STUDIA I ARTYKUŁY

MACIEJ HULICKI[1]

PAWEŁ LUSTOFIN[2]

WYKORZYSTANIE KONCEPCJI BLOCKCHAIN W REALIZACJI ZOBOWIĄZAŃ UMOWNYCH

STRESZCZENIE:

Przedmiotem artykułu jest analiza aspektów prawnych związanych z koncepcją blockchain ze szczególnym uwzględnieniem obszaru realizacji zobowiązań umownych. Dzięki zastosowaniu kilku złożonych mechanizmów kryptograficznych oraz procesom budowania porozumienia i znacznika czasu system blockchain pozwala na realizację transakcji bez instytucji pośredniczącej pomiędzy użytkownikami, którzy nie znają się nawzajem. Zastosowanie tego rodzaju koncepcji może przyczynić się do tworzenia inteligentnych umów, czyli programów komputerowych, które mogą podejmować decyzje w przypadku spełnienia określonych warunków. Implementacja inteligentnych umów może m.in. zwiększyć szybkość oraz pewność prawidłowego wykonania umowy. Niemniej jednak w kontekście inteligentnych umów krytyczne znaczenie posiada poprawność kodu. W związku z tym, brak powszechnej znajomości języków programowania może stanowić istotną barierę dla rozwoju tego rozwiązania. Pomimo tego, że obecnie rozwiązanie blockchain nie podlega żadnym szczególnym regulacjom, to jego rozwój i konkretne zastosowania powinny być dalej monitorowane.

SŁOWA KLUCZOWE:

blockchain, bitcoin, inteligentne umowy, zobowiązania umowne, automatyzacja prawa, regulacja nowych technologii

[1] Adiunkt, Wydział Prawa i Administracji UKSW.
[2] Doktorant, Uniwersytet Ekonomiczny w Krakowie.

***

1. WPROWADZENIE

Obecnie żyjemy w dobie rewolucji cyfrowej, przez niektórych nazywanej również transformacją cyfrową. Nie byłaby ona możliwa, gdyby nie stopień zaawansowania narzędzi technicznych w zakresie przesyłania danych, szybkości ich przetwarzania oraz dostępności urządzeń mobilnych. W chwili obecnej największe nadzieje wiąże się z takimi technikami i technologiami jak: Internet rzeczy (ang. *internet of things*), druk 3D (ang. *3D printing*), rzeczywistość rozszerzona (ang. *augmented reality*), sztuczna inteligencja i uczenie maszynowe (ang. *artificial intelligence* oraz *machine learning*), *big data*, a także z koncepcją rozproszonych baz danych w postaci tzw. łańcucha bloków (ang. *blockchain*), która przez niektórych określana jest jako innowacja przełomowa (ang. *disruptive innovation*)[3] i której poświęcono niniejszy artykuł. Wszystkie powyższe narzędzia techniczne implikują poważne zmiany w naszym codziennym otoczeniu i jednocześnie charakteryzuje je duży stopień złożoności, co w naszej opinii determinuje konieczność przeprowadzenia ich dogłębnej analizy prawnej.

Pod koniec 2015 roku Światowe Forum Ekonomiczne opublikowało raport poświęcony przełomowym technologiom (raport „Deep Shift – Technology Tipping Points and Societal Impact"). Uwzględniono w nim opinie ponad 800 menadżerów i ekspertów, a 'Bitcoin i blockachain' sklasyfikowano na 16 miejscu[4]. Począwszy od 2015 roku obserwujemy ciągły wzrost świadomość potencjalnego znaczenia koncepcji blockchain i jej wykorzystania w wielu dziedzinach gospodarki. Co roku Rada ds. Nowych Technologii Światowego Forum Ekonomicznego we współpracy z magazynem Scientific American przygotowuje ranking najbardziej przełomowych technologii (The Top 10 Emerging Technologies 2016 list), które będą miały największy wpływ na poprawę życia, transformacje różnych dziedzin gospodarki oraz ochronę środowiska naturalnego. W roku 2016 na trzecim miejscu tego zestawienia uplasowała się koncepcja rozproszonej bazy danych typu 'blockchain'[5]. Równolegle

[3] C.M. CHRISTENSEN, M. E. RAYNOR, R. MCDONALD, *What is disruptive innovation?*, Harvard Business Review, 12/1995.
[4] P. ROSATI, B. NAIR, T. LYNN; *Bitcoin Vs Blockchain: The Role of trust in disrupting financial services*; Proceedings of 7th European Business Research Conference 15 – 16 December 2016, University of Roma Tre, Rzym, 10.2016, s. 1.
[5] O. CANN, *These are the top 10 emerging technologies of 2016*, World Economic Forum, Dostęny na: https://www.weforum.org/agenda/2016/06/top-10-emerging-technologies-2016/; odwiedzony 30.01.2017 r.

obserwujemy wzrost liczby publikacji naukowych traktujących o blockchain i poddających ją naukowej analizie. Przeszukiwanie bazy 'Web of Science', która obejmuje zaledwie wycinek wszystkich publikacji naukowych, pokazało 109 artykułów poświęconych temu zagadnieniu. Nawet tak mała próbka pokazuje bardzo wyraźny trend. Ponad 70 % publikacji ukazało się w 2016 roku, przy czym ponad 90 % dotyczy informatyki, telekomunikacji i pokrewnych dziedzin. Uwzględniając potencjalnie olbrzymi wpływ na wiele dziedzin gospodarki, jak również funkcjonowanie państwa i społeczeństw, można spodziewać się z jednej strony dalszego wzrostu zainteresowania badaniami, które dotyczą rozproszonych baz danych typu 'blockchain', a z drugiej strony większej liczby prac w dziedzinach wykraczających poza obszar informatyki.

Artykuł rozpoczyna zarys koncepcji rozproszonej bazy danych w postaci łańcucha bloków. W dalszej części opisano jej architekturę oraz implementację, a następnie przeanalizowano potencjalne skutki prawne, jakie implikuje jej zastosowanie w obszarze prawa ze szczególnym uwzględnieniem inteligentnych kontraktów (ang. *smart contracts*).

2. KONCEPCJA ROZWIĄZANIA BLOCKCHAIN

Jak już wspomniano, innowacja przełomowa to taka innowacja, która tworzy nowe rynki i sieci wartości, zastępując nimi już istniejące i eliminuje obecnych liderów rynku, produkty oraz usługi. Należy podkreślić, że koncepcja blockchain jest jednym z czołowych i najbardziej obiecujących rozwiązań technicznych, które są obecnie rozwijane, tym niemniej trudno w tej chwili przewidzieć czy okaże się ono również innowacją przełomową. Sektor finansowy wskazano jako podstawowy obszar zastosowania tego rozwiązania (koncepcję blockchain użyto po raz pierwszy tworząc podstawy waluty Bitcoin). Coraz częściej pojawiają się jednak głosy, że to rozwiązanie będzie raczej narzędziem, które przyczyni się do wyeliminowania niedoskonałości obecnego systemu finansowego, ale nie będzie bezpośrednim zagrożeniem dla jego głównych podmiotów[6]. Trzeba podkreślić, że sektor finansowy docenia możliwości i potencjalne znaczenie rozproszonej bazy danych blockchain i znalazło to już odzwierciedlenie w znaczących inwestycjach kapitałowych takich instytucji, jak np. Santander, Citi Group czy też Barclays[7]. W październiku 2015 roku 13 banków dołączyło do konsorcjum

[6] M. MASSIMO, *From 'Blockchain Hype' to a Real Business Case for Financial Markets*; Banca IMI; Bocconi University; 21.12.2016 r.
[7] K. MARZANTOWICZ, *Największe banki na świecie inwestują w Blockchain, podstawę Bitcoin*, dostępny na: http://itwiz.pl/najwieksze-banki-na-swiecie-inwestuja-w-blockchain-podstawe-bitcoin; odwiedzony 30.01.2017 r.

powołanego przez start-up R3CEV wspólnie z 9 bankami, którego głównym celem jest rozwijanie rozproszonej księgi głównej, pozwalającej na transfer aktywów finansowych między różnymi instytucjami finansowymi[8]. Pod koniec 2016 konsorcjum liczyło już około 70 instytucji sektora finansowego[9]. Prognozuje się, że koncepcja blockchain będzie miała duże znaczenie nie tylko dla sektora finansowego, ale znajdzie wiele zastosowań w sektorach handlu i usług publicznych. Co więcej, przewiduje się, że to rozwiązanie może w znaczący sposób wpłynąć na sposób realizacji wewnętrznych procesów biznesowych (np. w obszarze nadzoru korporacyjnego), a także umożliwi bliższą współpracę pomiędzy firmami w ramach rozszerzonego łańcucha dostaw. Zanim bardziej szczegółowo opiszemy potencjalne zastosowania koncepcji rozproszonej bazy danych, podkreślimy cechy, które wyróżniają ją na tle innych technik przetwarzania informacji. Architekturę rozproszonej bazy danych typu 'blockchain' po raz pierwszy zaproponował twórca pierwszej cyfrowej waluty Satoshi Nakamoto w roku 2008 [10] (przyp. Satoshi Nakamoto jest pseudonimem twórcy (lub twórców) pierwszej cyfrowej waluty oraz koncepcji blockchain). Sama waluta Bitcoin pojawiła się na rynku w styczniu 2009 roku. Bitcoin to pierwszy globalny system elektronicznych operacji handlowych (kupna, sprzedaży), u podstaw którego nie leży zaufanie do centralnej instytucji (w kontekście waluty taką instytucją jest Bank Centralny odpowiedzialny min. za kreowanie pieniądza i kontrolę podaży pieniądza w gospodarce). Brak zaufania między użytkownikami systemu wyeliminowano, stosując kilka złożonych mechanizmów kryptograficznych takich jak: kryptograficzne funkcje skrótu (ang. *hash*), które pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych, podpis elektroniczny korzystający z kryptografii asymetrycznej, mechanizm budowania porozumienia (ang. *consensus*) między użytkownikami systemu[11] oraz znacznik czasu. Opiniotwórczy tygodnik *The Economist* określił koncepcję blockachain mianem „maszyny do tworzenia zaufania" (ang. *the trust machine*)[12]. Rozproszona („demokratyczna") architektura systemu bitcoin umożliwia każdemu z użytkowników wgląd w pełną historię transakcji, zapewniając im jednocześnie anonimowość (tzn. użytkownicy systemu widoczni są pod numerem klucza publicznego).

Rozproszona baza danych typu 'blockchain' jest zdecentralizowanym rejestrem danych przechowywanych w łańcuchu bloków. Rejestr danych nie jest kontrolowany przez jednego,

[8] Tamże.
[9] K. JEMIMA, *Exclusive: Blockchain platform developed by banks to be open-source*, Reuters UK, odwiedzony 20.10.2016 r.
[10] S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System.*
[11] Z. ZHENG, S. XIE, H.N. DAI, H. WANG, *Blockchain Challenges and Opportunities: A Survey*, International Journal of Electric and Hybrid Vehicles, 01.2017 r.
[12] J. BERKLEY, *The promise of the blockchain The trust machine*, The Economist, 31.10.2015 r.

ale przez wszystkich użytkowników zdecentralizowanego systemu. Jak już wspomniano w systemie bitcoin (u którego podstaw leży pierwsze, „tradycyjne" rozwiązanie blockchain) nie ma centralnej instytucji, która byłaby odpowiedzialna za jego kontrolę. W przypadku systemu bankowego rolę instytucji zaufania pełnią banki. Banki kontrolują poprawność transakcji zapobiegając między innymi możliwości podwójnego wydania tej samej jednostki waluty. Satoshi Nakamoto zauważył jednak, że transakcje w ramach tradycyjnego systemu systemu finansowego nie są operacjami nieodwracalnymi. W przypadku sporów pomiędzy uczestnikami transakcji rolę mediatora przyjmują właśnie banki i inne instytucje finansowe, co wg. Nakamoto podwyższa koszty transakcji. System bitcoin(jak również inne publiczne rozwiązania typu blockchain) cechuje nieodwracalność odbywających się w nim transakcji[13]. Od pojawienia się pierwszej waluty cyfrowej i tym samym pierwszej implementacji łańcucha bloków koncepcja ta uległa znacznej ewolucji.

Obecnie wyróżniamy trzy główne rodzaje rozwiązania typu blockchain: system publiczny, korporacyjny oraz prywatny. Różnią się przede wszystkim stopniem zaufania pomiędzy użytkownikami systemu, począwszy od całkowitego braku zaufania w przypadku systemu publicznego do relatywnie wysokiego poziomu zaufania w przypadku systemu prywatnego, co znajduje swoje odzwierciedlenie w ich różnej architekturze. Jedynym prawdziwie zdecentralizowanym rozwiązaniem typu blockchain jest system publiczny, którego użytkownikiem może być każdy. Prywatne rozwiązanie typu blockchain w pełni kontroluje jedna organizacja i nie można go uznać za zdecentralizowane, natomiast system korporacyjny będzie jedynie częściowo zdecentralizowany. Kolejną, istotną techniczną różnicą pomiędzy ww. rozwiązaniami jest możliwość zmiany danych historycznych. W systemie publicznym jest to niemożliwe, podczas gdy w pozostałych dopuszcza się to, jeśli taka jest wola głównych użytkowników.

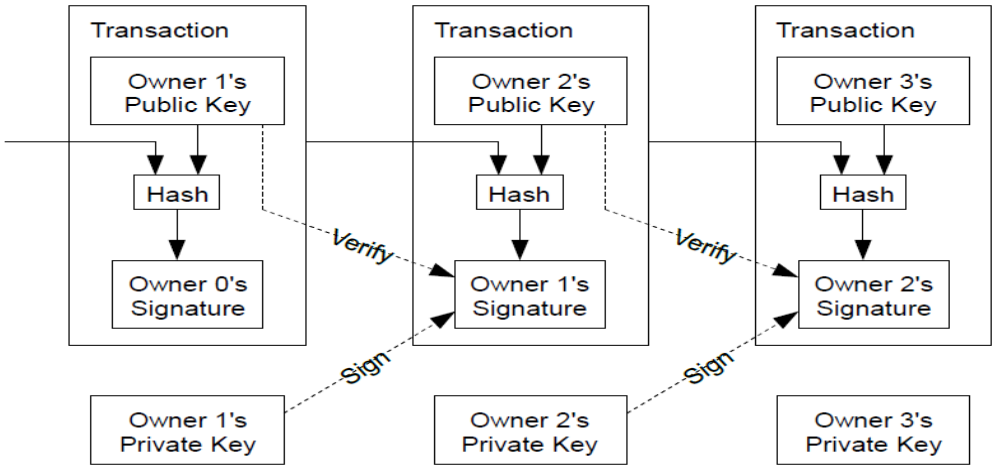
3. ARCHITEKTURA ROZPROSZONEJ BAZY DANYCH TYPU BLOCKCHAIN

W tym punkcie, na przykładzie systemu bitcoin, omówimy strukturę rozproszonej bazy danych w postaci łańcucha bloków. Chociaż opis procesów zachodzących w systemie blockchain bazuje na przykładzie rozwiązania bitcoin, to należy pamiętać, że ogólne zasady mają zastosowanie również w innych systemach korzystających z koncepcji blockchain. Ponieważ tę koncepcję wciąż się rozwija dostosowując ją do konkretnych zastosowań, to nie

[13] S. NAKAMOTO, op. cit.

wszystkie elementy systemu bitcoin są obecne w innych publicznych systemach korzystających z łańcucha bloków. Jak już wcześniej wspomniano publiczny system blockchain ma architekturę zdecentralizowaną[14].

W przypadku zdecentralizowanych baz danych, ich codziennym utrzymaniem zajmuje się osoba pełniąca funkcję administratora, która często ma prawo do zapisu i odczytu danych, co naturalnie rodzi ryzyko nadużyć i manipulacji. W systemie blockchain takie ryzyko wyeliminowano. Pierwszym obszarem, w którym zastosowano rozwiązanie typu blockchain, była wymiana aktywów. W systemie blockchain takie transakcje realizują użytkownicy, którzy nie znają się nawzajem, co implikuje zupełny brak zaufania. Istnienie takich systemów i dokonywanie transakcji na masową skalę, przy jednoczesnym braku centralnej instytucji, która odpowiada za kontrolę i bezpieczeństwo, jest możliwe dzięki unikatowemu zastosowaniu kilku metod kryptograficznych. W systemie bitocoin, użytkownik/właściciel, który przekazuje/przesyła jednostki waluty, używa do podpisu kryptograficznej funkcji skrótu (ang. *hash*) poprzedniej transakcji oraz publicznego klucza kolejnego właściciela (ten proces dobrze ilustruje zamieszczony niżej diagram)[15].



Rys. 1. Transakcje w systemie Bitcoin [Źródło: S. NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System]

[14] Zob. np. P. BARAN, *On distributed communication networks*, Rand Corporation, 1962, s. 4 (Fig. 1).
[15] S. NAKAMOTO, op. cit.

W systemie, w którym brak jakiejkolwiek centralnej instytucji odpowiedzialnej za weryfikację płatności (zapobieganie podwójnemu wydawaniu tej samej jednostki waluty), akceptacja transakcji odbywa się na zasadzie porozumienia (ang. *consensus*), co oznacza, że więcej niż połowa węzłów musi potwierdzić daną operację (handlową) i uzgodnić kolejność transakcji. Jest to możliwe dzięki temu, że rejestr transakcji ma publiczny charakter i funkcjonuje w postaci łańcucha bloków, oraz stosuje datownik (ang. *timestamp*), żeby oznaczyć czas operacji. Co ok. 10 minut, transakcje realizowane przez użytkowników systemu (ang. *nodes*) zbierane są w paczki, które tworzą bloki.

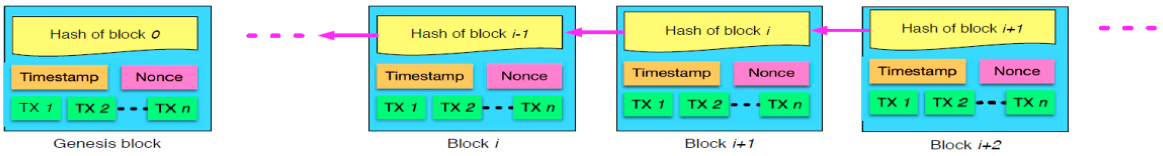
Dany blok musi być zweryfikowany przez specjalne węzły systemu (ang. *miners*), których łączna moc obliczeniowa stanowi co najmniej 51 % całkowitej mocy obliczeniowej wszystkich węzłów w tym systemie (co jest równoznaczne z osiągnięciem porozumienia). Opisany mechanizm to tzw. świadectwo (mocy) przetwarzania (ang. *proof-of-work*), które stanowi podstawę jednego z kilku funkcjonujących algorytmów matematycznych, stosowanych w celu osiągnięcia wspomnianego porozumienia w systemie zdecentralizowanym. Po zebraniu transakcji w bloku, wyspecjalizowane węzły systemu (ang. *miners*) współzawodniczą ze sobą w rozwiązaniu zadania matematycznego. Trudność zadania jest dostosowana do całkowitej mocy obliczeniowej tych węzłów (ang. *miners*) tak, aby zapewnić walidację kolejnych bloków w odstępach czasu równych ok. 10 minut. Po rozwiązaniu problemu matematycznego blok rozpowszechnia się w systemie, a zawarte w nim transakcje podlegają weryfikacji. Co bardzo istotne, taki wyspecjalizowany węzeł (przetwarzania danych), który pierwszy rozwiązał zadanie matematyczne otrzymuje wynagrodzenie. System motywacyjny jest konieczny, aby zapewnić odpowiednią liczbę uczestników procesu przetwarzania (informacji), który przekłada się bezpośrednio na poziom bezpieczeństwa systemu. Sam proces przetwarzania jest energochłonny a przez to kosztowny co stanowi jedną z wad ww. świadectwa przetwarzania, które dokładniej opiszemy w dalszej części artykułu. Sam Satoshi Nakamoto podkreśla również, że system wynagradzania zachęca węzły do uczciwego działania[16]. Obecnie całkowita moc wyspecjalizowanych węzłów jest przeszło 1000 razy większa niż moc 500 największych superkomputerów[17]. Świadczy to o wysokim stopniu bezpieczeństwa systemu bitcoin, tzn. pokazuje jak duża moc obliczeniowa, co za tym idzie nakład finansowy byłby wymagany, aby dokonać oszustwa. Satoshi Nakamoto wymienia następujące fazy działania systemu bitcoin:

[16] Tamże.

[17] K. PIECH, *Leksykon pojęć na temat technologii blockchain i kryptowalut*, 08.11.2016 r., dostępny na: https://mc.gov.pl/files/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf;

1) przesyłanie nowych transakcji do wszystkich węzłów w systemie,
2) gromadzenie transakcji w bloku przez każdy z węzłów,
3) poszukiwanie przez każdy z węzłów świadectwa przetwarzania dla swojego bloku,
4) po znalezieniu rozwiązania przesłanie bloku do wszystkich pozostałych węzłów,
5) akceptacja bloku tylko wtedy, kiedy wszystkie zawarte w nim transakcje są prawidłowe,
6) dowodem akceptacji bloku jest uruchomienie przetwarzania kolejnego bloku, który przyjmuje skrót (ang. *hash*) zaakceptowanego właśnie bloku[18].

Należy podkreślić, że kolejne bloki łączą się w nierozerwalny łańcuch, (co m.in. świadczy o nieodwracalnym charakterze transakcji w systemie. W praktyce oznacza to, że próba dokonania zmiany w jednym z bloków wymusiłaby ponowne zatwierdzenia wszystkich występujących po nim bloków. Kryptograficzne „zespolenie" bloków bardzo dobrze ilustruje zamieszczony niżej rysunek.



Rys. 2. Struktura łańcucha bloków [Źródło: Z. ZHENG, S. XIE, H.N. DAI, H. WANG, *Blockchain Challenges and Opportunities: A Survey*, International Journal of Electric and Hybrid Vehicles, 01.2017 r., str. 4]

Główną alternatywą dla świadectwa przetwarzania (*proof-of-work*) jest algorytm świadectwa udziału (ang. *proof-of-stake*), w którym dominującą rolę odgrywa najbogatszy użytkownik systemu. Stosując algorytm świadectwa udziału zakłada się że najbogatsi użytkownicy sieci są najmniej skłonni do nadużyć i kradzieży.

Pomimo licznych zalet, w obecnym stadium rozwoju, koncepcja blockchain nie jest pozbawiona wad, tzn. jej istotnym ograniczeniem jest skalowalność, rozumiana jako możliwość przetwarzania setek tysięcy transakcji na sekundę. Dla porównania, system bitcoin aktualnie wykonuje około 7 transakcji na sekundę. Co więcej, w celu walidacji nowych bloków, każdy węzeł systemu przechowuje całą historię transakcji, a to, w kontekście braku możliwości zapewnienia bezwzględnej anonimowości, stanowi poważne źródło ryzyka. Ponadto blockchain jest podatny na atak kierowany z maszyn o łącznej mocy obliczeniowej równej co

[18] S. NAKAMOTO, op. cit.

najmniej 51 % całkowitej mocy obliczeniowej systemu[19]. Jest to o tyle istotne, że obserwuje się centralizację węzłów w systemie bitcoin i nie można wykluczyć, że podobne zjawisko będzie występować w innych publicznych systemach typu blockchain. Trzeba zaznaczyć, że centralizacja przeczy głównej idei (demokratyczny charakter) rozwiązania blockchain. Zjawisko można również zaobserwować w systemach prywatnych (dominacja dużych firm). Kolejnym potencjalnym źródłem ryzyka jest publiczny charakter transakcji w systemie typu blockchain. Algorytmy, na podstawie których w systemie ustala się porozumienie nie są pozbawione wad tzn. ich realizacja (uzyskanie świadectwa przetwarzania) absorbuje bardzo dużą moc obliczeniową i tym samym generuje duże koszty. Z kolei algorytm *proof-of-stake* oznacza skupienie decyzyjności w rękach najbogatszych użytkowników systemu.

4. ZASTOSOWANIE KONCEPCJI BLOCKCHAIN

Istotą i jednoczenie największą zaletą rozwiązania blockchain (od strony funkcji jakie spełnia) jest decentralizacja różnego rodzaju rejestrów danych. Co więcej, dzięki transparentności ww. rejestrów, osoby będące użytkownikami systemu typu blockchain, mają pełny wgląd w historię transakcji, co w połączeniu z zastosowaniem algorytmów konsensusu i narzędziami kryptograficznymi sprawia, że koncepcja blockchain staje się podstawą stabilnego i bezpiecznego systemu wymiany „wartości" (należy jednak przy tym uwzględniać ryzyka, jakie krótko opisano w poprzednim punkcie). Wynika stąd, że w danym systemie można wyeliminować instytucję pośredniczącą, której nadrzędnym celem jest zapewnienie bezpieczeństwa systemu oraz kontrola poprawności zachodzących w nim zdarzeń. Bez ww. instytucji, do czasu pojawienia się pierwszego zastosowania koncepcji blockchain tj. systemu bitcoin, realizacja transakcji na dużą skalę, ponad granicami państw i pomiędzy ludźmi, którzy nie znają się wzajemnie, nie była możliwa. To właśnie możliwość bezpośredniej współpracy pomiędzy obcymi sobie jednostkami stanowi o przełomowym charakterze rozwiązania blockchain. Spektrum zastosowania tego rozwiązania, co pokazano w zamieszczonej niżej tabeli, jest bardzo szerokie. Jednocześnie trzeba podkreślać, że z racji nowatorskiego charakteru rozwiązania, większość poniżej przedstawionych zastosowań jest jeszcze w fazie rozważań lub fazie *proof-of-concept*. Mnogość potencjalnych zastosowań pokazuje jak ważna jest gruntowna analiza prawna wszelkich zdarzeń jakie może implikować zastosowanie tego rozwiązania.

[19] Tamże.

Tabela 1. – Przykładowe zastosowania koncepcji blockchain

Obszar Zastosowania	**Przykłady zastosowań**
Bankowość, Finanse, Sektor przedsiębiorstw	• Rynki finansowe *peer-to-peer* (np. handel różnego rodzaju aktywami, papierami dłużnymi itp.). Z ankiety przeprowadzonej przez firmę IBM wynika, że 15 % banków oraz 14 % instytucji działających na rynkach finansowych planuje wprowadzenie rozwiązania blockchain w 2017 r.; 65 % (z 400 przebadanych) instytucji potwierdziło, że planuje implementację koncepcji blockchain w przeciągu najbliższych 3 lat[20]. • Ujednolicone bazy danych transakcji w systemach bankowych (co powinno się przełożyć na istotne przyspieszenie realizacji transakcji oraz zmniejszenie kosztów operacyjnych w bankowości); • Możliwości bliższej współpracy firm[21,22], w tym bliższej współpracy w ramach rozszerzonego łańcucha dostaw [23.] Takie zastosowanie może przełożyć się na optymalizację kosztów w ramach łańcucha dostaw poprzez lepszą koordynację działań pomiędzy współpracującymi firmami; • Otwarte sieci produkcji (ang. *open production networks*) – koncepcja pełnej transparentności w ramach całego łańcucha dostaw[24]. Konsekwencje implementacji idei naukowców oznaczałyby pojawienie się potężnego narzędzia do weryfikacji kraju pochodzenia poszczególnych komponentów danego produktu (kontrola zmian na każdym etapie łańcuch dostaw),

[20] M. HABLEN, *Financial sector expands use of blockchain databases*, dostępny na: www.cio.com (artykuł został pierwotnie opublikowany przez Computerworld), 28.09.2016 r. odwiedzony 05.02.2016 r.
[21] A. NORTA, *Establishing distributed governance infrastructure for enacting cross-organizational collaborations*, 01.2016, s. 1-13.
[22] I. WEBER, X. XU, R. RIVERT, G. GOVERNATORI, A. PONOMAREV, J. MENDLING; *Untrusted Business Process Monitoring and Execution Using Blockchain*, 08.09.2016 r., s. 1-16.
[23] B. GOERTZEL, T. GOERTZEL, Z. GOERTZEL, *The global brain and the emergance of the world of abundance, Mutualism, open collaboration, exchange networks and the automated commons*, Technological forecasting and Social Change, 114/2017, s. 65-73.
[24] Tamże, s. 68.

	kontroli jakości itp. Szczególnym zastosowaniem wydają się być certyfikaty jakości[25]. • *Smart contracts* – inteligentne umowy, czyli autonomiczne programy, których uruchomienie następuje automatycznie co tym samym stanowi gwarancję i nieodwracalność realizacji postanowień pomiędzy „stronami" kontraktu. (bliżej o o inteligentnych umowach powiemy w dalszej części artykułu). • Wsparcie dla systemów zarządzania.
Medycyna	• Zapobieganie manipulacji wyników testów klinicznych[26]. Zastosowanie technologii blockchain do kontroli procesu przeprowadzania testów klinicznych podniesie zaufanie do ich wyników i wyeliminuje dopuszczanie leków o niskiej skuteczności klinicznej oraz niskim profilu bezpieczeństwa.
Internet Rzeczy (internet of things - IoT)	• Integracja technologii blockchain i Internetu Rzeczy może przyczynić się do zwiększenia anonimowości aplikacji IoT[27]. Z kolei wykorzystanie inteligentnych umów będących istotną częścią rozwiązania blockchain 2.0 przyczyni się do zwiększenia przewidywalności w Internecie Rzeczy. IBM przedstawił tzw. *proof-of-concept* dla nowego systemu ADEPT (ang. *Autonomous Decentralized Peer-to-Peer Telemetry*), który umożliwi budowę zdecentralizowanego Internetu Rzeczy[28].
Usługi publiczne	• Potwierdzenie praw własności w tym rejestracja budynków, ziemi, patentów itp. Rozwiązanie blockchain charakteryzuje się wysoką odpornością na manipulacjęę danych zawartych w łańcuch bloków, co ma fundamentalne znaczenie w kontekście wrażliwości danych przechowywanych w ww. rejestrach. Co więcej rozwiązanie blockchain jest odporne na korupcję.

[25] G. R.T. WHITE, J. HOLDEN, *Future Applications of Blockchain: toward a value-based socjety*, INCITE Conference, Amity University, India, 10.2016 r., s. 3.
[26] G. IRVING, J. HOLDEN , *How blockchain-timestamped protocols could improve the trustworthiness of medical science*, 31.05.2016, s. 1-6.
[27] Z. ZHENG, S. XIE, H.N. DAI, H. WANG, op. cit., s. 12.
[28] Tamże, s. 12.

	• Systemy zachęcające do używania „zielonych" technologii[29]. Istnieją koncepcje rozwiązań systemów motywacyjnych (wynagradzanie producentów energii słonecznej) bazujących na rozwiązaniu blockchain. • Rozwiązanie blockchain zarekomendowano jako narzędzie służące ochronie przed piractwem komputerowym oraz to, które wspiera ochronę przed cenzurą w internecie.
Bezpieczeństwo	• W literaturze poświęconej koncepcjii blockchain można znaleźć propozycję zastosowania łańcucha bloków do ochrony prywatności w aspekcie: 1) praw własności do danych; 2) transparentności i audytowalności danych oraz 3) kontroli dostępu[30]. • Poprawa bezpieczeństwa infrastruktury klucza publicznego (PKI).
Systemy uwierzytelniające	• Weryfikacja recenzji klientów[31]. Istnieje koncepcja zastosowania blockchain do ograniczenia liczby niewiarygodnych/ podejrzanych recenzji. • Weryfikacja procesu *due dilligence* (*Verified Corporate Due Diligence*)[32]. Koncepcję blockchain można również zastosować do zabezpieczenia praw własności intelektualnej w przypadku zakończenia aliansów strategicznych i fuzji. • Systemy zarządzania tożsamością cyfrową.

Technika *blockchain 2.0* umożliwiła implementację pierwszych inteligentnych umów. Inteligentne umowy, pod postacią kodu, mogą zostać rozpowszechnione w rozproszonych rejestrach danych takich sieci jak Corda, Ethereum, Hypeledger[33]. Podstawą ww. sieci jest

[29] N. GOGERTY, J. ZITOLI, *An electricity-backed currencey proposal*, 2011, dostępny na: http://bravenewcoin.com/assets/Whitepapers/DeKo-An-Electricity-Backed-Currency-Proposal.pdf, odwiedzony 05.02.2017 r.
[30] G. ZYSKIND, O. NATHAN (et al.), *Decentralizing privacy: Using blockchain to protect personal data,* Security and Privacy Workshops (SPW), 2015, s. 180-184.
[31] G. R.T. WHITE, K. BROWN, op. cit., s. 3.
[32] Tamże, s. 3.
[33] C. Clack (et al.), *Smart Contract Templates: foundations, design landscape and research directions*, dostępne na:

koncepcja łańcucha bloków, która umożliwia automatyczne wykonanie programu komputerowego (kodu inteligentnej umowy) w momencie osiągnięcia konsensusu. W praktyce ma to zapewnić, że zobowiązania wynikające z kontraktu zostaną bezwzględnie zrealizowane. W tym kontekście jednak zwraca się uwagę na możliwość pojawienia się błędów w samym kodzie umowy. Błąd w kodzie przełoży się na realizację warunków stojących w sprzeczności z intencją stron lub brak jakichkolwiek działań. Z drugiej strony błąd w kodzie może być przyczyną ataków hakerów takich jak ten na instytucję the DAO (podstawą której jest sieć Etherum) w roku 2016, w wyniku którego skradziono 55 mln USD. Powyższe implikuje, że w chwili obecnej nie można założyć realizacji umów bez nadzoru i ewentualnych działań „naprawczych" strony trzeciej. Co więcej nie ma powszechnie akceptowanego języka programowania do spisywania inteligentnych umów, chociaż opracowywane są wzorcowe umowy wraz z niezbędnymi parametrami umożliwiającymi ich operacjonalizację[34]. Brak powszechnie uznawanych standardów w obszarze inteligentnych umów może być istotnym czynnikiem spowalniającym ich szeroką i szybką adopcję.

5. REGULACYJNE ASPEKTY WYKORZYSTANIA KONCEPCJI BLOCKCHAIN

W tej części artykułu zostaną przeanalizowane aspekty regulacyjne, które pojawiają się w kontekście zastosowania koncepcji rozproszonych baz danych w postaci łańcucha bloków, którą w skrócie będziemy nazywać rozwiązaniem typu blockchain. W pierwszej kolejności należy wyraźnie podkreślić, że blockchain jest stosunkowo nową koncepcją, której wykorzystanie w obszarze prawnym znajduje się dopiero w początkowej fazie, zaś jej poszczególne aplikacje mogą się istotnie różnić. Tym samym, poniższe rozważania nie mają charakteru wyczerpującego, lecz są raczej przyczynkiem do dalszej dyskusji w tej dziedzinie, przede wszystkim sygnalizując znaczenie tego rodzaju rozwiązań w otoczeniu prawnym[35].

Możliwości zastosowania omawianego wzorca w obszarze prawa wydają się być bardzo szerokie. Blockchain jest w pierwszej kolejności testowany na rynku kontraktów finansowych, ale prowadzone są również projekty zmierzające do zastosowania tego rozwiązania w wielu innych dziedzinach prawa[36]. Wydaje się, że potencjalny zasięg oddziaływania tej koncepcji jest

http://www0.cs.ucl.ac.uk/staff/C.Clack/SCT2016.pdf , s. 2.

[34] Tamże, s. 3.

[35] Dynamikę gwałtowności wzrostu znaczenia tej koncepcji dobrze ilustruje liczba nowych zgłoszeń patentowych, które jej dotyczą. W praktyce pojawiają się już opinie, że w związku z tym rozwiązaniem może dojść do nowej „wojny patentowej". Zob. *A rush to patent the blockchain is a sign of the technology's promise*, The Economist, 14.01.2017 r., dostępny na: http://www.economist.com/, odwiedzony 30.01.2017 r.

[36] M. GARSTKA, K. PIECH (red.), *Konsorcja i rady blockchain na świecie*, Materiał analityczny Strumienia

bardzo szeroki. Niniejszy artykuł zasadniczo koncentruje się na zastosowaniu rozwiązania typu blockchain do realizacji zobowiązań umownych.

Rozpatrując techniczne zalety wprowadzenia danego rozwiązania, należy mieć na uwadze, że niejednokrotnie z perspektywy obowiązujących regulacji prawnych, skutki wykorzystania danej technologii mogą być problematyczne. Można w tym miejscu zauważyć, że często prawodawstwo nie jest odpowiednio dostosowane do nowych zjawisk społecznych, ekonomicznych i technicznych. Analizując stronę formalną zastosowania rozwiązania typu blockchain należy wskazać, że w polskim porządku prawnym nie ma przepisów, które go bezpośrednio dotyczą, lub na podstawie których można by było dokonać jego szczególnej kwalifikacji normatywnej. Zatem, należy stwierdzić, że samo wykorzystanie rozwiązania typu blockchain w obrocie gospodarczym jest w pełni legalne, gdyż prawodawstwo nie różnicuje sytuacji prawnej tego rozwiązania[37].

W literaturze naukowej już sporo publikacji opisuje – również od strony prawnej - najpopularniejszą emanację koncepcji blockchain, tj. system bitcoin[38].

Analiza prawno-porównawcza wykazuje, że nawet w tym zakresie zdecydowana większość państw nie reguluje zagadnienia, pozostawiając wypracowanie rozwiązań orzecznictwu i doktrynie. Jednakże tam, gdzie wprowadzono regulacje odnośnie używania kryptowalut, mają one zazwyczaj charakter restrykcyjny (zakazujący)[39]. W Polsce mimo braku szczególnego unormowania sytuacji prawnej bitcoina w prawodawstwie, jego status prawny nie budzi dotychczas większych zastrzeżeń[40], a jego legalność została również potwierdzona w wyroku TS[41]. Jednakże, wypowiedzi doktryny i orzecznictwa dotyczą bitcoina jako kryptowaluty, nie zaś samego zastosowania rozwiązania typu blockchain, leżącej u jej podstaw. Należy zaznaczyć, że artykuł ten nie będzie zasadniczo odnosił się do walut cyfrowych oraz ich prawno-podatkowych aspektów, jak również penalnych elementów ich - niezgodnej z prawem - eksploatacji.

dotyczący trendów w zakresie wspólnych inicjatyw blockchainowych podejmowanych na świecie, 18.01.2017 r., Dostępne na: https://mc.gov.pl/files/porozumienia-v1.pdf

[37] Zgodnie z zasadą *quod lege non prohibitum, licitum est*.

[38] W Polsce pisał na ten temat w szczególność K. Zacharzewski. Zob. K. ZACHARZEWSKI, *Bitcoin jako przedmiot stosunków prawa prywatnego*, Monitor Prawniczy, Nr. 21/2014; K. ZACHARZEWSKI, *Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego*, Monitor Prawniczy, Nr 4/2015.

[39] G. SOBIECKI, *Regulowanie Bitcoina*, Prezentacja przygotowana na III Międzynarodowy Kongres Płatności Bezgotówkowych, 03.2015, dostępne na: http://www.kongresplatnosci.pl/

[40] Przyjmuje się, że bitcoin stanowi na gruncie prawa cywilnego prawa majątkowe. Tak: K. Zacharzewski, *Bitcoin...*, s. 1133.

[41] TS wskazał, że bitcoin jest środkiem płatniczym. Zob. Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 22.10.2015 r. w sprawie *Skatteverket v. David Hedqvist* (C-264/14).

W konsekwencji braku szczególnych unormowań tego rozwiązania nie należy go – przynajmniej na razie, na obecnym etapie jego rozwoju – kwalifikować inaczej niż inne narzędzia informatyczne stosowane w obrocie gospodarczym. W zakresie zobowiązań umownych, formuła ta może umożliwiać m.in. składanie i przyjmowanie oświadczeń woli, dokonywanie czynności prawnych, ale przede wszystkim będzie służyła automatyzacji procesu realizowania zobowiązań. Nie wydaje się, aby przepisy prawa cywilnego, nie były odpowiednio przystosowane do objęcia swoim zakresem również tego rodzaju sytuacji. Zgodnie z jedną z podstawowych zasad prawa cywilnego, strony mogą swobodnie wybrać formę umowy – chyba, że przepis prawa wymaga szczególnej formy[42] - zatem nie powinno być wątpliwości, co do możliwości wykorzystania rozproszonych sieci i systemów do zawierania umów.

Oczywiście do umów, zawieranych przy użyciu rozwiązań typu blockchain, zastosowanie znajdzie cały szereg przepisów prawnych, które regulują transakcje zawierane drogą elektroniczną, np. przepisy prawa konsumenckiego, czy z zakresu ochrony danych osobowych. Nie będą one omawiane w tym miejscu, gdyż podobnie jak przepisy prawa cywilnego nadają się do odpowiedniego zastosowania. Analiza przeprowadzona przez Strumień „Blockchain i kryptowaluty", w ramach programu „Od papierowej do cyfrowej Polski" Ministerstwa Cyfryzacji, wykazała, że obecny status prawny w zakresie rozwiązań typu blockchain jest wystarczający i nie ma powodów do szczególnego dostosowywania regulacji prawnych w tym zakresie[43]. Jednakże, założenia realizowanych projektów wykorzystania koncepcji blockchain niejednokrotnie zakładają konieczność analizy normatywnej i rozważenia wprowadzenia zmian legislacyjnych, które dostosują zastosowanie sieci i systemów rozproszonych do obowiązującego prawodawstwa[44]. W tym kontekście postuluje się wprowadzenie tzw. regulacyjnej piaskownicy (*regulatory sandbox*), czyli rozwiązań prawnych, które ułatwią, zwłaszcza przedsiębiorstwom typu start-up, kontytuowanie prac badawczo-rozwojowych oraz wdrożeniowych bazujących na eksploatacji rozwiązania blockchain. Podkreśla się bowiem, że podmioty te opracowując tego rodzaju rozwiązania, podejmują

[42] Zasada swobody wyboru formy umowy stanowi część szerszej zasady swobody umów, która została opisana w art. 353[1] k.c.

[43] K. ZACHARZEWSKI, K. PIECH (red.), *Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych*, Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych, 19 stycznia 2017 r. Dostępne na: https://mc.gov.pl/files/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf.

[44] M. GARSTKA, K. PIECH (red.), op. cit.

znaczne ryzyko, a zatem powinny liczyć na wsparcie państwa poprzez zapewnienie bezpieczeństwa ekosystemu prawnego[45].

Można oczekiwać stopniowego wprowadzania zmian do prawodawstwa wraz z rozwojem omawianego rozwiązania, choć wiele aspektów ulegnie prawdopodobnie mechanizmowi samo-regulacji na podobnej zasadzie, jak w przypadku Internetu[46]. W pierwszej kolejności, stosując zasadę *de lege ferenda,* tam gdzie prawodawstwo wymaga zgody osoby trzeciej, lub szczególnej weryfikacji (np. kwalifikowany podpis elektroniczny), wymogi te mogą zostać z czasem wyeliminowane przez samą istotę działania sieci i systemów rozporoszonych. Wyeliminowanie pośrednika z procesu transakcyjnego, nie musi powodować ograniczenia pewności i bezpieczeństwa transakcji, bowiem funkcje te w przypadku rozwiązania blockchain zostają zdecentralizowane, gdyż to niezależne podmioty dokonują weryfikacji zawieranej transakcji. Decentralizacja za pomocą sieci *peer-to-peer* umożliwia z kolei pełną globalizację i nie dyskryminuje użytkowników. Co ciekawe, rozwiązanie typu blockchain, które działa na zasadach podobnych do opisanych wcześniej w odniesieniu do systemu bitcoin, zapewnia również anonimowość, ale jednocześnie pełną przejrzystość zawieranych transakcji, poprzez dostęp do publicznego rejestru. Eliminacja strony trzeciej nie powoduje tym samym degradacji stopnia bezpieczeństwa prawnego transakcji, lecz w założeniu ma go zwiększyć.

6. ZASTOSOWANIE KONCEPCJI BLOCKCHAIN A INTELIGENTNE UMOWY

Jak już wyżej wspomniano, koncepcja blockchain ma duży potencjał zastosowań w sferze realizacji zobowiązań umownych. Korzystając z tego rozwiązania można tworzyć tzw. inteligentne umowy, które polegają na tym, że za ich pomocą można definiować i wypełniać warunki umowy w pełni automatycznie i bez interakcji strony trzeciej.

Obecnie, prace nad tworzeniem tego rodzaju inteligentnych umów prowadzą nie tylko największe przedsiębiorstwa, ale również cały szereg instytucji typu start-up. Samą ideę inteligentnej umowy przypisuje się Nickowi Szabo, który w latach 90-tych wprowadził to pojęcie, określając je jako skomputeryzowany protokół realizujący warunki umowy[47].

[45] K. ZACHARZEWSKI, K. PIECH (red.), op. cit.
[46] J. DOGUET, *The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System*, Louisiana Law Review, Nr 73/2012, s. 1143-1147.
[47]D. HE (et. al.), *Virtual Currencies and Beyond: Initial Considerations*, Międzynarodowy Fundusz Walutowy, 01.2016, SDN/16/03 za N. Szabo, *Smart Contracts,* 1994.

Poszukując syntetycznej definicji inteligentnej umowy można określić ją jako „cyfrową reprezentację zasad lub procesów funkcjonujących w danej organizacji biznesowej, które regulują sposób dokonywania i przebieg transakcji" (…) oraz mogą kontrolować „aktywa lub mogą wywoływać zdarzenia, ustalone za pomocą technik programistycznych"[48], lub prościej, jako program komputerowy, który może podejmować decyzje w przypadku spełnienia określonych warunków[49]. Z pewnością jednak istotnie wyróżniającą cechą inteligentnych umów jest to, iż potrafią się „samo-realizować". Użyteczność takich programów przejawiać się może na całym etapie „życia" umowy, od etapu negocjacji do jej zrealizowania. W efekcie zaś strony mogą w łatwy i szybki sposób przeprowadzić cały proces transakcyjny bez udziału stron trzecich – np. notariusza.

Jednym z możliwych systemów, w jakich inteligentne umowy można realizować jest rozwiązanie blockchain w systemie bitcoin, ale wprowadzenie tego rodzaju rozproszonych baz danych jest możliwe również przy korzystaniu z innej formy rozproszonych rejestrów. W literaturze podkreśla się, że system bitcoin-u może być zastosowany do przenoszenia jakiegokolwiek dobra cyfrowego, ale również rzeczy, które są podłączane do sieci/systemu i korzystają z koncepcji blockchain[50].

Jednym z najbardziej rozbudowanych przykładów – choć wciąż w stadium rozwojowym – opracowania mechanizmu inteligentnych umów jest projekt R3CEV, w którego skład wchodzi wiele spośród największych międzynarodowych instytucji finansowych[51]. Podstawowym zadaniem projektu było ustalenie sposobu, w jaki inteligentne umowy, korzystające z rozwiązania blockchain, mogłyby być powiązane z rzeczywistymi umowami. Dlatego obecnie prace w projekcie koncentrują się na opracowaniu szablonów inteligentnych umów[52]. Celem opracowania takich szablonów jest możliwość wykorzystania ich w negocjacjach i zawieraniu umów między kontrahentami, a także umożliwienie automatycznej realizacji zobowiązania, zaś w przypadku sporu, wskazania odniesienia do odpowiedniej dokumentacji prawnej[53]. Warto podkreślić, że dostęp do rejestru w tym przypadku nie ma charakteru publicznego, lecz ekskluzywny, co ma zapewnić odpowiedni stopień poufności[54].

[48] K. PIECH (red.), *Leksykon…*
[49] M. KÕLVART (et al.), *Smart Contracts*, [w:] *The Future of Law and eTechnologies*, T. Kerikmäe, A. Rull (red.), Springer 2016, s. 134.
[50] P. FRANCO, *Understanding Bitcoin: Cryptography, engineering and economics*, Chichester 2014, s. 183-186.
[51] Zob. informacja na http://www.r3cev.com/about/
[52] L. BRAINE, *Smart Contract Templates*, Presentation to CoinDesk, 25 kwietnia 2016 r., dostępne na: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/, odwiedzony: 30.01.2017 r.
[53] C. CLACK (et al.), op. cit., s. 1.
[54] P. RIZZO, *How Barclays Used R3's Tech to Build a Smart Contracts Prototype*, 26 kwietnia 2016 r., dostępna

Opracowanie przygotowane przez Międzynarodowy Fundusz Walutowy wskazuje na następujące korzyści wykorzystania inteligentnych umów: zwiększona szybkość, efektywność i pewność, że umowa zostanie wykonana zgodnie z ustaleniami stron. Ponadto mogą one prowadzić do eliminacji potencjalnych nadużyć, a także obniżyć koszty weryfikacji umowy i jej realizacji[55]. Wydaje się, że obniżenie kosztów może dotyczyć całego procesu jej zawarcia, zaś za dodatkowe zalety należy uznać większą poufność, a zarazem przejrzystość, bezpieczeństwo i kontrolę procesu transakcyjnego. W kontekście korzyści związanych z rozwiązaniem blockchain warto zwrócić uwagę również na to, że właściwie niemożliwe staje się złamanie warunków umowy, gdyż jej realizacja ma miejsce w czasie rzeczywistym, co jednocześnie odciąża system sądowniczy i egzekucyjny[56].

Tego rodzaju rozwiązanie, choć posiada niewątpliwy potencjał, niesie ze sobą również szereg zagrożeń. Jak każda inna koncepcja, również rozwiązanie typu blockchain może zostać wykorzystane do realizacji celów niezgodnych z prawem. Jednakże, takie zagrożenie nie powinno ograniczać rozwoju tego rozwiązania, gdyż jak każde narzędzie może być ono użyte do realizacji zarówno celów legalnych, jak i przestępczych. Jest to nieodzowny element ryzyka związanego z wprowadzaniem w życie nowych rozwiązań technicznych i technologii. W dłuższej perspektywie, wraz ze wprowadzeniem nowych rozwiązań technicznych w przedmiotowym zakresie, zasadnym będzie przeanalizowanie prawnych możliwości przeciwdziałania nadużyciom tego rodzaju rozwiązań do realizacji celów niezgodnych z prawem. Niezależnie, w obecnym stanie prawnym, umowy, które zmierzałyby do obejścia prawa lub byłyby sprzeczne z zasadami współżycia społecznego, byłyby z mocy prawa nieważne[57, 58].

Niektórzy autorzy wskazują, że wdrożenie idei inteligentnej umowy i „przejęcie" w procesie transakcyjnym przez system roli prawnika, który potrafiłby ocenić złożoność licznych elementów umowy (np. różnice pomiędzy systemami prawnymi poszczególnych

na: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/

[55] D. HE (et. al.), op. cit., s. 23.

[56] Może to być również uznane za zagrożenie związane z eksploatacją rozwiązania blockchain. Mianowicie, wskazuje się, że wolność do naruszenia postanowień umowy jest elementem tradycyjnych kontraktów, gdzie wykonanie zobowiązania ma charakter *ex post*. Za niewykonanie grożą określone sankcje – np. odszkodowanie. Zatem cecha niemożliwości złamania umowy może *de facto* prowadzić do ograniczenia wolności i autonomii stron. A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Scholarly Paper ID 2580664. Social Science Research Network, Rochester 2015, s. 26 i 43.

[57] Zob. art. 58 k.c.

[58] Możliwości zastosowania systemu bitcoin do celów niezgodnych z prawem były wykorzystywane praktycznie od początku jego wprowadzenia. T. SIMONITE, *Bitcoin's Dark Side Could Get Darker*, 13 sierpnia 2015 r., MIT Technology Review, dostępne na: https://www.technologyreview.com/s/540151/bitcoins-dark-side-could-get-darker/; odwiedzony 30.01.2017 r.

państw), wymagałoby zaangażowania sztucznej inteligencji[59]. Należy jednak zwrócić uwagę, że obecnie stan techniki w tym zakresie jest na bardzo wczesnym etapie rozwoju. Wbrew swojej nazwie, inteligentne umowy nie potrzebują do wdrożenia sztucznej inteligencji[60]. Kwestia ta jest niezwykle złożonym problemem kognitywnym i z pewnością wykracza poza zakres niniejszego artykułu, jednakże warto w tym kontekście przywołać ponownie szablony inteligentnych umów, tworzone w projekcie R3CEV. Mianowicie, ich pomysłodawcy w ramach prowadzonych prac, analizują kwestię „znaczenia" umowy i jej interpretacji. W tym kontekście, proponują oni założenie, zgodnie z którym umowa posiada dwie interpretacje: „operacyjną semantykę" („*operational semantics*") oraz „oznaczeniową semantykę" („*denotational semantics"*). O ile ta pierwsza zakłada wykładnię umowy, polegającą na określeniu precyzyjnych działań, które mają zrealizować strony, o tyle ta druga stanowi interpretację prawniczą całości umowy, a także dokumentacji, do których się odnosi, tj. znaczenie, jakie postanowienia umowy posiadają dla czytającego ją prawnika. Zdaniem autorów tych założeń, semantyki te nie stanowią różnych elementów umowy, są jednakże ukierunkowane na inne cele. Semantyka operacyjna – w przeciwieństwie do oznaczeniowej (która może być bardzo złożona nawet w przypadku krótkiego tekstu) – może zostać w prosty sposób zaprogramowana do automatycznej realizacji[61]. Interpretacja oznaczeniowa może być potrzebna dopiero na etapie ewentualnego sporu.

W tym miejscu dochodzimy do ciekawego wniosku, związanego z istotą inteligentnych umów. Mianowicie, w ramach inteligentnych umów, algorytm wyrażony w języku programowania stanowi treść norm prawnych, na zasadzie „*code is law*". Implikuje to poważne konsekwencje prawne. Mianowicie, aby inteligentne kontrakty mogły spełniać swoją rolę, algorytmy stojące u podstaw takiej umowy muszą być precyzyjne, gdyż inaczej zrodzi to duże pole do nadużyć i umowy takie nie będą przynosić korzyści, jakich się od nich oczekuje. Poprawność kodu jest kluczowa ze względu na pewność prawną użytkowników programu (stron umowy), co do tego, że tego rodzaju umowy zrealizują intencje stron[62]. Zresztą przełożenie języka oprogramowania na treść umowy wiąże się z dodatkowym problemem, jakim jest brak powszechnej znajomości języków programowania. Przygotowanie inteligentnej

[59] M. KÕLVART (et al.), op. cit., s. 135.
[60] L. LAUSLAHTI (et al.), *Smart Contracts–How will Blockchain Technology Affect Contractual Practices?* The Research Institute of the Finnish Economy, ETLA Reports, Nr 68, 9.01.2017 r., s.3.
[61] C. CLACK (et al.), op. cit., s. 5.
[62] G. PETERS, P. EFSTATHIOS, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, Banking Beyond Banks and Money. Springer, 2016. s. 246-247.

umowy i jego zrozumienie może wymagać rozbudowanej/wszechstronnej wiedzy[63], zaś problem ten w szczególności dotyczyć może konsumentów, którzy będą mieli dodatkową trudność zrozumienia tego, co jest treścią umowy[64].

W tym kontekście pojawia się pytanie o relację inteligentnej umowy do rzeczywistej umowy prawnej zawieranej pomiędzy stronami. Można trafnie pytać o to, czy taki kontrakt to w rzeczywistości umowa, w znaczeniu, jaki nadają jej przepisy prawa. Nie wchodząc w tym miejscu szczegółowo w formalne elementy zawarcia umowy, należy wskazać na to, że do jej zawarcia potrzebna jest zgodna wola stron[65]. Należy się zatem zgodzić, że inteligentna umowa nie musi być wcale umową prawną. Co do zasady istnieje niejako obok rzeczywistej umowy, a żeby doszło do ich „połączenia", strony muszą wykazać chęć związania się umową ze wszystkimi skutkami prawnymi, jakie ona wywołuje[66]. Zatem, na chwilę obecną nie jest możliwa jednoznaczna kwalifikacja prawna inteligentnych umów, gdyż będzie ona uzależniona od praktycznego wdrożenia tego rodzaju idei w danym rozwiązaniu[67]. Możliwe zatem, że tego rodzaju rozwiązania będą służyły tylko jako narzędzie do realizacji zobowiązań, zaś rzeczywista umowa pomiędzy stronami będzie stanowić podstawę dla ustalenia warunków inteligentnej umowy[68]. Innym możliwym rozwiązaniem jest zawarcie umowy w formule inteligentnej, a następnie jej zdalna transformacja do fizycznego dokumentu spisanego językiem naturalnym[69].

7. CZY ROZWIĄZANIE BLOCKCHAIN STANOWI PRZEŁOM NA MIARĘ POWSTANIA INTERNETU?

W literaturze naukowej pojawiają się zdania, że wprowadzenie rozwiązania blockchain może być przełomem na miarę powstania Internetu, który przeobrazi wiele obszarów działalności społecznej, w tym branżę prawniczą. Inteligentne umowy stanowią emanację już drugiej generacji tego rozwiązania, które wykracza daleko ponad zainteresowanie kryptowalutami. Umożliwia zaś zaprogramowanie różnorodnych transakcji, w których można zaimplementować daną logikę biznesową. W tym sensie blockchain drugiej generacji zapewnia cyfrowy i otwarty system transakcji pomiędzy użytkownikami sieci, gdzie bazy danych zostały

[63] T. SIMONITE, op. cit.
[64] D. HE (et. al.), op. cit.
[65] Do zawarcia umowy na gruncie prawa cywilnego wymagany jest konsens, czyli zgodne oświadczenia woli stron. Zob. art. 65 k.c. Sama forma umowy, jaką strony mogłyby zawrzeć za pomocą inteligentnej umowy, będzie raczej zależeć od zastosowanego rozwiązania.
[66] M. KÕLVART (et al.), op.cit., s. 135.
[67] L. LAUSLAHTI [et al.], op. cit., s. 13.
[68] Tamże, s. 21.
[69] Tamże, s. 21-22.

poddane procesowi decentralizacji[70].

Zaproponowane zostało już pojęcie „prawa kryptograficznego" („*lex cryptographia*"), jako nowej dziedziny nauk prawnych, dotyczącej samo-regulujących się umów i zdecentralizowanych autonomicznych organizacji (dalej jako: DAO)[71]. Autorzy tego pojęcia twierdzą, że nadchodzi nowa rewolucja cyfrowa związana z decentralizacją Internetu, zaś dla branży prawniczej jest to przełom na miarę wynalezienia druku[72]. Kluczową rolę w tym procesie mają DAO. Są one autonomiczne poprzez sam fakt umieszczenia w rejestrze i samowystarczalne poprzez fakt, że mogą gromadzić kapitał, a także obciążać użytkowników opłatami za świadczone usługi[73].

Jak podkreślono wcześniej, rozwiązania bazujące na koncepcji blockchain są wciąż niezaawansowane, więc trudno jednoznacznie przesądzić, czy, i w jakim zakresie, będą implikować określone skutki dla systemu prawa. Być może w konsekwencji daleko idących zmian w tym obszarze, konieczne będzie dostosowanie obowiązujących regulacji. Bez wątpienia konkretne aplikacje koncepcji blockchain mogą okazać się problematyczne zwłaszcza przez swoją decentralizację i przez to mogą stwarzać duże problemy prawne. W chwili obecnej wciąż pozostaje więcej pytań niż odpowiedzi w odniesieniu do istoty inteligentnych umów. Nie wiadomo czy natura rozwiązania blockchain ostatecznie spowoduje, że kwalifikacja prawna umów zawieranych przy jej pomocy będzie istotnie różniła się od obecnie dostępnych środków zawierania umów drogą elektroniczną. Wiele jednak wskazuje na to, że to nastąpi, gdyż automatyzacja procesu realizacji zobowiązań, poza wymienionymi powyżej zaletami, może spowodować istotne zmiany w praktyce prawa, a szerzej nawet w relacjach społeczno-ekonomicznych. Podstawowym skutkiem wdrożenia tego rozwiązania będzie eliminacja strony pośredniczącej w zawieranych transakcjach i zastąpienie jej roli przez zdecentralizowany, rozproszony rejestr[74].

---

[70] R. BECK, C. MÜLLER-BLOCH, *Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization*, Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, s. 3-4.

[71] Zdecentralizowana autonomiczna organizacja to „rozbudowany kod programistyczny posiadający cechy inteligentnej umowy, rozszerzający ją o duży zakres samodzielności", który najczęściej jest „wdrażany jako szereg inteligentnych umów powiązanych ze sobą wspólną domeną działań i dzielącymi się swoim interfejsem API". Zaś tym co odróżnia je od zwykłych inteligentnych jest rola DAO, którą „może być autonomiczne zarządzanie aktywami, podejmowanie decyzji i aktywna interakcja z otoczeniem (stronami umów, siecią, światem zewnętrznym etc.) jako strona/osoba". Tak w: K. PIECH (red.), *Leksykon*...

[72] A. WRIGHT, P. DE FILIPPI, op. cit., s.2, 10.

[73] Tamże, s. 17.

[74] Warto jednak zwrócić uwagę na to, że nawet w przypadku inteligentych umów opartych o rozwiązania typu blockchain może pojawić się konieczność zaangażowania zaufanej strony trzeciej. Na chwilę obecną możliwość wykorzystania w pełni automatycznych, tj.samorealizujących się, umów w wielu obszarach jest ograniczona.

Bez wątpienia wiele procesów związanych z automatyzacją prawa jest nieodzownych. W połączeniu z komunikacją pomiędzy użytkownikami sieci, oraz koncepcją Internetu rzeczy, rozwiązanie blockchain może stanowić prawdziwy przełom. Obecnie wiąże się z nim duże nadzieje, ale ostatecznie możliwość jego pełnego wdrożenia będzie zależeć od rzeczywistych aplikacji powstałych przy jego zastosowaniu.

8. WNIOSKI KOŃCOWE

Rozwiązania bazujące na modelu blockchain, opisanym w artykule, stanowią narzędzia, których zastosowanie w obszarze prawnym może rodzić poważne implikacje dla praktyki prawniczej. Jak wskazano, wykorzystanie tego rozwiązania nie podlega obecnie żadnym szczególnym regulacjom i wydaje się, że obowiązujący stan prawny jest w tym zakresie odpowiednio przygotowany. Choć wiele wskazuje na to, że nie istnieje potrzeba wprowadzania dodatkowych unormowań rozwiązań typu blockchain, w rzeczywistości sytuacja ta będzie uzależniona od faktycznego sposobu ich zastosowania.

Można się spodziewać stopniowego rozwoju, a zarazem wzrostu znaczenia inteligentnych umów w obrocie gospodarczym. Jak wskazano, istotną cechą, która wyróżnia inteligentne umowy jest ich funkcja samorealizacji zobowiązań, dzięki wykorzystaniu sieci rozproszonych. Należy jednak podkreślić, że obecne prace nad wprowadzeniem inteligentnych umów są jeszcze niezaawansowane, stąd ich dokładna analiza nie jest jeszcze możliwa. Niewątpliwie jednak można wskazać na potencjalne zalety inteligentnych umów. Są nimi przede wszystkim szybkość realizacji umowy, bezpieczeństwo transakcji, a także obniżenie jej kosztów poprzez ograniczenie roli strony trzeciej. Tego rodzaju rozwiązanie nie jest jednak pozbawione zagrożeń, a jednym z nich jest przekształcenie norm prawnych w algorytmy programistyczne. Relacja języka prawniczego i programistycznego powinna bez wątpienia być przedmiotem dalszych badań. Wciąż nie jest możliwe jednoznaczne określenie, czy inteligentna umowa pokrywa się z umową zawieraną i realizowaną w rzeczywistości. Wdrożenie rozwiązań bazujących na inteligentnych umowach i DAO może stanowić prawdziwą rewolucję w przedmiotowym zakresie.

Należy bowiem założyć, że w pewnych obszarach pojawi się konieczność zasilenia kontraktu danymi z zewnątrz. W związku z tym może się okazać że wartości dla danego parametru będą musiały być dostarczone z zewnątrz poprzez zaufaną stronę trzecią.

UTILIZATION OF BLOCKCHAIN TECHNOLOGY IN CONTRACT PERFORMANCE

This article concerns the issue of blockchain technology use in the area of law, in particular with respect to performance of contractual obligations. The aim of the article is to conduct a study of literature and current solutions on the subject matter in question. First we introduced the concept of blockchain technology which enabled implementation of decentralized data ledgers, smart contracts, decentralized autonomous organizations and elimination of trust institution in large scale, transnational transactions. Introduction of basic concepts underlying blockchain technology is in our opinion necessary to fully appreciate and understand legal consequences of its broad adoption among legal parties in the society and among businesses.

The study found that blockchain technology could be applied in a wide range of fields, including law. This technology has not been subject to any specific regulations, and one may conclude that its application does not require any special regulatory adjustments. Yet, the rapid development of this technology and its specific applications may lead to a need of legislative actions.

One of the more advanced implementations of solutions based on the distributed ledgers are smart contracts, which are a main focus of this article. A distinguishing feature of smart contracts is their ability of self-performance. This feature might have several advantages, including speed, security, and lower transactional costs. At the same time we acknowledge that the smart contract concept is at the very early stage of development and possesses some significant limitations, which we describe in more detail in our article. Moreover for obligations to be executed automatically a collateral must be secured. Collateral siphons off cash thus diminishing liquidity and leverage in the economy.

Implementation of smart contracts may have a substantial impact on the legal practice. However, it is yet too early to make any definite conclusions in this respect, since smart contracts are still not advanced. Depending on specific applications smart contracts may constitute contracts in a legal sense or simply fulfil a role as their facilitator.

KEYWORDS:

blockchain, bitcoin, smart contracts, contractual obligations, automation of law, emerging technologies regulation

BIBLIOGRAFIA

BARAN P., On distributed communication networks, Rand Corporation, 1962

BECK R., MÜLLER-BLOCH C., Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization, Proceedings of the 50th Hawaii International Conference on System Sciences, 2017

BERKLEY J., The promise of the blockchain The trust machine, The Economist, 31.10.2015 r.

BRAINE L., Smart Contract Templates, Presentation to CoinDesk, 25.01.2016 r., http://www.coindesk.com

CANN O., These are the top 10 emerging technologies of 2016, 2016, World Economic Forum

CLACK C. (et al.), Smart Contract Templates: foundations, design landscape and research directions, 2016, researchgate.net

CHRISTENSEN C.M., RAYNOR M. E., MCDONALD R., What is disruptive innovation? Harvard Business Review, 12/1995

DOGUET J., The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System, Louisiana Law Review, Nr 73/2012

FRANCO P., Understanding Bitcoin: Cryptography, engineering and economics, Chichester 2014.

GARSTKA M., PIECH K. (red.), Konsorcja i rady blockchain na świecie, Materiał analityczny Strumienia dotyczący trendów w zakresie wspólnych inicjatyw blockchainowych podejmowanych na świecie, 18.01.2017 r.

GOERTZEL B., GOERTZEL T., GOERTZEL Z., The global brain and the emergance of the world of abundance, Mutualism, open collaboration, exchange networks and the automated commons, Technological forecasting and Social Change, 114/2017

GOGERTY N., ZITOLI J., An electricity-backed currencey proposal, 2011, http://bravenewcoin.com

HABLEN M., Financial sector expands use of blockchain databases, 28.09.2016 r., www.cio.com

HE D. (et. al.), Virtual Currencies and Beyond: Initial Considerations, Międzynarodowy Fundusz Walutowy, 01.2016, SDN/16/03

IRVING G., HOLDEN J., How blockchain-timestamped protocols could improve the trustworthiness of medical science, F1000Research, 31.05.2016 r.

JEMIMA K., Exclusive: Blockchain platform developed by banks to be open-source, Reuters UK, 20.10.2016 r.

KÕLVART M. (et al.), Smart Contracts, [w:] The Future of Law and eTechnologies, T. KERIKMÄE, A. RULL (red.), Springer 2016

LAUSLAHTI L. (et al.), Smart Contracts–How will Blockchain Technology Affect Contractual Practices? The Research Institute of the Finnish Economy, ETLA Reports, Nr 68, 9.01.2017 r.

MARZANTOWICZ K., Największe banki na świecie inwestują w Blockchain, podstawę Bitcoin, 15.12.2015 r., http://itwiz.pl

MASSIMO M., From 'Blockchain Hype' to a Real Business Case for Financial Markets; Banca IMI; Bocconi University; 21.12.2016 r.

NAKAMOTO S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.

NORTA A., Establishing distributed governance infrastructure for enacting cross-organizational collaborations, [w:] NORTA A., GAALOUL W., GANGADHARAN G., DAM H. (red.) Service-Oriented Computing – ICSOC 2015 Workshops, Lecture Notes in Computer Science, Nr 9586, Springer 2016

PETERS G., EFSTATHIOS P., Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, Banking Beyond Banks and Money, Springer 2016

PIECH K., Leksykon pojęć na temat technologii blockchain i kryptowalut, Strumień „Blockchain i Kryptowaluty" programu „Od papierowej do cyfrowej Polski", 08.11.2016 r.

ROSATI P., NAIR B., LYNN T., Bitcoin Vs Blockchain: The Role of trust in disrupting financial services; Proceedings of 7th European Business Research Conference, University of Roma Tre, Rzym, 15-16.12.2016 r.

RIZZO P., How Barclays Used R3's Tech to Build a Smart Contracts Prototype, 26.04.2016 r., http://www.coindesk.com

SIMONITE T., Bitcoin's Dark Side Could Get Darker, MIT Technology Review, 13 sierpnia 2015 r.

SOBIECKI S., Regulowanie Bitcoina, Prezentacja przygotowana na III Międzynarodowy

Kongres Płatności Bezgotówkowych, 03.2015

WEBER I., XU X., RIVERT R., GOVERNATORI G., PONOMAREV A., MENDLING J., Untrusted Business Process Monitoring and Execution Using Blockchain, [w]: LA ROSA M., LOOS P., PASTOR O. (red.) Business Process Management, Lecture Notes in Computer Science, Nr 9850, Springer, 08.09.2016 r.

WHITE G. R.T., HOLDEN J., Future Applications of Blockchain: toward a value-based society, INCITE Conference, Amity University, Indie, 10.2016 r.

WRIGHT A., DE FILIPPI P., Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN Scholarly Paper ID 2580664. Social Science Research Network, Rochester 2015

ZACHARZEWSKI K., Bitcoin jako przedmiot stosunków prawa prywatnego, Monitor Prawniczy, Nr. 21/2014

ZACHARZEWSKI K., Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego, Monitor Prawniczy, Nr 4/2015

ZACHARZEWSKI K., PIECH K. (red.), Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych, Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych, 19.01.2017 r.

ZHENG Z., XIE S., DAI H.N., WANG H., Blockchain Challenges and Opportunities: A Survey, International Journal of Electric and Hybrid Vehicles, 01.2017

ZYSKIND G., NATHAN O. (et al.), Decentralizing privacy: Using blockchain to protect personal data, Security and Privacy Workshops (SPW), 2015