

Katarzyna Ciupa

Kolegium Zarządzania i Finansów
Szkoła Główna Handlowa w Warszawie

Warianty zastosowania koncepcji blockchain a modele ich doboru

Streszczenie

Blockchain, w ciągu zaledwie 10 lat, urósł do rangi rozwiązania cechującego się znaczną kompleksowością i różnorodnością, posiadającego wiele wariantów zastosowania o odmiennej strukturze i właściwościach. Mimo szerokiego zainteresowania nową koncepcją, wciąż brakuje regulacji, klasyfikacji czy strukturyzacji, które pomogłyby zarówno w łatwiejszej interpretacji skomplikowanego rozwiązania, jak również pozwoliłyby na analizy i porównania oferowanych możliwości. Przyczynia się to do wydłużonego procesu decyzyjnego, który dodatkowo jest obciążony znacznym ryzykiem popełnienia błędów bądź też może skutkować wyborem nie najbardziej optymalnego rozwiązania. Celem niniejszego artykułu jest ustrukturyzowanie właściwości blockchain i ich intensywności w odniesieniu do poszczególnych wariantów zastosowania, a tym samym stworzenie podstaw do budowania modeli doboru najbardziej optymalnej dla danego podmiotu kombinacji, wynikającej z indywidualnych czy biznesowych preferencji, modelu biznesowego oraz strategii działania.

Słowa kluczowe: blockchain, prywatny, publiczny, licencjonowany, nielicencjonowany
Kody klasyfikacji JEL: A1; B25; C7; D82; O3

1. Wprowadzenie

Blockchain, zgodnie z pierwotną wersją zaprezentowaną w 2008 r. [Nakamoto, 2008], to koncepcja zdecentralizowanej, rozproszonej i zsynchronizowanej bazy danych, której działanie opiera się na zasadach zdefiniowanych w ogólnodostępnym protokole i w której uczestnictwo nie jest w żaden sposób ograniczone [Casey, Wong, 2017; Pilkington, 2016; Tasca, Tessone, 2018]. Jako rozwiązanie pozwalające na odejście od paradygmatu często nadużywanej centralizacji [Davidson, De Filippi, Potts, 2018] oraz przyczyniające się do minimalizacji asymetrii informacyjnej pomiędzy nieznanymi się podmiotami [Tabarrok, Cowen, 2015], blockchain nie tylko umożliwia poprawę efektywności czy bezpieczeństwa w odniesieniu do licznych i powszechnie znanych procesów biznesowych, ale przede wszystkim inspirowanie do tworzenia nowych rozwiązań czy budowania innowacyjnych modeli biznesowych [Nowiński, Kozma, 2017]. Będąc początkowo określanym jedynie w kategoriach nowych technologii, blockchain coraz częściej zyskuje miano nowej formy organizacji systemów, procesów i instytucji, która jest w stanie funkcjonować w warunkach decentralizacji, określanej mianem ekonomii blockchain [Catalini, 2017; Davidson, De Filippi, Potts, 2018; Iansiti, Lakhani, 2017; The Economist, 2018]. Co więcej, koncepcja blockchain nie oznacza jednego wariantu jej zastosowania, ale daje możliwość stworzenia licznego zestawu zróżnicowanych pod względem właściwości rozwiązań. Pozwala to tym samym na jej wykorzystanie w odniesieniu do wielu procesów czy branż, takich jak przykładowo: sektor finansowy, w tym rozliczenia międzynarodowe [Catalini, 2017; Ito, Narula, Ali, 2017; McWaters, Galaski, 2017; Oh, Shong, 2017; Scott, 2016], logistyka i przepływ towarów [Casey, Wong, 2017; IBM, 2017; Kim, Laskowski, 2018; Kshetri, 2018; Petersen, Hackius, See, 2017; PR Newswire, 2017] czy też zarządzanie energią [Albrecht i in., 2018; Basden, Cottrell, 2017; Chitchyan, Murkin, 2018]. Ogromny potencjał blockchain potwierdzają chociażby szacunki Światowego Forum Ekonomicznego, zakładające przechowywanie w ramach bazy danych 10% produktu narodowego brutto w ujęciu globalnym do 2027 r. (2015).

Tak szerokie spektrum możliwego zastosowania technologii, jak również nowatorskie mechanizmy jej działania, przyczyniają się do coraz częstszego zaliczania blockchain do grona technologii ogólnego przeznaczenia (*general purpose technology*) [Bresnahan, Trajtenberg, 1995; Catalini, Gans, 2018]. Z jednej strony tak duża różnorodność i olbrzymi potencjał są zjawiskiem pozytywnym, z drugiej jednak oznaczają ogromne wyzwanie w odniesieniu do strukturyzacji wariantów koncepcji i analizy ich zastosowania w zależności od zakładanych celów czy posiadanych możliwości. Brak uporządkowanej terminologii, jednoznacznej struktury oraz zaufanych zestawień, początkowo określane mianem twórczego chaosu, coraz częściej staje się przeszkodą utrudniającą bądź niepozwalającą na przeniesienie koncepcji blockchain do realiów biznesowych. W związku z powyższym celem niniejszego artykułu jest podjęcie próby ustrukturyzowania wariantów technologii blockchain w zależności zarówno od intensywności możliwości wykorzystania właściwości koncepcji, jak i od

stawianych przez podmioty wymagań. Przeprowadzona analiza cech i właściwości koncepcji, jak również skali ich wykorzystania przez poszczególne warianty zastosowania technologii ma za zadanie wesprzeć proces doboru jak najbardziej optymalnej kombinacji, w zależności od stawianych celów, posiadanych możliwości czy też dóbr będących przedmiotem zapisu.

2. Charakterystyka technologii blockchain

Blockchain, czyli technologia łańcucha bloków, jako jeden z wariantów technologii rozproszonego rejestru (*distributed ledger technology*, DLT¹) [Bank for International Settlements, 2017; Leon i in., 2017], jest innowacyjną koncepcją bazy danych, która to nie jest zapisana na centralnym serwerze, ale stanowi sieć równoważnych replik, będących w posiadaniu wszystkich zainteresowanych uczestników systemu [Böhme, Christin, Edelman, Moore, 2015; Davidson, De Filippi, Potts, 2018; Evans, 2014; Iansiti, Lakhani, 2017; Nakamoto, 2008; Pilkington, 2016]². Łączy ona w sobie najnowsze osiągnięcia z dziedziny kryptografii z założeniami odwróconej teorii gier (a dokładniej teorii projektowania mechanizmów – *mechanism design theory*) [Berg, Davidson, Potts, 2018; Catalini, 2017; Hurwicz, 1973, 1994], proponując tym samym rozwiązanie, w ramach którego podmioty są w stanie uzyskać zgodność co do zapisów, bez konieczności centralnego monitorowania czy zarządzania. Możliwe jest to dzięki wbudowanemu systemowi zachęt (*consensus mechanism*), skonstruowanych w taki sposób, aby jednostki dążące do maksymalizacji własnej użyteczności postępowały w sposób maksymalizujący użyteczność całego systemu [Chitchyan, Murkin, 2018; Pilkington, 2016; Salviotti, De Rossi, Abbatemarco, 2018]. Architektura bazy danych, zakładająca powiązanie wszystkich wcześniejszych bloków z blokami nowo dodawanymi za pomocą specjalnych identyfikatorów (*hash*) [Back, 2002; Pilkington, 2016], praktycznie uniemożliwia dokonywanie niezauważonych przez resztę użytkowników zmian³. W rezultacie, tak powstała baza danych jest, z założenia, rozwiązaniem bezpiecznym, odpornym na ataki i wiarygodnym [Davidson, De Filippi, Potts, 2018; Salviotti, De Rossi, Abbatemarco, 2018].

Określenie „technologia blockchain” jest pojęciem nadrzędnym, skupiającym pod sobą całe grono różnego rodzaju platform, różniących się pomiędzy sobą zarówno parametrami, jak również przeznaczeniem czy możliwościami zastosowania. Jeden z najczęściej spotykanych sposobów klasyfikacji technologii blockchain rozróżnia podział ze względu na dwa kryteria: kryterium praw dostępu do bazy danych (*read/submit access*) oraz kryterium dotyczące

¹ W celu możliwości porównania proponowanych stwierdzeń z poglądami prezentowanych w literaturze międzynarodowej, zdecydowano się na umieszczenie angielskich tłumaczeń używanych zwrotów w nawiasie, umiejscowionym jednorazowo po będącym przedmiotem tłumaczenia wyrażeniu.

² W dalszej części artykułu nazwy technologia blockchain, baza danych, platforma, system czy też łańcuch bloków zostały użyte zamiennie.

³ Chęć przeprowadzania zmian wcześniejszych zapisów wymagałaby dokonania ich na wszystkich istniejących replikach, co czyni to zadanie bardzo kosztownym, a przez to praktycznie niewykonalnym.

się możliwości tworzenia rejestrów/weryfikacji stanu aktualnego (*write/commit/verify access*) [Hileman, Rauchs, 2017; Wüst, Gervais, 2017]⁴.

W odniesieniu do wspomnianego kryterium praw dostępu, rozwiązania blockchain dzieli się na⁵:

- publiczny rejestr danych (*public blockchain*), dostępny dla wszystkich i pozwalający wszystkim podmiotom na analizę zachodzących transakcji (*read*), jak również na zgłaszanie transakcji do zapisu w ramach sieci (*submit*),
- prywatny rejestr danych (*private blockchain*), dostępny jedynie dla wybranych uczestników, mających prawo wglądu do dokonywanych transakcji (*read*), czy też mogących zgłaszać transakcje do umieszczenia ich w bloku (*submit*).

Odnosząc się natomiast do drugiego kryterium, bazy danych dzieli się na:

- licencjonowany rejestr danych (*permissioned blockchain*), gdzie jedynie wybrane podmioty mogą dokonywać zmian (takich jak np. dodawanie bloków) bądź weryfikacji zmian w ramach rejestru,
- nielicencjonowany rejestr danych (*permissionless blockchain*), pozwalający wszystkim uczestnikom na udział w procesie dokonywania i weryfikowania zmian.

W przypadku pierwszego z wymienionych podziałów kluczowe pytanie dotyczy zatem tego, kto ma możliwość bieżącego analizowania zsynchronizowanych zapisów dokonywanych w ramach bazy i na jakim poziomie szczegółowości są te zapisy dostępne zarówno członkom (*peers*), jak i użytkownikom (*users*) [Feig, 2018]. Jeśli chodzi natomiast o drugie kryterium, rozstrzygająca jest kwestia weryfikacji zgłaszanych zapisów, a tym samym możliwość dokonywania zmian w ramach bazy danych, pozwalająca na jej ciągłą aktualizację.

W rezultacie, zestawiając wymienione powyżej kategorie, możliwe jest wskazanie następujących wariantów: (i) publiczno-licencjonowanego, (ii) publiczno-nielicencjonowanego, (iii) prywatno-licencjonowanego oraz (iv) prywatno-nielicencjonowanego. Stanowią one jednakże jedynie swego rodzaju punkty odniesienia na całej mapie potencjalnych do utworzenia kombinacji, zróżnicowanych zarówno z uwagi na właściwości blockchain, jak i ich intensywność [Brown, 2014]. Co więcej, żaden z możliwych wariantów nie jest rozwiązaniem lepszym czy gorszym *per se*, lecz jego zastosowanie jest mniej lub bardziej zasadne w zależności od stawianych wymagań, planowanych do osiągnięcia celów czy też posiadanych możliwości. Rysunek 1 przedstawia omówione zestawienie.

Popularnym podejściem, często wykorzystywanym przez podmioty opisujące nowe rozwiązania, jest podział jedynie na trzy kategorie: wariant publiczno-nielicencjonowany, prywatno-licencjonowany czy też wariant konsorcjum, który to stanowi rozwiązanie licencjonowane głównie w wariantcie prywatnym, dopuszczające współpracę pomiędzy podmiotami [Albrecht

⁴ Należy zaznaczyć, że podział ten dotyczy się możliwego wykorzystania technologii, natomiast celem porównania parametrów technicznych, wykorzystywane są inne, często dużo bardziej rozbudowane charakterystyki [Pilkington, 2016; Tasca, Tessone, 2018].

⁵ W dalszej części pracy nazwy rozwiązanie blockchain, wariant, kombinacja, kategoria zostały użyte zamiennie.

i in., 2018; De Kruiff, Weigand, 2017]. W niniejszym artykule zdecydowano się na wykorzystanie pełnego wachlarza możliwości klasyfikacji rozwiązań, w celu dokładniejszej analizy oferowanych korzyści i potencjalnych zagrożeń, dodatkowo uznając wariant współpracy w ramach konsorcjum jako podkategorie wariantu licencjonowanego, możliwego do wystąpienia zarówno w wersji publicznej, jak i prywatnej.

Rysunek 1. Warianty klasyfikacji technologii blockchain

WGLĄD/WERYFIKACJA	PUBLICZNY		PRYWATNY	
LICENCJONOWANY	WGLĄD WERYFIKACJA PRZYKŁADY	OTWARTY OGRANICZONA WEPOWER, AMPYL*	WGLĄD WERYFIKACJA PRZYKŁADY	ZAMKNIĘTY OGRANICZONA HYPERLEDGER, CORDA
NIELICENCJONOWANY	WGLĄD WERYFIKACJA PRZYKŁADY	OTWARTY OGRANICZONA BITCOIN, ETHEREUM	WGLĄD WERYFIKACJA PRZYKŁADY	ZAMKNIĘTY NIEOGRANICZONA BRAK

* Podane przykłady są propozycjami projektów, które wykorzystują publiczny blockchain w wersji licencjonowanej. Nie znane są przykłady samych platform o podanych właściwościach.

Źródło: opracowanie własne.

3. Analiza wariantów technologii blockchain

Z uwagi na istotne różnice pomiędzy poszczególnymi wariantami zastosowania technologii blockchain, przed podjęciem decyzji dotyczącej preferowanej koncepcji wymagana jest dogłębna analiza dostępnych rozwiązań, zakładanych do osiągnięcia efektów jak również aktywów mających być przedmiotem zapisu, celem wyboru jak najlepszego wariantu w zależności od procesu, branży czy oczekiwań użytkowników. Każde rozwiązanie jest bowiem pewnego rodzaju kompromisem, stąd niezwykle ważne jest wybranie takiej kombinacji właściwości, która zmaksymalizuje oczekiwane do osiągnięcia rezultaty.

Wybór prawidłowej kombinacji oznacza tym samym konieczność posiadania odpowiedniego modelu analizy zestawiającego właściwości koncepcji blockchain oraz intensywności ich wykorzystania w zależności od konfiguracji wariantu zastosowania. Odniesienie tych właściwości do indywidualnych preferencji podmiotu pozwoli bądź na dobór najbardziej optymalnego wariantu, bądź też przyczyni się podjęcia decyzji o rezygnacji z wykorzystania koncepcji blockchain, uznając ją za niewłaściwą z uwagi na posiadany model biznesowy czy zakładane cele.

Kryteria składające się na wspomniany model analizy i pozwalające na porównanie dostępnych wariantów koncepcji blockchain można podzielić na dwie grupy: pierwszą analizującą

charakterystyki blockchain pod kątem planowanych do osiągnięcia celów czy stawianych przed rozwiązaniem wymagań, oraz drugą tycząca się rodzaju aktywów będących przedmiotem zapisu⁶.

3.1. Pierwsza grupa kryteriów

Pierwsza grupa obejmuje zestaw właściwości koncepcji zestawionych w dwuelementowe podzbiory, celem ich lepszego odniesienia co do realiów biznesowych, jak również ułatwionej interpretacji.

3.1.1. Automatyzacja i decentralizacja (*automation and decentralisation*)

Automatyzacja procesów nie jest zjawiskiem nowym, a jej rozwój w dużej mierze kształtowały rewolucje przemysłowe. Odkrywane wynalazki umożliwiały zwiększenie efektywności prac czy pozwalały na zdefiniowanie nieznanych dotychczas procesów. Niemniej jednak, nawet pomimo wielu udoskonaleń, etap kontroli bądź weryfikacji pozostał domeną czynnika ludzkiego, będąc jednocześnie procesem znacznie zcentralizowanym lub nawet zmonopolizowanym.

Pojawienie się koncepcji blockchain dało tymczasem podstawy do dyskusji nad formą organizacji wspomnianych procesów, gdyż blockchain jako technologia proponująca zdecentralizowaną bazę danych, może znacznie odmienić obecną architekturę systemów. Może, gdyż blockchain posiada wiele wariantów, które zdecydowanie różnią się pomiędzy sobą potencjałem możliwych do osiągnięcia korzyści.

Pełna automatyzacja jest możliwa jedynie w podejściu publiczno-nielicencjonowanym, gdyż weryfikacja poprawności zapisu jest dokonywana przez odpowiednio zdefiniowany mechanizm, niewymagający ingerencji czynnika ludzkiego⁷. Natomiast w wariantcie prywatno-licencjonowanym automatyzacja ma tylko zastosowanie do procesów zachodzących wewnątrz grupy czy organizacji, co zdecydowanie ogranicza jej potencjał.

W odniesieniu do aspektu decentralizacji, całkowite wyeliminowanie centralnego zarządcy procesu jest możliwe w przypadku wariantu publiczno-nielicencjonowanego, otwierając tym samym możliwość budowania nowych zdecentralizowanych struktur czy modeli biznesowych [Chitchyan, Murkin, 2018; Pilkington, 2016]⁸. Rozwiązania prywatno-licencjonowane oznaczają tymczasem jedynie zmniejszenie złożoności procesów i w pewnym sensie skutkują

⁶ Należy również zaznaczyć, że w dalszej części artykułu posłużono się dwoma skrajnymi wariantami zastosowania blockchain, a każda ich pośrednia wersja znajduje się pomiędzy wspomnianymi dwoma rozwiązaniami

⁷ W przypadku Bitcoin blockchain etap weryfikacji wymaga rozwiązania łamigłówek, co z kolei wiąże się z wykonaniem wielu obliczeń pozwalających na znalezienie zdefiniowanej przez protokół wartości (*proof of work*) [Nakamoto, 2008].

⁸ Należy przy tym pamiętać, że dotyczy się to często tylko zachowań wewnątrz sieci, natomiast sam proces decyzyjny dotyczący ewentualnych aktualizacji protokołu jest zadaniem wyznaczonej grupy lub całej społeczności

przeniesieniem centralizacji na wyższy poziom, gdzie podmioty wprawdzie zaczynają współpracować bezpośrednio ze sobą, eliminując rolę niezbędnych dotychczas pośredników (*trusted third parties*), jednakże jedynie w obrębie specjalnie w tym celu utworzonych konsorcjów czy grup. Dzięki wspólnemu działaniu opartemu na posiadanej przez wszystkich zsynchronizowanej bazie danych, uzupełnionej często o inteligentne kontrakty (*smart contracts*⁹), następuje zminimalizowanie jakichkolwiek zależności czy zaufania, ale tylko w odniesieniu do współpracujących uczestników. Dodatkowo, proces decyzyjny dotyczący rozwoju bazy danych często jest również domeną albo jedynie zarządzających, albo należy do zadań wybranego grona uczestników, ograniczając jednocześnie potencjał decentralizacji czy automatyzacji oferowany przez technologię [Garzik, 2015]. W rezultacie rozwiązania te dzięki swej architekturze i regułach działania pozwalają przede wszystkim na poprawę efektywności procesów wewnątrz często bardzo złożonych struktur przedsiębiorstw czy też obniżenia kosztów transakcyjnych pomiędzy współpracującymi podmiotami [Catalini, 2017; Nowiński, Kozma, 2017; Oh, Shong, 2017], jednocześnie nie tworząc nowych modeli prowadzenia działalności.

3.1.2. Odporność na zmiany/wiarygodność zapisu i transparentność zapisu (*immutability and transparency*)

Analiza zdarzeń z ostatnich lat wskazuje, jak bardzo podatne na ataki czy manipulacje mogą być rozwiązania centralne [Atzori, 2015; Forde, 2017; Mainelli, 2017; Tapscott, Tapscott, 2016]. Co więcej, z uwagi na ogromną ilość danych, jakie są w ramach nich przechowywane, ich kompleksowość rośnie często w galopującym tempie [Agrawal, Gans, Goldfarb, 2016; Athey, Catalini, Tucker, 2017]. W rezultacie proces analizy dokonywanych zapisów, efektywnego wyszukiwania ewentualnych niezgodności i szybkiego reagowania na zauważone problemy staje się niezwykle trudnym, czy wręcz niemożliwym, zadaniem. Tymczasem blockchain, dzięki posiadanym właściwościom, pozwala na minimalizację ryzyka manipulacji [Xu i in., 2017], jak również zapewnia transparentny zapis, stanowiąc tym samym możliwe remedium na zgłaszane problemy. Jednakże, podobnie jak w przypadku automatyzacji czy decentralizacji, również w odniesieniu do transparentności i wiarygodności, skala proponowanych ulepszeń jest różna dla poszczególnych wariantów.

Rozwiązania publiczno-licencjonowane pozwalają wszystkim podmiotom na wgląd do zsynchronizowanych zapisów dokonywanych w ramach bazy danych, czyniąc te warianty najbardziej transparentnymi. Co więcej, posiadanie replik bazy danych przez wiele rozproszonych podmiotów sprawia, że rozwiązania te są również najmniej podatnymi na zmiany

(*off chain governance*). Coraz częściej wprawdzie pojawiają się pomysły proponujące rozwiązania zakładające umieszczenie również tego etapu decyzyjnego w ramach bazy danych (*on chain governance*).

⁹ Inteligentne kontrakty to programy komputerowe, które wykonują polecenie zgodnie ze zdefiniowanymi regułami. Odpowiednie kryteria zostają zapisane w zarządzającym nimi protokole i podlegają samoegzekwowaniu, gdy zostaną spełnione odpowiednie kryteria (można je porównać do rozbudowanej wersji powszechnie używanej funkcji w programie Excel „jeśli->to” (*if->then*)).

czy manipulacje [Chitchyan, Murkin, 2018; Pilkington, 2016]. Oznacza to zatem, że próba jakiegokolwiek modyfikacji zapisów została albo nie tylko natychmiastowo wykryta (ze względu na niespójne wersje na replikach), albo – z uwagi na ogromne koszty procesu – jest zadaniem praktycznie niewykonalnym [Feig, 2018]¹⁰.

Jeśli chodzi natomiast o warianty prywatno-licencjonowane, to w odniesieniu do nich jedynie zautoryzowani, prywatni uczestnicy mają dostęp do zapisów, co sprawia, że rozwiązania te są zdecydowanie mniej transparentne. Dodatkowo, z uwagi na fakt, iż sama baza jest w posiadaniu jedynie albo centralnego zarządcy, albo tylko wybranego grona, jej manipulacja jest znacznie łatwiejsza niż w porównaniu z wariantem publicznym. Podyktowane jest to mniejszą skalą bazy danych, względną znajomością podmiotów korzystających z rozwiązania, jak również częściowym zcentralizowaniem. Jednocześnie, w przypadku jakiegokolwiek pomyłek, możliwe staje się dokonanie poprawek, które to stanowi często kluczową kwestię podyktowaną modelem biznesowym, rodzajem zapisywanych danych czy też branżą, w ramach której działalność jest prowadzona [Buterin, 2015].

3.1.3. Koszt procesu i szybkość procesu/decyzyjność (*cost and speed/governance*)

Wspomniana na początku rozważań zdecentralizowana forma bazy danych ma niestety swoją cenę, co oznacza, że konieczne są kompromisy odnoszące się do jej innych właściwości czy parametrów [Feig, 2018]. Podmioty chcące skorzystać z publiczno-nielicencjonowanego rozwiązania muszą być przygotowane na konieczność poniesienia stosunkowo dużych nakładów na wspomniany w poprzednim podrozdziale proces weryfikacji zapisów. Może mieć to odzwierciedlenie w wysokich kosztach energii niezbędnej do wykonania obliczeń w przypadku wariantu *proof of work*, czy też w konieczności zastawienia dużej kwoty, jak ma to miejsce w odniesieniu do podejścia *proof of stake*¹¹. Co więcej, wariant publiczno-nielicencjonowany oznacza także mniejszą szybkość zarówno procesu weryfikacji transakcji, jak również podejmowania decyzji odnośnie do aktualnego stanu bazy danych i ewentualnych zmian, co może być kluczową kwestią w przypadku konieczności dynamicznego wzrostu platformy czy jej dużej skalowalności [Albrecht i in., 2018; Oh, Shong, 2017; Tasca, Tessone, 2018]. W wariacie prywatno-licencjonowanym natomiast, zarówno koszt weryfikacji, jak i szybkość procesu decyzyjnego mogą być znacznie niższe, szczególnie w sytuacji, gdy uczestnicy przykładowo zdecydują się na wykorzystanie innego, mniej kosztownego, mechanizmu weryfikacji¹² lub gdy zastosują uproszczony proces podejmowania decyzji, czyniąc te obowiązki na przykład kompetencjami jedynie wąskiego grona zarządzających. Niemniej jednak, oba

¹⁰ Oczywiście, niemożność zmiany może stanowić także potencjalne zagrożenie, gdyż ewentualne poprawki pomyłkowych zapisów (*garbage in-garbage in*) czy też usunięcie przypadkowo umieszczonych prywatnych informacji jest zadaniem wręcz nierealistycznym [Feig, 2018].

¹¹ Metody te mają jednak swoje uzasadnienie i są stosowane celem zniechęcenia podmiotów do manipulacji, gdyż ona się im z ekonomicznego punktu widzenia po prostu nie opłaca.

¹² Za przykład takiego mechanizmu można uznać podejście *proof of authority*.

omówione warianty oznaczają poprawę efektywności zarówno kosztowej, jak i biznesowej w porównaniu z obecnie dostępnymi rozwiązaniami, różniąc się jedynie skalą możliwych do osiągnięcia korzyści [Garzik, 2015].

3.1.4. Anonimowość i bezpieczeństwo (*anonymity and security*)

Ochrona danych osobowych czy też innych informacji pozwalających na identyfikację jednostek oraz posiadanego przez nich majątku, historii choroby bądź preferencji zakupowych to proces, który w obliczu stale ulepszanych technologii, staje się zadaniem bardzo skomplikowanym, wymagającym fachowej wiedzy i profesjonalnych rozwiązań [Cochrane, 2018]. Co więcej, w przypadku, gdy baza danych skupiająca dane zarówno dotyczące przedsiębiorstwa, jak i wszystkich jego klientów zapisana jest na zcentralizowanym serwerze, którego posiadaczem jest jedynie analizowany podmiot, nawet w sytuacji, gdy tworzone są odpowiednie kopie zapasowe czy są stosowane najnowsze zabezpieczenia, cały układ jest często bezbronny w obliczu potencjalnego ataku [Tapscott, Tapscott, 2016; The Economist, 2018].

Inaczej rzecz ma się w odniesieniu do bazy danych blockchain, której zdecentralizowany charakter, polegający na zsynchronizowanym zapisie umieszczanym na wszystkich replikach, będących w posiadaniu uczestników systemu, pozwala na uniknięcie ryzyka związanego z pojedynczym, centralnym serwerem (*single point of failure*) [Albrecht i in., 2018]. Oczywiście pełne zdecentralizowanie, a tym samym największe bezpieczeństwo jest możliwe jedynie w przypadku wariantu publicznie-nielicencjonowanego, podczas gdy warianty prywatnie-licencjonowane nakładają na ten aspekt mniejsze lub większe ograniczenia.

Co więcej, blockchain charakteryzuje jeszcze – poza podnoszącą bezpieczeństwo decentralizacją – anonimowość (*anonymity*) bądź pseudoanonimowość (*pseudonymity*) [Oh, Shong, 2017], która również w pewnym sensie przyczynia się do lepszej ochrony danych osobowych. W przypadku koncepcji blockchain możliwa jest bowiem taka reprezentacja jednostek, która praktycznie uniemożliwia identyfikację ich rzeczywistych personaliów. Podmioty posługują się specjalnie zdefiniowanymi kodami, które w przypadku Bitcoin blockchain są określane mianem adresów. Pseudoanonimowość wynika natomiast z faktu, że transakcje są przyporządkowane do adresów podmiotów dokonujących transakcji. W sytuacji gdy jednostka choć raz podała swoje rzeczywiste dane celem dołączenia do bazy danych blockchain (przykładowo podczas rejestracji na jednej z obsługujących wymianę giełd), możliwe będzie powiązanie jej rzeczywistej tożsamości z tożsamością na blockchain, a tym samym monitorowanie przeprowadzonych transakcji¹³. Opisywana charakterystyka potencjalnej do osiągnięcia anonimowości dotyczy się oczywiście jedynie wariantów publicznie-nielicencjonowanych. W odniesieniu natomiast do wariantów prywatnie-licencjonowanych, czy też wszelkich pośrednich prywatnych kombinacji, dołączenie do sieci jest poprzedzone

¹³ Tworzone są również rozwiązania pozwalające na pełną anonimowość, takie jak przykładowo projekty Monero, Z-Cash.

identyfikacją i weryfikacją tożsamości, co często praktycznie całkowicie pozbawia te rozwiązania aspektu anonimowości, czyniąc je tym samym, w odniesieniu do tego aspektu, podobnymi do podejść zcentralizowanych.

3.1.5. Skalowalność i elastyczność (*scalability and flexibility*)

Wzrost, zarówno dynamiczny, jak i zrównoważony, oraz zwiększanie liczby klientów są jednymi z głównych celów działalności przedsiębiorstw. Co więcej, duża konkurencja, zmniejszające się bariery wejścia czy wyjścia, jak również zmieniające się często oczekiwania klientów stawiają przed producentami wyzwanie ciągłego dopasowywania się do preferencji użytkowników i warunków rynkowych, celem podtrzymania czy przyspieszenia procesu osiągania zakładanych celów.

Wymuszana przez chęć wzrostu skalowalność oraz elastyczność tycająca się możliwości przeprowadzania zmian w architekturze czy właściwościach bazy danych, zdecydowanie różnią się w odniesieniu do możliwych do zastosowania rozwiązań blockchain. Platformy publiczno-nielicencjonowane, których działanie odbywa się zgodnie z ogólnie dostępnym algorytmem, cechują się dużo mniejszą elastycznością i skalowalnością niż platformy prywatno-licencjonowane. Kluczowe właściwości, takie jak przykładowo pojemność bloku czy czas weryfikacji transakcji, muszą być w odniesieniu do publiczno-nielicencjonowanych platform znane wszystkim uczestnikom, a ich jakakolwiek zmiana wymaga albo zgody wszystkich użytkowników, albo wyznaczonych do tego celu podmiotów (*core developers*), co często jest bardzo długim i trudnym procesem [Chitchyan, Murkin, 2018; De Kruiff, Weigand, 2017; Xu i in., 2017]¹⁴. W rezultacie, w przypadku wzrostu liczby użytkowników, trudności ze skalowalnością przekładają się na dłuższy czas oczekiwania, wyższy koszt procesu czy nawet na odejście zainteresowanych jednostek.

Platformy prywatno-licencjonowane pozwalają natomiast na dużo większą skalowalności i elastyczność. Wynika to z faktu, że procesy decyzyjne dotyczące potencjalnych zmian są podejmowane albo przez jeden podmiot, albo przez wybrane grono, które działa zgodnie z wcześniej ustalonym regulaminem. Co więcej, kod, na którym baza danych się opiera, jest wewnętrznym rozwiązaniem, pozwalając tym samym na jego dużo szybszą i łatwiejszą zmianę i implementację.

3.1.6. Równe prawa i zaufanie (*equal rights and trust*)

Twórca koncepcji blockchain wskazywał na aspekt zaufania i jego częste nadużywanie przez podmioty zobligowane do reprezentowania interesów publicznych bądź prywatnych [Forde, 2017; Mainelli, 2017]. Szczególnie spektakularnym w tej kategorii wydarzeniem był

¹⁴ Dodatkowo, możliwe jest nawet, że proponowane zmiany nie zostaną zaakceptowane przez całą społeczność, co w rezultacie doprowadzi do rozwidlenia sieci (*fork*), oznaczającego utworzenie równoległej bazy danych (*hard fork*), co tylko podkreśla, jak dużym wyzwaniem jest ewentualne dopasowywanie architektury systemu.

upadek banku inwestycyjnego Lehman Brothers, który oficjalnie zapoczątkował największy po Wielkiej Depresji kryzys finansowy [Konopczak, Sieradzki, Wiernicki, 2010]. Zdarzenie to stanowiło jednakże tylko symboliczny wierzchołek góry lodowej nadużywanej centralizacji, powiększającej się asymetrii informacji, niedopasowania regulacji do zmieniającej się gospodarki czy też nieradzenia sobie z analizą rosnącej liczby danych. Koncepcja „za duży, aby upaść” (*too big to fall*) [Nurisso, Prescott, 2017], z uwagi na ogromną skalę nadużyć i brak odpowiednich zabezpieczeń, nie miała w odniesieniu do Lehman Brothers zastosowania, dodatkowo podkreślając rozmiar problemu już nie samego banku, ale całej gospodarki.

Problem pryncypała-agenta [Laffont, Martimort, 2009], pogoń za rentą [Tullock, 1988] czy też możliwość wystąpienia zachowań oportunistycznych [Coase, 1937] są od dawna bolączkami wielu ekonomistów, przy czym dotychczas niemożliwe było znalezienie rozwiązania pozwalającego na ich minimalizację czy też eliminację. Koncepcja blockchain jako zdecentralizowanej, rozproszonej i zsynchronizowanej bazy danych, otwartej dla wszystkich i zapewniającej każdemu podmiotowi równy dostęp do jednakowej informacji, może zatem stanowić pierwsze potencjalne rozwiązanie wymienionych problemów. Stwierdzenie to jednak odnosi się tylko do pierwotnego wariantu koncepcji, a mianowicie wersji publicznie-licencjonowanej. Ta opcja wyklucza bowiem w pewnym sensie konieczność ufania komukolwiek, gdyż wszystkie podmioty mają jednakowy dostęp do informacji i samodzielnie mogą sprawdzić aktualny stan dokonanych zapisów¹⁵ [De Kruijff, Weigand, 2017; Salviotti, De Rossi, Abbatemarco, 2018; Xu i in., 2017]. Dodatkowo, każda jednostka ma prawo samodzielnie być posiadaczem najbardziej aktualnej repliki bazy danych, co wymaga jedynie pobrania i instalacji odpowiedniego programu [Böhme i in., 2015].

Odwrotnie ma się rzecz w odniesieniu do wariantów prywatnie-licencjonowanych. W przypadku tych wariantów jedynie zweryfikowane podmioty mogą stać się użytkownikami bądź uczestnikami, a sam proces weryfikacji leży często w kompetencji tylko wybranej grupy osób. Sugeruje to występowanie silnej asymetrii informacyjnej w odniesieniu do podmiotów spoza współpracującej grupy, które są albo całkowicie pozbawione dostępu do bazy danych, albo mają ograniczone prawo do jej użytkowania czy też do wglądu w będące przedmiotem zapisu dane. W rezultacie, wariant prywatnie-licencjonowany oznacza zarówno brak równości praw, jak również konieczność ufania wyznaczonym administratorom czy weryfikatorom. Może mieć to oczywiście swoje uzasadnienie, podyktowane charakterem dobra lub jego dystrybucją, stad też tak ważna jest analiza celów, aby zastosowanie technologii blockchain przyczyniło się do ich realizacji.

¹⁵ Niemniej jednak aspekt zaufania nadal występuje. Tyczy się on zaufania do twórców kodu, na którym platforma bazuje, aczkolwiek biorąc pod uwagę ogólnodostępny charakter budujących technologie protokołów, wspomniana zależność jest bardzo zminimalizowana.

3.1.7. Integralność zapisu i dostępność danych (*data integrity and availability*)

Ciągły dostęp do zsynchronizowanego i niepodatnego na ryzyko ewentualnych ataków źródła informacji jest kluczowym aspektem szczególnie w odniesieniu do procesów podejmowania decyzji. Minimalizuje on bowiem asymetrię informacji, a tym samym potencjalne ryzyko wystąpienia konfliktów czy nadużyć. Pozwala wszystkim jednostkom na samodzielne oszacowanie sytuacji, wyciągnięcie wniosków i ułożenie własnej strategii działania¹⁶.

Publiczno-nielicencjonowane rozwiązania blockchain zakładają spełnienie wymienionych oczekiwań. Dzięki możliwości udziału wszystkich podmiotów w weryfikacji zapisów, kolejno aktualizowanych na rozproszonych replikach, jak również powiązaniu wcześniejszych zapisów z bieżącymi zapisami za pomocą specjalnych identyfikatorów (*hash*), praktycznie niemożliwe staje się dokonywanie jakichkolwiek zmian. Co więcej, brak centralnego punktu zapisu, wspomnianego również już przy analizie aspektu bezpieczeństwa, oznacza, że nawet w przypadku zaatakowania kilku podmiotów, pozostali uczestnicy nadal będą w posiadaniu repliki bazy, co pozwoli na utrzymanie ciągłości zapisu [Pilkington, 2016; Tasca, Tessone, 2018]. Natomiast zaatakowanie wszystkich kopii jest, podobnie jak ewentualna zmiana wcześniejszych zapisów, zbyt kosztowne, a przez to praktycznie niemożliwe [Albrecht i in., 2018; Xu i in., 2017]. W przypadku wariantów prywatno-licencjonowanych czy ich różnych kombinacji, konieczne są natomiast kompromisy zarówno w odniesieniu do integralności danych, jak i do ich dostępności. Podmioty korzystające z takich rozwiązań robią to albo w grupie, albo w ramach własnych, często bardzo rozbudowanych i międzynarodowych struktur, co czyni te rozwiązania zdecydowanie bardziej podatnymi na ewentualne ataki¹⁷. Co więcej, często jedynie wybrane jednostki w obrębie omawianych baz są zaangażowane w weryfikację nowych zapisów, co z kolei może spowodować ewentualne problemy w integralności danych, szczególnie gdy potencjalny atak zostanie przeprowadzony na repliki będące w posiadaniu weryfikatorów [Albrecht i in., 2018; Chitchyan, Murkin, 2018; Xu i in., 2017]. Dodatkowo z uwagi na ogromną liczbę podmiotów i ich stosunkowo mniejsze rozproszenie, łatwiejsze staje się przeprowadzenie potencjalnych zmian w przeszłych zapisach, przekładające się na większe ryzyko co do zapewnienia integralności danych.

¹⁶ Oczywiście, wybrana strategia działania może być różna dla każdego podmiotu, jednakże zróżnicowanie to wynika wówczas z indywidualnych preferencji, a nie z braku dostępu do pełnego zapisu sytuacji. Ciekawe podejście reprezentują ekonomiści z nurtu ekonomii wiedzy niedoskonałej [Frydman, Duncan i Goldberg, 2007].

¹⁷ Należy zaznaczyć, że w ramach konsorcjów wszystkie podmioty często są w posiadaniu repliki bazy, co czyni je zdecydowanie bardziej odpornymi na ataki niż rozwiązania prywatne.

3.2. Druga grupa kryteriów

Druga grupa charakterystyk koncepcji blockchain pomocna w analizie i wyborze odpowiedniego wariantu zastosowania dotyczy się rodzaju aktywów będących przedmiotem zapisu w ramach bazy danych. Odnosząc się do tej klasyfikacji, należy rozważyć poniższe kategorie.

3.2.1. Aktywa zdigitalizowane i aktywa digitalne (*digitalised and digital assets*)

Technologia blockchain w pierwszej kolejności znalazła zastosowanie w sektorze finansowym, głównie z uwagi na fakt, iż większość aktywów będących przedmiotem wymiany w odniesieniu do tego obszaru gospodarki występowała już w postaci digitalnej (cyfrowej). Oznaczało to tym samym, że nie było problemu z utworzeniem ich postaci cyfrowej¹⁸, a tym samym ułatwione stało się umieszczanie ich w ramach bazy danych blockchain [Tucker, Catalini, 2018]. W przypadku natomiast gdy przedmiotem zapisu mają być transakcje dokonywane w odniesieniu do dóbr niemających postaci digitalnej, należy uprzednio stworzyć ich digitalnego reprezentanta, który umożliwi śledzenie obrotu nimi (dokonywanego w wymiarze rzeczywistym) w ramach bazy danych blockchain. Należy przy tym zaznaczyć, że wspomniany etap weryfikacji, a tym samym tokenizacji, jest etapem kluczowym i w związku z tym najbardziej podatnym na manipulacje, stąd też konieczne jest stworzenie odpowiednich procedur, regulujących jego przebieg. Co więcej, im bardziej rzadkie są dobra będące przedmiotem weryfikacji, tym łatwiejsze jest monitorowanie procesu tokenizacji¹⁹, natomiast w odniesieniu do dóbr powszechnie występujących, proces ten może być bardzo rozbudowany, co przyczynia się do zwiększenia i tak dużego już ryzyka wspomnianej manipulacji.

Weryfikacja dobra może być dokonywana albo za pośrednictwem wyspecjalizowanych urzędzeń, takich jak przykładowo nowoczesne liczniki energii (*smart metres*) bądź szerzej jako zaliczanych do IoT (*Internet Of Things*) [Catalini, 2017], lub też może być przeprowadzona przez upoważnione do tego jednostki – weryfikatorów, odpowiedzialnych za identyfikowanie i tworzenie cyfrowych odpowiedników fizycznych dóbr. W obu przypadkach sama konieczność weryfikacji oznacza wręcz nieuchronne skorzystanie z wariantów licencjonowanych, zarówno w publicznej, jak i prywatnej formie, w zależności od charakteru dobra, procesu lub zakładanej współpracy.

Jednocześnie należy zwrócić uwagę na aspekt dotyczący się warstw występujących w odniesieniu do zawieranych transakcji, pozwalający na lepsze zrozumienie konieczności i istotności procesu weryfikacji czy tokenizacji. Chodzi tu dokładniej o warstwę wymiany informacji (*information layer*), wymiany wartości (*value layer*) oraz wymiany dobra (*infrastructure layer*). Jest to szczególnie istotne w przypadku dóbr niemających postaci digitalnej, w odniesieniu do

¹⁸ Proces ten określanym jest również pojęciem tokenizacji.

¹⁹ Dobrym przykładem jest projekt Everledger, który dokonuje tokenizacji diamentów, traktowanych jako dobro niewystępujące powszechnie, a dodatkowo o bardzo dużej wartości.

których tokenizacja zaspokaja wprawdzie dwie warstwy, jednak sama dostawa dobra nadal ma wymiar fizyczny. Oznacza to tym samym z jednej strony konieczność stworzenia właściwego tokena, pozwalającego na śledzenie zmian rzeczywistych w wymiarze cyfrowym, z drugiej natomiast wymaga dostosowania albo bieżącej infrastruktury do nowych rozwiązań, albo stworzenia nowych rozwiązań dopasowanych do istniejącej infrastruktury. Aspekt ten, choć bardzo istotny, jest często pomijany przy prezentacji projektów wykorzystujących technologie blockchain, takich jak przykładowo nowe rozwiązania zarządzania energią, stąd też warto o nim pamiętać przy analizie potencjału nowych pomysłów.

3.2.2. Aktywa porównywalne/weryfikowalne i aktywa specyficzne/trudne w weryfikacji (*fungible/verifiable and non-fungible/non-verifiable assets*)

Facebook, Uber czy Airbnb powszechnie znane jako platformowe modele biznesowe pozwoliły zarówno na kwantyfikację, jak i monetaryzację interakcji pomiędzy jednostkami. Określane często mianem zdecentralizowanych są one tak naprawdę przykładami centralnie sterowanych modeli [Alstyn, Parker, Choudary, 2016; Kenney, Zysman, 2015; Schrage, 2016; Täuscher, Laudien, 2018], wykorzystujących dodatkowo procesy rekomendacyjne do weryfikacji oferowanych usług. Czyni je to tym samym podatnymi zarówno na ataki skierowane na będące w ich posiadaniu zbiory danych, jak również naraża je na potencjalne manipulacje w odniesieniu do zarządzanych przez nie systemów rekomendacyjnych²⁰.

Blockchain, jako rozwiązanie eliminujące element pośrednika i pozwalające na zawieranie bezpiecznych i odpornych na oszustwa interakcji bezpośrednio pomiędzy zainteresowanymi podmiotami, wydaje się zatem jeszcze lepszą alternatywą niż wspomniane platformy. Dodatkowo dzięki oparciu mechanizmu weryfikacji na ilości zainwestowanej energii, a nie ilości posiadanych kont użytkowników (jak ma to miejsce w przypadku przytoczonych platform), praktycznie wykluczona zostaje możliwość jakiegokolwiek manipulacji także w odniesieniu do systemów weryfikacji. Niestety potencjał osiągnięcia wspomnianych korzyści ma swego rodzaju ograniczenia, tym razem w odniesieniu do aspektu porównywalności i łatwości weryfikacji będących przedmiotem wymiany aktywów.

W przypadku porównywalności aktywów, których dostępność podlega prostej weryfikacji, gdyż przykładowo mają one pierwotnie formę cyfrową, staje się możliwe rozważanie publiczno-nielicencjonowanego wariantu zastosowania technologii. Jeśli natomiast dostępność dóbr musi być zweryfikowana w świecie rzeczywistym, a dodatkowo dobra nie są bezpośrednio porównywalne, czego przykładem są mieszkania będące przedmiotem obrotu w ramach platformy Airbnb, uzasadnionym wydaje się obecnie rozważenie wariantu licencjonowanego, który jednocześnie może być dostępny albo do publicznego wglądu, albo tylko dla zweryfikowanych użytkowników.

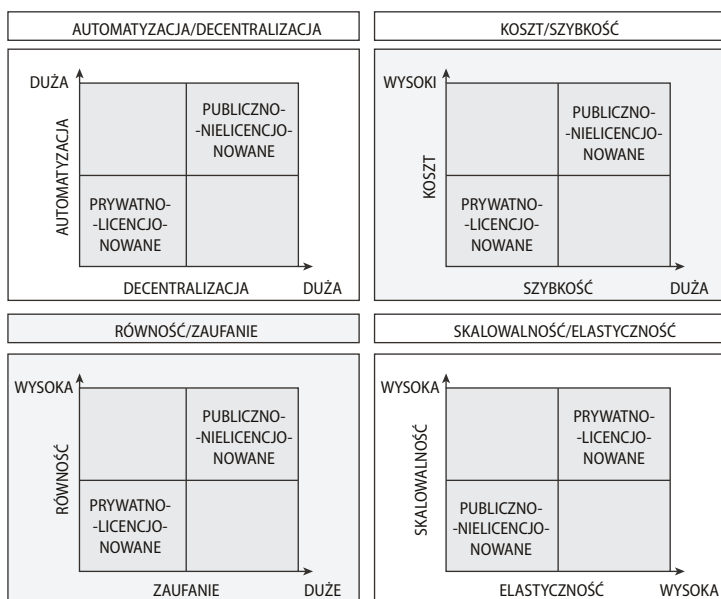
²⁰ W literaturze proces ten jest określany mianem *Sybil attack* i ma miejsce, gdy jednostka może utworzyć wiele kont użytkowników w ramach systemu, a tym samym, poprzez wielostronne publikowanie pozytywnych opinii, w sposób sztuczny podnieść sobie ocenę (ranking).

3.2.3. Aktywa prywatne i publiczne (*private and public assets*)

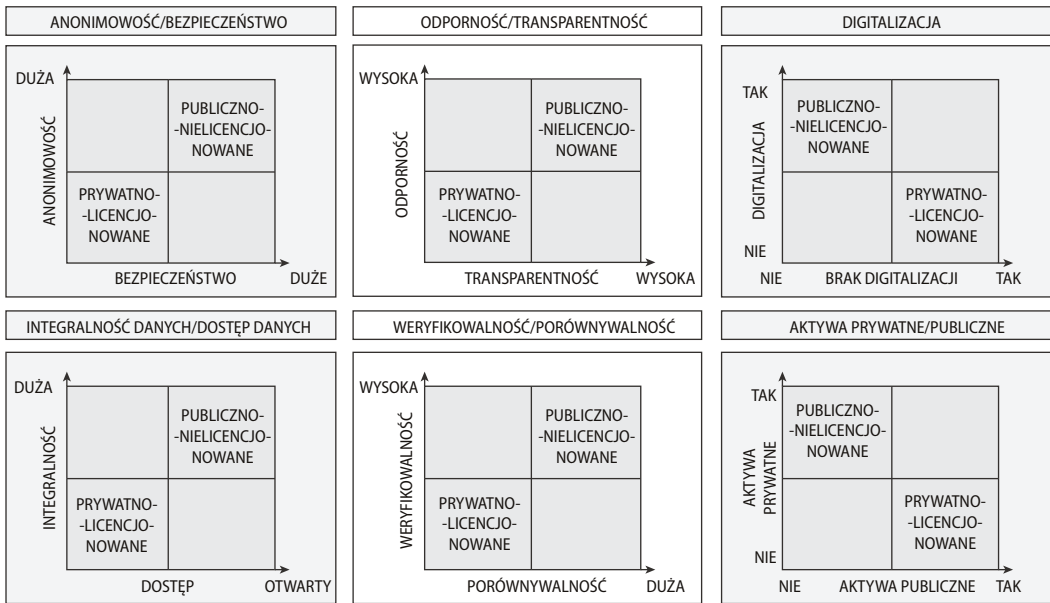
Kolejnym kryterium wymagającym rozważenia przy podejmowaniu decyzji odnośnie do wariantu zastosowania technologii blockchain jest podział na aktywa prywatne i publiczne. W przypadku, gdy przedmiotem obrotu są aktywa określane mianem prywatnych, możliwe jest tworzenie nielicencjonowanych rozwiązań, gdyż popyt czy też podaż tych dóbr nie wymagają dodatkowych regulacji (oczywiście przy założeniu, że nie są to dobra zabronione czy też szkodliwe dla całej społeczności). Jeśli natomiast są rozważane dobra publiczne oraz dobra, których dostępność jest niezbędna podmiotom do egzystencji (jak na przykład energia), stosowne wydaje się wprowadzenie odpowiednich zasad ich obrotu, celem uniknięcia możliwych do wystąpienia „monopoli 2.0”. W przypadku bowiem gdyby tokenizacja i obrót tymi dobrami odbywały się w ramach platform tworzonych przez prywatne podmioty pozbawione jakiegokolwiek nadzoru, mogłoby to doprowadzić do zbyt dużej pokusy nadużycia i tworzenia wspomnianych nowych struktur monopolistycznych tym razem tylko z wykorzystaniem technologii blockchain, czyniąc te platformy prywatno-licencjonowanymi, do których dostęp może stać się bardzo kosztowną usługą.

Zestawienie omówionych charakterystyk z potencjałem ich wykorzystania w zależności od wariantów zastosowania zostało pokazane na rysunku 2. Odniesienie ich do stawianych przed rozwiązaniem wymagań czy też do zakładanych do osiągnięcia celów pozwala na wybór wariantu stanowiącego najbardziej optymalną dla danego podmiotu kombinację.

Rysunek 2. Charakterystyki koncepcji blockchain i warianty jej zastosowania



cd. rysunku 2



Źródło: opracowanie własne.

Analizując przedstawione rysunki i poprzedzające je opisy, można stwierdzić, że rozwiązania prywatno-licencjonowane sprawdzają się najlepiej w przypadku, gdy baza danych ma się cechować stosunkowo łatwą skalowalnością, niskimi kosztami, jak również znaczną szybkością w odniesieniu do dokonywanych zapisów. W przypadku gdy głównym celem jest najwyższe bezpieczeństwo, odporność na manipulacje, wiarygodność zapisu, jak również równy dostęp, to preferowane są rozwiązania publiczno-nielicencjonowane. Co więcej, jedynie dwa warianty wymagają tworzenia nowych platform, podczas gdy jedno nie ma logicznego uzasadnienia, a drugie może być utworzone przez odpowiednie dopasowanie istniejących rozwiązań, co zostało zaprezentowane na rysunku 3.

Rysunek 3. Strategie w odniesieniu do rozwiązań wykorzystujących koncepcje blockchain

STRATEGIA	PUBLICZNY	PRYWATNY
LICENCJONOWANY	MOŻLIWOŚĆ WYKORZYSTANIA ISTNIEJĄCEJ PUBLICZNEJ PLATFORMY	BUDOWA NOWEJ PLATFORMY BLOCKCHAIN
NIELICENCJONOWANY	BUDOWA NOWEJ PLATFORMY BLOCKCHAIN	BRAK LOGICZNEGO UZASADNIENIA DLA BUDOWY/WYKORZYSTANIA PLATFORMY

Źródło: opracowanie własne.

4. Podsumowanie

Blockchain to zarówno nowa technologia pozwalająca na poprawę efektywności czy obniżkę kosztów, jak i nowa koncepcja otwierająca możliwości zawierania nieznanych dotychczas transakcji czy też budowania innowacyjnych modeli biznesowych. Szeroki wachlarz potencjalnych zastosowań wynika z jednej strony z nowatorskiego podejścia do rozwiązań znanych od dawna problemów, z drugiej natomiast jest podyktowany dużą elastycznością właściwości technologii, pozwalającą na jej stosunkowo swobodne dopasowywanie.

Główne warianty zastosowania blockchain obejmują cztery możliwe grupy rozwiązań, zróżnicowanych zarówno międzygrupowo, jak i wewnątrzgrupowo, takich jak rozwiązania: (i) publiczno-licencjonowany, (ii) publiczno-nielicencjonowany, (iii) prywatno-licencjonowany oraz (iv) prywatno-nielicencjonowany. Różnorodność międzygrupowa wynika z odmiennego doboru parametrów technologii, podyktowanego różnymi celami, właściwościami rozwiązania (pierwsza grupa) bądź posiadaniem innych aktywów planowanych do umieszczenia w bazie danych blockchain (druga grupa). Jeśli natomiast chodzi o odmienność wewnątrzgrupową, jest ona konsekwencją różnego wykorzystania poszczególnych właściwości, co w rezultacie przekłada się na niejednolite potencjalne korzyści, jakie dane zastosowanie może zaoferować.

Przy analizie parametrów technologii, pozwalających na dobór właściwego wariantu zastosowania technologii w zależności od planowanych do osiągnięcia celów czy też właściwości rozwiązania (pierwsza grupa), warto rozważyć takie zestawienia tych charakterystyk, jak: (i) automatyzacja i decentralizacja, (ii) odporność na zmiany/wiarygodność zapisu i transparentność, (iii) koszt i szybkość procesu, (iv) anonimowość i bezpieczeństwo, (v) skalowalność i elastyczność, (vi) równe prawa i zaufanie, (vii) integralność zapisu i dostęp do danych. Biorąc natomiast pod uwagę aktywa planowane do umieszczenia w bazie danych (druga grupa), pomocne może być zwrócenie uwagi na takie aspekty, jak: (i) aktywa zdigitalizowane i aktywa digitalne, (ii) aktywa porównywalne/weryfikowalne i aktywa specyficzne/niejednorodne, (iii) aktywa prywatne i aktywa publiczne.

Rezultatem analizy jest możliwie jak najbardziej dokładne dopasowanie rozwiązania do wymogów i możliwości biznesowych, a tym samym osiągnięcie potencjalnie najwyższych korzyści czy też uniknięcie kosztownych porażek wynikających z nieprawidłowego zastosowania blockchain. Zaprezentowane w artykule ogólne zestawienie pozwoliło na wskazanie, iż w przypadku gdy kryteriami priorytetowymi są łatwa skalowalność, niższe koszty zapisu danych czy też stosunkowo duża szybkość procesu, najlepiej sprawdzają się rozwiązania prywatno-licencjonowane. Natomiast gdy za cel stawiane jest bezpieczeństwo, wiarygodność zapisu, równy dostęp czy odporność na manipulacje, preferowane są rozwiązania publiczno-nielicencjonowane. Jak zatem można zauważyć, posiadanie ustrukturyzowanego podejścia do analizy ułatwia proces decyzyjny i pozwala na efektywniejsze porównanie dostępnych możliwości, z których każde przyczynia się do rozwiązania innego problemu bądź też stara się sprostać odmiennym wymaganiom.

Przedstawione zestawienie jest tym samym jedną z pierwszych prób strukturyzacji, która z uwagi na początkowe stadium rozwoju technologii może ulegać zmianom. Kolejne lata, a tym samym efekty pierwszych wdrożeń pokażą, jak blockchain jest wykorzystywany, wskazując jednocześnie na najlepsze opcje jego zastosowania i eliminując przykłady, które nie są w stanie przynieść zakładanych efektów.

Bibliografia

1. Agrawal A., Gans J., Goldfarb A. [2016], *The Simple Economics of Machine Intelligence*, „Harvard Business Review”, hbr.org/2016/11/the-simple-economics-of-machine-intelligence [dostęp 2.07.2018].
2. Albrecht S., Reichert S., Schmid J., Strüker J., Neumann D., Fridgen G. [2018], *Dynamics of Blockchain Implementation – A Case Study from the Energy Sector*, 51st Hawaii International Conference on System Science, scholarspace.manoa.hawaii.edu/handle/10125/50334 [dostęp 22.07.2018].
3. Alstynne M.W.V., Parker G.G., Choudary S.P. [2016], *Pipelines, Platforms, and the New Rules of Strategy*, „Harvard Business Review”, hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy [dostęp 1.07.2018].
4. Athey S., Catalini C., Tucker C. [2017], *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, National Bureau of Economic Research, people.stanford.edu/athey/sites/default/files/digital_privacy_paradox_02_13_17.pdf [dostęp 2.07.2018].
5. Atzori M. [2015], *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, [SSRN Scholarly Paper] Rochester, NY: Social Science Research Network, papers.ssrn.com/abstract=2709713 [dostęp 2.07.2018].
6. Back A. [2002], *Hashcash – A Denial of Service Counter-Measure*, s. 10.
7. Bank for International Settlements [2017], *Distributed Ledger Technology in Payment, Clearing and Settlement*, s. 29.
8. Basden J., Cottrell M. [2017], *How Utilities Are Using Blockchain to Modernize the Grid*, „Harvard Business Review”, hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid [dostęp 1.07.2018].
9. Berg C., Davidson S., Potts J. [2018], *Some Public Economics of Blockchain Technology*, [SSRN Scholarly Paper] Rochester, NY: Social Science Research Network, papers.ssrn.com/abstract=3132857 [dostęp 2.07.2018].
10. Böhme R., Christin N., Edelman B., Moore T. [2015], *Bitcoin: Economics, Technology, and Governance*, „Journal of Economic Perspectives”, 29(2), s. 213–238.
11. Bresnahan T.F., Trajtenberg M. [1995], *General Purpose Technologies ‘Engines of Growth?’*, „Journal of Econometrics”, 65(1), s. 83–108.
12. Brown R.G. [2014], *The “Unbundling of Trust”: How to Identify Good Cryptocurrency Opportunities?* Richard Gendal Brown, gendal.me/2014/11/14/the-unbundling-of-trust-how-to-identify-good-cryptocurrency-opportunities/ [dostęp 28.07.2018].
13. Buterin V. [2015], *On Public and Private Blockchains*, blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [dostęp 28.07.2018].

14. Casey, M.J., Wong P. [2017], *Global Supply Chains Are About to Get Better, Thanks to Blockchain*, „Harvard Business Review”, hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain [dostęp 1.07.2018].
15. Catalini C. [2017], *How Blockchain Applications Will Move Beyond Finance*, „Harvard Business Review”, hbr.org/2017/03/how-blockchain-applications-will-move-beyond-finance [dostęp 1.07.2018].
16. Catalini C., Gans J.S. [2018], *Some Simple Economics of the Blockchain*, National bureau of economic research, (22952).
17. Chitchyan R., Murkin J. [2018], *Review of Blockchain Technology and its Expectations: Case of the Energy Sector*. *arXiv:1803.03567 [cs]*, arxiv.org/abs/1803.03567 [dostęp 22.07.2018].
18. Coase R.H. [1937], *The Nature of the Firm*, „Economica”, 4(16), s. 386–405.
19. Cochrane K. [2018], *To Regain Consumers’ Trust, Marketers Need Transparent Data Practices*, „Harvard Business Review”, hbr.org/2018/06/to-regain-consumers-trust-marketers-needed-transparent-data-practices [dostęp 2.07.2018].
20. Davidson S., De Filippi P., Potts J. [2018], *Economics of Blockchain*, Social Science Research Network.
21. De Kruiff J., Weigand H. [2017], *Towards a Blockchain Ontology*, The Netherlands, pdfs.semanticscholar.org/0782/c5badb4f407ee0964d07eda9f74a92de3298.pdf [dostęp 22.07.2018].
22. Evans D.S. [2014], *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms*, „SSRN Electronic Journal”, www.ssrn.com/abstract=2424516 [dostęp 2.07.2018].
23. Feig E. [2018], *A Framework for Blockchain-Based Applications*. *arXiv:1803.00892 [cs]*, arxiv.org/abs/1803.00892 [dostęp 22.07.2018].
24. Forde B. [2017], *Using Blockchain to Keep Public Data Public*, „Harvard Business Review”, hbr.org/2017/03/using-blockchain-to-keep-public-data-public [dostęp 1.07.2018].
25. Frydman R., Duncan I., Goldberg M.D. [2007], *Imperfect Knowledge Economics: Exchange Rates and Risk*, Princeton University Press.
26. Garzik J. [2015], *Public Versus Private Blockchains*, USA, bitfury.com/content/downloads/public-vs-private-pt1-1.pdf [dostęp 22.07.2018].
27. Hileman G., Rauchs M. [2017], *2017 Global Blockchain Benchmarking Study*, [SSRN Scholarly Paper] Rochester, NY: Social Science Research Network, papers.ssrn.com/abstract=3040224 [dostęp 2.07.2018].
28. Hurwicz L. [1973], *The Design of Mechanisms for Resource Allocation*, „The American Economic Review”, 63(2), s. 1–30.
29. Hurwicz L. [1994], *Economic Design, Adjustment Processes, Mechanisms, and Institutions*. „Economic Design”, 1(1), s. 1–14.
30. Iansiti M., Lakhani K.R. [2017], *The Truth About Blockchain*, „Harvard Business Review”, hbr.org/2017/01/the-truth-about-blockchain [dostęp 29.03.2018].
31. IBM [2017], *CNW | 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*, 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 [dostęp 2.07.2018].

32. Ito J., Narula N., Ali R. [2017], *The Blockchain Will Do to the Financial System What the Internet Did to Media*, „Harvard Business Review”, hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media [dostęp 7.01.2018].
33. 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, www.brie.berkeley.edu/wp-content/uploads/2015/02/PlatformEconomy2DistributeJune21.pdf [dostęp 1.07.2018].
34. 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), s. 18–27.
35. 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).
36. Kshetri N. [2018], *1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives – Business – ProQuest*, „International Journal of Information Management”, 39, www.sciencedirect.com/science/article/pii/S0268401217305248 [dostęp 2.07.2018].
37. Laffont J.-J., Martimort D. [2009], *The Theory of Incentives: The Principal-Agent Model*, Princeton University Press.
38. Leon D.C. de, 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), s. 286–300.
39. Mainelli M. [2017], *Blockchain Could Help Us Reclaim Control of Our Personal Data*, „Harvard Business Review”, hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data [dostęp 1.07.2018].
40. McWaters J., Galaski R. [2017], *Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services*.
41. Nakamoto S. [2008], *Bitcoin: A Peer-to-Peer Electronic Cash System*.
42. Nowiński W., Kozma M. [2017], *How Can Blockchain Technology Disrupt the Existing Business Models?*, „Entrepreneurial Business and Economics Review”, 5(3), s. 173–188.
43. Nurisso G., Prescott E.S. [2017], *The 1970s Origins of Too Big to Fail*, www.clevelandfed.org/newsroom-and-events/publications/economic-commentary/2017-economic-commentaries/ec-201717-origins-of-too-big-to-fail [dostęp 6.07.2018].
44. 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), s. 335–344.
45. Petersen M., Hackius N., See B.V. [2017], *Mapping the Sea of Opportunities: Blockchain in Supply Chain and Logistics*.
46. Pilkington M. [2016], *Blockchain Technology: Principles and Applications*, University of Burgundy.
47. 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*, www.transparency-one.com/microsoft-blockchain-supply-chain-transparency [dostęp 2.07.2018].

48. Salviotti G., De Rossi L.M., Abbatemarco N. [2018], *A Structured Framework to Assess the Business Application Landscape of Blockchain Technologies*, hdl.handle.net/10125/50328 [dostęp 22.07.2018].
49. Schrage M. [2016], *Instead of Optimizing Processes, Reimagine Them as Platforms*, „Harvard Business Review”, hbr.org/2016/12/instead-of-optimizing-processes-reimagine-them-as-platforms [dostęp 1.07.2018].
50. Scott B. [2016], *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?*, The United Nations Research Institute for Social Development (UNRISD), s. 25.
51. Tabarrok A., Cowen T. [2015], *The End of Asymmetric Information*, www.cato-unbound.org/2015/04/06/alex-tabarrok-tyler-cowen/end-asymmetric-information [dostęp 2.07.2018].
52. Tapscott D., Tapscott A. [2016], *The Impact of the Blockchain Goes Beyond Financial Services*, „Harvard Business Review”, hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services [dostęp 29.03.2018].
53. Tasca P., Tessone C. [2018], *Taxonomy of Blockchain Technologies. Principles of Identification and Classification*, University of Zurich.
54. Täuscher K., Laudien S.M. [2018], *Understanding Platform Business Models: A Mixed Methods Study of Marketplaces*, „European Management Journal”, 36(3), s. 319–329.
55. The Economist [2018], *Blockchain Technology May Offer a Way to Re-decentralise the Internet*, „The Economist”, www.economist.com/special-report/2018/06/30/blockchain-technology-may-offer-a-way-to-re-decentralise-the-internet [dostęp 9.07.2018].
56. Tucker C., Catalini C. [2018], *What Blockchain Can't Do*, „Harvard Business Review”, hbr.org/2018/06/what-blockchain-cant-do [dostęp 1.07.2018].
57. Tullock G. [1988], *Efficient Rent-Seeking Revisited*, w: *The Political Economy of Rent-Seeking*, Topics in Regulatory Economics and Policy, Springer, Boston, MA, s. 91–94, link.springer.com/chapter/10.1007/978-1-4757-1963-5_7 [dostęp 28.07.2018].
58. World Economic Forum [2015], *Deep Shift Technology Tipping Points and Societal Impact*, www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf [dostęp 2.07.2018].
59. Wüst K., Gervais A. [2017], *Do You Need a Blockchain?*, Department of Computer Science, ETH Zurich, Switzerland, s. 7.
60. Xu X., Weber I., Staples M., Zhu L., Bosch J., Bass L., Pautasso C., Rimba P. [2017], *A Taxonomy of Blockchain-Based Systems for Architecture Design*, w: *2017 IEEE International Conference on Software Architecture (ICSA)*, 2017 IEEE International Conference on Software Architecture (ICSA), s. 243–252.

Blockchain Application Options and Their Selection Models

Summary

Over only 10 years, blockchain has developed into a highly complex and diverse solution with a number of application options representing diverse structures and properties. Despite such a wide interest in the new concept, there is still no regulation, classification or structure that would help to more easily interpret this rather complex technology as well as to analyse and compare possibilities that it offers. This leads to an extended decision-making process additionally burdened with a substantial risk of making mistakes or selecting a solution that is not the optimum one. This paper aims at a structured presentation of blockchain properties and their intensity in subsequent application options, which could provide foundations for building selection models assisting in finding an optimum combination for a given entity based on its individual or business preferences, business model or strategy.

Keywords: blockchain, private, public, licensed, unlicensed
