MISCELLANEA

Bank i Kredyt 50(3), 2019, 295-328

BANK I KREDYT
BANK & CREDIT

Blockchain – zdecentralizowany system o scentralizowanej logice

Katarzyna Ciupa*

Nadesłany: 20 lipca 2018 r. Zaakceptowany: 6 maja 2019 r.

Streszczenie

Blockchain, koncepcja zaprezentowana przez autora bądź autorów o pseudonimie Satoshi Nakamoto, od początku swego istnienia wzbudzała wiele kontrowersji. Pomimo już ponaddziesięcioletniej historii i licznych prób zastosowania koncepcji nadal niewiele jest funkcjonujących przykładów pozwalających na poznanie jej prawdziwego potencjału i wyjaśniających oferowane przez nią możliwości. W związku z powyższym celem artykułu jest omówienie wieloaspektowego zagadnienia, jakim jest koncepcja blockchain, ze zwróceniem szczególnej uwagi na aspekty techniczne i wynikające z nich możliwości. Podstawowym narzędziem badawczym zastosowanym w artykule jest metoda indukcyjna oraz metoda dedukcyjna. Na potrzeby artykułu przyjęto i udowodniono następujące tezy badawcze: (i) powstanie blockchain było motywowane pogłębiającym się kryzysem zaufania, jak również powiększającym się wymiarem cyfrowym gospodarki; (ii) blockchain to trzyelementowy system składający się z cyfrowych reprezentantów wartości, zdecentralizowanej infrastruktury i scentralizowanych zasad (logiki systemu); (iii) koncepcja blockchain pozwala na usprawnienie funkcjonujących i konstruowanie nowych rozwiązań.

Słowa kluczowe: blockchain, decentralizacja, baza danych, kryptoaktywa, zaufanie

JEL: O3

* Szkoła Główna Handlowa w Warszawie, Kolegium Zarządzania i Finansów; e-mail: katarzyna.ciupa@gmail.com.

1. Wprowadzenie

Blockchain, określany często w literaturze jako zdecentralizowany, rozproszony i zsynchronizowany system, od 2008 r., w którym został po raz pierwszy zaprezentowany (Nakamoto 2008), jest nieprzerwanie tematem licznych kontrowersyjnych wypowiedzi i skrajnych opinii. Szacowane i analizowane są jego ogromne możliwości jako koncepcji oferującej rozwiązania i ulepszenia w odniesieniu do wielu aktualnie znanych problemów i procesów, takich jak rozliczenia międzynarodowe (Catalini 2017; Ito, Narula, Ali 2017; McWaters, Galaski 2017), przepływ towarów (Casey, Wong 2017; IBM 2017; Kim, Laskowski 2018; Kshetri 2018; PR Newswire 2017), zarządzanie przepływem energii (Basden, Cottrell 2017), jednakże wciąż brak jest rezultatów potwierdzających planowany do osiągnięcia potencjał. W 2017 r. środki zebrane przez start-upy za pomocą zbudowanego w oparciu o blockchain mechanizmu określanego terminem ICO (*initial coin offering*)[1] przewyższyły kwoty zainwestowane przez fundusze *venture capital* w innowacyjne przedsięwzięcia (FabricVentures, TokenData 2018; Hacker, Thomale 2017; Howell, Niessner, Yermack 2018; Williams-Grut 2018)[2]. Co więcej, często postrzega się zaproponowaną koncepcję jedynie w kategoriach nowej technologii, a nie dostrzega się jej wieloaspektowego charakteru wynikającego z jej konstrukcji czy właściwości, które prowadzą do określania przez coraz liczniejszą grupę badaczy nowej koncepcji terminem „ekonomii blockchain" (Davidson, De Filippi, Potts 2018; Iansiti, Lakhani 2017; The Economist 2018). Ponadto znaczne zainteresowanie mediów koncepcją blockchain, przekładające się na wzrost liczby artykułów czy wydarzeń dedykowanych omawianej tematyce, dodatkowo przyczynia się do jeszcze większego zaciekawienia ze strony zarówno podmiotów indywidualnych, jak i instytucjonalnych (Mai i in. 2018). Naturalne wydaje się zatem pytanie, czym blockchain tak naprawdę jest, z czego wynika jego złożoność i wieloaspektowość oraz jaki w rzeczywistości potencjał w sobie kryje.

W związku z powyższym celem artykułu jest omówienie wieloaspektowego zagadnienia, jakim jest koncepcja blockchain, ze zwróceniem szczególnej uwagi na aspekty techniczne i wynikające z nich możliwości zastosowania technologii zarówno do ulepszenia obecnie istniejących, jak i konstrukcji nowych rozwiązań. Podstawowym narzędziem badawczym zastosowanym w artykule była metoda indukcyjna, czyli bezpośrednia analiza dokumentów źródłowych, której zastosowanie podyktowane było głównie wczesnym stadium rozwoju technologii, oraz metoda dedukcyjna, tj. wykorzystanie literatury fachowej oraz specjalistycznej. Studium literaturowe opierało się na przeglądzie pozycji zarówno polskich, jak i zagranicznych, jednakże z uwagi na niewielką ilość opracowań w języku polskim w przygotowaniu artykułu w przeważającej części skorzystano z publikacji obcojęzycznych. W artykule przyjęto trzy tezy badawcze: (i) powstanie blockchain było motywowane pogłębiającym się kryzysem zaufania, jak również powiększającym się wymiarem cyfrowym gospodarki; (ii) blockchain to trzyelementowy system składający się z cyfrowych reprezentantów wartości, zdecentralizowanej infrastruktury i scentralizowanych zasad (logiki systemu); (iii) koncepcja blockchain pozwala na usprawnienie funkcjonujących i konstruowanie nowych rozwiązań.

[1] W celu porównania proponowanych stwierdzeń z poglądami prezentowanymi w literaturze międzynarodowej zdecydowano się na umieszczenie angielskich odpowiedników używanych zwrotów w nawiasie umiejscowionym jednorazowo po będącym przedmiotem tłumaczenia wyrażeniu.

[2] Warto zaznaczyć, iż projekty wykorzystujące mechanizm ICO nie miały często nawet dokładnego opisu zamierzeń, nie wspominając już o biznesplanie. Opisem modeli wykorzystujących blockchain był zazwyczaj tylko jeden, przeważnie bardzo techniczny dokument (*whitepaper*) (Adhami, Giudici, Martinazzi 2018).

Na wstępie zarysowano przesłanki powstania blockchain, kładąc szczególny nacisk na narastające problemy i wydarzenia towarzyszące opublikowaniu pierwszej wersji koncepcji. Następnie dokonano charakterystyki aspektów technologicznych koncepcji blockchain, zwracając uwagę na jej właściwości, schemat działania i warianty klasyfikacji, przyjmując za cel przede wszystkim ukazanie, jakie możliwości wynikające z owych technicznych charakterystyk koncepcja blockchain oferuje aniżeli zakładając dokonanie dokładnego technicznego ich opisu[3]. Na zakończenie zamieszczono analizę potencjału biznesowego blockchain. W podsumowaniu zawarto natomiast najważniejsze wnioski.

2. Przesłanki powstania i uwarunkowania rozwoju technologii blockchain[4]

Rozważania dotyczące koncepcji blockchain należy rozpocząć od nakreślenia tła jej powstania i podjęcia próby zidentyfikowania motywacji do stworzenia nowego rozwiązania, które pozwolą na udowodnienie bądź odrzucenie pierwszej tezy badawczej.

W kontekście blockchain nie sposób nie zwrócić uwagi na fakt, iż koncepcja ta została zaprezentowana po raz pierwszy w dokumencie opublikowanym zaledwie 46 dni po upadku jednej z najbardziej prestiżowych instytucji finansowych. Wydarzenie to stanowiło oficjalny początek drugiego największego kryzysu finansowego. Zaistniała wówczas, niezwykle niekorzystna, sytuacja nie dotyczyła jednakże tylko sektora finansowego, ale objęła całą gospodarkę i wykazała liczne, systematycznie narastające nieprawidłowości. Warto wiec się zastanowić, co stanowiło prawdziwe źródło problemów i jakie zmiany czy zjawiska stały się przesłankami poszukiwania alternatywnych rozwiązań.

Z uwagi na fakt, iż pierwszy opis zastosowania koncepcji blockchain pojawił się w dokumencie proponującym alternatywne rozwiązanie w odniesieniu do funkcjonujących praktyk finansowych, zasadne jest rozpoczęcie analizy problemu od charakterystyki zmian dotyczących tego obszaru.

Historia rozwoju pieniądza, jak również ewolucja systemów wymiany i towarzyszących im modeli biznesowych są przedmiotem licznych analiz podejmowanych zarówno w środowiskach naukowych, jak i biznesowych. Wskazuje się na przyczyny powstania i konsekwencje zastosowania takich rozwiązań, jak: (i) barter i wymiana bezpośrednia, (ii) system waluty złotej i działalność pośredników, (iii) mechanizm oparty na pieniądzu papierowym/bezgotówkowym i rola banków centralnych (Ametrano 2016; Burn-Callander 2014; Davies 2002; Friedman 1992). Równocześnie prowadzone są badania dotyczące zmian zachodzących w obszarze modeli biznesowych, których autorzy odnoszą się do zachodzących modyfikacji i rozwoju nowych wariantów prowadzenia działalności (Fjeldstad, Snow 2018; Osterwalder, Pigneur 2010). Często wskazuje się przy tym, że zaobserwowane zmiany były w pewnym sensie odpowiedzią na potrzeby zgłaszane przez uczestników rynku, a ich ewolucja stała się możliwa w dużej mierze dzięki rozwojowi technologicznemu (Nowiński, Kozma 2017).

System barterowy przeszedł naturalną ewolucję z uwagi na chęć uniknięcia problemu określanego terminem „zgodność potrzeb" (*double coincidence of wants*) (Davies 2002), który stawał się, wskutek

[3] Od czasu powstania koncepcji pojawiło się bardzo wiele publikacji podejmujących temat technicznych aspektów, jednakże wciąż niewiele jest opracowań prezentujących możliwości, jakie z owych technologicznych aspektów wynikają, co jest przedmiotem niniejszego artykułu.

[4] W niniejszym artykule skupiono się na narastających problemach, w szczególności pogłębiającym się kryzysie zaufania, stanowiących przesłanki powstania koncepcji blockchain, natomiast nie podejmowano się opisu ewolucji rozwiązań technologicznych pozwalających na skonstruowanie nowej koncepcji, głównie z uwagi na ograniczenia co do objętości tekstu, gdyż dokładny opis owych technologicznych ewolucji spowodowałby znaczne wydłużenie się artykułu. Ponadto opis owych technologicznych rozwiązań jest przedmiotem licznych publikacji, pozwalających na ich dokładne poznanie.

powiększającego się katalogu dóbr, coraz silniej odczuwalny. Co więcej, możliwość przemieszczania się wymusiła wprowadzenie środka płatniczego[5] zarówno łatwego w transporcie, jak również akceptowanego na nowych obszarach, którym początkowo były dobra o wysokiej użyteczności, a następnie srebrne i złote monety. Następnie, głównie z uwagi na trudności i niebezpieczeństwa wiążące się z wykorzystywaniem monet do rozliczania transakcji wymiany, postanowiono wprowadzić papierowe poświadczenia, którym później nadano rangę pełnowartościowego środka płatniczego gwarantowanego przez zaufane instytucje (Wray 2012).

Równolegle dokonywały się zmiany w systemie wymiany: początkowo transakcje zawierane były bezpośrednio pomiędzy zainteresowanymi stronami; następnie, z uwagi na dystans dzielący obie strony transakcji i chęć podjęcia działalności na większą skalę, rosnącą rolę zaczęli odgrywać zaufani pośrednicy. W sposób naturalny następowała zarówno automatyzacja, jak i centralizacja procesów, które z jednej strony umożliwiały większą szybkość zawierania transakcji, z drugiej jednak wymagały polegania na centralnych jednostkach czy pośrednikach, a tym samym zaufania do prowadzonych przez nich działań. Równolegle rozwój nowych technologii, w tym Internet, umożliwił przeniesienie zarówno środków płatniczych, jak i systemów wymiany do sfery cyfrowej, gdzie pieniądze papierowe zostały zastąpione elektronicznym zapisem, a stacjonarny sklep stał się internetową platformą (Alstyne, Parker, Choudary 2016; Choudary 2015; Kenney, Zysman 2015; Schrage 2016; Täuscher, Laudien 2018).

Bez względu na to, czy proces odbywa się w wymiarze fizycznym czy cyfrowym, kluczową rolę odgrywa w nim zaufanie: do środka płatniczego, do pośrednika i do partnera biznesowego (Blomqvist 1997; Chakravorti, Bhalla, Chaturvedi 2018; Cochrane 2018; Pennington, Wilcox, Grover 2003). Z uwagi na fakt, iż często nawet niewielki uszczerbek w odniesieniu do reputacji prowadzonych działań może prowadzić do całkowitego zniechęcenia klientów, a tym samym oznaczać porażkę biznesową, zakłada się, że przedsiębiorstwa dążące za wszelką cenę do utrzymania pozycji na rynku będą starały się postępować zgodnie z ustalonymi zasadami, nie przekraczając jednocześnie ustalonych granic zaufania (Mattila, Seppälä 2016; Partnoy 2013).

Niestety znanych jest wiele przykładów z historii, kiedy te i podobne założenia się nie sprawdziły, a zaufanie zostało poważnie nadszarpnięte (Casey, Wong 2017; Chakravorti, Bhalla, Chaturvedi 2018; Forde 2017; Mainelli 2017b). Świadczą o tym chociażby nadużycia finansowe z ostatnich lat (Clikeman 2013). Jednym z najbardziej spektakularnych wydarzeń był upadek Lehman Brothers ogłoszony 15 września 2008 r., uznany wówczas za największe bankructwo w historii gospodarki (Konopczak, Sieradzki, Wiernicki 2010). Koncepcja „za duży, aby upaść" (*too big to fail*) (Nurisso, Prescott 2017) nie miała w odniesieniu do tego banku zastosowania. Ranga nadużyć dokonanych przez Lehman Brothers, który zaledwie trzy lata wcześniej uzyskał tytuł „najlepszego banku inwestycyjnego" (Euromoney 2005), była zbyt duża, a brak zabezpieczeń zaciągniętych zobowiązań nie pozwolił na wsparcie banku przez instytucje państwowe (Knight 2009; Koehn 2009).

Rok 2008, będący w pewnym sensie momentem kulminacyjnym w kontekście nadużyć, to zatem nie tylko oficjalny początek największego po Wielkiej Depresji kryzysu finansowego (Konopczak, Sieradzki, Wiernicki 2010), ale również, albo przede wszystkim, oficjalny początek kryzysu zaufania. Zaufanie, jak już wcześniej zasugerowano, leży bowiem u źródła wszelkich procesów. W momencie, kiedy pojawia się kryzys z nim związany, to z jego przyczynami należałoby przede wszystkim walczyć. Zaniechanie tych działań przyczynia się bowiem tylko do pogłębienia problemu i powiększa skalę negatywnych skutków jego braku obserwowanych w wielu dziedzinach gospodarki.

[5] W pracy zamiennie używa się pojęć środek płatniczy, środek rozliczeniowy i środek wymiany.

Jednocześnie kryzys zaufania, pomimo spektakularnych wydarzeń w branży finansowej, odczuwalny był również w innych obszarach społecznego i biznesowego życia. Zarysowane problemy, a zarazem przyczyny kryzysu zaufania, takie jak centralizacja, oznaczająca nadmierną koncentrację istotnych działań w ramach jednego podmiotu i mogąca prowadzić do zjawiska pokusy nadużycia ze strony centralnych podmiotów (Davidson, De Filippi, Potts 2018), nie dotyczyły bowiem jedynie sektora finansowego, lecz obserwowane były również w odniesieniu do innych gałęzi gospodarki.

Zyskujące na popularności platformowe modele biznesowe, wykorzystywane przez takie firmy jak chociażby Facebook, które często określały się terminem *free*, mającym sugerować ich nieodpłatny charakter, okazywały się bardzo scentralizowanymi jednostkami, gromadzącymi ogromne ilości danych, które stawały się jednocześnie doskonałym źródłem przychodów i potęgi owych podmiotów. Podmioty te często nadużywały opartej na danych siły i dyktowały warunki, często niekorzystne dla użytkowników, a co więcej – z uwagi na scentralizowany model działania tych podmiotów – coraz częściej stawały się obiektem manipulacji i ataków hakerskich (Alstyne, Parker, Choudary 2016; Choudary 2015; Kenney, Zysman 2015; Schrage 2016; Täuscher, Laudien 2018). Przykładem potwierdzającym opisywane problemy był chociażby skandal, jaki dotyczył firmy Facebook w 2018 r., którego podstawą były nadużycia w wykorzystaniu pozyskiwanych danych (Wikipedia 2019).

Dane, z uwagi na powiększający się cyfrowy wymiar gospodarki, z początkowo bardzo niedocenianych aktywów stawały się coraz cenniejszym zasobem. Podyktowane było to rozwojem umiejętności ich analizowania i wykorzystywania w celach zarobkowych. Niemniej jednak najczęściej owe możliwości osiągania zysków dotyczyły jedynie bardzo wąskiego grona podmiotów, natomiast sami dostarczyciele danych często byli jedynie w niewielkim stopniu wynagradzani. O ile początkowo skala zjawiska nie wymuszała posiadania odpowiednich rozwiązań, o tyle w obliczu powiększającej się liczby danych (Agrawal, Gans, Goldfarb 2016; Athey, Catalini, Tucker 2017; Forde 2017) nie sposób było dalej ignorować nadużycia, a tym samym koniecznością stało się posiadanie odpowiedniego rozwiązania dopasowanego do nowych warunków gospodarki cyfrowej.

W obliczu pogłębiającego się kryzysu zaufania, coraz bardziej odczuwalnej nieefektywności stosowanych rozwiązań, jak również powiększającego się wymiaru cyfrowego gospodarki, a dokładniej zaledwie 46 dni po ogłoszeniu bankructwa Lehman Brothers, opublikowany został dokument przedstawiający możliwe rozwiązanie: blockchain.

Bitcoin: A Peer-to-Peer Electronic Cash System, wydany przez Satoshi Nakamoto[6] w październiku 2008 r. (Nakamoto 2008), to zaledwie kilkustronicowy zapis ram funkcjonowania nowego systemu. Sam autor nazwał nową koncepcję *a peer to peer cash system*, co można przetłumaczyć jako „bezpośredni system gotówkowy", wskazując jednocześnie na jej wieloaspektowość i zaznaczając istotność roli odgrywanej przez wchodzące w jej skład poszczególne elementy. Co więcej, w wydanym dokumencie ani razu nie użył terminu blockchain, chcąc zapewne pokazać możliwości systemu jako całości, a nie tylko jednego z elementów wchodzących w jej skład.

[6] Tożsamość autora dokumentu znanego pod pseudonimem Satoshi Nakamoto nie została ujawniona (stan na 30 maja 2019 r.).

System zgodnie z koncepcją opublikowaną przez Nakamoto składał się z: (i) reprezentanta wartości, w tym przypadku reprezentanta uniwersalnej wartości, jakim był bitcoin[7], (ii) infrastruktury niezbędnej do obiegu, emitowania czy raportowania wyżej wymienionych reprezentantów, czyli blockchain oraz (iii) zestawu reguł determinujących przebieg procesów, takich jak przykładowo *proof of work*[8].

Zaproponowana koncepcja[9], zdecydowanie różniąca się od powszechnie występujących rozwiązań i procesów działania, jest swego rodzaju zmianą podejścia mówiącego o celowości centralizacji i zasadności instytucjonalizacji. Owa koncepcja pozwala bowiem na stworzenie samoregulującego się systemu, w ramach którego obrót i wycena podlegających obrotowi reprezentantów wartości[10] wynikają z zachodzących pomiędzy podmiotami interakcji, a ponadto nie są podyktowane decyzjami jednej centralnej instytucji, tylko opierają się na powszechnie dostępnych zasadach, opisanych w dokumencie określanym „whitepaper" (Antonopoulos 2014; Mengelkamp i in. 2017). Rozwiązuje to tym samym problem konieczności korzystania z usług pośrednika, jak również proponuje mechanizm praktycznie natychmiastowego rozliczenia transakcji (De Filippi 2017), opierający się na utworzonych w ramach systemu reprezentantach wartości, określanych często terminem kryptoaktywów (Böhme i in. 2015).

Jednocześnie tak utworzony system pomimo swojej zdecentralizowanej organizacji ma scentralizowaną logikę. Logika ta, czyli zbiór zasad, jest przy tym niezwykle istotna, gdyż do poprawnego funkcjonowania systemu konieczne jest opieranie się na jednym zestawie powszechnie dostępnych i obowiązujących reguł i zasad.

Przytoczone argumenty pozwalają zatem na udowodnienie pierwszej tezy, mówiącej, iż powstanie blockchain było motywowane pogłębiającym się kryzysem zaufania, obserwowanym w wielu dziedzinach gospodarki, jak również powiększającym się wymiarem cyfrowym gospodarki. Przesłanki te skłaniały tym samym do podejmowania prób znalezienia mechanizmu rozwiązującego zauważoną nieefektywność.

Jednocześnie w związku z powyższym wydawać się by mogło wręcz naturalne, że zaproponowane rozwiązanie jest odpowiedzią na długo zgłaszane problemy, a tym samym powinno się spotkać z entuzjazmem, zarówno jednostek indywidualnych, przedsiębiorstw, jak i rządów. Koncepcja, która pozwala na odejście od paradygmatu centralnego zarządzania, której działanie jest zgodne z powszechnie dostępnymi regułami, która jest pozbawiona barier wejścia i wyjścia i która eliminuje asymetrię informacji tyczącą się obiegu reprezentantów wartości w ramach utworzonej infrastruktury (Tabarrok,

[7] Nakamoto nazwał swój system „cash system", co sugeruje, iż dotyczy on najbardziej uniwersalnego wymiaru wartości, jakim jest właśnie gotówka. Gotówka bowiem jest uniwersalnym medium, niemającym żadnego fizycznego zastosowania, opierającym swoją wartość na zaufaniu do podmiotów odpowiedzialnych za jej emisję. Termin „wartość" jest używany, aby oddać istotę systemu, gdyż głównym celem koncepcji nie jest dostawa dóbr czy przekazywanie informacji, lecz właśnie wymiana wartości, a dokładniej unikalnych reprezentantów wartości (unikalność wynika ze zdolności systemu do rozwiązania problemu „dwukrotnego wydawania", co potwierdza niemożność kopiowania owych reprezentantów).

[8] *Proof of work* to mechanizm wymagający rozwiązania ustalonej przez system łamigłówki poprzez wykonanie serii obliczeń wymagających znacznej mocy obliczeniowej. Zwycięzca, któremu uda się jako pierwszemu ową łamigłówkę rozwiązać, zyskuje ustaloną na dany okres ilość nowo wyemitowanych bitcoinów.

[9] W niniejszej publikacji terminy „koncepcja blockchain" czy „technologia blockchain" są używane zamiennie i określają trzyelementowy zestaw, co ma za zadanie podkreślić istotność poszczególnych jego elementów dla poprawności działania całego systemu.

[10] Przedmiotem obiegu i zapisu w ramach nowo powstałej infrastruktury są różnego rodzaju reprezentanci wartości, określani często terminem tokenów, których format i treść są zależne od modelu samej infrastruktury (tj. tego, czy występuje ona w wersji prywatnej czy publicznej), jak również od konkretnego przypadku biznesowego. Kryptowaluty starają się być przykładowo reprezentantami najbardziej uniwersalnego wymiaru wartości, jakim są środki pieniężne emitowane przez banki centralne.

Cowen 2015) oraz która dodatkowo umożliwia rozliczanie transakcji za pomocą wewnętrznie wytworzonych środków, wydaje się dokładnie tym, czego wszystkie podmioty działające na rynku od dawna poszukiwały.

Jednakże, jak się można przekonać, analizując rozwój koncepcji blockchain w ciągu ostatnich niespełna dziesięciu lat, proces jej adaptacji nie przebiega tak łatwo, jakby się można było spodziewać, uwzględniając wspomniane powyżej charakterystyki. Z uwagi na fakt, iż sama koncepcja blockchain została zaprezentowana na przykładzie dotyczącym możliwości stworzenia nowego rodzaju środka płatniczego, wywołało to początkowo liczne kontrowersje i głosy krytyki. Dodatkowo, ze względu na jej pierwsze, bardzo techniczne opisy utrudniona była jej poprawna analiza przez osoby o kompetencjach nietechnicznych. Co więcej, liczne podmioty zaczęły podejmować próby eksperymentowania z technologią, wybierając jedynie te jej elementy, które uznawały za ciekawe i nie będąc zainteresowanymi wykorzystaniem wszystkich oferowanych możliwości, a tym samym przyczyniając się do zaburzonego obrazu wykorzystania technologii. Blockchain to bowiem bardzo nowatorski system, jednakże w przypadku niezrozumienia oferowanych przez niego możliwości może dochodzić do jego niepoprawnych zastosowań. Jednocześnie jest to trzyelementowy system, organizacyjnie zdecentralizowany i logicznie scentralizowany, co nakłada różne ograniczenia na możliwości jego wykorzystania. Pierwsza propozycja zastosowania systemu miała ową zdecentralizowaną organizację i scentralizowaną logikę, jak również opierała się na cyfrowych reprezentantach uniwersalnej wartości, co pozwalało jej na rozwiązanie zarysowanych problemów czy zaoferowanie wspomnianych korzyści. Niemniej jednak nie zawsze jest możliwe takie skonstruowanie systemu, a ewentualne zmiany parametrów tyczących poszczególnych elementów jego konstrukcji mogą nawet prowadzić do powstania ryzyka większego niż pierwotnie obserwowane.

W rezultacie kontrowersyjność i nowatorstwo przykładu pierwszego zastosowania blockchain oraz techniczne skomplikowanie koncepcji prowadziły do licznych nieporozumień. Brakowało literatury pozwalającej na głębszą analizę technologii (Yli-Huumo i in. 2016), a sam twórca, Satoshi Nakamoto, nigdy się nie ujawnił, co dodatkowo utrudniało proces poznawczy.

3. Charakterystyka aspektów technologicznych koncepcji blockchain

3.1. Właściwości i charakterystyka koncepcji[11]

Mając świadomość narastających problemów stanowiących przesłanki powstania koncepcji blockchain, można przystąpić do jej charakterystyki. Jednym z pierwszych wyzwań, z jakimi należy się zmierzyć, jest kwestia definicji nowej koncepcji. Technologia blockchain czy też technologia łańcucha bloków, często określana również jako technologia rozproszonego rejestru (DLT – *distributed ledger technology*), jest zdecentralizowanym, rozproszonym zapisem danych (systemem)[12], pogrupowanych w połączone ze sobą bloki, gdzie zachodzące transakcje, zgodnie z pierwotnym założeniem, są transmitowane jednocześnie

[11] Przedstawiona charakterystyka dotyczy pierwotnej wersji technologii blockchain w wariancie publicznie nielicencjonowanym.

[12] W dalszej części niniejszej publikacji nazwy technologia blockchain, koncepcja blockchain, system czy łańcuch bloków zostały użyte zamiennie. Niemniej jednak należy zwrócić uwagę, że owe określenia są jedynie pomocniczymi określeniami i bardzo ważne przy analizie rozwiązań jest przestudiowanie wszystkich poszczególnych elementów celem zrozumienia zarówno właściwości nowej koncepcji, jak i oferowanych możliwości.

do wszystkich uczestników systemu (Davidson, De Filippi, Potts 2018; Evans 2014; Iansiti, Lakhani 2017; Nakamoto 2008, 2008; Pilkington 2016).

Należy zaznaczyć, że technologia łańcucha bloków (*blockchain*) jest określeniem podrzędnym w stosunku do technologii rozproszonego rejestru (DLT – *distributed ledger technology*) ze względu na różnice m.in. w architekturze danych[13]. Blockchain bowiem z reguły składa się z sieci powiązanych ze sobą bloków, co nie jest wymagane w przypadku DLT (BIS 2017; Leon i in. 2017). Wspólną cechą jest odejście od konieczności kontrolowania rozproszonego systemu przez centralną jednostkę, która decydowałaby o przynależności do systemu i gwarantowałaby, że uczestniczący gracze postępują zgodnie z zasadami. Proponowany system pozwala na osiąganie zgodności co do poprawności zapisu i synchronizacji danych nawet w przypadku, gdy należące do niego podmioty nie znają się (Shapiro 2018). Jednocześnie, jak już zaznaczono, system ten składa się z trzech elementów, jakimi są sami reprezentanci wartości[14], infrastruktura i reguły działania. Dalsza cześć niniejszego podrozdziału, jak również podrozdziały 3.2 i 3.3 dotyczą przede wszystkim opisu i zasad działania ostatnich dwóch elementów, natomiast podrozdział 3.4 poświecono pierwszemu z wymienionych elementów.

Blockchain, w szczególności element infrastruktury, jest zatem w pewnym sensie przykładem bazy danych[15], która nie jest przechowywana i zarządzana przez centralny podmiot, ale jest siecią powiązanych ze sobą kopii, które są równoważne i łącznie stanowią kompletny system (Böhme i in. 2015; Gupta 2017a; Tapscott, Tapscott 2017). Warto przy tym zwrócić uwagę, iż słowo „kopia" nie powinno sugerować istnienia jednej wersji głównej i posiadania przez uczestników jedynie jednakowych jej replik. W ramach blockchain nie ma bowiem centralnej wersji głównej, a każdy uczestnik ma taki sam zapis stanu aktualnego (Hacker, Thomale 2017).

Każdy może stać się pełnoprawnym uczestnikiem (*node*). Wymagane jest jedynie pobranie i zainstalowanie specjalnego programu (w przypadku bitcoina jest to to Bitcoin Core[16]) (Böhme i in. 2015), który umożliwia dołączenie do rozproszonego systemu. Użytkownicy zainteresowani tylko sprawdzeniem aktualnego stanu danych mają taką możliwość za pośrednictwem specjalnych stron internetowych, jak na przykład blockchain.info[17]. Oznacza to, że jedynie użytkownicy, którzy albo chcą stać się górnikami (*miners*)[18] weryfikującymi zapis, albo ci, którym zależy na niezależnej kontroli aktualnego stanu, są zainteresowani instalacją wspomnianego programu. Należy zaznaczyć, że powyższy schemat jest podobny w odniesieniu do pozostałych rozwiązań publicznie nielicencjonowanych, natomiast w przypadku wariantu prywatnie licencjonowanego sposób weryfikacji i dołączania do sieci jest inny dla każdego z projektów (opis wariantów znajduje się w części 3.3).

---

[13] W literaturze przedmiotu i praktyce biznesowej podane określenia są często używane zamiennie, jednakże warto mieć na uwadze istniejące różnice i ich konsekwencje.

[14] Owe reprezentacje wartości stanowią jednocześnie przedmiot zapisu, co pozwala na określanie ich również terminem „dane".

[15] Określenie blockchain terminem „bazy danych" jest oczywiście dużym uproszczeniem, jednakże pozwala na zrozumienie nowatorstwa zaproponowanej struktury, a tym samym zarysowanie różnic pomiędzy nową koncepcją a wcześniejszymi rozwiązaniami.

[16] Program ten można pobrać ze strony https://bitcoin.org/ en/choose-your-wallet.

[17] Podana strona pozwala jedynie na sprawdzenie aktualnego stanu jednej platformy, a mianowicie Bitcoin Blockchain. W przypadku innych platform należy skorzystać z innych stron, dedykowanych konkretnym blockchain, jak na przykład etherscan.io w odniesieniu do Ethereum Blockchain.

[18] Terminem górnika (*miner*) określa się podmiot, który decyduje się na (i) posiadanie repliki zapisu danych oraz (ii) uczestniczenie w procesie weryfikacji zachodzących transakcji, a tym samym przyczynia się zachowania bezpieczeństwa systemu, jak również jego ciągłego aktualizowania i powiększania. Motywacją dla górników jest nagroda, wynosząca w 2019 r. 12,5 bitcoina. Zdobywa ją górnik, który jako pierwszy rozwiąże wskazaną przez system łamigłówkę.

Dobrym sposobem opisania koncepcji jest wskazanie jej głównych charakterystyk, przy czym należy pamiętać, że owe charakterystyki są zgodne z pierwotnym założeniem koncepcji zaprezentowanym w 2008 r., a obecnie istniejące rozwiązania różnią się w mniejszym lub większym stopniu od podstawowego schematu.

Do charakterystyk koncepcji blockchain zalicza się (Bonneau i in. 2016; Clark, Narayanan 2017; Wüst, Gervais 2017):

1) organizacyjne zdecentralizowanie (*decentralisation*), co oznacza, że nie ma jednego centralnego ośrodka odpowiedzialnego za weryfikowanie, przetwarzanie i obróbkę zachodzących w ramach systemu interakcji/transakcji;

2) rozproszenie (*distribution*) wskazujące na sieć połączonych ze sobą podmiotów, które są w posiadaniu jednakowej kopii systemu (różnice pomiędzy siecią scentralizowaną, zdecentralizowaną i rozproszoną zaprezentowano na schemacie 1 w Aneksie);

3) zsynchronizowany zapis, możliwy dzięki automatycznemu aktualizowaniu się zapisu na wszystkich kopiach będących w posiadaniu uczestników systemu;

4) użycie kryptografii w celu szyfrowania danych, pozwalające na bezpieczne transferowanie i egzekwowanie praw własności (rola stosowanych w tym celu kluczy, prywatnego i publicznego, została opisana w paragrafie 3.2);

5) wbudowany mechanizm decydowania o poprawności i ciągłości zapisu (*consensus mechanizm*), pozwalający na osiąganie zgodności co do zapisów, bez konieczności znajomości i zaufania do innych uczestników czy też bez potrzeby ingerencji strony trzeciej;

6) wykorzystanie mechanizmów wymagających przykładowo rozwiązania zdefiniowanej przez system łamigłówki (*proof of work*) czy zastawienia posiadanych środków (*proof of stake*)[19] celem weryfikacji i dodania nowych bloków do istniejącej sieci;

7) nieodwracalność zapisu (*append only*), uniemożliwiającą usunięcie przeszłych zdarzeń dzięki powiązaniu nowych zdarzeń ze zdarzeniami przeszłymi;

8) niemożność dokonywania zmian bez wiedzy pozostałych uczestników systemu (*tamper-proof*), gwarantującą wiarygodny i audytowalny zapis;

9) transparentność, pozwalającą w każdym momencie na dokładną i przejrzystą analizę wszelkich dotychczasowych działań.

Blockchain pozwala zatem na zniesienie nadrzędnej roli centralnej jednostki, niezbędnej dotychczas do weryfikacji zachodzących transakcji[20], nadaje wszystkim uczestnikom jednakowe prawa dostępu i w sposób ciągły potwierdza poprawność danych, zapewniając jednocześnie nieodwracalność zapisów. Jednocześnie powyższe właściwości opisują zarówno element infrastruktury, jak również odnoszą się do scentralizowanej logiki. Logika ta jest bowiem niezbędna do rozwiązania problemu zaufania, gdyż zaufanie do jednej, centralnej jednostki zostaje zastąpione przez brak konieczności ufania ko-

[19] Obecnie występuje wiele rodzajów mechanizmu weryfikacji zapisu, takich jak *proof of importance, delegated proof of stake*, z uwagi na wielość baz danych i preferowanych przez ich twórców rozwiązań. Niemniej jednak zawsze ten sam mechanizm ma zastosowanie w odniesieniu do konkretnej bazy danych.

[20] Należy jednocześnie mieć na uwadze, iż owa weryfikacja tyczy się jedynie przebiegu transakcji dokonywanych w ramach wewnętrznego systemu i jest możliwa jedynie wówczas, gdy przedmiotem transakcji są wytworzone w ramach systemu reprezentacje wartości. W przypadku gdy owe reprezentacje wartości są reprezentacjami wartości obiektów pochodzących ze świata zewnętrznego w stosunku do infrastruktury blockchain (przykładowo reprezentacja fizycznych diamentów), sam blockchain nie poradzi sobie z weryfikacją ich jakości czy poprawności ich fizycznej dostawy. W tym celu konieczne jest posiadanie odpowiednich podmiotów odpowiedzialnych za weryfikację, tworzenie cyfrowych reprezentacji umieszczanych w ramach blockchain, jak i aktualizację zdarzeń zachodzących w wymiarze realnym.

mukolwiek, a każdy uczestnik może samodzielnie i w dowolnym momencie sprawdzić dokładny zapis i dokonać oceny dokonanych operacji (Antonopoulos 2014; Gupta 2017b; Murck 2017). Należy zaznaczyć, że w tej sytuacji ufać należy przykładowo twórcom kodu, który stanowi podstawę działania technologii, ale z uwagi na fakt, iż tworzone rozwiązania są ogólnodostępne (*open-source*), można przyjąć, że jakakolwiek zależność od strony trzeciej nie występuje lub że została ograniczona do minimum.

Owa scentralizowana logika jest też obserwowalna i wymagana w odniesieniu do procesu decydowania o poprawności zachodzących w ramach bloku transakcji i dołączania nowych bloków do łańcucha bloków wcześniejszych, co wprawdzie również odbywa się w ramach sieci rozproszonych podmiotów, jednakże zgodnie z ustalonymi i jednoznacznymi regułami. Podmioty, mając dostęp do przeszłych zapisów, są w stanie samodzielnie, bez konieczności udziału centralnego zarządcy sprawdzić i zadecydować o poprawności lub niezgodności działań. Zaproponowany mechanizm osiągania zgodności (*consensus mechanism*) rozwiązał uznawany za niemożliwy do rozwiązania „problem bizantyjskich generałów" (*Byzantine generals problem*) i pozwolił na przesyłanie cyfrowych reprezentantów wartości w sposób uniemożliwiający ich dwukrotne wydawanie (*double spending*) (Catalini, Gans 2018b; Dwyer 2015; Wayner 1997).

Co więcej, nowatorski system jest z reguły odporny na wrogie ataki mające na celu manipulację dokonywanym zapisem, gdyż jakakolwiek zmiana jednej repliki jest niewystarczająca i zostanie odrzucona przez pozostałych uczestników systemu. Dokonanie zmian we wszystkich replikach jest praktycznie niemożliwe, ze względu zarówno na ich rozproszenie, jak i na ogromną moc obliczeniową konieczną do wykonania operacji (Adhami, Giudici, Martinazzi 2018)[21]. Podkreśla to tylko istotność opisanego powyżej zdecentralizowanego zorganizowania.

Warto przy tym zwrócić uwagę na istotną rolę pełnoprawnych uczestników sieci (*nodes*)[22], którzy są w posiadaniu kompletnych replik aktualnej wersji. Większa liczba tych podmiotów oznacza większe bezpieczeństwo samego systemu, gdyż przy próbie ataku konieczne byłoby dokonanie zmian we wszystkich replikach, co przy ich większej liczbie staje się zadaniem trudnym do wykonania[23]. Jednocześnie należy zaznaczyć, że ataki, które zostały do tej pory przeprowadzone, były możliwe nie ze względu na problemy samej technologii blockchain *sensu stricto*, ale wynikały z błędów w kodzie, z braku zachowania należytej staranności przy dokonywaniu transakcji czy też były rezultatem defektów w zewnętrznych systemach obrotu (Moore, Christin 2013)[24].

W ramach technologii blockchain niemożliwe jest również dokonywanie zmian wcześniejszych zapisów dzięki wbudowanemu systemowi weryfikacji (np. *proof of work, proof of stake*) (Bach, Mihaljević, Žagar 2018; Clark, Narayanan 2017) i powiązaniu bloków za pomocą systemu unikalnych identyfikatorów (*hash*). Każdy nowy blok zawiera identyfikator (*hash*) bloku poprzedniego, który wraz z innymi elementami (takimi jak wchodzące w skład bloku transakcje oraz dodatkowy element – *nonce*) podawany jest kryptograficznej funkcji hashowania (*cryptographic hash function*), celem uzyskania nowego identyfikatora (*hash*) spełniającego ustalone przez system parametry, a tym samym pozwalającego na

[21] Manipulacja jest możliwa w przypadku, gdy podmioty zaczną współpracować i osiągną przewagę decyzyjną, jednakże takie działanie spowodowałoby spadek zaufania do całego systemu, a tym samych mniejsze zyski dla podmiotów współpracujących, stąd też takie działania są raczej ograniczone.

[22] Należy przy tym pamiętać, że w wariancie publicznie nielicencjonowanym każdy ma prawo stać się pełnoprawnym uczestnikiem systemu i wymagana jest jedynie instalacja odpowiedniego programu.

[23] Znane są również opinie wskazujące na techniczną nieefektywność systemu wymagającego dużej liczby pełnoprawnych członków weryfikujących zapis.

[24] Przykładem mogą być chociażby kradzieże mające miejsce na giełdach kryptoaktywów, których skala wzrasta, i w samym 2018 r. wykradzione środki osiągnęły równowartość około 950 mln USD.

dodanie nowego bloku do systemu. Szczególną rolę odgrywa w tym procesie wspomniany dodatkowy element (*nonce*), gdyż górnicy, którzy są zaangażowani w proces poszukiwania rozwiązania, mogą jedynie manewrować owym dodatkowym elementem celem znalezienia poprawnej odpowiedzi. Wspomniany identyfikator (*hash*) jest w rezultacie często określany cyfrowym podpisem bloku (*digital signature*), a z uwagi na fakt, iż powstaje w wyniku odpowiedniej kombinacji zarówno aktualnych transakcji, jak i poprzedniego identyfikatora, zmiana, choćby najmniejsza, któregokolwiek z wchodzących w jego skład elementów prowadzi do uzyskania zupełnie nowego identyfikatora. W rezultacie podmiot chcący dokonać zmiany musiałby dopasować poprzednie zapisy umieszczone na wszystkich rozproszonych kopiach systemu. Oznacza to przykładowo rozwiązanie wszystkich poprzednich łamigłówek (co jest praktycznie niemożliwe ze względu na ogromną ilość pracy potrzebnej do wykonania operacji[25]) czy zastawienie dużej kwoty środków.

Powyższa charakterystyka dowodzi zatem, iż blockchain to system o zdecentralizowanej organizacji i scentralizowanej logice. Elementy te są niezbędne do jego prawidłowego działania.

3.2. Schemat transakcji przeprowadzonej w ramach blockchain[26]

Mając świadomość właściwości koncepcji, warto się przyjrzeć sposobowi dokonywania zapisów w ramach systemu. Odbywa się to w następujący sposób (Böhme i in. 2015; Bonneau i in. 2016; Clark, Narayanan 2017):

1. Transakcja dokonywana przez podmiot inicjujący jest odpowiednio przez ten podmiot szyfrowana (z wykorzystaniem identyfikatora poprzedniej transakcji – *hash* i ze wskazaniem adresu odbiorcy), a następnie rozsyłana do wszystkich uczestników systemu (*nodes*). Na tym etapie istotną rolę odgrywają klucze: publiczny i prywatny, które zostały omówione poniżej opisu przebiegu transakcji.

2. Transakcja staje się jednocześnie zapisem na bloku, który jest przedmiotem pracy górników (*miners*), i jest widoczna dla wszystkich pozostałych uczestników systemu.

3. Górnicy po zapełnieniu bloku pracują nad rozwiązaniem łamigłówki (*proof of work*) i górnik, który pierwszy znajdzie rozwiązanie, dodaje blok do istniejącego już łańcucha bloków w taki sposób, że identyfikator (*hash*) bloku poprzedzającego jest częścią składową identyfikatora bloku aktualnego. Zapewnia to ciągłość systemu i chroni go przed dokonywaniem zmian przeszłych zapisów (zmiana jednego z wcześniejszych bloków wymaga zmiany wszystkich wcześniejszych bloków i tym samym rozwiązania wszystkich wcześniejszych łamigłówek). Co więcej, górnicy w taki sposób dobierają transakcje, aby zmaksymalizować możliwą do uzyskania opłatę transakcyjną udzielaną każdorazowo przy inicjacji transakcji. Wszyscy uczestnicy systemu są natychmiast informowani o dodanym bloku, a posiadane przez nich kopie automatycznie się aktualizują, pokazując aktualny stan, zgodny z zapisem na wszystkich kopiach posiadanych przez pozostałych uczestników.

[25] W odniesieniu do technologii blockchain koszt pracy liczony jest ilością zużytej energii niezbędnej do wykonania operacji obliczeniowych.

[26] Prezentowany opis przebiegu transakcji dotyczy transakcji wykonywanej w ramach bitcoin blockchain. W przypadku innych platform podstawowy mechanizm ich działania jest podobny. W przykładzie użyto, celem uproszczenia opisu, pojęcia transakcja, jednakże schemat działania jest taki sam również w przypadku przepływu pozostałych rodzajów informacji czy aktywów.

4. Gdy więcej niż 51% uczestników potwierdzi zgodność zapisów dokonanych w bloku, staje się on częścią sieci i podstawą do budowania kolejnego bloku. Wówczas górnik, który jako pierwszy rozwiązał zadanie umożliwiające mu dołączenie bloku do sieci, zostaje odpowiednio przez system wynagrodzony[27].

Przykładowy przebieg transakcji przelewu środków pieniężnych został przedstawiony na schemacie 2 (numeracja na schemacie 2 nie odpowiada numeracji z opisu zamieszczonego powyżej, gdyż jest ona jedynie uproszczonym zobrazowaniem procesu, natomiast powyższy opis ma za zadanie dokonać jego dokładniejszej charakterystyki).

Należy zaznaczyć, że wszelkie podejmowane transakcje w ramach systemu wymagają użycia dwóch kluczy: klucza prywatnego (*private key*) oraz powiązanego z nim klucza publicznego (*public key*) (Clark, Narayanan 2017). W uproszczeniu klucz publiczny odbiorcy pozwala podmiotowi dokonującemu transakcji na odpowiednie zaszyfrowanie zapisu, tak że jedynie odbiorca jako posiadacz pasującego klucza prywatnego jest w stanie odkodować zapis, a tym samym stać się posiadaczem przedmiotu transakcji. Jednocześnie klucz prywatny nadawcy pozwala mu na przeprowadzenie planowanej transakcji, gdyż znajdujące się w ramach przypisanego mu adresu[28] środki tylko wskutek użycia powiązanego z nimi klucza prywatnego mogą zostać wydane. Klucze są generowane w ramach portfela (*wallet*) i możliwe jest posiadanie wielu kluczy zgromadzonych w ramach jednego portfela. Dzięki umieszczeniu w zapisie transakcji identyfikatora transakcji wcześniejszej (*hash*) (Back 2002; Nakamoto 2008), świadczącego o transferze, możliwe jest zweryfikowanie, że podmiot dokonujący transakcji jest w posiadaniu wartości będącej przedmiotem aktualnej transakcji.

Koncepcja zaproponowana przez Satoshi Nakamoto jest zatem doskonałym połączeniem odkryć z dziedziny kryptografii i teorii gier bądź, dokładniej, z obszaru zajmującego się projektowaniem mechanizmów (*mechanism design*), określanego często terminem odwróconej teorii gier (Berg, Davidson, Potts 2018; Hurwicz 1973, 1994). Podstawowe zasady jej funkcjonowania zostały bowiem zaprojektowane w taki sposób, aby zachęcać podmioty zainteresowane maksymalizacją własnej użyteczności do działania zgodnego z regułami gry, gdyż takie zachowanie gwarantuje największą wypłatę, a modelowanie tego rodzaju zachowań jest właśnie przedmiotem zainteresowania wspomnianej powyżej teorii. Maksymalizacja własnej użyteczności oznacza, iż górnicy biorący udział w procesie poszukiwania rozwiązania łamigłówki (a dokładniej starający się znaleźć właściwy element (*nonce*), który pozwoli na uzyskanie identyfikatora (*hash*) spełniającego ustalone przez system kryteria) decydują się na postępowanie zgodnie z zasadami, gdyż to działanie może prowadzić do cennej wygranej (aktualnie 12,5 bitcoina[29]). Manipulacja z ekonomicznego punktu widzenia się nie opłaca, gdyż oznaczałaby utratę zaufania do całego systemu, co w rezultacie prowadziłoby do utraty atrakcyjnej możliwości uzyskiwania nowych bitcoinów za każdy nowy blok. Co więcej, dzięki zastosowaniu zaawansowanych technik kryptograficznych (takich jak opisane powyżej klucze prywatne i publiczne, kryptograficzna funkcja hashowania) owa manipulacja staje się niezwykle trudnym i kosztownym zadaniem, co tylko stanowi dodatkową gwarancję bezpieczeństwa systemu (Davidson, De Filippi, Potts 2018).

---

[27] Wynagrodzenie górnika, który dodał blok do sieci, składa się z dwóch elementów: sumy opłat transakcyjnych zebranych z umieszczonych w bloku transakcji (*transaction fee*) oraz z wynagrodzenia za blok (*block reward*).

[28] Adres powstaje w wyniku odpowiednich przekształceń klucza publicznego, takich jak zastosowanie kryptograficznej funkcji hashowania SHA-256. Oznacza to, że klucz publiczny jest powiązany z kluczem prywatnym i tym samym adres jest również powiązany z konkretnym kluczem prywatnym. Jednoczenie jedynie adres jest widoczny dla innych użytkowników, a klucz prywatny powinien być znany jedynie jego właścicielowi.

[29] Owa wygrana początkowo wynosiła 50 bitcoinów i ulega pomniejszeniu o połowę co 210 000 bloków, czyli co około 4 lata.

3.3. Klasyfikacja dostępnych wariantów w ramach technologii blockchain

Podobnie jak Internet blockchain często jest określany mianem technologii ogólnego przeznaczenia (*general purpose technology*) (Bresnahan, Trajtenberg 1995; Catalini, Gans 2018b) z uwagi na zastosowane mechanizmy działania i szerokie możliwości zastosowania. Należy przy tym zaznaczyć, że określenie „technologia blockchain" jest ogólną nazwą stosowaną w odniesieniu do szerokiego katalogu projektów i inicjatyw, które bazują na tym samym podstawowym schemacie działania, jednakże różnią się cechami i wariantami zastosowań.

Od momentu opisania koncepcji blockchain pojawiło się wiele jej wariantów, będących często kombinacją różnych jej cech i właściwości. Najczęściej stosowany podział opiera się na dwóch kryteriach i klasyfikuje rozwiązania ze względu na prawa dostępu do bazy danych (*read access*) oraz z uwagi na możliwość tworzenia rejestrów (*write/commit access*[30]) (Hileman, Rauchs 2017; Wüst, Gervais 2017). W odniesieniu do praw dostępu wyróżnia się:

– publiczny blockchain (*public blockchain*), dostępny dla wszystkich i pozwalający każdemu podmiotowi na analizę zachodzących transakcji,

– prywatny blockchain (*private blockchain*), dostępny jedynie dla wybranych uczestników, którzy mają prawo wglądu do dokonywanych transakcji.

Jeśli natomiast chodzi o możliwość tworzenia rejestrów, dostępne systemy dzieli się na:

– licencjonowany blockchain (*permissioned blockchain*), gdzie jedynie wybrane podmioty mogą dokonywać zmian czy weryfikacji (takich jak dodawanie bloków) w rejestrze,

– nielicencjonowany blockchain (*permissionless blockchain*), pozwalający wszystkim uczestnikom na udział w procesie dokonywania i weryfikowania zmian.

Czasami zdarza się, że podawane przez media informacje uwzględniają w opisie jedynie jeden wymiar, jednakże należy pamiętać, iż praktycznie zawsze głębsza analiza rozwiązania pozwoli na wskazanie również drugiego. Dobrym sposobem prezentacji omówionej klasyfikacji, pozwalającym także na wskazanie zachodzących pomiędzy nimi zależności, jest umieszczenie omawianych wariantów w macierzy rozwiązań, co zostało przedstawione na schemacie 3. Jak wynika z zaprezentowanego schematu, dwa wymiary są od siebie wprawdzie niezależne, jednakże niespotykane są rozwiązania charakteryzowane jedynie przez jeden wymiar, gdyż jest to zarówno z technicznego, jak i z logicznego punktu widzenia niewłaściwe bądź nawet niemożliwe. Każdy model powinien bowiem mieć mechanizm decydujący zarówno o prawach dostępu, jak i prawach weryfikacji/dokonywania zmian.

Warto mieć na uwadze fakt, że oba wymiary i ich rodzaje także różnią się znacznie pod względem zastosowania biznesowego i celów, jakie dzięki ich zastosowaniu planuje się osiągnąć, stąd też decyzja odnośnie do wariantu działania jest kluczowa i powinna być podjęta na początku procesu tworzenia nowych rozwiązań (Ito i in. 2017). Jednocześnie wskazanych wariantów nie należy interpretować jako skończonej listy możliwości, a jedynie jako punktów odniesienia na całej mapie możliwych do stworzenia kombinacji (Brown 2014).

Należy przy tym zaznaczyć, że jedynie publicznie nielicencjonowany blockchain pozwala na pełne wykorzystanie właściwości nowatorskiej koncepcji. Każda inna modyfikacja jest swego rodzaju kompromisem, umożliwiającym wprawdzie wykorzystanie technologii w odniesieniu do zaobserwowanych

[30] Należy zaznaczyć, że spotykane jest określenie kryterium dostępu jako *read/write access,* a kryterium tworzenia rejestrów jedynie jako *verify access*. Określenie *write* w tym przypadku oznacza tylko możliwość zgłaszania nowych transakcji, natomiast nie odnosi się do możliwości zapisywania ich w ramach łańcucha danych.

problemów, jednakże przykładowo za cenę braku pełnej niezależności czy decentralizacji. Niemniej jednak nie można ich określać w kategoriach „lepszy – gorszy", gdyż każda z owych wersji służy rozwiązaniu innych problemów. Przeglądając aktualnie podejmowane inicjatywy, można stwierdzić, iż obecnie najczęściej spotykanymi rozwiązaniami są połączenia wariantu prywatnego (lub quasi-prywatnego) z licencjonowanym (np. Corda, Hyperledger Fabric), jak również wariantu publicznego z nielicencjonowanym (np. Bitcoin, Ethereum). Analiza biznesowego potencjału przedstawionych charakterystyk, jak również przesłanki pozwalające na podjęcie decyzji odnośnie do wariantu zastosowania zostały zaprezentowane w rozdziale 4.

3.4. Rola i znaczenie reprezentantów wartości

Jak już zostało zaznaczone, jednym z kluczowych elementów opisywanego wieloaspektowego systemu, jakim jest koncepcja blockchain, są reprezentanci wartości, czyli obiekty będące przedmiotem zapisu i obiegu w ramach nowatorskiej infrastruktury. Procesy te przebiegają zgodnie z ustalonymi regułami[31]. Pierwszym z takich obiektów był bitcoin, który z uwagi na to, iż dokument opisujący jego działanie nazwano *a peer-to-peer cash system*, zaczęto nazywać kryptowalutą. Następnie, wskutek rozwoju koncepcji pojawiały się nowe propozycje, często mniej lub bardziej odlegle od pierwotnej koncepcji, w odniesieniu do których stosowano coraz to nowe nazwy, takie jak: kryptowaluta, token, kryptoaktywa czy też kryptowłasność (Beaumier, Kalomeni 2018; Burniske, Tatar 2017). Autorka w niniejszej pracy będzie używała pojęcia kryptoaktywa lub wspomnianego już we wcześniejszych częściach terminu „reprezentant wartości", gdyż w jej opinii jest to pojęcie najszersze, zawierające również pozostałe warianty.

Samo pojęcie „reprezentant wartości" może być przyczyną wielu niejasności, stąd wymaga wyjaśnienia. Zostało ono użyte i wprowadzone celem uwypuklenia możliwości oferowanych przez blockchain. Blockchain bowiem może dotyczyć jedynie cyfrowych obiektów, które są albo nowo tworzone i nic innego poza wspomnianą uniwersalną wartością sobą nie reprezentują, albo są reprezentantami wartości obiektów zewnętrznych, a tym samym wymagają odpowiednich mechanizmów weryfikujących[32]. Blockchain potrafi bowiem jedynie zweryfikować prawidłowość zachodzących wpisów, nie jest natomiast w stanie zweryfikować jakości samych reprezentantów czy faktu, że są oni reprezentantami rzeczywiście istniejących obiektów.

Jedną z trudności jest zrozumienie istoty i roli, jaką poszczególne kryptoaktywa pełnią w ramach proponowanych rozwiązań, i tego, na jakich zasadach działają (Evans 2014; Howell, Niessner, Yermack 2018). Często można spotkać kontrowersyjne opinie mówiące, iż kryptoaktywa są w ogóle niepotrzebne do prawidłowego działania technologii blockchain lub że ich występowanie jest konieczne z uwagi na planowane do osiągnięcia cele. Niemniej jednak w ramach każdego modelu działania koncepcji blockchain konieczne jest posiadanie uwarunkowanych danym przykładem reprezentantów wartości, gdyż w przeciwnym razie nie byłoby elementów podlegających zarówno obiegowi, jak i opisowi w ramach nowatorskiego systemu. W przypadku bitcoin blockchain jest on wspomnianym wpisem, jednakże tym wpisem może być każda inna forma reprezentująca cenną i rzadką informację (Evans 2014; Wright, De Filippi 2017).

[31] Przedmiotem niniejszego artykułu nie jest wprawdzie analiza i klasyfikacja dostępnych kryptoaktywów, jednakże ich całkowite pominięcie nie pozwoliłoby na zrozumienie schematu działania i możliwości wykorzystania omawianej koncepcji.

[32] Tłumaczy to istnienie różnych wariantów blockchain, pozwalających na odpowiednią organizację systemu i całego procesu.

W wariancie prywatnie licencjonowanym możliwe jest zastosowanie innych niż kryptowaktywa rozwiązań pozwalających na śledzenie zapisów, co jest często podkreślane przez autorów prezentowanych inicjatyw. Wynika to z faktu, iż technologia w tym wariancie jest używana przez zaufane grono zainteresowanych, a reguły gry i przebieg transakcji są często regulowane przez głównego twórcę/zarządcę. Niemniej jednak również w tych wariantach niezbędne jest posiadanie odpowiedniego reprezentanta wartości będącej przedmiotem zapisu i obiegu w ramach prywatnie licencjonowanego systemu.

W odniesieniu do wariantu publicznie nielicencjonowanego kryptoaktywa są również jego nieodłącznym elementem, gdyż odzwierciedlają oferowany produkt bądź usługę, a towarzysząca im infrastruktura informuje użytkowników o stanie aktualnym (Beaumier, Kalomeni 2018; Howell, Niessner, Yermack 2018). Przykładowo w odniesieniu do kryptowalut są one reprezentantami uniwersalnej wartości, a tym samym nie są w żaden sposób powiązane z realnymi obiektami (tj. nie są ich reprezentantem), co oznacza, iż blockchain jest w stanie samodzielnie dokonać wspomnianej weryfikacji.

Powyższa charakterystyka dowodzi zatem, że reprezentanci wartości są jednym z trzech głównych elementów nowatorskiego systemu, niezbędnym do jego prawidłowego działania.

3.5. Ewolucja koncepcji blockchain

Blockchain od 2008 r. podlega ciągłemu rozwojowi (Gupta 2017a). Pierwszy blockchain został stworzony na potrzeby bitcoina i na jego konstrukcji budowano kolejne projekty. Polegało to na wykorzystaniu stworzonej na potrzeby bitcoina bazy danych i odpowiedniej zmianie jej właściwości celem modyfikacji zauważonych ograniczeń, takich jak długi czas oczekiwania na potwierdzenie transakcji, stosunkowo niewielka pojemność bloku czy możliwość zastosowania jedynie w odniesieniu do prostych schematów. Za przykłady wyżej opisanych działań można uznać projekty Litecoin czy Namecoin. W literaturze ta faza rozwoju technologii określana jest mianem blockchain 1.0 (Manohar, Briggs b.r.; Zhang, Jacobsen 2018; Zhao, Fan, Yan 2016).

Z uwagi na fakt, iż blockchain zastosowany na potrzeby bitcoina ma wspomniane powyżej ograniczenia, równolegle podejmowano próby zbudowania nowego systemu, celem usunięcia zaobserwowanych problemów. Spektakularnym osiągnięciem było zaproponowanie w 2013 r. koncepcji ethereum przez zaledwie 19-letniego Vitalika Buterina (Buterin 2013). Ethereum miało stać się platformą pozwalającą na budowanie na niej aplikacji mających szerokie zastosowanie i wykraczających poza sektor finansowy. Największą innowacją nowego rozwiązania było natomiast umożliwienie tworzenia tak zwanych inteligentnych kontraktów (*smart contracts*) i stworzenie podstaw do definiowania programowalnych (*programmable*) kryptoaktywów. Po raz pierwszy w historii możliwe stało się zapisanie określonej reguły działania w formie kodu, który się samodzielnie aktywuje i podejmuje działania zgodnie z zawartymi w nim warunkami. Ta faza w historii rozwoju technologii blockchain, ze względu na jej innowacyjność w porównaniu z początkową fazą rozwoju, określana jest terminem blockchain 2.0 (Manohar, Briggs b.r.; Pieroni i in. Raso 2018; Zhang, Jacobsen 2018; Zhao i in. 2016).

Kolejnym etapem na drodze rozwoju koncepcji, określanym jako blockchain 3.0 (Pieroni i in. 2018; Zhang, Jacobsen 2018), było umożliwienie tworzenia zdecentralizowanych organizacji (*decentralised authonomous organisation* – DAO) czy zastosowanie blockchain w odniesieniu do procesów w takich dziedzinach, jak administracja publiczna, służba zdrowia (Halamka, Lippman, Ekblaw 2017) czy też za-

rządzanie przepływem energii (Basden, Cottrell 2017), czyli procesów składających się na budowanie społeczeństwa cyfrowego (*digital society)* (Jacobsen, Zhang 2018; Briggs, Menohar 2018).

Opisana ewolucja koncepcji stanowi dodatkowe potwierdzenie wieloaspektowości koncepcji blockchain, która w miarę upływu czasu znajdowała coraz więcej zwolenników i wiązała się z poszerzającym się katalogiem jej możliwych zastosowań.

4. Biznesowy wymiar blockchain i możliwości jego zastosowania

Blockchain, jak zostało opisane na początku pracy, pojawił się jako potencjalne rozwiązanie dotyczące narastającego kryzysu zaufania, jak również powiększającego się wymiaru cyfrowego gospodarki[33]. Jednocześnie blockchain nie jest tylko kolejną technologiczną rewolucją, ale przede wszystkim nowym rozwiązaniem pozwalającym na stymulowanie współpracy między rozproszonymi podmiotami, które dodatkowo nie wymaga koordynacji ze strony jednostki centralnej.

Centralizacja jest efektywnym podejściem, gdyż pozwala na stworzenie ram działania w odniesieniu do wielu, szczególnie nowych, procesów, tym samym gwarantując prawidłowy ich przebieg. Początkowo bowiem tworzone centralne ramy instytucjonalne czy formy organizacyjne mają za cel minimalizację zachowań oportunistycznych jednostek czy eliminowanie asymetrii informacji (Williamson 1985). Jednakże w miarę powiększania się kompleksowości, niepewności i rosnącej zależności od innych podmiotów wspomniane organizacje czy instytucje same dopuszczały się zachowań oportunistycznych i stają się obiektem licznych nadużyć. W rezultacie pojawia się problem zaufania w odniesieniu do podejmowanych przez nie działań i zakładanej niezależności czy obiektywności.

W takiej sytuacji doskonałym rozwiązaniem wydaje się decentralizacja, która pozwoliłaby na utrzymanie ciągłości prowadzonych działań, jednakże w sposób niezależny od osób trzecich. Wymaga to jednak odpowiedniej infrastruktury i rozwiązań, których dotychczas brakowało. Wraz z pojawieniem się technologii blockchain sytuacja się odmieniła, gdyż blockchain to właśnie rozwiązanie pozwalające na decentralizację (*technology for decentralisation*).

Warto zaznaczyć, iż technologia blockchain – pomimo że proponuje rozwiązanie alternatywne do scentralizowanego – nie kwestionuje roli centralnych instytucji, tylko zmusza do ponownej analizy pełnionych przez nie zadań i funkcji, a jednocześnie podkreśla, jak niezwykle istotne jest posiadanie scentralizowanej logiki. Stąd technologia ta nie powinna być traktowana jako zagrożenie w odniesieniu do istniejących schematów, lecz jedynie jako kolejny etap na drodze ich rozwoju. Blockchain umożliwia zautomatyzowanie powtarzalnych procesów, uwalniając tym samym zasoby ludzkie, które mogą być wykorzystane w procesach tworzenia wartości dodanej. Zastosowanie koncepcji nie prowadzi do minimalizacji roli przykładowo organów rządzących, lecz dodatkowo podkreśla ich kluczową rolę w definiowaniu reguł działania nowych systemów, jednocześnie odciążając te podmioty od obowiązku kontrolowania samego przestrzegania ustalonych reguł. Kontrola ta bowiem będzie się odbywała automatycznie dzięki mechanizmowi „inteligentnych kontraktów" (*smart contracts*), jednostki natomiast będą niezbędne w procesach nadrzędnych, takich jak ustalanie zasad czy negocjowanie warunków, jak również weryfikowanie istnienia obiektów i tworzenia ich odpowiednich cyfrowych reprezentantów.

[33] Przykładowo bitcoin został zaproponowany jako a *peer-to-peer cash system*, dający się przetłumaczyć jako „bezpośredni system gotówkowy", i zaproponował alternatywne rozwiązanie do znanej z wymiaru realnego gotówki, dopasowane do wymogów powiększającego się wymiaru cyfrowego gospodarki.

W konsekwencji koncepcja blockchain to wprawdzie nowe rozwiązanie technologiczne, jednakże z uwagi na umożliwienie stworzenia zdecentralizowanych struktur może być postrzegane jako nowy etap na ścieżce rozwoju modeli biznesowych i form organizacji. Technologia ta bowiem, dzięki wbudowanemu mechanizmowi zachęt oraz poprzez swój zdecentralizowany charakter, pozwala na eliminację dwóch czynników, które przyczyniły się do rozwoju wielu, często skomplikowanych, modeli biznesowych czy struktur rynkowych. Tworzone ustroje i warianty funkcjonowania były bowiem niezbędne celem zapobiegania działaniom oportunistycznym (Williamson 1973, 1975, 1985) oraz pozwalały na centralne monitorowanie zachowań (Alchian, Demsetz, 1972). Można zatem stwierdzić, odwołując się przy tym do założeń nowej ekonomii instytucjonalnej, w tym ekonomii kosztów transakcyjnych (Coase 1937, 1960), że technologia blockchain dzięki posiadanym właściwościom stwarza konkurencyjną dla rynków, organizacji i instytucji formę organizowania się jednostek i zawierania transakcji, która jest w stanie funkcjonować pomimo braku istnienia centralnego podmiotu pełniącego funkcję nadzorcy czy koordynatora.

Blockchain zatem nie jest nową technologią *per se*, lecz jest rozwiązaniem pozwalającym na budowanie nowych, zdecentralizowanych, ekonomiczno-społecznych zależności, tworzenie innowacyjnych modeli biznesowych, kształtowanie niespotykanych dotychczas ram instytucjonalnych. Co więcej, postrzeganie platform blockchain jako nowych form organizacyjnych czy instytucjonalnych nasuwa wniosek, że wskutek ich uzupełnienia o odpowiednie normy (Buchanan 1990), procesy warunkujące podejmowanie decyzji (Olson 2003; Ostrom 1990) czy środki rozliczeniowe (Hayek 1990) możliwe będzie rozpatrywanie ich w kategoriach nowych ekonomii – gospodarek zorientowanych na stymulowanie procesu zarządzania czy produkcji jednego dobra bądź usługi w wymiarze globalnym, a nie wielu usług i produktów w wymiarze lokalnym. Takie podejście jest coraz częściej spotykane w literaturze przedmiotu (Davidson, De Filippi, Potts 2018; Iansiti, Lakhani 2017; The Economist 2018). Warto tu również nawiązać do zyskującej od kilku lat na znaczeniu gospodarki współdzielenia, gdyż blockchain oferuje również w tym kontekście szerokie możliwości. Blockchain bowiem jest zdecentralizowanym organizacyjnie systemem, w ramach którego podmioty mogą się wymieniać posiadanymi zasobami (reprezentantami) w ramach utworzonej zdecentralizowanej infrastruktury, w taki sposób, że wzrost popularności owej platformy wymiany pozwala wszystkim uczestnikom na udział w zyskach, a dodatkowo z uwagi na brak centralnej jednostki potencjalne ryzyko manipulacji czy ataków zostaje zminimalizowane.

Pozwala to tym samym na określanie platform blockchain jako systemu gospodarek wyspecjalizowanych w produkcji określonych dóbr czy usług, które wcześniej często nie mogły być przedmiotem obrotu, czyniąc te platformy podobnymi do firm czy organizacji. Charakterystyka blockchain wymaga tym samym konieczności połączenia zdefiniowanych reguł stosowanych do oceny efektywności gospodarek, skuteczności norm prawnych, jak również modeli biznesowych i na ich podstawie zbudowania kryteriów pozwalających na kategoryzację i charakterystykę zdecentralizowanych rozwiązań. Należy przy tym zaznaczyć, że rozwiązania blockchain są głównie rozwiązaniami ogólnodostępnymi (*open source*), do których każdy może dołączyć czy na podstawie których każdy może budować, co dodatkowo podkreśla konieczność stworzenia nowego modelu analizy ich konkurencyjności i potencjału, odmiennego od powszechnie znanych rozwiązań.

Sam blockchain jako zdecentralizowany i rozproszony system jest szczególnie ciekawą alternatywą dla rozwiązań, w odniesieniu do których powodzenie operacji jest zależne od działań podejmowanych przez pozostałe strony transakcji bądź też wszelkie działania są kontrolowane przez stronę trzecią, która decyduje o końcowym wyniku. W takich systemach istnieje duże ryzyko, że druga strona trans-

akcji nie wypełni stawianych warunków przez stronę inicjującą bądź strona trzecia zostanie zmanipulowana, co w rezultacie zakończy się niepowodzeniem całego procesu i stratami po stronie podmiotu inicjującego czy nawet w odniesieniu do całego systemu (Wüst, Gervais 2017).

4.1. Zastosowanie koncepcji blockchain

Technologia sama w sobie jest jednak niewiele warta, dopóki nie zostanie zdefiniowane jej przeznaczenie i możliwe warianty wykorzystania. Celem zarysowania wspomnianych możliwości zostały przytoczone przykłady zastosowania blockchain w dwóch najpopularniejszych wariantach (są różne dla rejestru publicznie nielicencjonowanego i dla prywatnie licencjonowanego), co oczywiście nie oznacza, iż inne warianty są mniej istotne, a tylko potwierdza przeważającą liczbę projektów preferujących oba rozwiązania.

Zastosowanie koncepcji blockchain w wariancie publicznie nielicencjonowanym

Publiczny i nielicencjonowany blockchain jest podstawowym i pierwszym rozwiązaniem, które zostało zaprezentowane w 2008 r. (Nakamoto 2008). Należy podkreślić przy tym, że jedynie to rozwiązanie umożliwia pełną niezależność od jakiejkolwiek jednostki centralnej, gwarantując tym samym wiarygodność zapisów.

Omawiany wariant koncepcji pozwala na całkowite wyeliminowanie roli pośrednika, a system zasad działania zawarty jest w kodzie, na którym technologia bazuje (Iansiti, Lakhani 2017). Co więcej, dzięki rozwiązaniu problemu dwukrotnego wydawania (*double spending*) (Catalini, Gans 2018b; Dwyer 2015; Wayner 1997) ta wersja technologii daje podstawy do stworzenia warunków wymiany rynkowej w odniesieniu do dóbr cyfrowych, które wcześniej w ogóle nie były przedmiotem obrotu albo ich wymiana odbywała się jedynie dzięki pośrednikom, takich jak wolna przestrzeń na dysku (przykładem projektu jest Filecoin[34]), moc obliczeniowa (przykładem jest projekt Golem[35]) czy pliki muzyczne (projekty takie jak Mycelia[36]) (Heap 2017; Murck 2017; Tapscott, Tapscott 2017). Zastosowanie technologii pozwala tym samym, jak już zasygnalizowano, na stworzenie nowych modeli biznesowych, form organizacyjnych czy ram instytucjonalnych, działających w warunkach organizacyjnej decentralizacji, będąc jednocześnie logicznie scentralizowanymi (Forde 2017; Iansiti, Lakhani, 2017). Przykład klasyfikacji możliwych rozwiązań został zaprezentowany na schemacie 4.

Należy podkreślić, że w odniesieniu do wariantu publicznie nielicencjonowanego bardzo ważną rolę odgrywają kryptoaktywa, gdyż to na nich opiera się cały proces wymiany i zarządzania. Dzięki nim możliwe jest stymulowanie rozwoju projektu, jak również motywowanie uczestników zarówno do oferowania, jak i zakupu dobra będącego przedmiotem wymiany (Catalini, Gans 2018a; Evans 2014; Howell, Niessner, Yermack 2018; Popper 2015). Warto zwrócić jednocześnie uwagę na fakt, iż proces ten różni się od modelu, na którym bazują projekty wykorzystujące Internet. W odniesieniu do koncepcji blockchain twórcy podstawowej platformy partycypują we wzroście jej wartości. Dzięki wbudowanemu mechanizmowi kryptoaktywów (których określoną ilość zatrzymują jako pewnego rodzaju zapłatę

[34] https://filecoin.io/.
[35] https://golem.network/.
[36] http://myceliaformusic.org/.

za włożony wysiłek) w momencie, gdy stworzone rozwiązanie cieszy się dużą popularnością, przyczyniając się tym samym do wzrostu wartości kryptoaktywów, wzrasta wartość posiadanego przez założycieli kapitału. Inaczej ten mechanizm działa w przypadku technologii Internet, gdyż tam nie twórcy protokołu, a głównie producenci aplikacji, takich jak Google, Facebook, Netflix, korzystają na wzroście zainteresowania oferowanym rozwiązaniem (Monegro 2017).

Poza projektami oferującymi pewnego rodzaju dobro lub usługę znane są również przykłady platform, które za główny cel przyjmują stworzenie środków wymiany niezależnych od obecnie funkcjonującego systemu pieniężnego. Przykładami takich rozwiązań są bitcoin, litecoin czy monero, które różnią się pomiędzy sobą wybranymi parametrami, takimi jak szybkość transakcji bądź anonimowość. Są one wymienialne na oficjalne środki rozliczeniowe (*fiat money*), jak również pozwalają na zakup kryptoaktywów pochodzących z pozostałych platform, stając się tym samym w pewnym sensie środkiem rozliczeniowym technologii blockchain. Warto zwrócić w tym miejscu uwagę na fakt, iż sama koncepcja pieniądza międzynarodowego czy niezależnego nie jest nowa (Evans 2014; Stiglitz 2011). Można zatem stwierdzić, że wymienione przykłady projektów są częściowo urzeczywistnieniem długo zgłaszanych pomysłów, których realizacja stała się możliwa dzięki wynalezieniu technologii blockchain. Jednakże z uwagi na brak jakichkolwiek zasad obrotu zarówno te, jak i pozostałe kryptoaktywa stały się przedmiotem zainteresowania licznej grupy spekulantów. Podejmowane przez nich działania doprowadziły do spektakularnych wzrostów cen tych aktywów, wzbudzając tym samym zainteresowanie szerokiego grona odbiorców. W rezultacie wiele podmiotów, często w ogóle niemających pojęcia o technologii blockchain, decydowało się na ulokowanie posiadanych środków w innowacyjne przedsięwzięcia, nawet bez ich wcześniejszej analizy. Przyczyniło się to do powstania swego rodzaju bańki spekulacyjnej (Adriano 2018; Russo 2018) i jednocześnie spowodowało odwrócenie uwagi od ogromnego potencjału samej technologii. Co więcej, zaburzyło to proces prawidłowego postrzegania roli kryptoaktywów w rozwoju technologii blockchain i ich pierwotnej użyteczności.

Przykład wspomnianej banki spekulacyjnej jest również ciekawą obserwacją z socjologicznego punktu widzenia. Wskazuje on bowiem, iż nie same reguły działania systemu, ale reguły jego działania i użytkowania mogą zadecydować o powodzeniu proponowanych rozwiązań. Kryptoaktywa takie jak bitcoin mają „politykę monetarną" dokładnie zapisaną w kodzie, regulującą ich maksymalną ilość i system dystrybucji (Böhme i in. 2015; Catalini, Gans 2018a; Evans 2014; Ito i in. 2017), jednakże mimo wszystko podlegają one licznym atakom spekulacyjnym i manipulacjom. Zaproponowana technologia stworzyła możliwość budowania zdecentralizowanych systemów, jednakże nadal kluczowe jest działanie jednostki i to ono zadecyduje o powodzeniu podejmowanych inicjatyw. Systemy te, mimo że mają dokładnie zdefiniowane wewnętrzne reguły, motywujące uczestników do postepowania zgodnie z ustalonymi mechanizmami weryfikacji (Evans 2014), rzadko odnoszą się do zasad tyczących się obrotu kryptoaktywami i procesu dokonywania zmian czy aktualizacji kodu (*on/off chain governance*). Zagadnienie to jest, jak wykazano, niezwykle istotne i brak jego uwzględnienia i poprawnego zaplanowania może skutkować porażką całego systemu. Co więcej, jak zaznaczono, dopiero uwzględnienie tego aspektu w połączeniu z innymi pozwala na postrzeganie platform blockchain i tworzonych w oparciu o nie rozwiązań jako swego rodzaju nowych ekonomii.

Ogólnie rzecz biorąc, publicznie nielicencjonowany blockchain jest rozwiązaniem, którego brakowało, niosącym ze sobą zarówno wiele możliwości, jak i zagrożeń. Wymaga on kompleksowej analizy, jednakże potencjał, jaki się z nim wiąże, skłania ku stwierdzeniu, że błędem byłoby zaniechanie jego dalszego rozwoju i analizy.

Zastosowanie technologii blockchain w wariancie prywatnie licencjonowanym

Rozwiązania prywatnie licencjonowane, określane wprawdzie również mianem technologii blockchain bądź technologii rozproszonego rejestru, wykorzystują jedynie część oferowanych możliwości i często pozbawione są aspektu pełnej decentralizacji czy niezależności. Podmioty współpracujące w ramach tychże platform podlegają przykładowo weryfikacji i akceptacji przez zarządcę systemu, który również ma pełną władzę nad zdecentralizowaną bazą danych. Wątpliwy w takiej sytuacji jest aspekt niezależności i wiarygodności zapisu z uwagi na to, że istnieje ryzyko jego manipulacji przez jeden lub kilka podmiotów zarządzających platformą. Proponowane rozwiązanie wprawdzie nadal oferuje liczne ulepszenia czy nawet przewyższa pod względem niektórych aspektów rozwiązania publicznie nielicencjonowane, jednakże kluczowy aspekt, a mianowicie pełna decentralizacja, nie jest w odniesieniu do niego możliwy do osiągniecia.

Rozwiązania prywatnie licencjonowane, w odróżnieniu od modeli publicznie nielicencjonowanych, nie mają za zadanie stworzenia nowych modeli biznesowych, a ich głównym celem jest usprawnienie procesów biznesowych, poprawa efektywności czy obniżenie kosztów transakcyjnych[37] (Nowiński, Kozma 2017; Oh, Shong 2017).

Próby ich stworzenia podejmowane były początkowo głównie przez instytucje finansowe, które w ramach tworzonych konsorcjów czy przedsięwzięć *joint venture* testowały wykorzystanie technologii blockchain w odniesieniu do wspólnych dla wszystkich podmiotów procesów biznesowych. Przykładem takiej współpracy może być grupa R3, licząca ponad 200 członków, która opracowała blockchain Corda (Brown 2018).

Znaczącymi graczami w odniesieniu do prywatnie licencjonowanych rozwiązań są również firmy z sektora IT, głownie IBM i Microsoft. IBM proponuje przykładowo szereg rozwiązań wykorzystujących technologię blockchain, takich jak Hyperledger Fabric czy Hyperledger Composer (IBM 2018b). Firma ta współpracuje również z licznymi przedsiębiorstwami, na przykład z Wal-Mart (Business Wire 2017) czy Maersk (IBM 2018a) celem wspólnego opracowania rozwiązań wykorzystujących Hyperldger Fabric, czyli platformę blockchain zaproponowaną i zarządzaną przez firmę IBM.

Należy zaznaczyć, że możliwe są również warianty pośrednie, wykorzystujące z jednej strony publiczny blockchain, z drugiej natomiast zakładające zarządzanie nim w sposób licencjonowany[38]. Często jednak są one jedynie zarysem idei, a brak działających prototypów utrudnia ich prawidłową analizę.

Jak wykazano, wariant prywatnie licencjonowany różni się znacznie od wariantu publicznie nielicencjonowanego i dokonując jakichkolwiek porównań, należy mieć na uwadze zaobserwowaną odmienność, jak również ich przeznaczenie.

4.2. Stan rozwoju technologii, szanse i zagrożenia

Pomimo trudnych początków technologia blockchain już na dobre zadomowiła się w środowiskach naukowych i biznesowych. Światowe Forum Ekonomiczne w raporcie wydanym w 2015 r. oszacowało, że do 2027 r. 10% produktu narodowego brutto w ujęciu globalnym będzie przechowywane w ramach

[37] Obniżenie wspomnianych kosztów transakcyjnych jest możliwe, gdyż przykładowo w przypadku stworzenia cyfrowych reprezentantów wartości przedsięwzięć, których reprezentanci mogą być przedmiotem obiegu w ramach utworzonych platform blockchain, cały proces transakcyjny przebiega automatycznie, co znacznie redukuje wspomniane koszty.

[38] Jako przykład można podać projekt WePower proponujący rozwiązanie dla branży energetycznej.

technologii blockchain (World Economic Forum 2015). Coraz więcej instytucji – zarówno publicznych, jak i prywatnych – planuje jej wykorzystanie, o czym świadczą chociażby wyniki badania przeprowadzonego przez firmę IBM, informujące, iż 90% ankietowanych przedstawicieli władz rządowych, jak również 91% zapytanych dyrektorów banków planuje inwestycje w technologię blockchain w 2018 r. (IBM 2018c; Wee Kwang 2017). Kwota zebrana na projekty w ramach ICO (*initial coin offering* – nowa forma finansowania projektów budowanych w oparciu o technologię blockchain) w samym 2017 r. przekroczyła 5,6 bln USD (Williams-Grut 2018), zdecydowanie przewyższając tym samym środki zainwestowane przez fundusze podwyższonego ryzyka (*venture capital*) w przedsięwzięcia typu start-up. Znane są także przykłady firm, które zdecydowały się bądź na umieszczenie w nazwie terminu blockchain, bądź nawiązanie w strategii biznesowej do możliwości wykorzystania technologii celem zwiększenia wyceny swoich akcji czy zainteresowania ofertą szerszego grona potencjalnych inwestorów; jako przykład można podać firmę Long Island Ice Tea Corp. (Leinz, Shapira 2017) czy projekt KodakCoin (Shen 2018). Wśród zainteresowanych możliwościami wykorzystania technologii blockchain znajdują się również całe kraje, np. Estonia (e-Estonia b.r.; Mainelli 2017b), Dubaj (Dubai Future Foundation b.r.; Gupta, ConsenSys LLC 2017) czy Wielka Brytania (Lee 2016). Analizują one zastosowanie technologii w odniesieniu do takich procesów, jak głosowanie, zarządzanie i dostęp do dokumentacji medycznej, bezpieczeństwo danych czy identyfikacja społeczeństwa (Berg, Davidson, Potts 2018; Mainelli 2017a, 2017b; Pilkington 2016).

Przytoczone fakty potwierdzają zatem, z jak dużym zainteresowaniem aktualnie spotyka się omawiana technologia, pomimo iż wciąż brakuje projektów, które mogłyby zaświadczyć o jej potencjale. Co więcej, analiza przeprowadzone przez firmę EY (2017) potwierdza, że większość projektów podejmowanych w wariancie publicznie nielicencjonowanym kończy się niepowodzeniem. Wydawać by się mogło, że z uwagi na mniejszy stopień skomplikowania lepiej powinny radzić sobie projekty podejmowane w wariancie prywatnie licencjonowanym, jednakże również w odniesieniu do tej formy wykorzystania technologii blockchain brakuje rezultatów, które można byłoby poddać analizie.

Wykorzystanie możliwości oferowanych przez technologie wymaga analizy wielu elementów. Jednym z aspektów, które należy rozważyć celem zdefiniowania mechanizmu pozwalającego na rozwiązanie zgłaszanego problemu, jest rodzaj dobra będącego przedmiotem obrotu. W przypadku dóbr digitalnych utworzonych w ramach platformy blockchain nie występuje problem ich weryfikacji celem włączenia do sieci (Tucker, Catalini 2018). Ten aspekt jest tymczasem kluczowy w odniesieniu do dóbr fizycznych, które przed dołączeniem do sieci muszą zostać zdigitalizowane. Nie jest to zadaniem łatwym do wykonania bez naruszenia właściwości oferowanych przez technologię blockchain. Potwierdza to fakt, iż dotychczas przykłady zastosowania technologii podawane były głównie w odniesieniu do sektora usług finansowych, w ramach którego większość dóbr ma już formę cyfrową. Natomiast projekty zakładające zarzadzanie przepływem energii (Basden, Cottrell 2017) czy logistyką produktów dopiero w ostatnim czasie stają się popularne, będąc przy tym często rozwiązaniami prywatnie licencjonowanymi czy przyjmującymi formę mieszaną.

Co więcej, należy zaznaczyć, że blockchain jest jedynie infrastrukturą przepływu reprezentantów wartości, natomiast sam przepływ dóbr w przypadku, gdy mają one postać fizyczną czy nie są pierwotnie utworzone na platformie blockchain, odbywa się w ramach istniejącej infrastruktury. Coraz częściej mówi się o tokenizacji aktywów, jednakże należy pamiętać, że owa tokenizacja umożliwia jedynie śledzenie przepływu reprezentantów aktywów w ramach bazy danych blockchain, podczas gdy ich obrót odbywa się nadal w wymiarze rzeczywistym. Stwarza to dodatkową trudność dopasowania nowej technologii i jej potencjału do możliwości infrastruktury. Aspekt ten często jest pomijany bądź przemilczany przy prezentacji nowych projektów.

Dodatkowo, proponowane rozwiązania często tyczą się przepływu dóbr, które można zakwalifikować jako dobra publiczne lub quasi-publiczne, do których dostęp musi zostać zapewniony wszystkim obywatelom. Niezbędne jest uwzględnienie tego aspektu, aby przeciwdziałać „monopolowi 2.0", który może powstać w momencie, gdy operatorzy prywatnie licencjonowanych platform będą decydowali o przynależności do sieci i prawidłowości zapisu.

Jak wykazano, technologia blockchain nie jest rozwiązaniem idealnym, mającym zastosowanie we wszelkich obszarach, i poddając ją analizie, należy poprawnie rozważyć zarówno jej pozytywne, jak i negatywne strony. Dodatkowo jej prawidłowe wykorzystanie wymaga głębokiej analizy problemu biznesowego, jak również zakładanych do osiągnięcia celów. Bez tego proponowane rozwiązania zamiast przyczynić się do poprawy przebiegu procesów, mogą spowodować ich dodatkowe skomplikowanie. Niemniej jednak blockchain znajduje zastosowanie zarówno do konstrukcji nowych, jak i usprawnienia funkcjonujących rozwiązań. Jednocześnie jest on dopiero w początkowej fazie rozwoju, stąd też podlega ciągłym zmianom i ulepszeniom. Dopiero w ciągu kolejnych kilku bądź kilkunastu lat będzie można poznać jego pełne możliwości.

5. Podsumowanie

Koncepcja zdecentralizowanego, rozproszonego i zsynchronizowanego systemu, choć początkowo niedoceniana, znajduje zastosowanie zarówno do konstrukcji nowych, jak i do usprawnienia funkcjonujących mechanizmów działania. Blockchain jest systemem składającym się z trzech elementów: (i) cyfrowych reprezentantów wartości, (ii) zdecentralizowanej infrastruktury oraz (iii) scentralizowanej zasady (logiki systemu), przy czym każdy element jest niezwykle istotny dla prawidłowego działania systemu. Niemniej jednak konstrukcja poszczególnych elementów może być różna w zależności od planowanego zastosowania, przy czym często może to się wiązać z licznymi ograniczeniami w odniesieniu do całego systemu, co tylko podkreśla istotność zrozumienia zarówno samej koncepcji, jak i oferowanych przez nią możliwości.

Połączenie kryptografii z teorią projektowania mechanizmów (nazywaną również odwróconą teorią gier) pozwoliło na stworzenie rozwiązań eliminujących problem dwukrotnego wydawania i konieczność polegania na centralnych jednostkach celem zapewnienia poprawności przebiegu procesów w ramach systemu. Jednocześnie wbudowany został mechanizm zachęt oparty o reprezentantów wartości, umożliwiający motywowanie uczestników do postępowania według zdefiniowanych zasad w sposób niewymagający centralnego zarządzania czy monitorowania. Dało to tym samym podstawy do budowania nowego rodzaju zależności, schematów działania i organizacji, które z jednej strony pozwalają na definiowanie nowych modeli biznesowych, a z drugiej usprawniają funkcjonowanie znanych rozwiązań, takich jak chociażby rozliczenia międzynarodowe czy procesy głosowania.

Jako koncepcja proponująca alternatywną do centralnie zarządzanych czy wymagających pośrednika formę działania blockchain był odpowiedzią na pogłębiający się kryzys zaufania obserwowany w wielu dziedzinach gospodarki, jak również powiększający się wymiar cyfrowy gospodarki.

Niemniej jednak blockchain ma również swoje ograniczenia, a jego błędne zastosowanie może wręcz być przyczyną wystąpienia jeszcze większego ryzyka niż ryzyko obserwowane przed jego zastosowaniem. W rezultacie z uwagi zarówno na możliwe zagrożenia, jak również innowacyjny charakter koncepcji konieczne jest tworzenie nowych modeli pozwalających na jej klasyfikację i charakterystykę, jak również stymulujących jej prawidłowy rozwój i minimalizujących ryzyko błędów czy nadużyć.

Blockchain jest dopiero w początkowym stadium rozwoju, stąd trudno jest wykazać efekty zastosowania koncepcji czy zdecydować o jej prawidłowym przeznaczeniu. Niemniej jednak blockchain kryje w sobie ogromny potencjał i następne lata pokażą, w jaki sposób może on zostać najlepiej osiągnięty i wykorzystany.

Bibliografia

Adhami S., Giudici G., Martinazzi S. (2018), Why do businesses go crypto? An empirical analysis of Initial Coin Offerings, *Journal of Economics and Business*, 100, November–December, 64–75.

Adriano A. (2018), Crypto bubble? An historical analysis of financial crises, *IMF F&D Magazine*, 55(2), 20–21, http://www.imf.org/external/pubs/ft/fandd/2018/06/crypto-bubble-historical-analysis-of-financial-crises/adriano.htm.

Agrawal A., Gans J., Goldfarb A. (2016), The simple economics of machine intelligence, *Harvard Business Review*, November, https://hbr.org/2016/11/the-simple-economics-of-machine-intelligence.

Alchian A.A., Demsetz H. (1972), Production, information costs, and economic organization, *The American Economic Review*, 62(5), 777–795.

Alstyne M.W.V., Parker G.G., Choudary S.P. (2016*),* Pipelines, platforms, and the new rules of strategy, *Harvard Business Review*, April, https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy.

Ametrano F.M. (2016), *Hayek money: the cryptocurrency price stability solution,* SSRN Scholarly Paper, 2425270, https://papers.ssrn.com/abstract=2425270.

Antonopoulos A. (2014), Bitcoin security model: trust by computation, *O'Reilly Radar*, February, http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.

Athey S., Catalini C., Tucker C. (2017), *The digital privacy paradox: small money, small costs, small talk,* National Bureau of Economic Research, 23488,https://people.stanford.edu/athey/sites/default/files/digital_privacy_paradox_02_13_17.pdf.

Bach L.M., Mihaljević B., Žagar M. (2018), *Comparative Analysis of Blockchain Consensus Algorithms*, 41st International Convention of Information and Communication Technology, Electronics and Multielectronics (MIPRO), Opatija, May.

Back A. (2002), *Hashcash – a denial of service counter-measure*, http://www.hashcash.org/hashcash.pdf.

Basden J., Cottrell M. (2017), How utilities are using blockchain to modernize the grid, *Harvard Business Review*, March, https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid.

Beaumier G., Kalomeni K. (2018), *Cryptocurrencies: new rules for a new technology?*, Research Note, Universite Laval.

Berg C., Davidson S., Potts J. (2018), *Some public economics of blockchain technology,* SSRN Scholarly Paper, 3132857, https://papers.ssrn.com/abstract=3132857.

BIS (2017), *Distributed ledger technology in payment, clearing and settlement*, Bank for International Settlements.

Blomqvist K. (1997), The many faces of trust, *Scandinavian Journal of Management*, 13(3), 271–286.

Böhme R., Christin N., Edelman B., Moore T. (2015), Bitcoin: economics, technology, and governance, *Journal of Economic Perspectives*, 29(2), 213–238.

Bonneau J., Felten E., Miller A., Narayanan A. (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

Bresnahan T.F., Trajtenberg M. (1995), General purpose technologies 'engines of growth'?, *Journal of Econometrics*, 65(1), 83–108.

Brown R.G. (2014), *The "unbundling of trust": How to identify good cryptocurrency opportunities*, https://gendal.me/2014/11/14/the-unbundling-of-trust-how-to-identify-good-cryptocurrency-opportunities/.

Brown R.G. (2018), *The Corda Platform: an introduction*, https://www.corda.net/content/corda-platform-whitepaper.pdf.

J.M. (1990), The domain of constitutional economics, *Constitutional Political Economy*, 1(1), 1–18.

Burn-Callander R. (2014), The history of money: from barter to bitcoin, *The Telegraph*, https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html.

Burniske C., Tatar J. (2017), *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*, McGraw-Hill.

Business Wire (2017), *Walmart, JD.com, IBM and Tsinghua University launch a blockchain food safety alliance in China*, https://www.businesswire.com/news/home/20171213006244/en/Walmart-JD.com-IBM-Tsinghua-University-Launch-Blockchain.

Buterin V. (2013), *Ethereum whitepaper. A next generation smart contract & decentralized application platform*, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Casey M.J., Wong P. (2017), Global supply chains are about to get better, thanks to blockchain, *Harvard Business Review*, March, https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain.

Catalini C. (2017), How blockchain applications will move beyond finance, *Harvard Business Review*, March, https://hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance.

Catalini C., Gans J.S. (2018a), *Initial coin offerings and the value of crypto tokens,* NBER Working Paper, 24418, National Bureau of Economic Research.

Catalini C., Gans J.S. (2018b), *Some simple economics of the blockchain*, NBER Working Paper, 22952, National Bureau of Economic Research.

Chakravorti B., Bhalla A., Chaturvedi R.S. (2018), The 4 dimensions of digital trust, charted across 42 countries, *Harvard Business Review*, February, https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries.

Choudary S.P. (2015), *Platform scale. How an emerging business model helps startups build large empires with minimum investments,* Platform Thinking Labs Pte.

Clark J., Narayanan A. (2017), Bitcoin's academic pedigree, *Communication of the ACM*, 60(12), 36–45.

Clikeman P.M. (2013), *Called to Account: Financial Frauds that Shaped the Accounting Profession*, Routledge.

Coase R.H. (1937), The nature of the firm, *Economica*, 4(16), 386–405.

Coase R.H. (1960), The problem of social cost, *Journal of Law and Economics*, 3, 1–44.

Cochrane K. (2018), To regain consumers' trust, marketers need transparent data practices, *Harvard Business Review*, June, https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices.

Davidson S., De Filippi P., Potts J. (2018), *Economics of blockchain*, https:// ssrn.com/abstract=2744751.

Davies G. (2002), *A History of Money. From Ancient Times to the Present Day*, University of Wales Press.

De Filippi P. (2017), What blockchain means for the sharing economy, *Harvard Business Review*, March, https://hbr.org/2017/03/what-blockchain-means-for-the-sharing-economy.

Dubai Future Foundation (b.r.), *Global Blockchain Council*, http://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/.

Dwyer G.P. (2015), The economics of bitcoin and similar private digital currencies, *Journal of Financial Stability*, 17, 81–91.

e-Estonia (b.r.), *e-Estonia – We have built a digital society and so can you*, https://e-estonia.com.

Euromoney (2005), *Awards for excellence 2005*, https://www.euromoney.com/article/b1320xynwhdhwk/awards-for-excellence-2005.

Evans D.S. (2014), Economic aspects of bitcoin and other decentralized public-ledger currency platforms, *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2424516.

EY (2017), *EY research: initial coin offerings (ICOs)*, https://www.ey.com/Publication/vwLUAssets/ey-study-ico-research/$FILE/ey-study-ico-research.pdf.

FabricVentures, TokenData (2018), *The state of the token market Final2.pdf*, https://static1.squarespace.com/static/5a19eca6c027d8615635f801/t/5a73697bc8302551711523ca/1517513088503/The+State+of+the+Token+Market+Final2.pdf.

Fjeldstad Ø.D., Snow C.C. (2018), Business models and organization design, *Long Range Planning*, 51(1), 32–39.

Forde B. (2017), Using blockchain to keep public data public, *Harvard Business Review*, March, https://hbr.org/2017/03/using-blockchain-to-keep-public-data-public.

Friedman M. (1992), *Money Mischief: Episodes in Monetary History*, Harcourt Brace Jovanovich Publishers.

Gupta V. (2017a), A brief history of blockchain, *Harvard Business Review*, February, https://hbr.org/2017/02/a-brief-history-of-blockchain.

Gupta V. (2017b), The promise of blockchain is a world without middlemen, *Harvard Business Review*, March, https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen.

Gupta V., ConsenSys LLC (2017), *Building the hyperconnected future on blockchain. World Government Summit*, http://internetofagreements.com/files/WorldGovernmentSummit-Dubai2017.pdf.

Hacker P., Thomale C. (2017), *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law,* SSRN Scholarly Paper, 3075820, https://papers.ssrn.com/abstract=3075820.

Halamka J.D., Lippman A., Ekblaw A. (2017), The potential for blockchain to transform electronic health records, *Harvard Business Review*, March, https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

Heap I. (2017), Blockchain could help musicians make money again, *Harvard Business Review*, June, https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again.

Hileman G., Rauchs M. (2017), *2017 global blockchain benchmarking study,* SSRN Scholarly Paper, 3040224, Social Science Research Network, https://papers.ssrn.com/abstract=3040224.

Howell S.T., Niessner M., Yermack D. (2018), *Initial coin offerings: financing growth with cryptocurrency token sales,* National Bureau of Economic Research, w24774.

Hurwicz L. (1973), The design of mechanisms for resource allocation, *The American Economic Review*, 63(2), 1–30.

Hurwicz L. (1994), Economic design, adjustment processes, mechanisms, and institutions, *Economic Design*, 1(1), 1–14.

Iansiti M., Lakhani K.R. (2017), The truth about blockchain, *Harvard Business Review*, January, https://hbr.org/2017/01/the-truth-about-blockchain.

IBM (2017), *IBM announces major blockchain collaboration with Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to address Food Safety Worldwide*, https://www.newswire.ca/news-releases/ibm-announces-major-blockchain-collaboration-with-dole-driscolls-golden-state-foods-kroger-mccormick-and-company-mclane-company-nestle-tyson-foods-unilever-and-walmart-to-address-food-safety-worldwide-641378083.html.

IBM (2018a), *Maersk and IBM to form joint venture applying blockchain to improve global trade and digitize supply chains*, https://www.newswire.ca/news-releases/maersk-and-ibm-to-form-joint-venture-applying-blockchain-to-improve-global-trade-and-digitize-supply-chains-669513713.html.

IBM (2018b), *Blockchain solutions – IBM blockchain*, https://www.ibm.com/blockchain/aw-en/offerings.html.

IBM (2018c), *Build customer trust and enhance the banking experience with IBM Blockchain*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=92014192USEN&.

Ito J., Narula N., Ali R. (2017), The blockchain will do to the financial system what the Internet did to media, *Harvard Business Review*, March, https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.

Kenney M., Zysman J. (2015), *Choosing a future in the platform economy: the implications and consequences of digital platforms*, Kauffman Foundation New Entrepreneurial Growth Conference, http://www.brie.berkeley.edu/wp-content/uploads/2015/02/PlatformEconomy2DistributeJune21.pdf.

Kim H.M., Laskowski M. (2018), Toward an ontology-driven blockchain design for supply-chain provenance – business – ProQuest, *Intelligent Systems in Accounting, Finance and Management*, 25(1), 18–27.

Knight K., Berman J. (2009), Lehman's three big mistakes, *Harvard Business Review*, September, https://hbr.org/2009/09/lessons-from-lehman.

Koehn N. (2009), Lehman in context: a historical perspective, *Harvard Business Review*, September, https://hbr.org/2009/09/lehman-and-the-opportunity-for.

Konopczak M., Sieradzki R., Wiernicki M. (2010), Kryzys na światowych rynkach finansowych – wpływ na rynek finansowy w Polsce oraz implikacje dla sektora realnego, *Bank i Kredyt*, 41(6), 45–70.

Kshetri N. (2018), 1 blockchain's roles in meeting key supply chain management objectives – business – ProQuest, *International Journal of Information Management*, 39, April, 80–89, https://www.sciencedirect.com/science/article/pii/S0268401217305248.

Lee R. Dave C.-J. (2016), Blockchain and benefits – a risky mix?, *BBC News,* https://www.bbc.com/news/technology-36785872.

Leinz K., Shapira A. (2017), *Long Island Iced Tea soars after changing its name to Long Blockchain*, Bloomberg.Com, https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain.

Conte de Leon D., Stalick A.Q., Jillepalli A.A., Haney M.A., Sheldon F.T. (2017), Blockchain: properties and misconceptions, *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 286–300.

Mai F., Shan Z., Wang X.S., Chiang R.H.L. (2018), How does social media impact bitcoin value? A test of the silent majority hypothesis, *Journal of Management Information Systems*, 35(2018), 19–52.

Mainelli M. (2017a), Blockchain will help us prove our identities in a digital world, *Harvard Business Review*, March, https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world.

Mainelli M. (2017b), Blockchain could help us reclaim control of our personal data, *Harvard Business Review*, October, https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data.

Manohar A.K., Briggs J. 2018), *Identity management in the age of Blockchain 3.0*, CHI 2018 Workshop on HCI for Blockchain.

Mattila J., Seppälä T. (2016), *Digital trust, platforms, and policy*, Research Institute of the Finnish Economy, ELTA Brief, 42, 1–42.

McWaters J., Galaski R. (2017), *Beyond Fintech: a pragmatic assessment of disruptive potential in financial services,* Future of Financial Services series, Deloitte, World Economic Forum, 1–197, http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf.

Mengelkamp E., Gärttner J., Rock K., Kessler S., Orsin L., Weinhardt (2017), Designing microgrid energy markets. A case study: the Brooklyn Microgrid, *Applied Energy*, 210, 870–880.

Monegro J. (2017), *Fat protocols, union square ventures*, http://www.usv.com/blog/fat-protocols.

Moore T., Christin N. (2013), *Beware the middleman: empirical analysis of bitcoin-exchange risk*, w: A.-R. Sadeghi (red.), *Financial Cryptography and Data Security,* Berlin Heidelberg.

Murck P. (2017), Who controls the blockchain, *Harvard Business Review*, April, https://hbr.org/2017/04/who-controls-the-blockchain.

Nakamoto S. (2008), *Bitcoin: a peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf.

Nowiński W., Kozma M. (2017), How can blockchain technology disrupt the existing business models?, *Entrepreneurial Business and Economics Review*, 5(3), 173–188.

Nurisso G., Prescott E.S. (2017), *The 1970s origins of too big to fail*, https://www.clevelandfed.org:443/newsroom and events/publications/economic commentary/2017 economic commentaries/ec 201717 origins of too big to fail.

Oh J., Shong I. (2017), A case study on business model innovations using blockchain: focusing on financial institutions, *Asia Pacific Journal of Innovation and Entrepreneurship*, 11(3), 335–344.

Olson M. (2003), *The logic of collective action: public goods and the theory of groups,* Harvard University Press.

Osterwalder A., Pigneur Y. (2010), *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*.

Ostrom E. (1990), *Governing the Commons: the Evolution of Institutions for Collective Action*, Cambridge University Press.

Partnoy F. (2013), Five years after Lehman's collapse, bankers still haven't confronted their biases, *Harvard Business Review*, September, https://hbr.org/2013/09/five-years-after-lehmans-collapse-bankers-still-havent-confronted-their-biases.

Pennington R., Wilcox H.D., Grover V. (2003), The role of system trust in business-to-consumer transactions, *Journal of Management Information Systems*, 20(3), 197–226.

Pieroni A., Scarpato N., Di Nunzio L., Fallucchi F., Raso M. (2018), Smarter city: smart energy grid based on blockchain technology, *International Journal on Advanced Science, Engineering and Information Technology*, 8(1), 298–306.

Pilkington M. (2016), *Blockchain Technology: Principles and Applications*, University of Burgundy.

Popper N. (2015), *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, HarperCollins Publishers.

PR Newswire (2017), *Transparency-one and Microsoft announce blockchain service for supply chain transparency: Blockchain initiative will enhance security of global supply chain data – Business – ProQuest*, https://www.transparency-one.com/microsoft-blockchain-supply-chain-transparency/.

Russo C. (2018), *Binance's venture fund head is waiting for ICO bubble to burst*, Bloomberg.Com, https://www.bloomberg.com/news/articles/2018-06-04/binance-s-venture-fund-head-is-waiting-for-ico-bubble-to-burst.

Schrage M. (2016), Instead of optimizing processes, reimagine them as platforms, *Harvard Business Review*, December, https://hbr.org/2016/12/instead-of-optimizing-processes-reimagine-them-as-platforms.

Shapiro E. (2018), *Global cryptodemocracy is possible and desirable*, http://arxiv.org/abs/1804.02049.

Shen L. (2018), *Kodak's not-quite ICO to launch May 21, as the SEC cracks down*, http://fortune.com/2018/05/10/kodak-kodakcoin-ico-saft/.

Stiglitz J. (2011), The best alternative to a new global currency, *Financial Times*, https://www.ft.com/content/c2215510-5bc4-11e0-b8e7-00144feab49a.

Tabarrok A., Cowen T. (2015), *The end of asymmetric information*, https://www.cato-unbound.org/2015/04/06/alex-tabarrok-tyler-cowen/end-asymmetric-information.

Tapscott A., Tapscott D. (2017a), How blockchain is changing finance, *Harvard Business Review*, March, https://hbr.org/2017/03/how-blockchain-is-changing-finance.

Tapscott D., Tapscott A. (2017b), Blockchain could help artists profit more from their creative works, *Harvard Business Review*, March, https://hbr.org/2017/03/blockchain-could-help-artists-profit-more-from-their-creative-works.

Täuscher K., Laudien S.M. (2018), Understanding platform business models: a mixed methods study of marketplaces, *European Management Journal*, 36(3), 319–329.

The Economist (2018), Blockchain technology may offer a way to re-decentralise the internet, *The Economist*, https://www.economist.com/special-report/2018/06/30/blockchain-technology-may-offer-a-way-to-re-decentralise-the-internet.

Tucker C., Catalini C. (2018), What blockchain can't do, *Harvard Business Review*, June, https://hbr.org/2018/06/what-blockchain-cant-do.

Wayner P. (1997), *Digital Cash*, Morgan Kaufmann.

Wee Kwang T. (2017), *How are governments using blockchain technology?*, https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855.

Wikipedia (2019), *Facebook – Cambridge analytica data scandal*, https://en.wikipedia.org/w/index.php?title=Facebook%E2%80%93Cambridge_Analytica_data_scandal&oldid=883076173.

Williams-Grut O. (2018), *Startups raised $5.6 billion through ICOs in 2017,* Business Insider Deutschland, https://www.businessinsider.de/how-much-raised-icos-2017-tokendata-2017-2018-1?r=UK&IR=T).

Williamson O.E. (1985), *The Economic Institutions and Capitalism*, Free Press.

Williamson O.E. (1973), Markets and hierarchies: some elementary considerations, *The American Economic Review*, 63(2), 316–325.

Williamson O.E. (1975), *Markets and Hierarchies: Analysis and Antitrust implications: A Study in the Economics of internal Organization*, Free Press.

World Economic Forum (2015), *Deep shift technology tipping points and societal impact*, http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

Wray L.R. (2012), *Introduction to an alternative history of money,* SSRN Scholarly Paper, 2050427, Social Science Research Network, https://papers.ssrn.com/abstract=2050427.

Wright A., De Filippi P. (2017), *Decentralized blockchain technology and the rise of lex cryptographia*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

Wüst K., Gervais A. (2017), *Do you need a blockchain?*, Department of Computer Science, ETH Zurich.

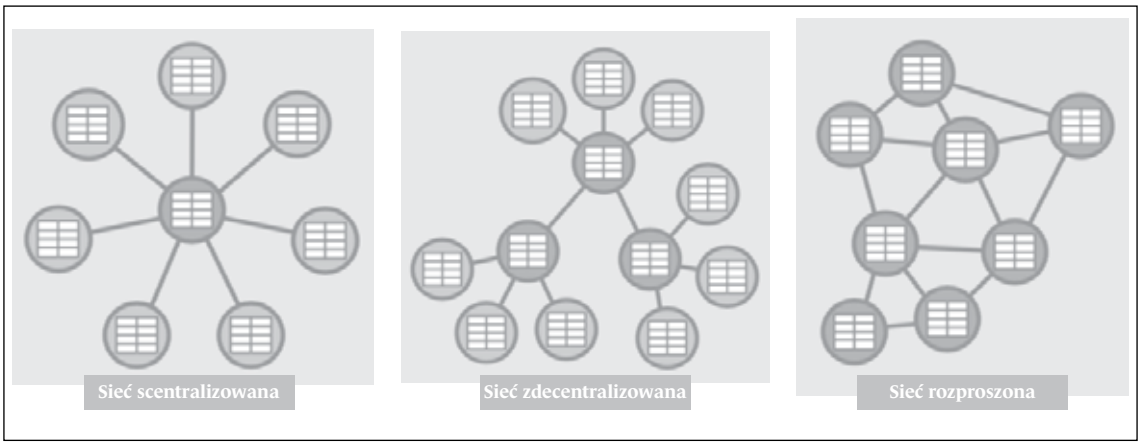
Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. (2016), Where is current research on blockchain technology? – a systematic review, *PLOS ONE*, 11(10).

Zhang K., Jacobsen H.-A. (2018), *Towards dependable, scalable, and pervasive distributed ledgers with blockchains*, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), https://doi.org/10.1109/ICDCS.2018.00134.

Zhao J.L., Fan S., Yan J. (2016), Overview of business innovations and research opportunities in block chain and introduction to the special issue, *Financial Innovation*, 2(1), 1–7.

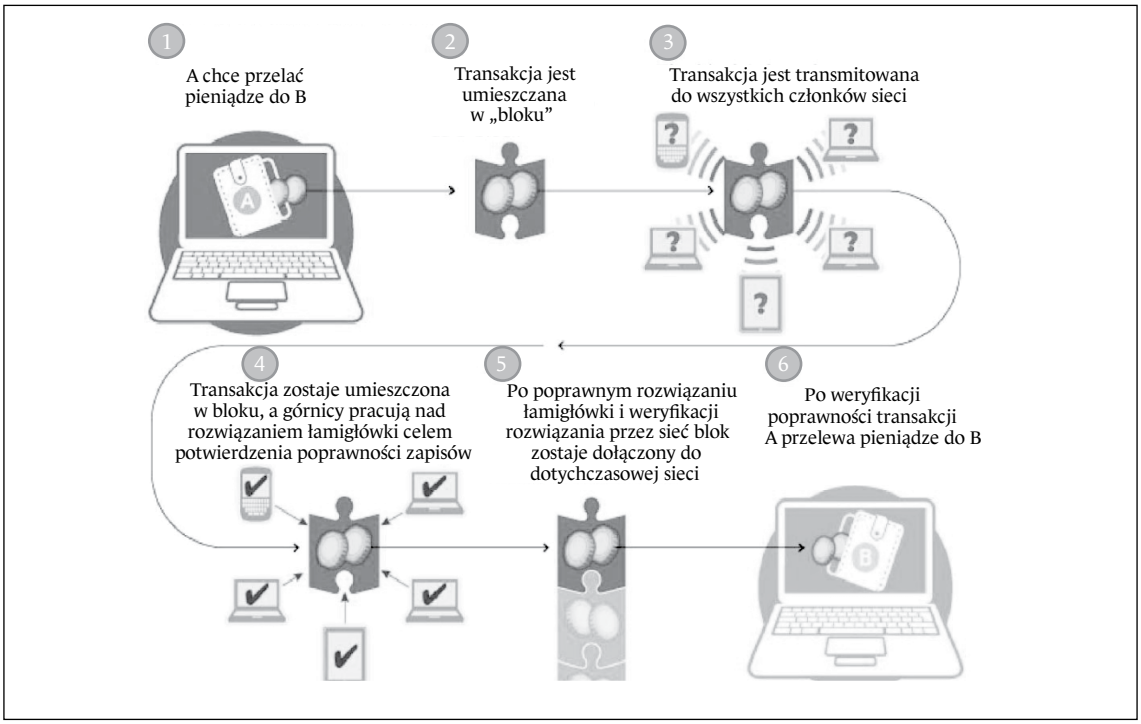
Aneks

Schemat 1
Rodzaje sieci



Źródło: opracowanie własne na podstawie BIS (2017).

Schemat 2
Uproszczony schemat przebiegu transakcji przelewu środków finansowych



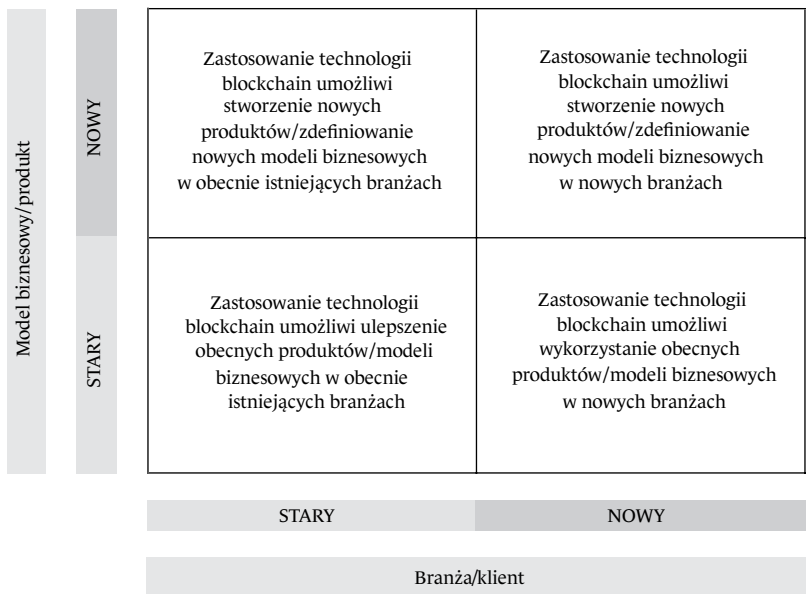
Źródło: opracowanie własne na podstawie Financial Times (2015).

Schemat 3
Warianty zastosowania technologii blockchain

		Licencjonowany	Nielicencjonowany
		Ograniczona weryfikacja	Otwarta weryfikacja
Prywatny	Prawa dostępu, czytania i dodawania transakcji nadane jedynie uczestnikom	Kombinacja możliwa, powszechnie występująca	Kombinacja możliwa, najmniej popularna
Publiczny	Nieograniczone prawa dostępu, czytania i dodawania transakcji	Kombinacja możliwa (np. WePower)	Kombinacja możliwa, powszechnie występująca (np. Bitcoin, Ethereum)

Źródło: opracowanie własne.

Schemat 4
Przykłady zastosowania technologii blockchain



Źródło: opracowanie własne.

Blockchain – decentralized system with a centralized logic

Abstract

Blockchain, since its first presentation in the document published by the anonymous Satoshi Nakamoto, has created widespread confusion. Despite its already ten-year history, there are still very few examples proving its applicability or able to explain its true potential. As a result, the main purpose of this paper is to describe the complex blockchain concept, paying attention to its technical features and its application possibilities. In order to answer the research questions, the author decided to use both inductive and deductive research approach. There have been three theses defined and proved: (i) the emergence of the blockchain was motivated by the growing scale of trust crisis and increasing size digital economy, (ii) blockchain is a three-element system which consist of digital value representatives, decentralized infrastructure and centralized logic; (iii) blockchain make it possible to create new and improve already existing solutions.

Keywords: blockchain, decentralisation, database, cryptoasset, trust