Mgr Karol Hermanowski
Zakład Prawa Policyjnego
Wydział Prawa i Administracji Uniwersytetu Rzeszowskiego

Bitcoin jako innowacyjna kryptowaluta oparta na technologii blockchain

Streszczenie:
We współczesnym świecie, w konsekwencji postępu technologicznego i dzięki pojawiającym się innowacjom, których jesteśmy świadkami, otwierają się sprawniejsze powiązania świata rzeczywistego ze światem wirtualnym. Niewątpliwie innowacją są nie tylko same kryptowaluty, ale novum stanowi sam system w oparciu o który one funkcjonują. Przedmiotem niniejszego artykułu jest przybliżenie istoty funkcjonowania bitcoina, sposobów jego uzyskiwania oraz innowacyjnej technologii blockchain na podstawie której działają kryptowaluty.
Słowa kluczowe: innowacje, kryptowaluty, bitcoin, blockchain.

Bitcoin as an innovative currency based on the blockchain technology

Abstract:
In the contemporary world, as a consequence of the technological developments and thanks to innovations that we may witness, the new connections between real and virtual world open. Certainly not only crypto-currency is a novelty, but the whole system on the basis of which it operates. This paper discusses the issue of bitcoin operating, methods of and the innovative technology blockchain on the basis of which the crypto-currency act.
Key words: innovations, crypto-currency, bitcoin, blockchain**.**

I. Wstęp

We współczesnym świecie, w konsekwencji postępu technologicznego i dzięki pojawiającym się innowacją, których jesteśmy świadkami, otwierają się sprawniejsze powiązania świata rzeczywistego ze światem wirtualnym. Innowacją są nie tylko same kryptowaluty, ale przede wszystkim technologia w oparciu o który one funkcjonują. Stworzenie łańcucha bloków, których nikt nie jest w stanie zmienić, a do których dostęp ma każdy może w najbliższym czasie zrewolucjonizować nie tylko działalność rynków finansowych, ale również być wykorzystane w działalności organów państwowych czy

administracji samorządowej. Technologia zabezpieczania przeprowadzanych transakcji oraz danych a także mechanizmy zaawansowanej kryptografii dające wysoki poziom bezpieczeństwa, zastosowane przy kryptowalutach stają się coraz bardziej popularne i użyteczne także w innych obszarach życia.

Przedmiotem niniejszego artykułu jest przybliżenie istoty funkcjonowania bitcoina, sposobów jego uzyskiwania oraz innowacyjnej technologii blockchain na podstawie której działają kryptowaluty. W artykule przedstawiono możliwości wykorzystania technologii blockchain w działalności organów administracji publicznej, a także zastosowania w innych obszarach funkcjonowania państwa.

II. Innowacje

Termin innowacja pochodzi od łacińskiego słowa „innovatio" lub „"innovare", czyli odnowienie i oznacza odnowę, tworzenie czegoś nowego, rzecz nowo wprowadzoną, nowość, reformę[1]. Pojęcie innowacji w dalszym ciągu jest przedmiotem licznych dyskusji. Oddziałuje na to fakt, że pojęcie innowacji jest bardzo obszerne i wyraża zdarzenia o charakterze technicznym, organizacyjnym i finansowo-ekonomicznym[2]. Pojęcie to jest więc kategorią interdyscyplinarną, co sprawia, że nie jest ono jednolicie definiowane.

W literaturze spotkać można różne podejścia do innowacji. Jedno z nich przyjmuje, za innowacje rozwiązania, które stanowią absolutną i niezaprzeczalną nowość, drugie podejście natomiast wskazuje, że innowacje to rozwiązania, które są nowe dla przedmiotu w kontekście ich wcześniejszego modelu[3].

Pojęcie innowacji pojawiło się w literaturze ekonomicznej na początku XX wieku i zostało wprowadzone przez J. A. Schumpetera. Ten prekursor teorii innowacji uznał ją za katalizator wzrostu gospodarczego oraz jedno z najważniejszych źródeł bogactwa narodowego. Schumpeter pojmował innowację jako:

- wprowadzenie nowego towaru, z jakim konsumenci nie mieli jeszcze do czynienia, lub nowego gatunku jakiegoś towaru;

[1] R. Staniewski, M. W. Nowacki, Podejście innowacyjne w zarządzaniu, Warszawa 2010.
[2] K. Karpińska, A. Matel, A. Protasiewicz, Konsument w działalności innowacyjnej przedsiębiorstw, Polskie Towarzystwo Ekonomiczne, Białystok 2017, s. 9.
[3] I. Steinerowska–Streb, Innowacje w polskich mikroprzedsiębiorstwach, „Studia Ekonomiczne" Nr 183, Katowice 2014, s. 3.

- wprowadzenie nowej metody produkcji jeszcze praktycznie niewypróbowanej w danej dziedzinie przemysłu;
- otwarcie nowego rynku, czyli takiego, na którym dany rodzaj krajowego przemysłu uprzednio nie działał i to bez względu, czy rynek ten istniał wcześniej, czy też nie;
- zdobycie nowego źródła surowców lub półfabrykatów i to niezależnie od tego, czy źródło już istniało, czy tez musiało być dopiero stworzone;
- wprowadzenie nowej organizacji jakiegoś przemysłu[4].

Nie ma sformułowanej jednolitej definicji pojęcia innowacji, gdyż jest ona definiowana bardzo wąsko lub bardzo szeroko i wieloaspektowo, również w skali gospodarki światowej. Zakres innowacji w ujęciu postulowanym przez J. A. Schumpetera jest bardzo szeroki (sensu largo). Podobne podejście reprezentuje P.R. Whitfield, który określił innowacje jako ciąg skomplikowanych działań polegających na rozwiązywaniu problemów, w rezultacie czego powstaje kompleksowa i całkowicie opracowana nowość[5]. W wąskim znaczeniu (sensu stricto) innowacja stanowi „pomyślną ekonomicznie eksploatację pomysłu"[6]. W takim również znaczeniu przedstawia innowacje np. Ch. Freeman, który traktuje ją, jako „pierwsze handlowe zastosowanie nowego produktu bądź procesu"[7], czy też E. Mansfield, wskazując „pierwsze zastosowanie wynalazku" jako innowacje[8].

Na analogiczną różnorodność pojęć można się natknąć w literaturze polskiej i tak np. A. Pomykalski określa innowację jako wszelkie procesy badań i rozwoju, zmierzające do zastosowania i użytkowania ulepszonych rozwiązań w dziedzinie techniki, technologii i organizacji[9]. Z kolei W. Janasz i K. Kozioł dokonali podziału innowacji ze względu na ich nowość w zakresie: światowym, kraju lub działu przemysłu oraz w skali przedsiębiorstwa[10]. Według intensywności technologicznej i kapitałowej, wymienili innowacje „lekkie i ciężkie" o zaawansowanej technologii oraz „lekkie i ciężkie" o prostej technologii. Kolejnym kryterium podziału innowacji jest ich oryginalność – gdzie wyróżniono innowacje kreatywne i imitujące. Kreatywne, zwane również pionierskimi, mają swoje odzwierciedlenie w odkryciach i wynalazkach, co sprawia, że nabierają istotnego znaczenia. Z kolei innowacje imitacyjne to naśladownictwo i rozpowszechnianie istniejących już odkryć[11].

[4] J. Schumpeter, Teoria rozwoju gospodarczego, PWN, Warszawa 1960, s. 104.
[5] P.R. Whitfield, Innowacje w przemyśle, PWE, Warszawa 1979, s. 26.
[6] K. B. Matusiak (red.), Innowacje i transfer technologii – słownik pojęć, Warszawa 2005, s. 65.
[7] Ch. Freeman, Economics of Industrial Innovation, Frances Printer, London 1982, s. 7.
[8] E. Mansfield, Industrial Research and Technological Innovation, Norton, New York 1968, s. 83.
[9] A. Pomykalski, Zarządzanie innowacjami, PWN, Warszawa-Łódź 2001, s. 17.
[10] W. Janasz, K. Kozioł, Determinanty działalności innowacyjnej przedsiębiorstw, Polskie Towarzystwo Ekonomiczne, Warszawa 2007, s. 20.
[11] W. Spruch, Strategia postępu technicznego, Państwowe Wydawnictwo Naukowe, Warszawa 1976, s. 37.

Potocznie innowacja rozumiana jest jako coś nowego, innego od dotychczasowych rozwiązań, istniejącego stanu rzeczy[12]. Podkreśla się, że to właśnie nowość stanowi wyróżnik w stosunku do innych zmian. Innowacja innymi słowy to zmiana polegająca na wprowadzeniu czegoś jakościowo nowego w danej dziedzinie życia społecznego, a zwłaszcza w gospodarce[13].

Twórca kryptowaluty bitcoin połączył różne koncepcje, a ponadto wprowadził nowatorskie rozwiązania technologiczne w postaci łańcucha bloków funkcjonujących w ramach rozproszonego, publicznego rejestru transakcji. Stworzył on również nową koncepcję rozprzestrzeniania innowacji i utrzymywania funkcjonowania systemu opartego na działaniach zaangażowanej społeczności użytkowników. Stwierdzić należy, że analizowany w artykule system obsługujący płatności z własną jednostką wartości stanowi innowacje zarówno w wąskim, jak i szerokim znaczeniu. W wąskim ujęciu, innowacyjnym rozwiązaniem jest kryptowaluta, natomiast w szerszym innowacją jest bitcoin rozumiany jako system umożliwiający realizację płatności. System bitcoin nie wdraża zmian w sektor instytucji i narzędzi w działającym już rynku, gdyż w zasadzie nie opiera się on na tradycyjnej strukturze rynku finansowego. Rewolucyjność innowacji systemu bitcoin upatrywać należy w tym, że buduje on odrębny rynek, konsolidujący uczestników tego rynku z instytucjami działającymi w jego systemie[14]. Bez wątpienia technologia blockchain oraz działające w oparciu o nią kryptowaluty słusznie określane są innowacją.

III. Kryptowaluty

W aspekcie ekonomicznym oprócz rozwoju technologicznego i rozpowszechnienia sieci internetowej podatnym gruntem dla rozwoju alternatywnych form płatności są obserwowane w ostatnich latach zawirowania na rynkach finansowych i niepewność co do przyszłego kształtu systemu finansowego. Kryzys na rynkach finansowych podważył zaufanie ludzi do funkcjonującego systemu bankowego, zasad działania instytucji finansowych, kontroli i nadzoru sprawowanego przez odpowiednie organy, a przede wszystkim ograniczył ufność do pieniądza[15]. Zwiększony niepokój w stosunku do dotychczasowych reguł funkcjonowania systemu finansowego stanowił w konsekwencji podatne podłoże powstawania nowych środków nawiązywania relacji ekonomicznych. Jednym z tego

[12] Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1983, s. 39.
[13] G. Osbert-Pociecha, Innowacje – zagadnienia ogólne i definicyjne, [w:] Innowacje w biznesie, (red. nauk.) A. Styś, A. Dejnaka, Difin, Warszawa 2016, s. 17-18.
[14] Szerzej A. I. Piotrowska, Bitcoin. Płatnicze i inwestycyjne zastosowania kryptowaluty, Warszawa 2018, s. 45.
[15] Por. E. Chrabonszczewska, Bitcoin – nowa wirtualna globalna waluta?, „International Journal of Management and Economics" Nr 40, Warszawa 2013, s. 51.

przejawów jest pojawienie się i rozwój kryptowalut jako ewentualnej alternatywy dla tradycyjnych środków płatniczych oraz rozliczania zawieranych w gospodarce transakcji[16]. Pojawienie się kryptowalut stanowi początek nowej ery, w której zaawansowane możliwości technologiczne zmieniły spojrzenie na zasady funkcjonowania systemu finansowego i rozszerzyły pojmowanie kategorii pieniądza[17].

Kryptowaluta (ang. cryptocurrency) – czyli inaczej waluta kryptograficzna to pieniądz wirtualny bazujący na prawach i procedurach kryptografii[18]. Według D. Homy kryptowaluta, inaczej waluta cyfrowa jest to forma waluty oparta na prawach matematyki. Są one tworzone w procesie rozwiązywania problemów matematycznych związanych z kryptografią[19]. Z kolei według A. I. Piotrowskiej, kryptowaluta to jednostka wartości wyrażona w postaci zapisu cyfrowego, będąca formą waluty wirtualnej, funkcjonująca w ramach systemu informatycznego, opartego na kryptografii i wykorzystująca rozproszony rejestr transakcji. Określone w definicji cechy są wspólne dla wszystkich kryptowalut, mimo, że kryptowaluty nie stanowią jednolitej kategorii. Różnią się pod względem sposobu emisji, weryfikacji transakcji, czy też modelu uczestniczenia w systemie[20]. Do podstawowych cech kryptowalut należą:

- kryptowaluty są w pełni „zwirtualizowane" i w przeciwieństwie do walut tradycyjnych nie mają odpowiedników w postaci banknotów czy monet;
- całkowita decentralizacja emisji i wprowadzania jednostek do obrotu (działanie w sieci równoprawnych podmiotów);
- emisja danej kryptowaluty realizowana jest przez użytkowników w warunkach sieci P2P przez rozwiązywanie skomplikowanych równań matematycznych;
- niezależność od rządów i instytucji finansowych, czego przejawem jest brak nadzoru organów państwowych nad procesem emisji kryptowaluty i jej wykorzystaniem w obrocie gospodarczym;
- funkcjonowanie kryptowaluty oparte jest na zasadach kryptografii, a zaufanie w decydującej mierze na dowodzie kryptograficznym;
- brak pośredników przy dokonywaniu transakcji z wykorzystaniem kryptowaluty;

[16] S. Bala, T. Kopyściański, W. Srokosz, Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne, Wrocław 2016, s. 52.
[17] A. Piotrowska, Bitcoin a definicja i funkcje pieniądza, „Annales Universitatis Mariae Curie-Skłodowska", Sectio H, Oeconomia 2014, Vol. XLVIII, 3, s. 275.
[18] W. Nowakowski, Postęp w technologii systemów kryptowalutowych, „Elektronika" 2015, Nr 11, s. 105.
[19] D. Homa, Sekrety bitcoina i innych kryptowalut, HELION 2015, s. 21.
[20] A. I. Piotrowska, Bitcoin. Płatnicze i inwestycyjne zastosowania kryptowaluty, Warszawa 2018, s. 27.

- funkcjonowanie danej kryptowaluty w oparciu o aplikację open source zapewniającej jawność procesu powstawania danej kryptowaluty;
- anonimowość, co związane jest z faktem, że przy założeniu konta (portfela kryptowaluty) żadne dane osobiste nie są wymagane;
- transakcje są nieodwracalne[21].

Jak wskazuje G. Sobiecki kryptowaluty stanowią największą podgrupę tzw. walut alternatywnych (komplementarnych i substytucyjnych), mających na celu uzupełnienie lub zastąpienie istniejących systemów pieniężnych[22]. Według W. Srokosza, systemy kryptowalut stanowią największą innowację jaka miała miejsce na początku XXI wieku[23].

Ukoronowanie prób powstania kryptowalut zostało zrealizowane w 2008 roku, kiedy to niejaki Satoshi Nakamoto[24] opublikował drobiazgową koncepcję pierwszego na świecie łańcucha bloków, czyli publicznej, zdecentralizowanej bazy danych, której elementy rozproszone na tysiącach komputerów są synchronizowane w określonych odstępach czasu. Miała stanowić odporny na ataki rejestr transakcji umożliwiający wprowadzenie nowej waluty cyfrowej, którą Satoshi Nakamoto nazwał bitcoinem[25]. Został on wyemitowany w samym środku kryzysu finansowego w latach 2008 – 2009, przez co wskazuje się, że bitcoin zrodził się ze względu na coraz mniejsze zaufanie do tradycyjnego systemu finansowego oraz przez eliminację pośredników w celu obniżenia kosztów transakcji. Dzięki swojemu rozwojowi technologicznemu, pomagającemu w budowie bezpiecznego środka wymiany pomiędzy podmiotami w sieci miał stanowić ochronę przed atakami. Innowacje są czasem następstwem sytuacji, w której ludzie stają w obliczu problemu i próbują go za wszelką cenę rozwikłać. Innym razem innowacja pojawia się wtedy, gdy ktoś stawia przed sobą ideę godną wizjonera.

VI. Bitcoin i blockchain

Bitcoin został wymyślony w 2008 roku w wyniku publikacji artykułu Satoshiego Nakamoto „Bitcoin: A Peer-to-Peer Electronic Cash System”[26]. Połączył on kilka

[21] S. Bala, T. Kopyściański, W. Srokosz, Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne, Wrocław 2016, s. 76-77.
[22] G. Sobiecki, Regulowanie kryptowalut w Polsce i na świecie na przykładzie Bitcoina – status prawny i interpretacja ekonomiczna, „Problemy zarządzania” vol. 13, Nr 3 (54), t. 1 Warszawa 2015, s. 145.
[23] W. Srokosz, Publicznoprawne ograniczenia kryptowalut, [w:] Jednostka wobec działań administracji publicznej, (red.) E. Ura, E. Feret, S. Pieprzny, Rzeszów 2016, s. 602.
[24] Do tej pory nie wiadomo kto kryje się za tajemniczą postacią Satoshi Nakamoto, czy jest to jedna osoba, grupa osób, np. grupa genialnych informatyków, kryptografów.
[25] J. Pavlus, *Świat bitcoina*, „Świat Nauki” 2018, Nr. 2 (318), s.32.
[26] M. Szymankiewicz, Bitcoin wirtualna waluta internetu, HELION 2014, s. 23.

wcześniejszych wynalazków, aby zbudować w pełni zdecentralizowany system pieniędzy elektronicznych, który nie jest zależny od jednostki centralnej w zakresie emisji pieniędzy lub zatwierdzenia i walidacji transakcji[27]. Bitcoin jest pierwszą na świecie kryptowalutą, która znalazła się w powszechnym użyciu, wykorzystującą metody kryptograficzne w celu zapewnienia bezpieczeństwa. Jest kryptowalutą doskonalszą od pieniądza z którego korzystamy dotychczas, z tego względu, że mamy do czynienia z walutą zdecentralizowaną, nad która nie ma kontroli żaden podmiot, który byłby odpowiedzialny za jego emisję. Oznacza to, że nikt odgórnie nie zarządza tą strukturą, ponieważ całym kryptograficznym aparatem nadzoruje algorytm. To chociażby odróżnia go od klasycznych walut. Ilość została ograniczona przez jej twórcę (twórców) do 21 milionów. Może się to wydawać niewystarczającą liczbą, biorąc pod uwagę dzisiejsze zapotrzebowanie na waluty, jednak bitcoiny są podzielne. Jeden bitcoin dzieli się na podjednostki, które nazywa się, stosując łacińskie przedrostki skalujące, podobnie jak jednostki wielkości fizyczne w układzie SI. Np.

1 BTC = 1 bitcoin,

0,01 BTC = 1 cBTC – 1 bitcent,

0,001 BTC = 1 mBTC – 1 milibitcoin (milibit),

0,000 001 BTC = 1 μBTC - 1 microbitcoin (mikrobit),

0,000 000 01 BTC = 1 satoshi (najmniejsza jednostka)[28].

System bitcoin umożliwił wyeliminowanie trzeciej strony zabezpieczającej transakcję, jak i jednostki centralnej odpowiedzialnej za emisję kryptowaluty. Stało się tak poprzez oparcie funkcjonowania systemu na rozproszonym modelu komunikacji (open-source), a dokładniej na sieci równoprawnych podmiotów (P2P[29])[30]. Użytkownicy przeprowadzają transakcje finansowe bezpośrednio między sobą, bez udziału innych podmiotów pośredniczących. Zrealizowane transakcje są zapisywane w publicznej księdze rachunkowej przechowywanej w postaci łańcucha bloków.

Niektóre przełomy są kwestią zbiegu okoliczności, pojawienia się innowacyjnego pomysłu równolegle z technologią potrzebną do jego realizacji[31]. Pierwszoplanową materią dla funkcjonowania systemu bitcoin jest sposób powstawania jednostek kryptowaluty. Działanie kryptowalut oparte jest na technologii blockchain. Technologia ta umożliwia przechowywanie danych w rozproszony, zdecentralizowany sposób. To zapobiega wyciekom

[27] A. M. Antonopoulos, Bitcoin dla zawansowanych, HELION 2018, s. 33.
[28] D. Homa, *Sekrety bitcoina i innych kryptowalut,* HELION 2015, s. 21.
[29] P2P – ang. pear to pear – równy z równy, sieć w której wszystkie węzły są równorzędne.
[30] A. I. Piotrowska, *Bitcoin.…*, s. 46.
[31] W. Isaacson, Innowatorzy, New York 2014, s. 61.

danych i umożliwia przeciwdziałanie manipulowaniu danymi, ponieważ wszelkie zmiany są od razu widoczne dla wszystkich podłączonych do danej sieci blockchain. Jest to rejestr, do którego dopisywana jest każda transakcja. Żeby tak się stało, musi zostać zaakceptowana przez tzw. „górników", czyli osoby zajmujące się wykopywaniem bitcoinów.

Potwierdzeniem płatności w sieci bitcoin zajmują się komputery o ogromnych mocach obliczeniowych. Proces ten polega na swoistej rywalizacji, który z komputerów jako pierwszy zautoryzuje konkretną transakcję[32]. Transakcje te są grupowane w blokach w celu ich weryfikacji, po czym bloki te są po kolei dołączane do łańcucha poprzednio zweryfikowanych bloków tworząc kompletny zapis wszystkich transakcji dokonanych w systemie od początku jego istnienia. Ten właśnie rejestr bloków to blockchain[33].

Satoshi Nakamoto porównał proces kreacji bitcoinów do kopania złota, a wiec kruszcu, z którego wykonywany był pieniądz[34]. Kopanie polega na dostarczaniu przez nich do sieci bitcoin mocy obliczeniowej, pozwalającej na jej funkcjonowanie. Wydatkiem wytworzenia bitcoina jest energia elektryczna zużywana przez procesor oraz koszt alternatywnej możliwości wykorzystania komputera. Zwiększenie rozmiaru sieci za pomocą nowych użytkowników zwiększa tempo niezależnej weryfikacji transakcji, w której są one wykonywane[35]. Kopaniem kryptowaluty nazywamy proces tworzenia nowych bloków wraz z doborem odpowiedniej funkcji skrótów. Znalezienie właściwej wartości funkcji skrótu wymaga pracy związanej z zaangażowaniem mocy obliczeniowej. Utworzenie nowego bloku wiąże się z powstaniem nowej wartości kryptowaluty, która jest zapłatą za znalezienie odpowiedniej wartości funkcji skrótu przypisanej rozwiązanemu blokowi. Nowo powstała wartość jest rezultatem kopania[36]. Kopanie, czy też wydobywanie to proces w którym węzły sieci kryptowaluty rywalizują ze sobą, starając się bezpiecznie dodać nowy blok z danymi transakcji do łańcucha bloków. Nagrodą za sukces przedsięwzięcia są jednostki kryptowaluty, stanowiące zachętę materialną za zapewnienie bezpieczeństwa. Kopanie polega na pobraniu ostatnich transakcji w celu ich weryfikacji, a następnie powtarzaniu prób rozwiązania trudnej zagadki matematycznej związanej z haszowaniem. Haszowanie (tworzenie skrótu) – to metoda kryptograficzna, która dzięki wykorzystaniu funkcji matematycznej dla pewnego zbioru danych generuje unikalny ciąg znaków alfanumerycznych o ustalonej długości tzw. skrót (wartość hash). W ten sposób otrzymuje się łatwy do sprawdzenia identyfikator cyfrowy

[32] A. Dobosz, Bitcoin – efemeryda czy solidna przyszłość, „Kwartalnik Naukowy Uczelni Vistula Vistula Scientific Quarterly, Nr 3 (41) Warszawa 2014, s. 22.
[33] W. Nowakowski, Technologie Bitcoin w Internecie Rzeczy (IoT)?, „Elektronika" 2015, Nr 10, s. 59.
[34] A. I. Piotrowska, Bitcoin…, s. 47.
[35] J. Przyłuska, *Wirtualny pieniądz*, „Gazeta Bankowa" 2012, Nr 5 (1133), s. 98.
[36] S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluty…*, s. 49.

danych poddanych haszowaniu. Zmiana lub uszkodzenie nawet jednego bitu danych wyjściowych drastycznie zmienia skrót, co bardzo ułatwia wykrycie błędów lub próby fałszerstwa[37]. Im większa moc obliczeniowa zostanie użyta, tym większa szansa sukcesu w procesie nazywanym dowodem wykonania pracy. Informacja o znalezieniu bloku rozsyłana jest następnie do wszystkich użytkowników sieci bitcoin. Blok zostaje zaakceptowany przez sieć, w przypadku potwierdzenia przez innych „górników" prawidłowości dowodu wykonanej pracy[38]. Leżąca u podstaw struktura danych, zwana łańcuchem bloków to nic innego, jak ciąg zaszyfrowanych bloków. Aby całość była niezawodna i bezpieczna, zawartość bloków można zmieniać po osiągnięciu konsensusu potwierdzonego za pomocą mechanizmów wymagających udziału ludzi i komputerów. W początkowym okresie funkcjonowania systemu „górnicy" byli w stanie wydobywać przy wykorzystaniu standardowych komputerów dziesiątki tysięcy bitcoinów w skali miesiąca[39]. Wraz z rozwojem sieci bitcoin, poprzez przyłączanie się do niej nowych użytkowników, wzrastała konkurencja ze strony innych „kopaczy", co systematycznie podnosiło również stopień trudności przy wydobyciu bitcoinów[40]. Bitcoin jest międzynarodowym środkiem płatniczym i łatwym instrumentem realizacji zobowiązań za towary i usługi, a ponadto stanowi przedmiot obrotu na giełdach. Zaletą bitcoina oprócz tego, że przy transakcjach międzynarodowych nie trzeba płacić prowizji bankom jest także możliwość przelewu środków w dowolne miejsce na świecie niezależnie od pory dnia do dowolnego posiadacza adresu bitcoin. Korzystanie z kryptowalut zapewnia szybkie dokonywanie transakcji oraz pozbawione jest generowania dodatkowych kosztów, związanych z prowizją, bądź kosztami przewalutowania.

W systemie bitcoina stosowana jest kryptografia klucza publicznego, nazywana również kryptografią asymetryczną. Wykorzystywane są w niej dwa rodzaje kluczy: publiczny – potrzebny do generowania adresu sieciowego, oraz prywatny – potrzebny do autoryzacji transakcji. Przy czym są one ze sobą matematycznie powiązane, stąd też zmiana klucza prywatnego nie jest możliwa[41]. Adresy nie zawierają żadnych informacji na temat właściciela. Jeżeli użytkownik kryptowaluty będzie chciał przekazać część swoich bitmonet, musi podać adres portfela, na którym tworzy się odpowiednie saldo. Transakcja nie zostaje „ogłoszona publicznie" dopóki nie zostanie dodana do utrzymywanej chronologicznie listy wszystkich transakcji (blockchain). Każdy użytkownik kryptowaluty bitcoin wykonuje

[37] J. Pavlus, Świat bitcoina, „Świat Nauki" 2018, Nr. 2 (318), s.32.
[38] R. Caetano, *Learning Bitcoin*, Pact Publishing, Birmingham 2015, s. 96.
[39] P. Vigna, M.J. Casey, *The Age of Cryptocurrency. How Bitcoin and the Blockchain Are Challenging the Global Economic Order*, Picador, New York 2016.
[40] A. I. Piotrowska, *Bitcoin.…*, s. 46.
[41] J. Szewczyk, *O cywilnoprawnych aspektach bitcoina*, „Monitor Prawniczy" 2018, Nr. 5, s. 243.

transakcję, która następnie jest potwierdzana kluczem prywatnym. Transakcją jest przesyłanie pewnej wartości pomiędzy adresami. Każda potwierdzona przez użytkownika bitmoneta jest zapisywana na saldzie w portfelu, a łańcuch bloków pomaga zweryfikować ilości bitmonet na koncie użytkownika. Spójność oraz ciąg chronologiczny tego łańcucha opiera się na dowodach wykonanych działań zwanych popularnie Proof of Work (PoW) aby zapobiec podwójnemu wydaniu środków czy fałszerstwu. Portfel na którym zapisywany jest stan bitmonet jest zabezpieczony kluczem prywatnym użytkownika, który jest przypisany do każdego adresu. Są to dane zaszyfrowane. Podpis jest istotną częścią w procesie przekazywania bitmonet ponieważ zapobiega modyfikacjom przez osoby trzecie. Takie zabezpieczenie w łańcuchu bloków zawiera przebieg wszystkich transakcji od adresu emitenta po aktualnego posiadacza, dlatego też niemożliwe staje się ponowne wydanie tej samej monety. Każda transakcja wykonywana pomiędzy użytkownikami jest potwierdzona przez sieć P2P w procesie wydobycia[42].

Do używania bitcoinów, wystarczy zainstalować na komputerze odpowiedni program albo skorzystać z usług portali, które pozwalają na utworzenie osobistego portfela bitcoin. Użytkownik posiada wspomniane wyżej dwa klucze: publiczny i prywatny. Adres portfela bitcoin generowany jest z klucza publicznego, a do autoryzacji transakcji wymagany jest klucz prywatny.

Technologia blockchain, wykorzystywana przede wszystkim jako zasadniczy element kryptowalut, znajduje zastosowanie także w sektorze publicznym.

Rozproszona sieć blockchain eliminuje do minimum możliwość utraty zawartych tam danych, spowodowanych np. przez awarię nośników danych, awarię zasilania czy sprzętu komputerowego, a także eliminuje ona konieczność sporządzania dokumentacji w formie papierowej[43].

System ten wykorzystała Estonia w swojej infrastrukturze publicznej, w której używa infrastrukturę klucza publicznego oraz blockchain. Do połączenia różnych rejestrów stworzono system X-road, który zabezpieczony jest m.in. za pomocą technologii blockchain. Estończycy mogą głosować online z dowolnego miejsca, cyfrowo podpisywać dokumenty, bezpiecznie wysyłać dokumenty, składać deklaracje podatkowe, otrzymywać zwroty podatków, dostać cyfrową receptę od lekarza, a część z tych rzeczy odbywa się zabezpieczając ww. rejestry przed niepowołanym dostępem za pomocą technologii

[42] Ł. Dopierała, A. Borodo, Znaczenie waluty kryptograficznej jako środka wymiany, „Współczesna Gospodarka" 2014, vol. 5 Issue 2, s. 2-3.
[43] R. Szyryngo, Technologia blockchain i jej wykorzystanie, https://bithub.pl/felietony/technologia-blockchain-wykorzystanie/ (stan na 29.07.2018r.).

blockchain. Dzięki wprowadzeniu tych systemów zmniejszyła się kwota wydatków przeznaczanych na sektor publiczny w tym kraju, a ponadto społeczeństwo ma łatwiejszy dostęp do usług społecznych i do opieki medycznej[44].

Rozwiązania wykorzystujące blockchain mogą być także wykorzystywane do pobierania przez państwo podatków od wynagrodzeń, a także w rozliczeniach VAT. Sfera podatków wydaje się być idealnym podłożem do wykorzystania pełnego potencjału blockchain. Z jednej strony, zapewnia możliwość dostarczania zweryfikowanych i poprawnych danych w pewny sposób. Z drugiej strony, organy podatkowe zyskałyby możliwość szybkiej i pewnej weryfikacji przesyłanych informacji[45]. Poszukując możliwości zwiększenia wydajności i zapewnienia zgodności z przepisami, organy podatkowe wykorzystują technologie cyfrowe do gromadzenia i analizowania danych, co ułatwia opracowanie niezawodnych rozwiązań i oprogramowania. Podatnicy również oczekują uproszczenia i przyspieszenia procesu rozliczania podatków. Ze względu na zdolność dostarczania w czasie realnym rzetelnych informacji z wielu poziomów do dużych grup odbiorców, na przykład w sferze podatków, i to w skali międzynarodowej, Blockchain jest bez wątpienia jedną z najbardziej obiecujących technologii[46].

W Szwajcarskim mieście Zug zostało przeprowadzone próbne głosowanie z użyciem technologii blockchain. Władze miasta zorganizowały dla mieszkańców w dniach 25 czerwca – 1 lipca 2018 roku testowe głosowanie w oparciu o technologię blockchain. Z racji, iż był to tylko test technologiczny, wyniki głosowania nie były wiążące dla władz miejskich. Obywatele, którzy wzięli udział w głosowaniu, mogli wypowiedzieć się w mniej ważnych sprawach lokalnych i odpowiedzieć na pytanie, czy system eID powinien zostać wykorzystany do głosowania w referendach w przyszłości. Mieszkańcy głosowali pod kątem tego, czy opowiadają się za fajerwerkami na corocznym festiwalu i czy uważają, że cyfrowe identyfikatory powinny być używane do wypożyczania książek z biblioteki lub płacenia za parking samochodowy[47].

Zjednoczone Emiraty Arabskie planują do roku 2020 od nowa zbudować i uruchomić w oparciu o technologię blockchain wszystkie systemy administracji publicznej.

[44] K. Piech, P. Zyga, Wykorzystanie blockchain przez rząd estoński, https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/wykorzystanie-blockchain-przez-rzad-estonski/ (stan na 29.07.2018r.).

[45] P. Barański, M. Bronowska, Blockchain a podatki, https://www2.deloitte.com/pl/pl/pages/podcasty/articles/Technologia-blockchain-i-jej-zastosowania.html (stan na 29.07.2018r.).

[46] https://www2.deloitte.com/pl/pl/pages/tax/articles/blockchain-technology.html (stan na 29.07.2018r.).

[47] https://bithub.pl/wiadomosci/szwajcarskie-miasto-zug-organizuje-probne-glosowanie-z-uzyciem-technologii-blockchain/ (stan na 29.07.2018r.).

Implementacja ta ma podnieść konkurencyjność gospodarki oraz przynieść gigantyczne oszczędności[48]. Wprowadzone zostanie wiele udogodnień opartych na automatyzacji np. cyfrowe paszporty, które zakończą erę manualnej weryfikacji dokumentów i być może zaowocują powstaniem pierwszego na świecie portu lotniczego bez bramek kontrolnych, co zapewni szybki i bezproblemowy wjazd i wyjazd z kraju[49].

Gruzja, Honduras, Ghana i Szwecja uruchomiły projekty pilotażowe mające za zadanie przetestować zastosowania technologii łańcucha bloków w rejestrach tytułów własności ziemi. Singapur próbuje ją wykorzystać do wykrywania i eliminacji fałszywych faktur przedstawianych przez firmy w bankach. Rosja i Indie analizują, jak dzięki blockchainowi można wspomóc działanie systemu płatniczego i sektora finansowego[50].

Z klei w Wielkiej Brytanii doradca rządu ds. nauki Sir Mark Walport zalecił aktywne starania w rozwijaniu rozproszonych rejestrów do użytku w sektorze publicznym i prywatnym. Instytucje rządowe mają także wspierać testy i demonstracje dla samorządów oraz inwestować w badania nad zagadnieniami skalowalności i bezpieczeństwa. W swoim raporcie Mark Walport stwierdził, że technologia rozproszonego rejestru może wspomagać funkcjonowanie rządu w takich działaniach, jak: zbieranie podatków, organizacja pomocy społecznej, rejestracja firm, wydawanie paszportów, prowadzenie rejestrów nieruchomości, zabezpieczenie odpowiedniego łańcucha dostaw i zapewnienie integralności rządowych rejestrów i usług[51].

IV. Podsumowanie

Innowacyjne rozwiązania wykorzystane w kryptowalucie bitcoin pozwalają lepiej zrozumieć mechanizm działania wszystkich kryptowalut. Innowację stanowi sama kryptowaluta bitcoin, która funkcjonuje jako jednostka wartości wyrażona w postaci zapisu cyfrowego, w ramach systemu informatycznego, opartego na kryptografii i wykorzystująca rozproszony rejestr transakcji, a do tego nie podlega żadnej instytucji państwowej, ani bankowi centralnemu, gdzie kurs ustalany jest przez rynek. To waluta nieznająca granic, którą można błyskawicznie wysłać do dowolnego miejsca na świecie z ominięciem kosztownych pośredników. Stanowi walutę opartą o kryptografię, działającą na podstawie technologii blockchain, co sprawia, że jest najbardziej bezpieczną walutą na świecie nie dającą się

[48] M. Grzybkowski, S. Bentyn, Kryptowaluty, Poznań 2018, s. 120.
[49] http://zukiewicz.com/dubaj-pierwszy-na-swiecie-rzad-oparty-o-technologie-blockchain/ (stan na 29.07.2018r.).
[50] T. Goliński, Blockchain w administracji publicznej, https://www.computerworld.pl/news/Blockchain-w-administracji-publicznej,407343.html (stan na 29.07.2018r.).
[51] Ibidem.

sztucznie dodrukować, zablokować czy sfałszować. Technologia ta umożliwia przechowywanie danych w rozproszony sposób, co umożliwia przeciwdziałaniu manipulowaniu danymi, ponieważ wszelkie zmiany są od razu widoczne dla wszystkich podłączonych do sieci. Mimo, że technologia blockchain stanowi póki co zasadniczy element kryptowalut, może stać się coraz bardziej użyteczny w działalności organów administracji publicznej.

Literatura:

1. Antonopoulos A. M., Bitcoin dla zawansowanych, HELION 2018,
2. Bala S., Kopyściański T., Srokosz W., Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne, Wrocław 2016,
3. Caetano R., Learning Bitcoin, Pact Publishing, Birmingham 2015,
4. Chrabonszczewska E., Bitcoin – nowa wirtualna, globalna waluta?, „International Journal of Management and Economics" Nr 40, Warszawa 2013,
5. Dobosz A., Bitcoin – efemeryda czy solidna przyszłość, „Kwartalnik Naukowy Uczelni Vistula Vistula Scientific Quarterly, Nr 3 (41) Warszawa 2014,
6. Dopierała Ł., Borodo A., Znaczenie waluty kryptograficznej jako środka wymiany, „Współczesna Gospodarka" 2014, vol. 5 Issue 2,
7. Freeman Ch., Economics of Industrial Innovation, Frances Printer, London 1982,
8. Grzybkowski M., Bentyn S., Kryptowaluty, Poznań 2018,
9. Homa D., Sekrety bitcoina i innych kryptowalut, HELION 2015,
10. Isaacson W., Innowatorzy, 2014 (New York),
11. Janasz W., Kozioł K., Determinanty działalności innowacyjnej przedsiębiorstw, Polskie Towarzystwo Ekonomiczne, Warszawa 2007,
12. Karpińska K., Matel A., Protasiewicz A., Konsument w działalności innowacyjnej przedsiębiorstw, Polskie Towarzystwo Ekonomiczne, Białystok 2017,
13. Mansfield E., Industrial Research and Technological Innovation, Norton, New York 1968,
14. Matusiak K. B., (red.), Innowacje i transfer technologii – słownik pojęć, Warszawa 2005,

15. Nowakowski W., Postęp w technologii systemów kryptowalutowych, „Elektronika" 2015, Nr 11,
16. Nowakowski W., Technologie Bitcoin w Internecie Rzeczy (IoT)?, „Elektronika" 2015, Nr 10,
17. Osbert-Pociecha G., Innowacje – zagadnienia ogólne i definicyjne, [w:] Innowacje w biznesie, (red. nauk.) A. Styś, A. Dejnaka, Difin, Warszawa 2016,
18. Pavlus J., Świat bitcoina, „Świat Nauki" 2018, Nr. 2 (318),
19. Piotrowska A. I., Bitcoin. Płatnicze i inwestycyjne zastosowania kryptowaluty, Warszawa 2018,
20. Piotrowska A., Bitcoin a definicja i funkcje pieniądza, „Annales Universitatis Mariae Curie-Skłodowska", Sectio H, Oeconomia 2014, Vol. XLVIII, 3,
21. Pomykalski A., Zarządzanie innowacjami, PWN, Warszawa-Łódź 2001,
22. Przyłuska J., Wirtualny pieniądz, „Gazeta Bankowa" 2012, Nr 5 (1133),
23. Schumpeter J., Teoria rozwoju gospodarczego, PWN, Warszawa 1960,
24. Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1983,
25. Sobiecki G., Regulowanie kryptowalut w Polsce i na świecie na przykładzie Bitcoina – status prawny i interpretacja ekonomiczna, „Problemy zarządzania" vol. 13, Nr 3 (54), t. 1 Warszawa 2015,
26. Spruch W., Strategia postępu technicznego, Państwowe Wydawnictwo Naukowe, Warszawa 1976,
27. Srokosz W., Publicznoprawne ograniczenia kryptowalut, [w:] Jednostka wobec działań administracji publicznej, (red.) E. Ura, E. Feret, S. Pieprzny, Rzeszów 2016,
28. Staniewski R. Nowacki M. W., Podejście innowacyjne w zarządzaniu, Warszawa 2010,
29. Steinerowska–Streb I., Innowacje w polskich mikroprzedsiębiorstwach, „Studia Ekonomiczne" Nr 183, Katowice 2014,
30. Szewczyk J., O cywilnoprawnych aspektach bitcoina, „Monitor Prawniczy" 2018, Nr. 5,
31. Szymankiewicz M., Bitcoin wirtualna waluta internetu, HELION 2014,
32. Vigna P., Casey M.J., The Age of Cryptocurrency. How Bitcoin and the Blockchain Are Challenging the Global Economic Order, Picador, New York 2016.
33. Whitfield P.R., Innowacje w przemyśle, PWE, Warszawa1979,

Pozostałe źródła:

1. R. Szyryngo, Technologia blockchain i jej wykorzystanie, https://bithub.pl/felietony/technologia-blockchain-wykorzystanie/ (stan na 29.07.2018r.).
2. K. Piech, P. Zyga, Wykorzystanie blockchain przez rząd estoński, https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/wykorzystanie-blockchain-przez-rzad-estonski/ (stan na 29.07.2018r.).
3. P. Barański, M. Bronowska, Blockchain a podatki, https://www2.deloitte.com/pl/pl/pages/podcasty/articles/Technologia-blockchain-i-jej-zastosowania.html (stan na 29.07.2018r.).
4. https://www2.deloitte.com/pl/pl/pages/tax/articles/blockchain-technology.html
5. https://bithub.pl/wiadomosci/szwajcarskie-miasto-zug-organizuje-probne-glosowanie-z-uzyciem-technologii-blockchain/ (stan na 29.07.2018r.).
6. http://zukiewicz.com/dubaj-pierwszy-na-swiecie-rzad-oparty-o-technologie-blockchain/ (stan na 29.07.2018r.).
7. T. Goliński, Blockchain w administracji publicznej, https://www.computerworld.pl/news/Blockchain-w-administracji-publicznej,407343.html (stan na 29.07.2018r.).