryzyko niedotrzymania ustaleń umownych (np. zdefiniowanie warunków dostarczenia określonych dokumentów niezbędnych do aktu własności towaru i możliwość odbioru dokumentów po uiszczeniu zapłaty). W momencie spełnienia określonych warunków przez jedną ze stron (np. odpowiednie dokumenty) zobowiązanie drugiej strony jest wykonywane automatycznie (np. płatność) poprzez zapisanie uwarunkowanych decyzji w kodzie programistycznym inteligentnych kontraktów.

Ważnym atutem jest elastyczność konfiguracji *blockchain* w zależności od potrzeb uczestników. Przykładowo w modelu otwartym *blockchain* (wykorzystywanym na rynku kryptowalut) każdy uczestnik może dodawać bloki i uwierzytelniać nowe transakcje, czerpiąc z tego tytułu dodatkowe korzyści finansowe. Natomiast w modelu zamkniętym organizacja rozproszonej bazy danych znajduje się pod pełną kontrolą organizatora bazy, który jednak nie ma możliwości zmiany samych danych. Warto podkreślić, iż w odróżnieniu do szeregu innowacji o charakterze przełomowym technologia *blockchain* nie jest chroniona prawem patentowym, przez co jej wykorzystanie jest bezpłatne dla każdego uczestnika systemu. Fakt ten sprzyja prowadzeniu prac o charakterze rozwojowym i aplikacyjnym na całym świecie (bez względu na zasoby finansowe), przyczyniając się do bardzo szybkiego postępu technologicznego w tworzeniu rozproszonych baz danych.

Blockchain bardzo dobrze wpisuje się w trend digitalizacji obrotu gospodarczego, gdyż dane i aktywa są przechowywane wraz z pełnymi atrybutami poświadczenia własności w postaci całkowicie zdematerializowanej, prowadząc do znaczącego obniżenia kosztów transakcyjnych, a następnie kosztów stałych związanych z przechowywaniem nośników transakcji w wersji papierowej. Rejestry *blockchain* mogą obejmować tytuły własności gruntów, kredyty, tożsamość, listy przewozowe i inne elementy życia gospodarczego.

Blockchain sprzyja wdrażaniu rozwiązań bardziej przyjaznych użytkownikom z wykorzystaniem atutów technologii cyfrowych ze względu na przejrzystość i rozliczalność w całym łańcuchu dostaw. Dzięki technologii *blockchain* można śledzić dane i ustalać ich źródło, dowodzić autentyczności i pochodzenia, zapobiegać wycofaniu produktów i przyspieszać przepływ towarów.

W przypadku instytucji publicznych *blockchain* może stanowić fundament oficjalnego rejestr zasobów publicznych i obywateli, takich jak budynki, domy, pojazdy i patenty. Łańcuchy bloków mogłyby też ułatwić masowe rozsyłanie powiadomień (tzw. trwały nośnik), umożliwiać zdalne wybory, ograniczyć oszustwa poprzez sys-

tem nadzoru nad danymi i usprawnić działalność administracji państwowej w zakresie wydawania pozwoleń i decyzji urzędowych.

5. Zakończenie

Innowacyjność technologii *blockchain* opiera się na stworzeniu stabilnego systemu wymiany danych pod nieobecność instytucji zarządzającej. Protokół określa reguły systemu, które obowiązują wszystkich uczestników. Infrastruktura składa się z serwerów komputerowych, poprzez które działają tzw. górnicy, którzy wchodzą i opuszczają system zgodnie ze swoją wolą, tj. reagując na postrzegane możliwości zysku. Uczestnicy postępują zgodnie z protokołem *blockchain*, ponieważ leży to w ich najlepszym interesie, mając pewność, że pozostali uczestnicy też muszą przestrzegać protokołu.

Na przykładzie rynku kryptowalut można wskazać, że konstrukcja technologii *blockchain* oznacza ekonomiczną innowację opartą na zasadach teorii gier. W przeciwieństwie do innych systemów płatności, rynek kryptowalut funkcjonuje jako ekosystem płatności z ustalonymi sztywno regułami, które są określone przez protokoły kryptograficzne. Żaden uczestnik nie ma uprawnień do ustalania lub modyfikowania opłat lub zasad postępowania lub w inny sposób kontrolowania systemu. Równocześnie każdy uczestnik rynku, zarówno użytkownicy, jak i tzw. górnicy, jako cenobiorcy realizują indywidualne korzyści, bez obecności instytucji centralnej, która pobierałaby opłaty monopolistyczne i w ten sposób zwiększała koszty transakcyjne.

Literatura

Bashir I., *Mastering Blockchain*. *Distributed ledger technology, decentralization, and smart contracts explained*, 2nd Edition, Packt Publishing Ltd, 2017.

Crosby M., Pattanayak P., Verma S., Kalyanaraman V., *Blockchain technology: Beyond bitcoin*, Applied Innovation Review, issue no 2/2016.

Hileman G., Rauchs M., *Global Blockchain Benchmarking Study*, Cambridge Centre for Alternative Finance, 2017.

Huberman G., Leshno J.D., Moallemi C.C., *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, CEPR Discussion Paper, No. 12322/2017.

Nakamoto S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, working paper.

Nowakowski W., 2014, *Kryptografia współczesna, zagadnienia wybrane*, Instytut Maszyn Matematycznych, Warszawa.

Kisiel M., 2017, *Co to jest blockchain i kto powinien się go obawiać*?, Bankier, 21.11.

Swan M., 2015, *Blockchain: Blueprint for a new* economy, O'Reilly Media, Inc.

Tapscott D., Tapscott A., 2016, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, Penguin.

https://chrispacia.wordpress.com (dostęp: 13.02.2018).