

Blockchain, inteligentne kontrakty i DAO

Partnerzy:



KOALICJA
NA RZECZ
POLSKICH
INNOWACJI



userfeeds

imapp

© Copyright by Wardyński i Wspólnicy, 2016

Redakcja: Justyna Zandberg-Malec

Spis treści

Wstęp	4
Czym są inteligentne kontrakty i DAO	5
Kolejny etap w ewolucji internetu	10
Kilka słów o ładzie blockchaina	12
Czy inteligentny kontrakt może być umową?	16
Jak projektować inteligentne kontrakty i DAO	19
Czym jest DAO z perspektywy prawa?	22
Blockchain jest fundamentem cyfrowej gospodarki opierającej się na współpracy	26
Co historia The DAO mówi o prawie.....	29
Będziemy uzupełniać istniejące struktury	32
Co prawodawca i regulator powinien zrobić z DAO	34
DAO a podatki – wybrane zagadnienia	37
DAO a prawo karne.....	40
Prawne aspekty Initial Coin Offerings oraz Token Crowdsales.....	42
Zaawansowana cyfryzacja, czyli odkrywanie użytecznej kryptografii.....	47
Wnioski.....	51
Autorzy.....	55
Praktyka prawa nowych technologii.....	58
O kancelarii	59

Wstęp

Krzysztof Wojdyło, Jacek Czarnecki

Przygotowując dwa lata temu [raport o wirtualnych walutach](#), mieliśmy wrażenie, że dotykamy tematu, który może zrewolucjonizować gospodarkę oraz prawo. Z perspektywy czasu okazuje się, że był to dopiero początek.

Przyglądając się rosnącemu zainteresowaniu technologią blockchaina, na której opiera się Bitcoin, byliśmy świadkami niezwykłego rozwoju innowacji. Potencjał tej technologii, początkowo dostrzegany przez wąską grupę entuzjastów kryptografii, obecnie jest rozpoznawany przez banki centralne, rządy i największe instytucje finansowe. Już teraz jest jasne, że dalece wykracza on poza świat finansów, a prawdziwa rewolucja zaczyna się dopiero teraz, wraz z pierwszymi praktycznymi implementacjami koncepcji inteligentnych kontraktów oraz rozproszonych autonomicznych organizacji (DAO). Jest to również rewolucja dla prawa, o czym [pisaliśmy już w 2014 r.](#)

Przeprowadzona w maju tego roku akcja finansowania (ICO) jednego z pierwszych DAO, nazwanego The DAO, pod wieloma względami była momentem przełomowym nie tylko dla rozwoju nowych modeli gospodarki, ale również dla istniejących systemów prawa. W drodze ICO udało się zebrać równowartość 150 mln dolarów wyłącznie w oparciu o kontrakt istniejący w postaci algorytmu. Co więcej, te środki trafiły do niezależnej, zdecentralizowanej i autonomicznej organizacji, istniejącej wyłącznie w sieci.

Tradycyjna dokumentacja ICO pisana językiem naturalnym miała jedynie drugorzędne znaczenie. Uprawnienia i obowiązki uczestników ICO zostały zapisane w postaci kodu komputerowego. Wydarzenia, które rozegrały się po przeprowadzeniu ICO (wyprowadzenie

znacznej ilości zebranych środków przez nieznanego hakera), dodają dramaturgii całemu przedsięwzięciu, podkreślając to, z jak pionierskimi i nowatorskimi rozwiązaniami mamy do czynienia.

Jesteśmy przekonani, że upadek The DAO nie oznacza końca inteligentnych kontraktów oraz DAO. Przeciwnie, wiele wskazuje na to, że wydarzenia związane z The DAO zwiększyły zainteresowanie tymi rozwiązaniami. Mają one olbrzymi potencjał, zarówno dla rozwoju gospodarki, jak i dla sektora publicznego.

Pierwsze eksperymenty z DAO oraz inteligentnymi kontraktami pokazują dobitnie, że rozwiązania te funkcjonują w przestrzeni, która jest praktycznie w ogóle nieuregulowana. Już teraz widać, że dla wielu interesujących inicjatyw stanowi to coraz większą przeszkodę. Nasz raport jest próbą usystematyzowania najważniejszych zagadnień prawnych, które powstają w związku z DAO i inteligentnymi kontraktami. Niestety skala wyzwań jest znacząca. Systemy prawne, które jako pierwsze zaczną odpowiadać na te wyzwania, nawet za pomocą prowizorycznych rozwiązań, mają szansę skupić wokół siebie inicjatywy tworzące nowe modele gospodarcze oraz skorzystać z rosnącej fali innowacji, przez niektórych porównywanej z internetem. Przykład Szwajcarii pokazuje, że wbrew pozorom można bardzo skutecznie wesprzeć te inicjatywy stosunkowo niewielkim wysiłkiem.

Chcielibyśmy, aby teksty zawarte w raporcie stały się inspiracją do szerszej dyskusji na temat działań, które należy podjąć, aby ułatwić rozwój technologii opartych na blockchainie. W technologii tej drzemie olbrzymi potencjał,

który nie zostanie jednak wykorzystany bez wsparcia regulacji.



Czym są inteligentne kontrakty i DAO

Jacek Czarnecki

Idea przeniesienia obrotu prawnego w przestrzeń cyfrową sięga początków internetu. Pomysł, aby protokół komputerowy wykonywał warunki umowy, dalece wykraczał jednak poza ówczesne możliwości technologiczne.

Początkowo sieć składała się ze statycznych treści powiązanych ze sobą odnośnikami. Wraz z rozwojem internetu coraz większe znaczenie zaczęło odgrywać generowanie treści przez użytkowników oraz ich wzajemne interakcje, czego dowodem jest sukces serwisów społecznościowych. Sieć stała się miejscem, w którym tworzymy i pozyskujemy informacje oraz komunikujemy się ze sobą.

Wiele wskazuje, że kolejny rozdział w ewolucji internetu został otwarty przez technologię blockchaina, która bywa określana również szerszym pojęciem technologii zdecentralizowanego rejestru. Być może ten nowy etap umożliwi realizację wizji przeniesienia systemu prawnego do przestrzeni cyfrowej.

Czym jest blockchain?

Blockchain jest przede wszystkim strukturą bazy danych, zawierającą historię transakcji. Podobnie jak tradycyjne rejestry to księgi zawierające chronologiczne wpisy, historia transakcji zapisana w łańcuchu bloków odzwierciedla aktualny stan rzeczy – np. stan posiadania jakiegoś dobra.

Blockchain składa się ze znakowanych czasem bloków, które stanowią grupy transakcji i są ze sobą powiązane zabezpieczeniami kryptograficznymi. Każdy blok jest powiązany w ten sposób z blokiem poprzednim i następnym, co sprawia, że taki rejestr przyjmuje formę łańcucha bloków. Modyfikacja któregokolwiek z bloków sprawiłaby, że łańcuch zostanie przerwany.

Sama struktura bazy danych w formie blockchaina jest jedynie oryginalnym sposobem na organizację i uporządkowanie danych – niekoniecznie najbardziej wygodnym i efektywnym. Kluczowym aspektem jest jednak protokół, który zapewni, że poszczególne bazy danych (łańcuchy bloków), choć przechowywane w różnych miejscach i przez różne osoby, będą ze sobą identyczne.

Pierwszym takim protokołem był Bitcoin. Jego kluczowym elementem jest mechanizm osiągania konsensu przez uczestników sieci Bitcoina co do treści utrzymywanych przez nich baz danych – będących zapisem wszystkich historycznych transakcji bitcoinami. Niezwykle interesującym aspektem Bitcoina jest fakt, że w mechanizm osiągania konsensu

wbudowane są bodźce ekonomiczne. Sprawiają one, że każdy uczestnik sieci potwierdzający dokonane transakcje ma wymierny ekonomicznie powód (nagrodę w postaci nowo wygenerowanych bitcoinów), aby potwierdzać jedynie rzeczywiście dokonane transakcje i nie starać się oszukańczo dodawać transakcji, które nie zaistniały (np. podwójnego wydania tych samych środków).

Blockchain w praktyce – Bitcoin

Technologia blockchain powstała wraz z Bitcoinem. W jego przypadku blockchain jest rejestrem wszystkich dotychczas wykonanych transakcji w sieci Bitcoina. Kopie tych rejestrów przechowywane są na całym świecie.

Dzięki innowacyjnemu protokołowi i mechanizmowi osiągania konsensu co do prawidłowej zawartości rejestru kopie wszystkich rejestrów powinny być identyczne.

W rezultacie Bitcoin stanowi globalną sieć, w której rejestr transakcji – łańcuch bloków – przechowywany i tworzony jest przez tysiące węzłów sieci i dzięki wielu podmiotom utrzymującym infrastrukturę potwierdzania transakcji.

W przypadku Bitcoina dzięki mechanizmowi osiągania konsensu możliwe jest współdziałanie nieznających się nawzajem uczestników sieci. Skuteczne osiąganie konsensu sprawia, że te podmioty nie muszą się znać ani martwić brakiem zaufania pomiędzy sobą. Bitcoin pokazał, że możliwe jest wyeliminowanie zaufanej strony trzeciej – pośrednika w transakcjach (w tym przypadku banku centralnego i pośredników w płatnościach).

Kolejne zastosowania blockchaina

Za sprawą Bitcoina powstają plany zastosowania technologii blockchaina w innych obszarach. Jedne z aplikacji polegają na przyjęciu, że jednostkom w danym blockchainie (w przypadku sieci Bitcoina nazywanym bitcoinami)

przypisujemy walor innego niż pieniądź nośnika wartości, np. papieru wartościowego.

Blockchain w praktyce – rejestr diamentów

Technologia blockchain może być używana do tworzenia różnego rodzaju rejestrów. Przykładem, już wdrażanym w praktyce, jest rozproszony rejestr diamentów Everledger. Polega on na przypisaniu każdemu diamentowi unikatowego numeru, powiązanego z jego właściwościami, oraz wprowadzeniu go do rejestru opartego na blockchainie. Każdy zarejestrowany w ten sposób diament ma swój „paszport”, który umożliwia sprawdzenie jego pochodzenia, a także śledzenie historii transakcji. Ułatwia to wykrywanie nielegalnego handlu czy działań przestępczych związanych z obrotem diamentami.

Okazuje się, że olbrzymi potencjał ma możliwość dołączenia do danej transakcji w blockchainie dodatkowych warunków i cech w postaci kodu programistycznego. Wówczas weryfikacja danej transakcji dokonywana w ramach konsensu sieci obejmuje również wykonanie tego kodu.

Co może obejmować taki kod programistyczny wbudowany w daną transakcję? W przypadku Bitcoina te możliwości są ograniczone (choć istnieje wiele projektów, które starają się to zmienić). Jednak kolejne publiczne blockchajny, spośród których szczególnie wyróżnia się Ethereum, niosą znacznie większe możliwości. W ich przypadku kod programistyczny może przewidywać wszystko, co możliwe jest do wyrażenia w języku programowania. Dokonanie transakcji powoduje rozpoczęcie wykonywania tego kodu – niezależne od żadnej strony trzeciej, a także od stron tej transakcji.

Dzięki tej możliwości transakcja może stać się sposobem wykonania określonego programu komputerowego, zapisanego w jej treści. Ten kod może tworzyć określone warunki, np. uzależniać dokonanie transakcji od zaistnienia jakichś dodatkowych okoliczności.

Blockchain w praktyce – głosowanie

Technologia blockchain może zostać zastosowana w projektowaniu systemów głosowania za pośrednictwem środków elektronicznych. Obecnie głosy oddawane w różnego rodzaju głosowaniach są zapisywane, liczone i sprawdzane przez scentralizowane instytucje. Blockchain mógłby sprawić, że dokonany wybór zostanie natychmiast zapisany w odpowiednim rejestrze.

Smart contracts

W warstwie idei inteligentny kontrakt (*smart contract*) to więc prawna, która może samodzielnie funkcjonować w przestrzeni cyfrowej, bez potrzeby odwoływania się do świata realnego.

W praktyce realizacja tej idei powinna zapewniać, że:

- relacja prawna jest **zawierana** za pośrednictwem środków elektronicznych, bez potrzeby korzystania z papierowych dokumentów czy tradycyjnych podpisów, oraz może być w taki sposób **zmieniana**;
- również **wykonanie** tej relacji prawnej czy jej elementów nie musi być związane z jakimkolwiek działaniem w świecie realnym – jest ono automatyczne i podlega wyłącznie regułom ustalonym w danym inteligentnym kontrakcie.

Dodatkowa zaleta inteligentnego kontraktu polega na uniezależnieniu jego zawarcia, zmiany oraz wykonania od woli jakiejkolwiek osoby trzeciej (podmiotu niebędącego stroną inteligentnego kontraktu), w tym sądu. Inteligentne kontrakty to także więcej niż umowy. Mogą one służyć jako dowolne relacje prawne (np. jako elementy organizacji, systemu do głosowania, rejestru publicznego itd.).

Okazuje się, że powyższe kluczowe cechy inteligentnej umowy są realizowane przez wspomniane powyżej transakcje w sieci publicznego

blockchaina w rodzaju Ethereum, zawierające dodatkowy kod komputerowy.

Transakcje są bowiem dokonywane wyłącznie w przestrzeni cyfrowej. Ich uruchomienie wiąże się z wykonaniem załączonego kodu programistycznego, który może dowolnie kształtować zasady dokonania transakcji między stronami. Dzięki wspomnianym powyżej cechom technologii blockchaina i osiągnięciu konsensu w rozproszonej sieci wykonanie następuje niezależnie od woli stron czy jakiegokolwiek strony trzeciej. W ten sposób technologia blockchaina umożliwia nam rzeczywiste wykorzystanie idei inteligentnego kontraktu.

Inteligentny kontrakt w praktyce – rynki finansowe

Dużym zainteresowaniem cieszą się zastosowania inteligentnych kontraktów na rynkach finansowych. Chodzi o stworzenie instytucjom finansowym możliwości zawierania umów finansowych, wykonywanych automatycznie, wyłącznie w świecie cyfrowym.

Wzorce umów stosowane w obrocie przez sektor finansowy są zazwyczaj zstandaryzowane (zmianom podlegają wyłącznie dane stron oraz przedmiotu transakcji). Dzięki temu można je stosunkowo łatwo przełożyć na kod komputerowy.

Inteligentny kontrakt jest oprogramowaniem, które jest wykonywane za sprawą transakcji w danym blockchainie poprzez dokonanie zmian w tym blockchainie. Jest ono zapisane w blockchainie i wykonywane przez rozproszone węzły sieci, co eliminuje konieczność korzystania z zaufanej trzeciej strony. Modyfikacja albo wpłynięcie na działanie inteligentnego kontraktu wymaga zmiany konsensu całej sieci.

Szanse i ograniczenia inteligentnych kontraktów

Porywająca idea inteligentnych kontraktów – przeniesienie prawa do cyberprzestrzeni – napotyka kilka istotnych trudności. Po pierwsze, zasadniczo inteligentne kontrakty funkcjonują w jednym środowisku – danym blockchainie.

Jeżeli do wykonania inteligentnej umowy potrzebne są jakieś informacje ze świata zewnętrznego, niezbędnie jest pobranie i weryfikacja takich danych. Rozwiązaniu tego problemu służą wyrocznie (*Oracles*), o których więcej piszemy w artykule „Jak projektować inteligentne kontrakty i DAO” (na str. 19). Co więcej, podobny problem występuje, jeśli inteligentny kontrakt ma wywrzeć skutki w świecie zewnętrznym (poza blockchainem).

Po drugie, inteligentne kontrakty są deterministyczne. Zazwyczaj nie ma w nich miejsca na elementy podlegające ocenie czy używanie klauzul generalnych (jak „słuszność” lub „dobre obyczaje”). Wykorzystując inteligentny kontrakt, zyskujemy pewność wykonania założonego kodu, ale często tracimy możliwość wprowadzenia zamierzonej niejednoznaczności. Wynika to w dużej mierze z ograniczeń języka, którego możemy użyć w tworzeniu inteligentnego kontraktu. Jest to sztuczny język komputerowy, w przeciwieństwie do ludzkiego żywego języka naturalnego. Być może jednak rozwój „uczących się” komputerów kognitywnych i sztucznej inteligencji pozwoli rozwiązać i ten problem.

Tworzenie inteligentnych kontraktów stało się możliwe dzięki technologii blockchaina, stąd ograniczenia technologiczne stają się również ograniczeniami we wdrażaniu inteligentnych kontraktów. Należy jednak założyć, że kolejne generacje rozproszonych, zdecentralizowanych protokołów będą starały się rozwiązać pojawiające się problemy.

Niezależnie od ograniczeń inteligentne kontrakty już dziś świetnie nadają się do tych sytuacji w realnym obrocie prawnym, w których występują schematyczne relacje prawne. Przykładem są umowy na rynkach finansowych, gdzie często używane są zestandaryzowane wzory. Inteligentne kontrakty umożliwiają cał-

kowitą cyfryzację procesu zawierania i wykonania tych umów, eliminując przy tym pośredników oraz zapewniając pewność wykonania umowy.

Zastosowań inteligentnych kontraktów jest jednak znacznie więcej. Są one często postrzegane jako proste przeniesienie umowy cywilnoprawnej w świat cyfrowy. W rzeczywistości jednak mogą służyć do budowy znacznie bardziej skomplikowanych struktur. Przykładem jest DAO.

Inteligentny kontrakt w praktyce – świat robotów

Inteligentne kontrakty mogą odegrać kluczową rolę w świecie robotów i autonomicznych urządzeń. Możemy sobie wyobrazić firmę, w której towary są produkowane przez roboty oraz dostarczane za pośrednictwem autonomicznych pojazdów (w tym dronów). Technologia blockchain oraz inteligentne kontrakty zapewnią sposób dokonywania transakcji i komunikacji pomiędzy tymi maszynami oraz ludźmi – producentem i konsumentem produkowanych dóbr.

DAO

DAO (*Decentralised Autonomous Organisation*) jest szczególną formą inteligentnego kontraktu. Stoi za nią idea całkowicie autonomicznego podmiotu, istniejącego wyłącznie w przestrzeni cyfrowej.

DAO może pełnić rozmaite funkcje, tradycyjnie wykonywane przez instytucje takie jak spółka, fundacja, stowarzyszenie czy spółdzielnia. DAO mogą być tworzone dla różnych celów. Zapewne najczęściej będą to cele ekonomiczne, a więc DAO rzeczywiście będą w jakimś zakresie odpowiednikami spółek.

DAO w praktyce – The DAO

Pierwszym przykładem DAO była organizacja nazwana The DAO. W założeniu The DAO miał funkcjonować jako zdecentralizowany fundusz venture capital. Uczestnicy mogli wpłacać środki do The DAO, uzyskując odpowiednie tokeny. Te tokeny pozwalały wziąć udział w głosowaniu, na jaką inwestycję przeznaczone zostaną zebrane środki.

DAO jest inteligentnym kontraktem, który przyjmuje formę organizacji przedsięwzięcia grupy osób (przy czym może być otwarty na nowych członków). Na krańcach tej organizacji zawsze będą znajdowali się ludzie (przynajmniej dopóki dostatecznie nie rozwinie się sztuczna inteligencja), choć nie zawsze będą oni łatwi do zidentyfikowania. Za pośrednictwem DAO będą oni dążyli do realizacji wspólnego przedsięwzięcia. Nie ma przy tym konieczności, aby cele uczestników DAO były identyczne. Podobnie jest chociażby w przypadku zwykłej spółki z ograniczoną odpowiedzialnością – cele członków zarządu oraz wspólników mogą być nieraz diametralnie

różne. Konstrukcja tego typu spółki jest jednak tak pomyślana, aby jedni i drudzy mogli realizować swoje interesy przy jednoczesnym wspieraniu wykonania wspólnego przedsięwzięcia.

O ile w przypadku najprostszego inteligentnego kontraktu mamy do czynienia z relacją pomiędzy dwoma podmiotami, o tyle w przypadku DAO relacje mogą być znacznie bardziej skomplikowane. W DAO występują różnego rodzaju podmioty, które mają różne związki z danym DAO oraz przyświecają im różne cele. DAO może być również otwarte na udział kolejnych podmiotów. Schematycznie przedstawia to poniższa grafika.



DAO może służyć jako wehikuł współpracy (wspólnego przedsięwzięcia) pomiędzy podmiotami niemającymi ze sobą rzeczywistego kontaktu. „Pewność kodu” sprawia, że te podmioty nie muszą przeciwdziałać brakowi zaufania pomiędzy sobą nawzajem (np. poprzez skorzystanie z zaufanej trzeciej strony).

Z DAO wiążą się te same ograniczenia co z inteligentnymi kontraktami. Przykład The DAO (o którym piszemy na str. 29) wyraźnie pokazał, że próby całkowitego wyabstrahowania się od świata zewnętrznego – w tym panujących w nim reguł prawnych – mogą zakończyć się katastrofą.

Inteligentne kontrakty i DAO znajdują się jednak w bardzo wczesnej fazie rozwoju. Stanowią fascynujący przykład próby objęcia przestrzenią cyfrową kolejnych obszarów naszego życia, w tym prawa. Powinniśmy przyglądać się rozwojowi tej tematyki, ponieważ być może na naszych oczach kształtują się innowacje, które zmienią świat wokół nas. Przygoda z inteligentnymi kontraktami i DAO zaczęła się od technologii blockchaina, jednak z pewnością wkrótce doświadczymy kolejnych innowacji.



Kolejny etap w ewolucji internetu

Rozmowa z Maciejem Ołpińskim, założycielem projektu Userfeeds.io, platformy dla aplikacji mediowych opartych o otwarte protokoły blockchainowe, a także animatorem społeczności Ethereum w Polsce.

J.Cz.: Czym jest DAO?

M.O.: DAO to pojęcie, które narodziło się w środowisku entuzjastów technologii blockchain i oznacza nową formę organizacji, która jest w stanie organizować działalność ekonomiczną za pomocą kodu komputerowego.

W bardzo szerokim rozumieniu za jedną z form DAO możemy uznać np. Bitcoina. Twórcy Bitcoina jako pierwsi udowodnili, że można w kodzie komputerowym zawrzeć bodźce ekonomiczne, które spowodują, że w realnym świecie ludzie zaczną kontrybuować zasoby do sieci Bitcoina. Protokół Bitcoina, który nie ma osobowości prawnej i istnieje

jedynie w sferze wirtualnej, jest w stanie w bardzo realny sposób motywować ludzi, aby dostarczali mu realną wartość ekonomiczną.

Bodźce ekonomiczne zapisane w kodzie Bitcoina powodują, że „zdecentralizowana organizacja”, jaką jest Bitcoin, jest w stanie tworzyć wartość dodaną, dostarczać rynkowi produkt, jakim jest kryptowaluta o właściwościach ekonomicznych złota, a jednocześnie wynagradzać tych, którzy przyczynili się do jej sukcesu.

Czyli robi to, co jest celem każdej „klasycznej” organizacji. Jednak zamiast zatrudniać pracowników i wynajmować biura, Bitcoin jest w sta-

nie pozyskać te zasoby poprzez bodźce zapisane w kodzie komputerowym. Brzmi to niewiarygodnie, jednak mechanizm ten działa w praktyce.

I działa on nie tylko dla Bitcoina, ale także dla szeregu innych protokołów, które próbują zastosować tę samą mechanikę do szeregu innych form organizacji.

Czy DAO są właśnie takimi protokołami?

DAO jest zbiorczym określeniem na różnego rodzaju „sieci ekonomiczne”, które działają analogicznie do Bitcoina, jednak ich celem niekoniecznie jest stworzenie nowej kryptowaluty. Mogą to być platformy inwestycyjne, rynki predykcyjne, wirtualne światy, sieci społecznościowe itd.

Część z tych eksperymentów kończy się fiaskiem (tak jak np. The DAO), natomiast moim zdaniem nie podważa to sensowności całej idei.

Osobiście uważam, że infrastruktura internetu będzie stopniowo zastępowana przez otwarte protokoły podobne do Bitcoina i wiele usług, które dziś dostarczane są przez amerykańskie korporacje, będzie dostarczana przez rozmaite DAO.

W jednym ze swoich tekstów porównałeś DAO do pierwszych spółek akcyjnych w renesansowej Europie. Co jedne i drugie mają ze sobą wspólnego?

Jedne i drugie są formą koordynowania zasobów (takich jak np. wiedza, kapitał, praca) na dużą skalę i sposobem na dzielenie zysków płynących z efektywnej alokacji tych zasobów. Spółka akcyjna jest pewną abstrakcją, która pozwala dużym grupom ludzi koordynować swoją aktywność gospodarczą i budować wartość, która nie mogłaby być wytworzona w mniejszej skali.

To oczywiście pewna metafora, ale moim zdaniem DAO będą dla ery informacyjnej tym, czym globalne spółki akcyjne czy korporacje były dla ery przemysłowej.

Natomiast każda z tych form organizacji opiera się na innej infrastrukturze. Dla obecnych form działalności gospodarczej jest to literatura prawa i władza sądownicza. Dla DAO jest to kod komputerowy oraz technologia blockchain.

Jak Ethereum pozwala tworzyć, używać i zarządzać DAO?

Ethereum jest platformą dla aplikacji opartą o blockchain, która pozwala każdemu za pomocą kodu komputerowego zapisać dowolne relacje ekonomiczne i dystrybuować je poprzez sieć. W praktyce Ethereum pozwala eksperymentować z różnymi formami DAO bez uruchamiania własnego blockchajna. Wszystko dzieje się na istniejącym blockchainie Ethereum. Obniża to barierę wejścia i powoduje, że technologia dostępna jest dla szerszej liczby deweloperów.

Na chwilę obecną jest to dziedzina bardzo niszowa i dla większości na tym etapie niezrozumiała. Tworzenie DAO wymaga wiedzy na połączeniu technologii, ekonomii i teorii gier. Potencjalne dziury w kodzie mogą skutkować realnymi stratami finansowymi.

Nikt tak naprawdę nie wie, jakie modele ekonomiczne zadziałają w przyszłości. To trochę tak jak internet w pierwszej fazie swojego rozwoju. Skomplikowany w użyciu, niezrozumiały dla większości, jednak z ogromnym potencjałem na przyszłość.

Na chwilę obecną większość interakcji z DAO odbywa się przez specjalne aplikacje klienckie do sieci Ethereum. Wkrótce jednak będziemy mogli łączyć się z DAO z poziomu przeglądarki. Jednak jak zabezpieczyć przeciętnego Kowalskiego w interakcjach z DAO, to wciąż

temat, który jest otwarty i będzie wymagał sporo pracy.

Czy Ethereum, DAO i inteligentne kontrakty to coś więcej niż nowinki technologiczne?

Technologie, które w dłuższej perspektywie zmieniają świat, początkowo wyglądają jak nowinki, gadżety albo nawet zabawki dla wąskiej grupy. W tym przypadku będzie podobnie.

Moim zdaniem to kolejny etap w ewolucji internetu. Pierwszą fazą były sieci WWW, czyli dokumenty i statyczne strony. Następnie przeszliśmy w sieci społecznościowe, które dziś dla wielu są standardem komunikacji online.

DAO, Ethereum i blockchain to początek globalnych sieci ekonomicznych.

Mają one zupełnie inną naturę niż poprzednie rodzaje sieci. Ich siła oddziaływania będzie większa, bo opierają się na przesyłaniu realnej wartości ekonomicznej, a nie tylko informacji. Dziś trudno powiedzieć, jakie modele DAO się sprawdzają, ale na pewno warto obserwować ten fenomen.

Rozmawiał Jacek Czarnecki



Kilka słów o łańczie blockchaina

Maciej Jędrzejczyk, Karolina Marzantowicz

W szkole nie raz słyszeliśmy, że matematyka jest królową nauk. Rozwój technologii rozproszonego rejestru i konsensu (*Distributed ledger technologies*, DLT) pokazuje, jak bardzo to stwierdzenie jest prawdziwe. Jedną z głównych zalet tej technologii jest zdecentralizowane zaufanie wpisane w kod źródłowy programu informatycznego. Dzięki temu, w dobie cyfrowej gospodarki, możemy przejść od stanu, w którym zaufaną trzecią stroną były (są) osoby, instytucje czy organizacje centralne, do stanu, w którym ich role przejmują algorytmy zdecentralizowanego konsensu, czyli matematyka.

Jedną z form DLT jest blockchain. Technologia blockchain kieruje rozwój systemów informatycznych oraz cyfrowej komunikacji w stronę decentralizacji na dużą skalę. Czynniki ludzkie jest zminimalizowany, a zaufanie oraz poprawność transakcji są zapewniane przez kryptografię.

Doniosłość tej technologii powoduje, że należy się jej przyjrzeć pod kątem ładu (*governance*), na bazie którego powstaną nowe modele biznesowe i gałęzie gospodarki. Dzięki temu będziemy mogli zidentyfikować podsta-

wowe cechy i ryzyka właściwe dla rozwiązań opartych na blockchainie publicznym i prywatnym.

Blockchain publiczny, czyli powolna oligarchizacja

Charakterystyczną cechą blockchaina publicznego jest brak komponentów służących zarządzaniu tym rozwiązaniem. Ma to wpływ na funkcjonowanie i utrzymywanie całego systemu. Decentralizacja i rozproszona architektura zapobiegają koncentracji władzy, którą mogłaby zgromadzić jedna osoba, rola lub or-

ganizacja. Zwiększa się też niezawodność systemu ze względu na brak komponentów krytycznych (brak pojedynczego punktu awarii).

Niestety takie rozwiązanie nie wyklucza grupowania i gromadzenia zasobów sieci (ilości uczestników) w ramach głównych ról, z którymi mamy do czynienia w ramach wdrożonego procesu obsługiwanego przez funkcjonującą sieć. Chodzi zwłaszcza o tzw. górników (*miners*), którzy rozwiązują coraz trudniejsze zadania matematyczne, aby wziąć udział w procesie zatwierdzania transakcji i zapisywania bloku w rejestrze. Ten, kto rozwiąże zadanie jako pierwszy, jest wynagradzany poprzez zasilenie jego portfela odpowiednią wartością bitcoinów.

Algorytm Proof of Work zakłada, że w ramach sieci nie nastąpi kumulacja zasobów powyżej 51%. Ponieważ jednak stopień trudności zadań rośnie, górnicy grupują się w tzw. *mining pools* (grupy górników lub kopalnie), w których każdy rozwiązuje jedynie część zadania, a wynagrodzenie jest dzielone między wszystkich. Obecnie cztery największe kopalnie gromadzą ponad 65% wszystkich górników, którzy zajmują się rozwiązywaniem zadań w sieci Bitcoin. Jeżeli jeden podmiot przejął kontrolę nad większością zasobów weryfikujących transakcje, będzie mógł korzystać z tych zasobów i dyktować warunki pozostałej części sieci.

Coraz liczniejsze kopalnie są poważnym zagrożeniem dla decentralizacji i fundamentalnych zasad blockchained publicznego. Grupa (organizacja) posiadająca większość zasobów wykonujących wyliczenia zadań w ramach Proof of Work może manipulować zawartością zatwierdzanych bloków (wstawiać fałszywe transakcje, odrzucać rzeczywiste). I nie jest to tylko hipoteza, o czym świadczy niedawny udany atak na sieć Krypton, gdzie atakujący za pomocą wynajętej w chmurze mocy

obliczeniowej wpłynął na integralność blockchained oraz stan własności kryptowaluty KR.

Ponadto publiczne sieci nie mogą wybierać, kto decyduje o konsensie, a także ujawniać i kontrolować tożsamości węzłów. Dla wielu organizacji biznesowych, podlegających restrykcyjnym regulacjom, oznacza to wykluczenie publicznego blockchained z ich kręgu zainteresowania.

Anonimowość a prywatność – fundamentalna różnica między łańcem blockchained publicznego i prywatnego

Blockchained publiczny daje uczestnikom sieci anonimowość zabezpieczoną kryptograficznie. Nieodwracalny rejestr może być repozytorium dokumentów, umów, aktów własności i innych aktywów. Blockchained można wykorzystać do umieszczenia informacji i wskazówek o szerokim zakresie zastosowań. Potencjalne zastosowania tej technologii wykraczają daleko poza kryptowaluty, takie jak Bitcoin. Obszary zastosowania paradygmatu DLT są potencjalnie niezliczone, ponieważ umożliwia on decentralizację zatwierdzania i przechowywania wszelkiego typu transakcji pomiędzy wszystkimi stronami na skalę światową.

Jednak w wielu branżach gospodarki, gdzie zastosowanie może mieć technologia blockchained, uczestnicy nie mogą pozostać anonimowi.

Prowadząc biznes lub świadcząc usługi publiczne, najczęściej wiemy (i chcemy wiedzieć), kto jest naszym dostawcą i odbiorcą. Anonimowość nie jest cechą wymaganą ani tym bardziej konieczną. W ramach rozwiązania współdzielonego i rozproszonego pomiędzy wszystkich uczestników sieci potrzebne jest więc odpowiednie zarządzanie prywatnością. Blockchained prywatny (*permissioned blockchained*) daje możliwość rozszerzenia technologii rozpro-

szanego rejestru o komponenty takie jak zarządzanie uczestnikami oraz prywatność. Blockchain prywatny jest najczęściej tworzony przez konsorcja lub określoną grupę uczestników. Ustalają oni, kto i na jakich zasadach będzie funkcjonował w sieci. Dodatkowo sieć, w której uczestnicy nie są anonimowi, może wykorzystywać inne niż Proof of Work algorytmy rozproszonego zatwierdzania transakcji, jak np. Practical Byzantine Fault Tolerance.

Przykładem może być otwarty projekt Hyperledger, realizowany przez Linux Foundation. W ramach proponowanej architektury Hyperledger Fabric funkcjonują komponenty odpowiedzialne za zarządzanie uczestnikami i ich prywatnością, a także wydawanie certyfikatów wykorzystywanych do podpisywania transakcji oraz inteligentnych kontraktów w taki sposób, aby szczególnie widoczne były jedynie dla uczestników danej transakcji. Oddzielono też funkcje węzła potwierdzającego od węzła pasywnego, co pozwala na większą kontrolę aktorów biorących udział w konsensie oraz posiadających pełną kopię rejestru opartego na łańcuchu bloków. Usługi typu *membership services*, wskutek uznawania transakcji dopiero po autoryzacji na wielu poziomach (podpisane certyfikaty, autentykacja tożsamości), w zasadzie pozwalają na kontrolowany dostęp do sieci, a co za tym idzie na deanonimizację węzłów. Jednocześnie ta sama usługa pozwala zagwarantować prywatność transakcji poprzez dystrybucję certyfikatów transakcyjnych, które szyfrują poufną transakcję między dwiema konkretnymi stronami, przez co staje się ona nieczytelna dla innych. Warto zaznaczyć, że wszystkie te cechy zintegrowane są z tradycyjnymi korzyściami rozproszonego, współdzielonego rejestru oraz algorytmów konsensu.

Logika biznesowa wpisana w blockchain, czyli inteligentne kontrakty

Jedną z nowości, która została spopularyzowana wraz z projektem Ethereum, jest pojęcie inteligentnego kontraktu (*smart contract*), czyli skompilowanego kodu programistycznego, którego kopia wpisana jest w rejestr blockchain i którego treść reprezentuje zasady dokonania transakcji pomiędzy stronami. Raz rozpropagowany w ramach zdecentralizowanej sieci, inteligentny kontrakt jest uruchomiony na wszystkich węzłach jako program wykonywalny i uruchamia konkretną funkcję przewidzianą przez autora.

Można zatem stwierdzić, że inteligentny kontrakt jest cyfrową reprezentacją zasad lub procesów funkcjonujących w danej organizacji biznesowej, które regulują sposób dokonywania i przebieg transakcji. Technologia blockchain służy tu jako bezsprzeczny rejestr umów regulowanych przy pomocy inteligentnych kontraktów. W tym kontekście wspomina się o możliwości natychmiastowego (i praktycznie bezkosztowego) wykonywania transakcji między stronami pragnącymi zachować anonimowość, rozwiązywania sporów bez angażowania zaufanej trzeciej strony na bazie transparentnej treści blockchaina, a nawet automatyzacji zawierania umów bez udziału czynnika ludzkiego.

Nowa technologia, nowe problemy, nowe rozwiązania

Bezsprzeczność umów nie oznacza niestety eliminacji możliwych problemów prawnych. Jak w przypadku każdego innego podmiotu działającego w życiu gospodarczym, fundamentalnym aspektem analizy porównawczej publicznego i prywatnego blockchaina w tym kontekście jest:

- jasna identyfikacja podmiotu odpowiedzialnego za wadliwie sporządzony kontrakt oraz
- identyfikacja procesu pozwalającego na jego szybką remediację.

Warto również wspomnieć o innych problemach wynikających ze zdolności organizacji biznesowych do podporządkowania się istniejącym regulacjom prawnym, które często wymagają pewnych konkretnych zachowań wpisanych w proces biznesowy, jak deanonimizacja stron umowy, prywatność transakcji lub regulowany dostęp do danych.

Inteligentne kontrakty w blockchainie publicznym i prywatnym

W przypadku sieci opartych na publicznym łańcuchu bloków zasadność transakcji między stronami określa tylko i wyłącznie konsens sieci. Wpływ organizacji zrzeszających społeczność danej sieci jest znikomy, a bez uzyskania kwalifikowanej większości mocy sieci (np. 51% hashrate w przypadku sieci opartych na konsensie Proof-of-Work) nie ma praktycznej możliwości uznania pewnych transakcji lub umów wykonanych przez inteligentne kontrakty za wadliwe lub niebyłe. Problem ten znalazł się w centrum incydentu The DAO na przełomie czerwca i lipca 2016 r. Odkrycie inteligentnego kontraktu podatnego na atak hakerski (i wykorzystanie go przez nieznanego sprawcę do wyplukania ponad 60 mln USD w kryptowalucie) spowodowało kilkutygodniową batalię o zgodę co do tego, jak (jeśli w ogóle) należy zaaplikować remediację. Problemem samym w sobie było osiągnięcie zgody całej społeczności, co ukazało niemożliwą do pogodzenia sprzeczność interesów. Brak przewidzianego procesu na wypadek wadliwie spisane go inteligentnego kontraktu powodował, że podjęto decyzję o bezpośredniej

interwencji w adresy zarejestrowane w blockchainie Ethereum, używane do przetrzymywania ukradzionych środków. Z jednej strony pozwoliło to na zwrócenie środków ich właścicielom oraz zablokowanie ich przed przejęciem przez hakera. Z drugiej strony była to zdecydowana modyfikacja zasad gry w trakcie jej trwania i jako taka napotkała opór sporej części społeczności wierzącej w ideę nienaruszalności blockchaina (więcej na ten temat w artykule „Co historia The DAO mówi o prawie” na str. 29).

W sukurs przychodzą rozwiązania pozwalające wdrożyć technologię blockchain w zamkniętym, prywatnym środowisku. Większy poziom zaufania *a priori* pomiędzy stronami pozwala na uproszczenie mechanizmu konsensu, jasne zdefiniowanie ról oraz przypisanie odpowiedzialności do konkretnych jednostek. Pojawienie się wyspecjalizowanych audytorów i administratorów tożsamością ze specjalnymi uprawnieniami pozwala na sprawniejszą kontrolę nad transakcjami w ramach sieci opartej na technologii blockchain. W przypadku wadliwie działających transakcji opartych na inteligentnych kontraktach i przy małej skali prywatnej sieci (zwykle ok. 10-20 węzłów) istnieje możliwość natychmiastowej interwencji, a przy prostszym konsensie zmiana akceptowana jest dużo szybciej przez całą sieć.

Prawo zaszyte w kodzie, czyli przyszłość zawodów prawniczych w świecie blockchaina i inteligentnych kontraktów

Neutralność zasad rozproszonego konsensu i weryfikowalność transakcji może znacząco wpłynąć na przededefiniowanie obecnych procesów decyzyjnych zarówno w organizacjach centralnych, jak i w ramach implementacji rozwiązań obejmujących wszystkich uczestników danego rynku. Wiele nowych modeli biznesowych może bazować na zdecentralizowanych

rejestrach, rozproszonym konsensie oraz zdecentralizowanym zarządzaniu. W zależności od potrzeb i wymagań mogą to być sieci dla anonimowych uczestników, gdzie szczegóły transakcji są publicznie dostępne dla wszystkich, lub prywatne sieci otwarte dla określonej grupy uczestników, pozwalające na zarządzanie prywatnością. W obu przypadkach to matematyka i kryptografia umożliwiają zaszywanie w kodzie programistycznym zasad, według których sieć będzie realizować transakcje i je zatwierdzać.

Nie oznacza to, że zawód adwokata czy notariusza jest skazany na wymarcie. Wręcz przeciwnie, digitalizacja aktywów, transakcji, umów i logiki biznesowej między stronami w ramach blockchajna i inteligentnych kon-

traktów otwiera nowe możliwości i perspektywy. Z jednej strony najbardziej podstawowe, powtarzalne czynności prawne z łatwością da się zaprogramować i zautomatyzować. To pozwoli prawnikom skoncentrować się na bardziej złożonych i pracochłonnych sprawach. Z drugiej strony, orientacja w obowiązującym prawie będzie kluczem do nowych gałęzi działalności, takich jak formułowanie inteligentnych kontraktów opisujących umowę lub nową działalność gospodarczą czy sporządzanie opinii prawnych dla przedsiębiorców planujących oprzeć swoją działalność na blockchainie. Stąd kluczową umiejętnością prawników w przyszłości może się okazać znajomość programowania i algorytmiki.



Czy inteligentny kontrakt może być umową?

Rafał Kuchta

Określenie „inteligentny kontrakt” nawiązuje do pojęcia umowy. W najogólniejszym, potocznym ujęciu „umowa” oznacza porozumienie między co najmniej dwiema osobami, w którym określiły one swoje wzajemne prawa i obowiązki. Na pierwszy rzut oka inteligentny kontrakt zdaje się nie mieć cech tak rozumianej umowy. Jednocześnie inteligentny kontrakt stoi w pewnej opozycji do tradycyjnej umowy, od której ma być „mądrzejszy” dzięki wyeliminowaniu człowieka. W istocie jest to bowiem rodzaj programu komputerowego, zestaw instrukcji wyrażony w określonym języku programowania, takim jak np. Solidity, wykonywany przez komputery w sieci blockchajna, np. Ethereum. Czy inteligentny kontrakt jest więc czy nie jest kontraktem prawnym?

Jak prawo definiuje umowę?

Próbując udzielić odpowiedzi na to pytanie, należy odwołać się do prawnej definicji umowy. W przepisach polskiego prawa cywilnego nie sformułowano takiej definicji, ale sądy i prawnicy przyjmują w praktyce, że zawarcie umowy polega na złożeniu zgodnych

oświadczeń woli przez strony (osiągnięcie tzw. konsensu). Wskazuje się również, że umowa obejmuje zgodny zamiar stron doprowadzenia do wywołania powstania, zmiany lub ustania skutków prawnych, czyli ukształtowania praw i obowiązków jej stron w określony sposób.

Należy zatem przeanalizować, czy zainicjowanie i wykonanie inteligentnego kontraktu dotyczącego co najmniej dwóch użytkowników da się zakwalifikować jako złożenie przez nich zgodnych oświadczeń woli. Analizę rozpocząć wypada od przywołania art. 60 k.c. regulującego zasady składania oświadczeń woli. Ustanawia on jedną z podstawowych reguł prawa cywilnego – zasadę swobody formy oświadczeń woli. Zgodnie z tym przepisem z zastrzeżeniem wyjątków w ustawie przewidzianych (np. przepisów uzależniających ważność umowy zbycia nieruchomości od zawarcia jej w formie aktu notarialnego) wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli).

Niesamodzielnosc inteligentnych kontraktów

Z przytoczonego przepisu wynika przede wszystkim, że oświadczenie woli musi pochodzić od człowieka. Dotyczy to także osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej. W ich przypadku przepisy ustanawiają warunki, których spełnienie pozwala przypisać im oświadczenia woli składane przez działające w ich imieniu osoby fizyczne (np. członków organów czy pełnomocników).

Inteligentne kontrakty zaś z założenia mają „wykonywać się same”, bez udziału człowieka – ich funkcjonowanie ma być rezultatem przetworzenia instrukcji i wykonania zadanych operacji przez komputery. Mimo to na obecnym etapie ich rozwoju w wielu przypadkach inteligentne kontrakty nie poradzą sobie bez udziału człowieka. Jeśli w przyszłości uległoby to zmianie, to znajdziemy się w sferze zupełnie innych rozważań – jak kwalifikować prawnie

działania podejmowane przez sztuczną inteligencję.

W kontekście „samowykonywalności” inteligentnych kontraktów warto również pamiętać, że prawo dopuszcza zawarcie umowy poprzez przystąpienie do jej wykonania w odpowiedzi na złożoną ofertę (por. art. 69 k.c.). Niezależnie od tego warto zwrócić uwagę, że już obecnie prawo zna konstrukcję umów niejako „samowykonujących się”. Chodzi o tzw. umowy o podwójnym skutku: zobowiązująco-rozporządzające.

Jeśli np. zawieramy umowę, w której zobowiązujemy się do sprzedaży samochodu, to co do zasady z mocy prawa umowa ta przenosi zarazem prawo własności samochodu na kupującego. Dzięki temu nie trzeba już zawierać kolejnej umowy czy dokonywać innych czynności dodatkowych.

Rzecz jasna kwestią odrębną jest możliwość faktycznego korzystania z tego samochodu przez nabywcę, uzależniona od jego wydania przez sprzedającego. Jeśli sprzedawca nie chce oddać nam kluczyków, to wydania nabytej rzeczy musimy dochodzić na drodze sądowej. Inteligentne kontrakty będą starały się zmierzać do rozwiązania tego problemu. Dla przykładu twórcy Slock.it planują wprowadzenie elektronicznych „klódek” w przedmiotach podłączonych do Internet of Things, które byłyby powiązane z inteligentnymi kontraktami na blockchainie.

Charakter oświadczenia woli w inteligentnych kontraktach

Człowiek może być zaangażowany w funkcjonowanie inteligentnych kontraktów poprzez działanie dwójakiego rodzaju (biorąc pod uwagę to, co dzieje się już po opracowaniu kodu). Po pierwsze działanie człowieka może mieć miejsce przed wykonaniem inteligent-

nego kontraktu i polegać na jego zainicjowaniu, np. poprzez podanie wymaganych danych wejściowych czy wydanie dyspozycji wpłaty środków na adres kontraktu. Człowiek działa wtedy jako swoisty „pierwszy poruszyiciel”.

Po drugie człowiek może wpływać na inteligentny kontrakt, którego wykonywanie już się rozpoczęło, ale zostało zgodnie z instrukcją wstrzymane w oczekiwaniu na bodziec z zewnątrz. Dalsze działanie programu może być uzależnione np. od pozyskania informacji od tzw. wyroczni czy podjęcia przez człowieka decyzji o wyborze określonej opcji działania. Tak działał np. mechanizm podejmowania decyzji w opartym na inteligentnych kontraktach The DAO, polegający na głosowaniu jego członków. Skutkiem takiej decyzji może nawet być rozpoczęcie wykonywania kolejnego inteligentnego kontraktu.

Działania omówione wyżej mogą niekiedy być podejmowane tylko przez jedną ze stron, podczas gdy druga zdaje się zachowywać bierność. Do zawarcia umowy niezbędne są zaś zgodne oświadczenia co najmniej dwóch stron. Jednak w wielu sytuacjach również pozornie bierne zachowanie drugiej strony – polegające na umieszczeniu na blockchainie czy zaakceptowaniu w inny sposób inteligentnego kontraktu o określonych regułach działania – można zakwalifikować jako oświadczenie woli.

W zależności od konkretnych okoliczności może ono mieć charakter np. oferty skierowanej do nieokreślonego kręgu osób (*ad incertas personas*) czy też przyjęcia oferty drugiej strony przez przystąpienie do wykonania umowy. Wskazane jest, aby towarzyszyła temu jednoznaczna wzmianka o tym, że zainicjowanie inteligentnego kontraktu będzie poczytywane za zawarcie umowy.

Podsumowując, działanie niektórych inteligentnych kontraktów może być poprzedzone złożeniem zgodnych oświadczeń woli przez co najmniej dwie osoby, a co za tym idzie zawarcie między nimi umowy. Nie można jednak każdego inteligentnego kontraktu utożsamiać z umową w rozumieniu prawa cywilnego. Trudno byłoby tak zakwalifikować np. inteligentne kontrakty zawierane w ramach komunikacji pomiędzy oprogramowaniem, serwerami czy urządzeniami w ramach internetu rzeczy ze względu na brak uczestnictwa człowieka (chyba że uda się takie działania przypisać człowiekowi jako zaakceptowane przez niego). Podobnie gdyby organy administracji postanowiły wykorzystać technologię blockchaina do realizacji swoich zadań nadzorczych, to wykorzystywane do tego celu inteligentne kontrakty nie będą umowami. Takie działania państwa nie będą bowiem działaniami w obrocie cywilnoprawnym podlegającymi przepisom prawa cywilnego, lecz będą dotyczyć sprawowania władzy publicznej (należą do tzw. sfery *imperium*).

O języku inteligentnego kontraktu

Pewne trudności może sprawiać odczytanie treści umowy cywilnoprawnej zawartej przy użyciu inteligentnego kontraktu, zwłaszcza jeśli wyrażono ją wyłącznie w języku programowania. Nie chodzi przy tym o to, że treść oświadczeń nie jest wyrażona w języku naturalnym, bowiem zgodnie z zasadą swobody formy nie jest to wymagane.

Wydaje się natomiast, że nie można zrównywać kodu źródłowego z treścią umowy, a co za tym idzie uznawać go za bezpośredni zapis praw i obowiązków jej stron. Należy raczej przyjąć, że analiza kodu źródłowego stanowi pewną metodę rekonstrukcji tych praw i obowiązków (sposób interpretacji oświadczeń woli). Sam kod nie ma bowiem charakteru stanowczego i jako zestaw instrukcji nie zawsze

musi umożliwiać jednoznaczne przypisanie określonego prawa konkretnej stronie, zwłaszcza w przypadku bardziej złożonych inteligentnych kontraktów.

Zresztą w praktyce inteligentnemu kontraktowi będą zazwyczaj towarzyszyć inne uzgodnienia, czy to przyjmujące postać formalną umowy, czy też postać nieformalnych ustaleń, które pozwolą bardziej jednoznacznie ustalić treść stosunku prawnego łączącego strony. Dlatego bardzo istotne jest określenie relacji między inteligentnym kontraktem a treścią pozostałych uzgodnień między stronami. To od decyzji stron zależy, czy inteligentny kontrakt będzie jedynie rozwiązaniem technicznym pozwalającym na realizację umowy, ale pozostającym w dużej mierze poza nią, czy też istotnym elementem kształtującym jej treść.

Przepisy ustawowe determinujące treść umowy

Ponadto należy pamiętać, że na treść umowy będą wpływać także przepisy prawa. Z jednej strony mogą to być przepisy o charakterze uniwersalnym, np. uzupełniające treść umowy

przez odwołanie się do zasad współzycia społecznego i ustalonych zwyczajów (art. 56 k.c.) czy też uznające za nieważne postanowienia sprzeczne z prawem (por. art. 58 § 1 k.c.). Z drugiej strony treść umowy może być kształtowana również przez przepisy odnoszące się do konkretnego rodzaju umowy (umowy nazwanej), np. określające ustawowe terminy wypowiedzenia najmu (art. 673 § 1 i 2 k.c.).

Sytuacja, w której całokształt praw i obowiązków stron określa wyłącznie kod źródłowy inteligentnego kontraktu, będzie występować dość rzadko. Dlatego inteligentnych kontraktów nie należy stawiać w opozycji do tradycyjnych umów, lecz raczej traktować je jako ich uzupełnienie, nowatorski element konstrukcyjny stwarzający nowe możliwości. Trzeba przy tym mieć na względzie, że ich treść będzie kształtowana nie tylko przez polecenia zawarte w kodzie źródłowym, ale także przez przepisy ustawowe, zarówno bezwzględnie wiążące, jak i dyspozytywne, jeśli strony nie wyłączą ich zastosowania.

Jak projektować inteligentne kontrakty i DAO

Jacek Czarnecki

Inteligentne kontrakty mają różne oblicza. Z jednej strony rewolucjonizują one sposób zawierania i wykonywania umów, z drugiej strony ich potencjał jest znacznie większy. Inteligentne kontrakty mogą bowiem niczym klocki służyć do budowania złożonych struktur społecznych i ekonomicznych. Jednym z przykładów jest DAO.

Różne zastosowania inteligentnych kontraktów łączy jedno: potencjał gruntownej przemiany systemu prawnego. Inteligentne kontrakty to obietnica pełnego przeniesienia obrotu prawnego w świat cyfrowy.

Ta rewolucja nie dokona się natychmiast. Obecnie mamy dobrze rozwiniętą kulturę prawną opartą o tradycyjne, analogowe narzędzia. Jednocześnie na naszych oczach prężnie rozwijają się kolejne projekty dotyczące inteli-

gentnych kontraktów. Prawdopodobnie w przyszłości dojdzie do konwergencji i wzajemnej adaptacji tych dwóch nurtów.

Zanim to nastąpi, z pewnością niejednokrotnie staniemy wobec sytuacji, które rządzone będą z jednej strony kodem inteligentnego kontraktu, a z drugiej tradycyjnymi regulami prawa. To nie tylko problem teoretyczny. W praktyce tworzenie inteligentnych kontraktów, w tym DAO, będzie wymagało odpowiedniego i zręcznego użycia tradycyjnych narzędzi prawnych. Wierzę, że te ostatnie już dziś pozwalają skorzystać z potencjału inteligentnych kontraktów. Poniżej opisujemy, jak to zrobić.

1. Połącz inteligentny kontrakt i prawo

Tradycyjne rozwiązania prawne i inteligentne kontrakty nie muszą być przeciwstawne. Wręcz przeciwnie, mogą się bardzo dobrze uzupełniać. Umiejętne wykorzystanie zalet jednych i drugich może stworzyć synergię, która połączy pewność inteligentnego kontraktu z elastycznością tradycyjnego środka prawnego.

W praktyce może to polegać na integracji dwóch jednocześnie rozwijanych rozwiązań. Przykładowo tradycyjna umowa może mieć charakter ramowy i przewidywać szereg kolejnych działań. Te działania (transakcje) mogą być wykonywane przez inteligentne kontrakty. W innym przypadku umowa może przewidywać zasady korzystania z wyroczni (zob. poniżej), które mogą być niezbędne do prawidłowego wykonania inteligentnego kontraktu.

Ważne, aby inteligentny kontrakt i tradycyjna umowa (lub regulamin czy też dowolny inny klasyczny instrument prawny) nie tylko powstawały i istniały równoległe, ale również były ze sobą powiązane. Umowa może jako załącznik zawierać treść inteligentnego kon-

traktu, a inteligentny kontrakt może się odwoływać do kryptograficznego skrótu umowy podpisanej cyfrowo przez strony.

Zapewne w praktyce dużą rolę odgrywać będą zestandaryzowane wzory inteligentnych kontraktów (np. na potrzeby określonych transakcji finansowych). W takim modelu klasyczna umowa będzie swojego rodzaju parasolem czy opakowaniem dla inteligentnych kontraktów.

Czasami dobrym pomysłem będzie również osadzenie inteligentnego kontraktu w realnym świecie. Przykładem może być stworzenie spółki, która będzie powiązana z inteligentnym kontraktem w formie DAO i będzie jego łącznikiem ze światem rzeczywistym. Innym pomysłem jest powiązanie inteligentnego kontraktu (np. poprzez jego treść) z konkretną jurysdykcją. Dzięki temu można uniknąć wątpliwości, jakie prawo (którego kraju) jest właściwe dla danego inteligentnego kontraktu.

Pamiętajmy, że inteligentny kontrakt to nie tylko cyfrowy odpowiednik umowy cywilnoprawnej. Za pośrednictwem inteligentnego kontraktu można odzwierciedlić wiele różnych relacji prawnych, a nawet skomplikowanych instytucji, takich jak fundusz inwestycyjny czy rejestr publiczny. W takich przypadkach również przyda się integracja klasycznych rozwiązań prawnych z inteligentnymi kontraktami.

2. Uważaj na regulacje

Nawet jeżeli nie skorzystasz z rady zamieszczonej powyżej, nie oznacza to, że Twój inteligentny kontrakt nie wywrze skutków prawnych. Może okazać się, że jego zawarcie i wykonanie będzie miało pewne konsekwencje w tradycyjnej przestrzeni prawnej. Może np. zostać uznany za element tradycyjnej umowy. Chodzi tu także o kwestie podatkowe oraz regulacyjne, takie jak usługi płatnicze, pieniądź elektroniczny, obrót instrumentami finansowymi itd.

3. Zapewnij identyfikację stron

Blockchain daje możliwość efektywnej współpracy i osiągania konsensu przez nieznające się strony oraz zapewnia, że strony mogą być pewne dochowania zasad współpracy pomimo braku zaufania. Temu mogą dodatkowo służyć inteligentne kontrakty. Dzięki nim możesz dokonywać transakcji z kimś, kogo nie znasz i komu nie ufasz bez potrzeby korzystania z usług zaufanej trzeciej strony.

Aby zapewnić, że Twój inteligentny kontrakt będzie mógł zostać wyegzekwowany także w drodze tradycyjnej ścieżki prawnej (na przykład jeśli w kodzie coś pójdzie nie tak), powinieneś jednak zadbać o identyfikację drugiej strony umowy. Chodzi o jej dostateczne określenie, tak abyś nie miał np. problemu ze zdecydowaniem, wobec kogo powinieneś skierować swoje roszczenie.

4. Skorzystaj z gotowych (i rozpoznawanych przez prawo) narzędzi

Wbrew pozorom prawo i regulacje nie są zupełnie na bakier z nowymi technologiami. Dość szybko rozwijane są narzędzia w świecie cyfrowym, które są rozpoznawane przez prawo i stąd mogą służyć do osiągnięcia różnych skutków prawnych.

Dobrym przykładem jest unijne rozporządzenie eIDAS, które daje dobrą podstawę do tworzenia środków identyfikacji elektronicznej oraz narzędzi do świadczenia i korzystania z usług zaufania (takich jak podpis elektroniczny). Między innymi dzięki temu już wkrótce w przestrzeni cyfrowej będziemy identyfikowani lepiej niż z użyciem tradycyjnych dowodów tożsamości, a dzięki nowym usługom zaufania będziemy mogli cyfrowo podpisywać dokumenty, osiągając skutek równoznaczny z podpisem własnoręcznym.

Użycie takich narzędzi może znacznie uprościć korzystanie z inteligentnych kontraktów,

a także ułatwić określanie, jakie skutki prawne ma dany inteligentny kontrakt.

5. Zręcznie korzystaj z wyroczni (Oracles)

Za słabą stroną inteligentnych kontraktów uważa się ich ograniczoną zdolność do pozyskiwania, przetwarzania i weryfikowania informacji ze świata realnego (zewnętrznego, czyli poza blockchainem). Inteligentny kontrakt, którego wykonanie ma zależeć np. od dokonania jakiejś czynności w świecie realnym (np. zawarcia małżeństwa czy przejścia spółki), musi dla swojej skuteczności być w stanie zweryfikować, czy ta czynność nastąpiła.

Temu w praktyce służą wyrocznie (*Oracles*). Ich podstawową rolą jest stwierdzenie jakiegoś stanu rzeczy oraz przekazanie odpowiedniej informacji w postaci, która może zostać przyjęta przez dany inteligentny kontrakt w określonym blockchainie. Wyrocznia jest zatem swoistym łącznikiem pomiędzy światem realnym a światem cyfrowym oraz danym blockchainem.

Dobra konstrukcja wyroczni w inteligentnym kontrakcie jest kluczowa. Jeśli wyrocznią ma być człowiek, należy tradycyjnymi środkami prawnymi zapewnić, że przekaze on prawidłowe informacje. Wyrocznia może też mieć postać algorytmu. W obydwu przypadkach trzeba przewidzieć sytuację, w której w warstwie inteligentnego kontraktu coś pójdzie nie tak. Wówczas tradycyjne rozwiązania prawne mogą być jedynym ratunkiem.

6. Zastanów się, jak inteligentny kontrakt zostanie wykonany, i weź pod uwagę ograniczenia

Podobnie jak inteligentny kontrakt i blockchain, na którym on funkcjonuje, mogą potrzebować zewnętrznych źródeł informacji (zobacz punkt wyżej o wyroczniach), tak samo wykonanie inteligentnego kontraktu nierzadko

będzie wymagało połączenia ze światem realnym. Zasadniczo inteligentny kontrakt działa na jednym blockchainie, a efektem działania jest modyfikacja treści bazy danych (czyli blockchaina właśnie). Zastanów się zatem, czy taki skutek wykonania inteligentnego kontraktu będzie wystarczający dla stron. Być może ciągiem dalszym powinny być działania w ramach tradycyjnego stosunku prawnego.

7. Audytuj wszystkie przyjęte rozwiązania

Audytowi powinny podlegać nie tylko inteligentne kontrakty oraz dokumentacja prawna. Kluczowa jest ich wzajemna kompatybilność. Być może warto przewidzieć, co przeważy w przypadku konfliktu pomiędzy regulami inteligentnego kontraktu a zasadami ustalonymi w drodze klasycznych ustaleń prawnych.

8. Zadbaj o elastyczność inteligentnego kontraktu

Prosty inteligentny kontrakt to zestaw deterministycznych reguł, które zostaną wykonane automatycznie, gdy zajdą określone w nich zdarzenia. Po utworzeniu inteligentnego kontraktu strony nie mogą wpłynąć na zmianę jego zasad. Inteligentny kontrakt jest „ślepy” – zostanie wykonany dokładnie w taki sposób, w jaki został zaprogramowany. Z jednej strony to zaleta, ponieważ strony nie muszą martwić

się o egzekucję zobowiązań drugiej strony. Doświadczenie pokazuje jednak, że czasami trzeba zmienić umowę lub dostosować ją do nowych okoliczności. Temu służą różne tradycyjne instytucje prawne, takie jak *rebus sic stantibus* (nadzwyczajna zmiana okoliczności), które pozwalają na modyfikację pierwotnych ustaleń stron.

Warto zastanowić się nad uelastycznieniem zawieranego inteligentnego kontraktu. Może ono polegać na możliwości jego zmiany przez obydwie strony działające zgodnie lub przez zaufaną trzecią stronę.

9. Zastanów się nad wentylem bezpieczeństwa

Przykład The DAO jaskrawo pokazał, że wadliwy inteligentny kontrakt może prowadzić do nieprzewidzianych skutków. Co więcej, jak wspomniałem powyżej, inteligentny kontrakt jest „ślepy”. W związku z tym, nawet jeśli został skonstruowany zgodnie z wolą stron, zmiana okoliczności może spowodować, że strony mogą chcieć zmienić reguły gry. Warto zatem dodać „wentyl bezpieczeństwa”, czyli rozwiązanie, które pozwoli wyjść cało z inteligentnego kontraktu, nawet jeśli coś pójdzie źle.

Czym jest DAO z perspektywy prawa?

Krzysztof Wojdyło

Pytanie postawione w tytule byłoby w zasadzie zbyteczne, gdyby DAO funkcjonowało w całkowitym oderwaniu od istniejącego kontekstu prawno-gospodarczego. Tak jednak nie jest, przynajmniej na aktualnym etapie rozwoju DAO. Z uwagi na istniejące powiązania ze światem realnym (wymuszone chociażby przez istniejące systemy podatkowe) powstaje konieczność uchwycenia istoty DAO na potrzeby istniejących konstrukcji prawno-gospodarczych.

Wyjątkowość DAO

DAO jest niewątpliwie bytem niematerialnym. Ta okoliczność nie czyni jednak z DAO czegoś szczególnie wyjątkowego z perspektywy prawnej. Prawo od dawna rozpoznaje bowiem istnienie bytów niematerialnych. Znaczenie tych bytów zresztą systematycznie rośnie. W tym kontekście należy wspomnieć choćby o prawach własności intelektualnej czy wierzytelnościach, które nie mają postaci materialnej, a mogą mieć znaczącą wartość.

DAO jest rodzajem inteligentnego kontraktu. Należy go jednak odróżnić od inteligentnych kontraktów, które mogą być zawierane za jego pomocą. DAO należy traktować jako rodzaj metakontraktu, który organizuje schemat zawierania docelowych kontraktów pomiędzy uczestnikami danego DAO. Tym samym DAO ma zdolność tworzenia stosunków prawnych pomiędzy jego uczestnikami (tj. uczestnicy danego DAO posiadają określone prawa i zobowiązania). Stosunki prawne są wprawdzie w tym przypadku tworzone za pomocą niestandardowych metod, niemniej jednak dzięki DAO dochodzi do skutecznego zawiązania relacji prawnych pomiędzy jego uczestnikami.

Wyjątkowość DAO polega również na bardzo daleko posuniętej autonomiczności działania. Poszczególne DAO funkcjonują w sposób zautomatyzowany, poprzez realizację kodu będącego ich podstawą. DAO jest również pozbawione tradycyjnych reprezentantów, odpowiadających np. reprezentantom osób prawnych.

Mimo to DAO oraz jego uczestnicy wchodzą w relacje zewnętrzne z podmiotami spoza DAO. Taka sytuacja ma miejsce np. w odniesieniu do deweloperów oprogramowania DAO czy zewnętrznych dostawców treści do DAO (np. zaufanych dostawców danych

o wartości określonych aktywów, które mają znaczenie dla inteligentnych kontraktów zawieranych w ramach DAO).

Wiele stosunków prawnych tworzonych za pośrednictwem DAO będzie można zapewne zakwalifikować jako stosunki rozpoznane przez tradycyjne systemy prawa (np. umowa sprzedaży czy umowa najmu). Znacznie większe trudności stwarza natomiast prawne zakwalifikowanie samego DAO. Trudno jest przypisać DAO do konkretnej jurysdykcji, ponieważ aktualne systemy prawne w ogóle nie rozpoznają istnienia DAO. W tym sensie DAO to abstrakcyjny byt, który wymyka się prostym kwalifikacjom prawnym oraz który trudno jednoznacznie przypisać do określonego porządku prawnego.

Zdolność prawna

Takie podejście do DAO prezentuje również aktualnie prawo polskie. Jednym z fundamentalnych pojęć na płaszczyźnie prawa cywilnego jest pojęcie zdolności prawnej. Nie jest ono wprawdzie zdefiniowane w Kodeksie cywilnym, niemniej jednak przyjmuje się, że jest to zdolność do bycia podmiotem praw oraz zobowiązań cywilnych. Tak rozumianą zdolność mają wyłącznie podmioty określone przez prawo. Są to osoby fizyczne, osoby prawne (prawo przewiduje zamknięty katalog osób prawnych) oraz jednostki organizacyjne niebędące osobami prawnymi, którym jednak szczególny przepis ustawy nadaje zdolność prawną. DAO nie jest żadnym z tych podmiotów, w świetle polskiego prawa cywilnego nie ma więc zdolności prawnej i nie może być podmiotem praw i zobowiązań w zakresie prawa cywilnego. Rozpoznanie przez system polskiego prawa podmiotowości prawnej DAO wymagałoby interwencji ustawodawcy oraz wyraźnego nadania DAO zdolności prawnej.

Istota problemu

Brak zdolności prawnej DAO powoduje, że z perspektywy aktualnych przepisów prawa pozostaje ono transparentne. Ewentualne relacje prawne zachodzące w ramach DAO lub z DAO są więc teoretycznie relacjami zachodzącymi bezpośrednio pomiędzy uczestnikami końcowymi DAO. Na pierwszy rzut oka taki stan rzeczy może wydawać się neutralny. Dopóki DAO funkcjonuje poprawnie, powyższe rozważania wydają się jedynie zbędnymi, akademickimi dyskusjami.

Problem polega jednak na tym, że DAO nie jest i w krótkiej perspektywie raczej nie będzie bytem całkowicie wyabstrahowanym od rzeczywistości ujętej w tradycyjne ramy formalno-prawne. Dzieje się tak przede wszystkim dlatego, że użytkownikami końcowymi DAO są osoby fizyczne i osoby prawne, które podlegają określonym porządkom prawnym. Przykładowo na cele rozliczeń podatkowych może zająć konieczność precyzyjnego zidentyfikowania źródła przychodu pochodzącego z DAO. Ponadto DAO dla swojego funkcjonowania oraz rozwoju często będzie potrzebowało relacji z zewnętrznymi dostawcami usług (np. twórcami oprogramowania).

W takich przypadkach prawna transparentność DAO stwarza bardzo istotne problemy praktyczne. Jako strony relacji prawnych tworzonych w ramach DAO oraz strony relacji prawnych z DAO należałoby bowiem wskazywać wszystkich uczestników DAO. Identyfikacja tych podmiotów jest w praktyce niemożliwa. Ponadto sytuacja taka bardzo utrudnia nawiązywanie jakichkolwiek relacji prawnych z DAO przez dostawców zewnętrznych. Dostawcy działający z należytą starannością dążą do precyzyjnej identyfikacji swoich kontrahentów. Muszą wiedzieć, z kim faktycznie wchodzi w relacje prawne, do kogo będą mieć ewentualne roszczenie o zapłatę itp.

Rozwiązanie krótkoterminowe

Aby zaradzić powyższym trudnościom, należy rozważyć tworzenie struktur, które łączą relacje prawne powstałe w ramach DAO z tradycyjnym podmiotem posiadającym zdolność prawną rozpoznawaną przez tradycyjne systemy prawne. Warunki określonego DAO mogą wskazywać wprost, że np. stroną relacji z DAO jest określona spółka czy fundacja. Takie rozwiązanie niewątpliwie bardzo ułatwia tworzenie relacji prawnych z DAO. Umożliwia określenie podmiotu, który jest stroną relacji z DAO, oraz ustalenie porządku prawnego, który będzie miał zastosowanie do relacji z DAO.

Opisane rozwiązanie niewątpliwie przyczyni się do zwiększenia pewności obrotu z DAO. Jest też korzystne dla inicjatorów DAO, pozwala bowiem w miarę precyzyjnie oszacować ewentualne ryzyka prawne związane z uruchomieniem określonego DAO. DAO w takim rozwiązaniu przestaje być bowiem zawieszona w prawno-regulacyjnej próżni. Pojawiają się pierwsze przykłady DAO próbujące wykorzystać ten schemat. Wydaje się, że w perspektywie krótkoterminowej jest to jedyna szansa na zapewnienie bezpiecznego rozwoju DAO oraz wykorzystanie ich potencjału.

Rozwiązanie długoterminowe

Biorąc pod uwagę naturę DAO, wskazane powyżej rozwiązanie należy jednak uznać za prowizoryczne. Docelowo na potrzeby DAO należałoby stworzyć nową, specjalną konstrukcję zdolności prawnej. Takie rozwiązanie znacznie lepiej odpowiadałoby rzeczywistej naturze DAO. Przyjmując rozwiązanie tymczasowe, faktycznie tworzymy bowiem pewien rodzaj fikcji. Podmiot tradycyjny, który na potrzeby istniejącego porządku prawnego kojarzymy z DAO, często nie będzie w stanie kontrolować działania DAO. Istota DAO polega prze-

cięż w dużej mierze na autonomicznym charakterze. Nadanie DAO zdolności prawnej byłoby więc znacznie naturalniejszym rozwiązaniem.

DAO ma bardzo wiele elementów wspólnych z innymi niematerialnymi podmiotami, którym system prawa nadaje zdolność prawną. Przesłanki, które przemawiały za nadaniem zdolności prawnej takim podmiotom jak osoby prawne, niewiele różnią się od przesłanek odnoszących się do DAO. Zarówno osoby prawne, jak i DAO są bytami niematerialnymi. Osoby prawne zostały powołane m.in. po to, aby ułatwić i usprawnić obrót prawny poprzez upodmiotowienie sztucznego podmiotu, który znajdował się pomiędzy końcowymi uczestnikami wymiany gospodarczej (np. akcjonariusze, pracownicy, konsumenci, dostawcy). Dzięki temu końcowi uczestnicy systemu wymiany gospodarczej (np. dostawcy) nie muszą wchodzić w bezpośrednie relacje prawne z innymi końcowymi uczestnikami systemu wymiany (np. właścicielami środków produkcji).

Jednocześnie należy zdać sobie sprawę, że nadanie DAO zdolności prawnej byłoby ogromnym wyzwaniem dla aktualnego porządku prawnego. Tak jak wskazano powyżej, jedną z cech DAO jest niemożność przypisania ich do konkretnej jurysdykcji. DAO funkcjonują bowiem w rozproszonej sieci. Tymczasem aktualny porządek prawny nadal funkcjonuje

w oparciu o paradygmat zakładający konieczność przypisania każdego zjawiska prawnego do konkretnej, tradycyjnie rozumianej jurysdykcji. Na przykładzie wyzwań prawnych, które niesie ze sobą internet (np. cyberprzestępczość,

e-commerce, *cloud computing*), widać wyraźnie, że paradygmat ten nie jest do końca dostosowany do realiów globalnej sieci. Już dzisiaj w przypadku wielu zdarzeń w internecie powstają niezwykle trudne do rozstrzygnięcia konflikty pomiędzy poszczególnymi porządkami prawnymi (np. kłopoty z ustaleniem prawa właściwego dla przetwarzania danych w usługach *cloud computingu*). DAO w jeszcze większym stopniu uwypukla niedoskonałości aktualnego porządku prawnego.

Wydaje się, że rozwiązaniem najbardziej odpowiadającym naturze DAO byłoby nadanie DAO szczególnego rodzaju podmiotowości prawnej, przy jednoczesnym stworzeniu na potrzeby DAO koncepcji specjalnej, „rozproszonej” jurysdykcji, odmiennej od tradycyjnie rozumianych jurysdykcji. Takie rozwiązanie jest jednak na tyle odległe od obowiązującego porządku prawnego, że trudno oczekiwać jego realizacji w jakimkolwiek przewidywalnym horyzoncie czasowym.





Blockchain jest fundamentem cyfrowej gospodarki opierającej się na współpracy

Rozmowa z Maciejem Jędrzejczykiem i Karoliną Marzantowicz z IBM

J. Cz.: Blockchain jest określany jako „internet wartości”. Jak IBM postrzega potencjał tej technologii?

Maciej Jędrzejczyk: Blockchain to technologia rozproszonego rejestru, technologia nowej generacji, którą możemy stosować w systemach transakcyjnych. Daje ona gwarantowane kryptograficznie zaufanie oraz przejrzystość przy jednoczesnym usprawnieniu procesów biznesowych dzięki wykorzystaniu jednego rejestru zdecentralizowanego pomiędzy użytkownikami.

Dzięki tej technologii możemy w wiarygodny sposób automatyzować interakcje biznesowe pomiędzy wieloma partnerami, a potencjalnie także tworzyć nowe style interakcji cyfrowych. Blockchain pozwala znacznie zmniejszyć koszty operacyjne procesów biznesowych i uprościć złożoność procesów między różnymi organizacjami. Rozproszony rejestr daje możliwość tworzenia sieci biznesowych dla danego rynku czy grupy partnerów, gdzie praktycznie wszystko, każda transakcja, może być utrwalone, bez konieczności posiadania centralnego punktu kontroli.

Blockchain wprowadza nowe możliwości wymiany wartości i zasobów w cyfrowej gospodarce. Rozproszony rejestr zachęca do współpracy w ramach określonego ekosystemu, a to

właśnie współpraca jest jednym z fundamentów cyfrowej ekonomii. Blockchain daje też możliwość budowania cyfrowego zaufania, które nie musi być gwarantowane przez jakąkolwiek stronę trzecią. Technologia wyklucza bowiem korupcję, fałszerstwa czy manipulowanie faktami (transakcjami).

Rozproszenie, decentralizacja, a także niezaprzeczalność i ostateczność to kluczowe cechy technologii blockchain i wykorzystywanych przez nią algorytmów. Zastosowanie tej technologii jest bardzo szerokie, i dotyczy każdej branży, w której mamy wielu różnych uczestników, korzystamy z centralnych rejestrów, następuje wymiana wartości lub środków albo potrzebujemy gwarancji stanu danych.

Blockchain nie jest jednak lekarstwem na wszystkie wyzwania cyfrowej rewolucji. Daje odpowiedź tylko na niektóre z nich.

IBM rozwija superkomputer Watson, który może odpowiadać na pytania w języku naturalnym. Czy blockchain może zostać wykorzystany w tym projekcie?

Karolina Marzantowicz: IBM Watson to system kognitywny (*cognitive computing*). Rozumie język naturalny, wysuwa hipotezy i wnioski, pracując na dużych zbiorach danych nieustrukturyzowanych, w tym także multimedialnych, waliduje je, a także się uczy. Systemy kogni-

tywne będą zmieniać sposób interakcji człowieka z technologią oraz poszerzać nasze eksperckie możliwości. IBM Watson jest tak zbudowany, aby odzwierciedlać – na tyle, na ile pozwalają na to obecne osiągnięcia nauki – działanie ludzkiego mózgu w procesie poznawczym.

Blockchain z założenia daje potwierdzenie pochodzenia każdego bloku w łańcuchu (a co za tym idzie potwierdzenie pochodzenia tego, czego dotyczą transakcje w bloku) wraz z pełną historią zmian. Dodatkowo daje gwarancję poprawności transakcji zapewnianą przez zaawansowaną kryptografię. Blockchain pozwoli w przyszłości na dużo dalej idącą automatyzację przetwarzania w cyfrowej gospodarce, w szczególności w obszarze internetu rzeczy, umożliwiając biznesowe interakcje pomiędzy sensorami i coraz inteligentniejszymi urządzeniami. Firmy mogą wymieniać między sobą dane przetwarzane w ramach internetu rzeczy poprzez sieć blockchain, bo takie rozwiązanie będzie mniej skomplikowane i tańsze we wdrożeniu i utrzymaniu. Systemy kognitywne mogą być źródłem wiedzy, sygnałów, które będą zasilać sieć blockchain czy inteligentne kontrakty. Blockchain jest fundamentem cyfrowej gospodarki opierającej się na współpracy. Internet rzeczy rozszerza granice IT poza tradycyjne Data Center i wymaga nowego medium komunikacyjnego opartego o rozproszoną architekturę. Tradycyjna analityka jest bezsilna w wyciąganiu wniosków z ogromnych ilości danych niestrukturalnych. Systemy kognitywne nie tylko są w stanie pomóc w dostępie do odpowiedzi, których potrzebuje biznes, ale też zmieniają sposób, w jaki komunikujemy się z technologią, której będzie w naszym życiu coraz więcej.

Czym jest projekt Hyperledger?

M.J.: Hyperledger to konsorcjum ponad 80 firm reprezentujących różne gałęzie gospodarki (firmy z branży IT, banki, startupy, giełdy), rozwijających wspólnymi siłami technologię rozproszonych rejestrów (*Distributed Ledger Technology*, DLT) opartych na blockchainie. Projektem tym zarządza Linux Foundation, co gwarantuje pełną obiektywność i transparentność w podejmowaniu decyzji o kierunku działań. Cel przyświecający projektowi Hyperledger to stworzenie otwartego standardu, mającego na celu transformację relacji i procesów biznesowych.

Hyperledger można traktować jako swoisty parasol, pod którym inkubowane są obecnie trzy inicjatywy:

- Fabric: implementacja technologii blockchain dostosowana do potrzeb biznesowych;
- Sawtooth Lake: implementacja technologii blockchain zoptymalizowana pod kątem internetu rzeczy;
- Hyperledger Blockchain Explorer: uniwersalny panel graficzny do analizy wydarzeń i transakcji w sieciach opartych na technologiach bazujących na kodzie Fabric lub Sawtooth Lake.

Ponadto projekt Hyperledger wprowadza ramy architektoniczne, które powinny być zawarte w każdym inkubowanym projekcie. Po pierwsze, każda inicjatywa powinna opierać swoje rozwiązanie na otwartych standardach, protokolach i modelu licencjonowania. Po drugie, rozwiązanie powinno wspomagać komunikację między różnymi sieciami opartymi na technologii blockchain, innymi rozproszonymi rejestrami lub innymi tradycyjnymi systemami danych (*System of Record*, SOR).

Jako że docelowym odbiorcą rozwiązania są organizacje biznesowe, inkubowany kod powinien natywnie wspomagać transakcje każdego rodzaju aktywów (monetarnych lub niemonetarnych), które mogą odbywać się w ramach całkowitej prywatności pomiędzy stronami. Aby sprostać potrzebom biznesu, wymogiem jest również skalowalność, modularność i rozbudowywalność poszczególnych komponentów (np. mechanizm konsensu, zarządzanie rolami, administracja dostępem do sieci itp.), a co za tym idzie kompletna elastyczność bez potrzeby modyfikacji bazowego kodu źródłowego.

Czy Hyperledger może służyć do zawierania i wykonywania inteligentnych kontraktów?

K.M.: Ze względu na charakter docelowego odbiorcy oczywiste jest, że inkubowane rozwiązania muszą wspomagać inteligentne kontrakty. Wynika to z interpretowania tych ostatnich jako sposobu na przeniesienie istniejących procesów biznesowych do kodu zrozumianego przez strony umowy i węzły funkcjonujące w ramach sieci blockchain. Przykładowo w ramach inkubatora Fabric inteligentne kontrakty (nazywane tutaj Chaincode) są nie tylko nośnikiem zasad, na podstawie których strony przeprowadzają transakcje, ale stają się dosłownie pośrednikiem w interakcji między stronami, których przebieg rejestrowany jest później do blockchaina. Ma to fundamentalne znaczenie, ponieważ powoduje, że bazowy kod źródłowy Fabric nie narzuca zasad interakcji pomiędzy stronami, zostawiając to logicie inteligentnych kontraktów.

W tym miejscu warto wspomnieć, że w kontekście wymogu pełnej modularności inteligentne kontrakty na platformie Fabric mogą zostać napisane w różnych językach programowania, a interpretacja ich treści wykonywana jest automatycznie przez kod bazowy.

Obniża to zdecydowanie barierę wejścia dla firm chcących skorzystać z tego rozwiązania, ponieważ zdecydowanie łatwiej jest znaleźć programistę Java, Node.js czy GOLANG (Chaincode można przygotować we wszystkich tych językach na zasadzie out-of-the-box), niż np. Solidity (język programowania inteligentnych kontraktów dla Ethereum).

Jak we wszystkich rozwiązaniach przeznaczonych dla biznesu, kluczem do sukcesu jest bezpieczeństwo. W przypadku Fabric każdy inteligentny kontrakt uruchamiany jest w tzw. piaskownicy (*sandbox*), co pozwala na odizolowanie efektów uruchomionego kodu od reszty sieci oraz jej uczestników.

Czy prawo i regulacje są przeszkodą na drodze rozwoju technologii blockchaina?

K.M.: I tak, i nie. Z jednej strony codziennie jesteśmy świadkami narodzin nowych, często udanych projektów wdrażających rozwiązania oparte na technologii blockchain w wielu dziedzinach gospodarki. Ma to miejsce przy istniejącym ładzie prawno-regulacyjnym, jak również w sektorach podlegających silnej kontroli, jak bankowość i administracja publiczna. Drugą stroną medalu jest niezliczona ilość inicjatyw uruchamianych w ramach społeczności kryptowalut i w ramach poszczególnych konsorcjów blockchainowych, których celem jest uświadomienie prawodawcom doniosłości tych technologii oraz konieczności otwarcia się na nie. Sam fakt istnienia tych inicjatyw w wielu krajach oznacza, że istnieje potrzeba dyskusji nad obecnym stanem prawnym.

Analogiczne sytuacje można napotkać na lokalnym gruncie. Przykładem jest stanowisko dotyczące blockchaina i kryptowalut, owoc prac grupy prawników z tzw. strumienia Blockchain i kryptowaluty, powstałego z inicjatywy Ministerstwa Cyfryzacji. Prezentacje i wnioski prelegentów przedstawione w czasie

niedawnych konsultacji społecznych w Sejmie RP pokazują, że istnieje potrzeba stałego dialogu ze stroną rządową, aby stworzyć instrumenty prawne pozwalające na ochronę przedsięwzięć opartych na tych nowych technologiach.

Jak władze publiczne powinny podejść do zastosowań technologii blockchaina takich jak inteligentne kontrakty czy DAO?

M.J.: Technologia zwykle wyprzedza istniejący ład prawny i jest to normalny stan rzeczy. Jednakże elastyczność prawa pozwala dostosować istniejące normy do nowych zjawisk, a do takich należy zaliczyć inteligentne kontrakty. Z pewnością znajdują się strony dokonujące transakcji za pomocą tej formy i niepotrzebujące do tego oficjalnej wykładni prawnej. Jeżeli jednak zajdzie potrzeba rozwiązania konfliktu, który nie był przewidziany przez inteligentny kontrakt, będą odnosić się do prawodawstwa swojej jurysdykcji. Przypadek

DAO nie jest znacząco pod tym względem odmienny i powinien być traktowany w taki sam sposób. Władze publiczne powinny być przygotowane merytorycznie do takich sytuacji – na szczęście mogą pod tym względem polegać na ekspertach z ww. strumienia.

Prawodawcy powinni przychylnie odnosić się do tych nowych sposobów ustalania zasad interakcji międzyludzkiej, a także mieć na uwadze owoce tych interakcji, czyli cyfrowe aktywa oraz rejestr stosunków własności, które nie mają ekwiwalentów w świecie fizycznym. Blockchain znacząco ułatwi tworzenie takich aktywów, a inteligentne kontrakty znacząco przyspieszą transakcyjne procesy wymiany.

Rozmawiał Jacek Czarnecki



Co historia The DAO mówi o prawie

Agnieszka Kraińska

Saga związana z pojawieniem się i upadkiem The DAO wiele mówi o tym, jak rzeczywistość świata wirtualnego wyprzedza istniejące regulacje prawne i kreuje nowe problemy, na które nie ma jeszcze odpowiedzi.

The DAO

The DAO była rodzajem DAO, podmiotem *sui generis*, który z założenia miał przynosić dochód z działalności o charakterze inwestycyjnym, przy wykorzystaniu instrumentów przypominających instrumenty finansowe. Zgodnie z deklaracją twórców zamieszczoną na stronie daohub.org celem The DAO było wykorzystanie posiadanych przez organizację jednostek kryptowaluty Ethereum (etherów,

ETH) do wsparcia przedsięwzięć, które przyniosą korzystny zwrot z inwestycji dla organizacji i jej członków. Struktura ta miała więc cechy inwestycyjnej platformy crowdfundingowej lub funduszu venture capital.

Faza kreacji The DAO trwała od 30 kwietnia do 28 maja 2016 r. i polegała na tym, że inwestorzy mogli wpłacać ETH i w zamian otrzymywali tokeny The DAO. Posiadanie tokenów uprawniało do głosowania nad sposobem in-

westowania zebranych przez organizację środków. Faza kreacji okazała się ogromnym sukcesem, gdyż projekt zebral środki odpowiadające wartości ok. 150 mln dolarów.

Żeby zrozumieć późniejsze wydarzenia, trzeba wiedzieć, że The DAO było strukturą zależną od działań czterech typów podmiotów – twórców, inwestorów, kontrahentów i kuratorów. Twórcy to autorzy otwartego oprogramowania, dzięki któremu powstała platforma. Inwestorzy to osoby, które uzyskały prawa głosu w zamian za wniesione ETH. Kontrahenci przedstawiali propozycje przedsięwzięć, w które The DAO mogło zainwestować. Kuratorzy zbierali, weryfikowali i poddawali pod głosowanie zgłoszone propozycje.

Atak

17 czerwca 2016 r. przeprowadzony został atak na The DAO, wskutek którego z organizacji wyprowadzono ok. 1/3 ETH. Atak był możliwy dzięki wykorzystaniu furtki w kodzie The DAO, której nie dostrzegli jego twórcy. W konsekwencji powstało „DAO pochodne”, nazwane „Dark DAO”, w którym znalazły się wyprowadzone ETH.

Wykorzystana przez hakera furtka w systemie wynikała z cech funkcji „splitu” umożliwiającej przeniesienie środków inwestorów z The DAO do odrębnego DAO. Konsekwencją splitu była likwidacja (spalenie) tokenów The DAO po przeniesieniu odpowiadającej im kwoty ETH do nowego DAO pochodnego. Użyta przez hakera furtka w kodzie splitu umożliwiała wysłanie powtarzającego się żądania wycofania ETH i w konsekwencji wielokrotne transfery ETH z The DAO.

Reakcja na atak

Dark DAO pod względem kodu była klonem The DAO, więc wyprowadzenie środków z nowej organizacji było możliwe dopiero po zakończeniu okresu kreacji Dark DAO i po

upływie okresów koniecznych do dokonania kolejnych kroków. Z tego względu społeczność The DAO miała czas na analizę sytuacji.

Biorąc pod uwagę założenia dotyczące blockchaina i inteligentnych kontraktów, które nie mogą ulec sfalszowaniu, są autonomiczne i nie podlegają kontroli instytucjonalnej, pojawiło się pytanie, czy można w ogóle mówić o bezprawności działania hakera. W sieci pojawił się list osoby, nazywającej siebie Napastnikiem (the Attacker). Napastnik tłumaczył, że wyprowadzenie środków z The DAO wynikało z określonych cech programu, które wykorzystał, a więc że jego działania nie można uznać za kradzież.

Dyskusja na forach The DAO oraz Ethereum wskazała jednak, że większość użytkowników blockchaina Ethereum oczekuje przeciwdziałania skutkom ataku poprzez taką zmianę aktualnego stanu blockchaina, która umożliwi im odzyskanie zainwestowanych w The DAO ETH. Projekt The DAO okazał się porażką.

Równocześnie grupa „dobrych hakerów”, wykorzystując tę samą funkcję splitu co twórca Dark DAO, wyprowadziła pozostałe po ataku 2/3 ETH z The DAO do White DAO (nowego DAO pochodnego), aby uniemożliwić kolejne ataki.

Hard fork

Ostatecznie uzgodniono, że 20 lipca przeprowadzony zostanie „hard fork” na blockchainie Ethereum. Scenariusz tego „hard fork” polegał na stworzeniu nowego blockchaina, zawierającego modyfikację w odniesieniu do The DAO. Aby zmiana była skuteczna, musiała zostać zaakceptowana przez użytkowników blockchaina. Wprowadzona w zakresie The DAO modyfikacja miała polegać na stworzeniu kontraktu zwrotu ETH wszystkim posiadaczom tokenów The DAO (tak jakby Dark

DAO i White DAO nigdy nie powstały). Scenariusz „hard fork” dawał posiadaczom tokenów The DAO gwarancję odzyskania zainwestowanych środków, ale niósł za sobą ryzyko rozszczępienia sieci Ethereum na dwie odrębne sieci: użytkownicy, którzy do nie przystąpiliby do hard forku, pozostaliby w oryginalnym blockchainie Ethereum.

Hard fork został przeprowadzony w uzgodnionym terminie i przystąpiło do niego ponad 90% użytkowników. Kontrakt zwrotu ETH określał kurs 100 tokenów The DAO za 1 ETH. W ciągu kilku godzin po przeprowadzeniu hard forku 41% środków zostało zwróconych inwestorom (w ciągu miesiąca wycofano w sumie ok. 80% środków). Wydawać się mogło, że oryginalny blockchain, mimo że ułamek społeczności postanowił go utrzymać, „umrze”, ponieważ znajdująca się tam kryptowaluta będzie niewymienialna.

Jednakże, wbrew wcześniejszym deklaracjom, jedna z giełd kryptowalut, a w jej ślad kolejne, postanowiły dopuścić do obrotu ethery z oryginalnego blockchajna, pod nazwą ETC (nazwa ETH przeszła na nowy blockchain). Okazało się więc, że użytkownicy nowego blockchajna posiadają nie tylko ETH, ale również odpowiadające im ETC na starym blockchainie, które, chociaż mniej warte niż ETH, nie są bezwartościowe.

Zagadnienia prawne

Na stronie internetowej daohub.org przedstawione zostały reguły dotyczące projektu, wyłączenia odpowiedzialności oraz rozmaite zastrzeżenia. Podstawowym założeniem było to, że zasady działania The DAO oparte są o kod inteligentnych kontraktów w blockchainie Ethereum. Podkreślono również, że kod inteligentnych kontraktów The DAO oraz wytworzone tokeny implikują znaczne ryzyko finan-

sowe, w tym związane z użyciem eksperymentalnego oprogramowania. Zastrzeżono, że tokeny The DAO nie reprezentują akcji, udziałów ani ich odpowiedników w odniesieniu do żadnej spółki, korporacji lub innego podmiotu, w jakiegokolwiek jurysdykcji, a także że przedstawione dokumenty nie stanowią prospektu ani wezwania do inwestycji, jak też nie stanowią oferty nabycia papierów wartościowych w żadnej jurysdykcji.

Akceptacja przedstawionych zasad działania The DAO skutkowałą między innymi zrzeczeniem się prawa do wnoszenia pozwów zbiorowych lub wszczynania arbitrażu przeciwko jakiegokolwiek podmiotowi zaangażowanemu w stworzenie the DAO. Oznaczała akceptację eksperymentalnego charakteru The DAO oraz ryzyk związanych z testowaną platformą Ethereum.

Przeprowadzony na The DAO atak oraz działania mające na celu zapobieżenie wyprowadzeniu zebranych środków zrewidowały pogląd o obiektywnej, niefałszowalnej i niepodlegającej kontroli instytucjonalnej prawdzie blockchajna. Wbrew pierwotnym założeniom twórców projektu o regulach jego działania nie decydował wyłącznie kod (który zawierał nieprzewidzianą właściwość w funkcji splitu), ale również ogólnie uznane przez uczestników projektu normy dotyczące uczciwości kontraktowej. Inaczej rzecz ujmując, większość uczestników projektu była przekonana o nieprawidłowości obiektywnej prawdy przedstawionej na blockchainie i postanowiła ją zmienić, wprowadzając i akceptując hard fork. Tylko w świetle tego powszechnego przekonania można mówić o różnicy w ocenie działań hakera, który utworzył Dark DAO, i hakerów, którzy utworzyli White DAO, albowiem z punktu widzenia kodu działania te mają taki sam charakter.

Można stwierdzić, że wbrew założeniom dotyczącym autonomii blockchaina w historii The DAO wystąpiła społeczna kontrola i korekta stanu nieakceptowanego przez zdecydowaną większość uczestników. Zasadzie obiektywnej prawdy kodu przeciwstawiła się więc pewna ogólnie uznana norma i to ona przeważała.

Działania twórców projektu, pomimo wyłączeń odpowiedzialności i zastrzeżeń zawartych w założeniach projektu, zdecydowanie zmierzają do zwrotu środków wniesionych do The DAO. Podjęto czynności mające na celu zaspokojenie tych inwestorów, którzy ze względu na zmianę ceny tokena w odniesieniu do ETH w okresie kreacji The DAO są pokrzywdzeni kursem zwrotu (problem „extra balance”). Podjęto również działania na rzecz tych, którzy dokonali splitu do DAO pochodnego i spalili swoje tokeny the DAO, zanim został przeprowadzony atak i powstały Dark DAO i White DAO.

Paradoksem jest, że mimo wszystko utrzymany został oryginalny blockchain, co powoduje istnienie dwóch alternatywnych rzeczywistości. Sytuacja ta rodzi różne kontrowersje,

w tym kontrowersje prawne związane ze sposobem zwrotu inwestorom utrzymanych na tym blockchainie ETC. Wątpliwości budzi także sposób postępowania giełd kryptowaluty, które pomimo uprzednich zapewnień postanowiły handlować ETC, co utrzymało przy życiu oryginalny blockchain. Wymienialność ETC powoduje mniejszą wartość ETH, potencjalnie więc inwestorzy mogą formułować roszczenia wobec tych giełd.

Ponieważ jednak The DAO była podmiotem sui generis oraz bytem wyłącznie cyfrowym, nie istniało i nie istnieje prawo, które regulowałoby sposób postępowania w odniesieniu do pojawiających się w odniesieniu do niej problemów prawnych. Zasadniczo mogliśmy zaobserwować proces samoregulacji zgodnie z ogólnymi zasadami sprawiedliwości i uczciwości kontraktowej. Być może w ogóle nie ma możliwości uregulowania takiego fenomenu i to, co się wydarzyło, wskazuje, że społeczność poradziła sobie, stosując ogólnie uznane metanormy.



Będziemy uzupełniać istniejącą strukturę

Rozmowa z Julianem Zawistowskim, przedsiębiorcą i liderem Projektu Golem

J.Cz.: Czym jest projekt Golem?

Julian Zawistowski: W ramach projektu tworzymy oprogramowanie umożliwiające wykonywanie obliczeń rozproszonych w sieci P2P. Założenie jest takie, że każdy użytkownik łączący się z siecią może wysłać do niej zadania

obliczeniowe, które są wykonywane przez innych użytkowników. Oczywiście za taką usługę wysyłający musi zapłacić wykonującym obliczenia.

Charakterystyczną cechą sieci P2P jest to, że odbywa się ona bez tzw. punktów centralnych

– relacje między poszczególnymi uczestnikami systemu są bezpośrednie, nie występuje między nimi pośrednik, który np. regulowałby rynek, skupował i odsprzedawał moc obliczeniową. Fakt, że system jest całkowicie zdecentralizowany, daje niesamowite możliwości techniczne, rodzi też jednak bardzo poważne wyzwania.

Jaką rolę w projekcie pełni Ethereum?

Ethereum wykorzystywane jest jako warstwa transakcyjna. System zdecentralizowany z oczywistych względów powinien używać zdecentralizowanego systemu płatniczego: trudno mówić, że coś jest zdecentralizowane, niezależne od awarii centralnego węzła, jeśli jednocześnie transakcje rozliczane są np. kartami kredytowymi czy przelewami. To w naturalny sposób wskazuje, że w Golemie transakcje powinny być wykonywane za pomocą kryptowalut. Z pośród nich Ethereum jest najlepszym wyborem ze względu na szereg cech umożliwiających budowę znacznie bardziej wyrafinowanego rozwiązania, niż ma to miejsce w wypadku innych technologii blockchainowych.

Na potrzeby projektu wykorzystujecie inteligentne kontrakty tworzone w oparciu o Ethereum. Jakie możliwości dają Wam takie kontrakty?

Po pierwsze, pozwalają one zbudować dość złożony system transakcyjny. Transakcja nie musi polegać na prostym przesłaniu środków z konta na konto. Dzięki kontraktom można system znacznie rozwinąć, np. grupując transakcje i rozliczając je w większych grupach, czy nawet wprowadzając bardziej wyrafinowane rozwiązania, jak tzw. kanały płatności czy noplątności probabilistyczne. Nie wchodząc w szczegóły tych rozwiązań, umożliwiają one znaczne obniżenie kosztów transakcyjnych do poziomu, w którym możliwe jest wykonywanie

bardzo wielu transakcji o bardzo małej wartości.

Po drugie, kontrakty dają nam sporą elastyczność w wyborze modelu płatności w sieci Golem. Ma to szczególne znaczenie dla twórców oprogramowania, którzy decydując się na integrację z Golemem, będą mogli zdefiniować własny model opłat za korzystanie z ich oprogramowania.

Po trzecie, kontrakty zamierzamy wykorzystywać w rozwiązaniach z zakresu reputacji i identyfikacji – co jest w rozproszonym systemie kluczowe dla prawidłowego funkcjonowania sieci, z definicji nieposiadającej nadrzędnego moderatora, który mógłby np. usuwać z sieci użytkowników podejmujących szkodliwe działania.

Warto podkreślić, że nie będziemy musieli sami tworzyć wszystkich komponentów – społeczność Ethereum jest bardzo aktywna i w oparciu o tę technologię powstaje bardzo wiele projektów, z których będziemy mogli w przyszłości korzystać.

Czy myśleliście o użyciu DAO?

Tak, myśleliśmy. Jednak upadek The DAO jasno pokazał, że Ethereum jeszcze nie jest gotowe na tak złożone rozwiązania.

Przed upadkiem The DAO zamierzaliście skorzystać ze zgromadzonych tam środków. Czy Waszym zdaniem niepowodzenie tego projektu wpłynie na rozwój innych DAO?

Na pewno, chociaż warto pamiętać, że funkcjonują dwa projekty oparte na zbliżonych do The DAO założeniach (Maker i Digix), które póki co jak się zdaje radzą sobie na gruncie technologii. Niemniej DAO uzmysłowilo wszystkim, że Ethereum, a w szczególności wykorzystywany w nim język programowania Solidity, są znacznie trudniejsze w użyciu –

w tym zwłaszcza w pełni bezpiecznym użyciu – niż się z pozoru wydaje. Sądzę, że póki ten problem nie zostanie rozwiązany, tworzenie tak złożonych i autonomicznych struktur jak The DAO jest zbyt ryzykowne.

Tworzycie zatem zdecentralizowany rynek mocy obliczeniowej wraz z warstwą transakcyjną, która dzięki Ethereum i inteligentnym kontraktom również jest zdecentralizowana. Czy Waszym zdaniem takie rozwiązania będą zastępować obecnie istniejące struktury i modele biznesowe?

My będziemy raczej uzupełniać istniejące struktury, zmieniając do pewnego stopnia ich model biznesowy w zakresie pozyskiwania i utrzymywania klientów. Nie sądzą, by było

możliwe masowe zastąpienie profesjonalnych centrów obliczeniowych przez komputery indywidualne. Są pewne klasy zastosowań, dla których zwykły komputer będzie konkurencyjny do centrum obliczeniowego, jednak w większości wypadków to rozwiązania profesjonalne będą mieć przewagę jakości i ceny. To, co chcemy osiągnąć, to stworzenie efektywnego (bliskiego konkurencji doskonałej) rynku mocy obliczeniowej, zintegrowanego z rynkiem wykorzystującego tę moc oprogramowania.

Rozmawiał Jacek Czarnecki

Co prawodawca i regulator powinien zrobić z DAO

Jacek Czarnecki

Inteligentne kontrakty i DAO bez dwóch zdań stwarzają wiele wątpliwości prawnych. Wyzwań, które się z nimi wiążą, nie da się jednak rozwiązać wyłącznie interpretacjami prawnymi, nawet bardzo odważnymi i kreatywnymi.

Potrzebna jest przemyślana polityka publiczna, która pozwoli czerpać korzyści z tych innowacji, jednocześnie minimalizując ryzyka. Jej skuteczne zaplanowanie i wdrożenie to także sposób na budowanie przewag konkurencyjnych w obszarze, który – podobnie jak internet w latach 90. ubiegłego stulecia – dopiero się kształtuje i tworzy.

Istnieje wiele działań, które instytucje publiczne (przede wszystkim prawodawca i regulatorzy) mogą podjąć w celu stworzenia ram dla DAO. Poniżej podajemy przykłady takich działań, wraz ze wskazówkami, czego należy unikać.

Aktywne działania zamiast bezczynności

Innowacyjność inteligentnych kontraktów i DAO, a także wczesny etap ich rozwoju, mogą skłaniać instytucje publiczne do przyjęcia pozycji obserwatora. Wiele osób uważa, że państwo nie powinno ingerować w nowe zjawiska, tylko uważnie przyglądać się rozwojowi sytuacji.

To podejście ma swoje dobre strony. Z pewnością w wielu przypadkach brak ingerencji władz publicznych nie krępuje niepotrzebnie rozwoju nowych technologii, a realna potrzeba wprowadzenia regulacji i tak powstaje na późniejszym etapie.

Brak ingerencji nie może jednak oznaczać bezczynności. Szybki rozwój publicznych blockchainów takich jak Ethereum pokazał, że nawet pasywne obserwowanie i zrozumienie zachodzących zjawisk wymaga podjęcia wysiłku. Instytucje publiczne powinny zatem na bieżąco analizować rozwój DAO.

Jednak nawet ciągła praca analityczna może okazać się niewystarczająca. Potrzebne jest podjęcie dialogu z podmiotami, które tworzą rozwiązania oparte na publicznych blockchainach (takie jak inteligentne kontrakty czy DAO) oraz specjalizują się w tej tematyce. Zamiast biernej obserwacji niezbędna jest więc aktywna współpraca.

Może ona polegać np. na finansowaniu badań naukowych oraz wdrożeń albo organizowaniu przez instytucje publiczne konsultacji. Inne rozwiązania sygnalizujemy poniżej.

Rozwiązania możliwe już teraz

Z perspektywy prawniczej inteligentne kontrakty i DAO są wyzwaniem dla fundamentalnych pojęć i instytucji prawnych, takich jak jurysdykcja czy osobowość prawna. Ich zastosowania mogą być zaś alternatywą dla istniejących modeli biznesowych czy struktur społecznych i ekonomicznych.

Choć w dłuższej perspektywie prawo będzie zmuszone zmierzyć się z tymi kwestiami, w krótkiej perspektywie możliwe jest tworzenie prostych rozwiązań, które pozwolą DAO na rozwój przy zachowaniu kontroli ze strony instytucji publicznych.

W niektórych jurysdykcjach są już tworzone modele strukturyzacji DAO, które zapewniają pewność, wygodę i bezpieczeństwo ich twórcom, a jednocześnie eliminują obawy sektora publicznego. Możliwe jest np. powiązanie tworzonych DAO z tradycyjnym podmiotem prawnym, np. spółką lub fundacją. Zapewnia to związanie DAO z daną jurysdykcją oraz

rozpoznawaniem przez prawo podmiotem prawnym, co ma kluczowe znaczenie np. w rozstrzygnięciu kwestii podatkowych. Choć w świetle szybkiego rozwoju technologii jest to zapewne rozwiązanie tymczasowe, może być ono bardzo skuteczne.

Co istotne, do kreowania takich rozwiązań nie muszą być potrzebne zmiany w prawie. Ważne jest zapewnienie bezpieczeństwa prawnego i podatkowego podmiotom, które angażują się w dane DAO, takim jak twórcy czy osoby wspierające dany projekt poprzez udział w ICO (na temat ICO piszemy w tekście na str. 42). Chodzi o wykreowanie sytuacji, w której te osoby będą mogły zajmować się tworzeniem innowacyjnych rozwiązań w rodzaju DAO bez potrzeby sprawdzania na każdym kroku ryzyk regulacyjnych, które się z nimi wiążą (i nierzadko wynikają wyłącznie z nowatorskości tych przedsięwzięć).

Instytucje publiczne nie powinny zapominać, że tworzenie atrakcyjnych rozwiązań dla DAO i podobnych innowacji jest korzystne nie tylko dla ich twórców. W ten sposób państwo może efektywnie wesprzeć tworzenie innowacji w obszarze, w którym dopiero wylaniają się pierwsi liderzy.

Do tworzenia rozwiązań prawnych i regulacyjnych dla DAO i podobnych twórców bardzo przydatne może okazać się narzędzie w postaci tzw. „regulacyjnej piaskownicy” (*regulatory sandbox*). Taka piaskownica jest tworzona pod patronatem regulatora, który pozwala określonym podmiotom testować innowacyjne usługi lub produkty na rynku pod swoją kontrolą i zgodnie z określonymi warunkami, ale jednocześnie bez konieczności spełniania standardowych wymogów regulacyjnych (np. uzyskania określonej licencji).

Sandboksy regulacyjne stają się popularne przede wszystkim w odniesieniu do branży

technologii finansowych (fintech). Tego typu rozwiązanie mogłoby równie dobrze służyć bezpiecznemu wprowadzaniu na rynek innowacji w rodzaju DAO.

Potrzebne odważne środki: osobowość prawna na żądanie

Choć już skuteczne wdrożenie wskazanych rozwiązań byłoby sukcesem, wobec wyzwań, jakie stawiają przed nami struktury w rodzaju DAO, wciąż są to środki doraźne. Stanowią one kładkę łączącą tradycyjny, analogowy świat prawa z rozproszoną przestrzenią cyfrową, jednak prędzej czy później zaistnieje potrzeba zbudowania trwałych mostów.

Przykładowym rozwiązaniem mogłaby być osobowość prawna na żądanie. Prawo mogłoby przewidywać przyznanie DAO osobowości prawnej (oraz związanych z nią przymiotów zdolności sądowej czy ograniczonej odpowiedzialności) nie jedynie w drodze wpisu do rejestru, ale np. po spełnieniu określonych kryteriów czy na wniosek uprawnionych osób.

Taka quasi-osobowość prawna mogłaby pełnić różne role. Przede wszystkim chodzi o rozpoznanie istnienia DAO jako osobnego bytu w sytuacjach krytycznych, takich jak powstanie obowiązku podatkowego, spór pomiędzy DAO a innym podmiotem czy powstanie szkody (spowodowanej lub poniesionej przez DAO).

To rozwiązanie jest oczywiście trudne do wyobrażenia w tradycyjnym paradygmacie prawa. Wyzwania w rodzaju DAO sprawiają jednak, że powinniśmy zacząć przyzwyczajać się do

potrzeby używania niestandardowych środków.

Czego unikać?

Wprowadzane zmiany powinny opierać się na gruntownym zrozumieniu technologicznych podstaw oraz praktyki funkcjonowania innowacji takich jak inteligentne kontrakty i DAO. Przykładowo, obecnie za błąd uznalibyśmy próbę uregulowania platform, na których takie rozwiązania są tworzone – czyli przede wszystkim publicznych blockchainów takich jak Ethereum. Właściwa natomiast mogłaby być regulacja struktur tworzonych na ich podstawie.

Podobnie należy unikać pochopnej regulacji sektorowej. Na przykład ewentualne stosowanie do Bitcoina i innych kryptowalut danych przepisów (np. dotyczących usług płatniczych czy pieniądza elektronicznego) może spowodować, że te przepisy będziemy zmuszeni stosować do innych tokenów cyfrowych funkcjonujących na publicznych blockchainach (np. wydanych na potrzeby DAO) o zbliżonej charakterystyce technicznej, ale niepełniących funkcji pieniądza.

Z DAO wiąże się wiele problemów prawnych. Dla instytucji publicznych stanowi to jednak nie tylko szereg wyzwań, ale także liczne szanse, np. na przyspieszenie postępu cyfrowego czy rozwój innowacyjności gospodarki. Aby z nich skorzystać, potrzebne są aktywne i przemyślane działania.



DAO a podatki – wybrane zagadnienia

Joanna Prokurat

„Przedmiot podatku ma najistotniejsze znaczenie w ekonomicznej koncepcji podatku. To, od czego ma być płacony podatek, jest zarazem dowodem wyobraźni i wiedzy ustawodawcy co do możliwości uzyskania dochodów budżetowych, jak i stopnia rozwoju prawa podatkowego”¹. Nie tylko z perspektywy przedmiotu podatku, ale również innych jego elementów konstrukcyjnych, DAO może być arcytrudnym testem tak dla wiedzy, jak i wyobraźni ustawodawcy kreującego prawo podatkowe oraz wykonujących je organów.

System podatkowy zasadniczo charakteryzuje się powszechnością opodatkowania i tylko wyjątkowo pozostawia jakieś zdarzenia lub podmioty poza zakresem swojego zainteresowania. Będąc systemem abstrakcyjnym, przedmiotu opodatkowania zwykle upatruje w niemal każdym zdarzeniu kreującym określoną wartość, dla celów podatku dochodowego zwaną zasadniczo przysporzeniem, a dla celów podatku od towarów i usług – wartością dodaną. Z kolei podmiotem opodatkowania jest generalnie każdy podmiot, niezależnie od jego formy prawnej, z tym że zobowiązanie podatkowe może zostać przypisane w zależności od dodatkowych czynników, takich jak rezydencja podatkowa (na gruncie podatków dochodowych) czy status przedsiębiorcy i charakter świadczenia (dla celów podatku od towarów i usług). DAO, mogąc skutkować profitami w wymiarze ekonomiczno-finansowym, również może wiązać się z obowiązkiem podatkowym. Z pewnością taki rezultat jest przedmiotem zainteresowania fiskusa działającego w interesie maksymalizacji wpływów budżetowych.

W przypadku DAO – podmiotów nowatorskich i wylamujących się utartym schematom – tak sformułowane zadanie organów podatkowych może jednak napotykać liczne trudno-

ści. Mimo że wirtualna rzeczywistość nie stanowi zupełnego *novum* i od pewnego czasu stawia kolejne wyzwania również aparatowi skarbowemu (czego przykładem jest chociażby internet), DAO wydaje się tworzyć zupełnie nowy paradygmat nie tylko techniki, lecz również ekonomii i prawa, w tym w zakresie zobowiązań publicznoprawnych. Techniczne aspekty DAO rozumie aktualnie bardzo wąska grupa osób; na gruncie podatków może być ono niezrozumiałe dla nikogo. Tym trudniej jest przełożyć DAO na język elementów konstrukcyjnych podatków, tworzonych na początku lat 90., kiedy hasła takie jak blockchain, DAO, sztuczna inteligencja czy choćby powszechny dziś internet były właściwie tak samo abstrakcyjne jak podróże międzygalaktyczne.

Przede wszystkim DAO – zdecentralizowana organizacja autonomiczna – nie stanowi podmiotu znanego dotychczas systemowi podatkowemu. Ten oczywiście, nie będąc kazuistycznym, nie zamyka się na nowe formy prowadzenia działalności, inwestowania czy innych aktywności oraz osiągnięcia (z tego tytułu) przychodów (zysków). Można zresztą upatrywać w DAO znanej już systemowi podatkowemu, w szczególności podatkowi dochodowemu, konstrukcji wspólnego przedsięwzięcia.

¹ W. Modzelewski (red.), Wstęp do nauki prawa podatkowego, Warszawa 2005

Przypomnijmy, że wspólne przedsięwzięcie nie stanowi samo w sobie podatnika podatku dochodowego, gdyż podatnikami tego podatku są uczestnicy takiego wspólnego przedsięwzięcia. Są oni zobowiązani do deklarowania przychodów (przepisy dotyczące podatku dochodowego od osób fizycznych wyodrębniają dziesięć źródeł przychodów podlegających innym zasadom rozliczeń – jako pochodzących ze źródła „działalność gospodarcza”), kosztów i innych kategorii podatkowych ze wspólnego przedsięwzięcia proporcjonalnie do ustalonego udziału w zyskach (lub w równych częściach, jeśli takiego udziału nie ustalono). Potencjalnie zatem DAO można kwalifikować jako wspólne przedsięwzięcie w rozumieniu przepisów prawa podatkowego.

Taka kwalifikacja nie powinna godzić w możliwe zróżnicowane zaangażowanie poszczególnych podmiotów w podejmowane w ramach DAO procesy decyzyjne lub uprawnienia majątkowe. Taki sposób podatkowego ujęcia DAO zbliża je do spółki nieposiadającej osobowości prawnej (innej niż spółka komandytowo-akcyjna), która również nie jest podatnikiem podatku dochodowego, ale której przychody, koszty i inne generowane przez nią kategorie podatkowe są alokowane do jej wspólników (o ile sami nie pozostają oni transparentni do celów podatku dochodowego).

Takie traktowanie DAO może jednak nie być uniwersalne. Przykładowo DAO może nie być przedsięwzięciem o charakterze gospodarczym lub zarobkowym, a wydaje się, że tylko takie przedsięwzięcia są aktualnie traktowane jako ww. wspólne przedsięwzięcia w rozumieniu przepisów prawa podatkowego.

Ujęcie DAO jako wspólnego przedsięwzięcia może również nie być spójne z koncepcją przedmiotu opodatkowania i nie odpowiadać potencjalnym transferom w ramach DAO. Transfery te mogą mieć różnoraki charakter –

od takich, które nazwalibyśmy technicznymi (np. przyłączenie do innego DAO), po faktycznie finansowo-ekonomiczne (np. zbycie „praw” do DAO). Spoglądając przez pryzmat aktualnie obowiązujących regulacji, ujednolicone traktowanie DAO może prowadzić do wewnętrznej konkurencji w ramach systemu podatkowego, szczególnie w ramach podatku dochodowego od osób fizycznych, gdzie – jak wspomniano – wyróżnia się dziesięć źródeł przychodów. Ujęcie DAO jako podatkowego wspólnego przedsięwzięcia implikuje bowiem jego opodatkowanie w ramach źródła przychodów „działalność gospodarcza”, podczas gdy dane DAO może mieć charakter właściwie czysto inwestycyjny czy wręcz stanowić internetową spółkę odpowiadającą znanej spółce akcyjnej (przy czym nie chodzi o spółkę akcyjną tworzoną w internecie, ale o nową formułę spółki opartej na DAO).

Na marginesie można wspomnieć, że traktowanie DAO jako podatkowego wspólnego przedsięwzięcia może nie leżeć w interesie jego uczestników (jakkolwiek interes ten niekoniecznie będzie stanowił argument dla fiskusa realizującego określone zadania budżetowe). Przykładowo uczestnicy DAO o charakterze *non-profit* mogliby chcieć skorzystać ze zwolnienia od podatku dochodowego dla organizacji realizujących społecznie pożyteczne cele określone przez ustawodawcę podatkowego.

Ponadto kwalifikacja DAO jako wspólnego przedsięwzięcia (a także, jak się wydaje, każda inna znana dotychczas prawu podatkowemu kwalifikacja podmiotowa DAO) nie odpowiada na pytanie, jak przełamać wpisaną w DAO anonimowość jego uczestników. Sama w sobie może ona stanowić pokusę dla podmiotów chcących unikać opodatkowania. Trzeba jednak pamiętać, że aparat skarbowy dysponuje instrumentami sankcyjnymi, np. możliwością opodatkowania przychodów

(dochodów) pochodzących z nieujawnionych źródeł, chociażby z DAO, stawką 75% podatku dochodowego (oczywiście pozostaje jeszcze kwestia identyfikacji podmiotu zobowiązanego i egzekucji zobowiązań podatkowych).

Na wcześniejszym etapie anonimowość DAO – w połączeniu z jego transgranicznym zasięgiem – może natomiast co najmniej utrudniać alokację ewentualnych przychodów (zysków) do poszczególnych jurysdykcji. Na gruncie podatku dochodowego, nie udzielając odpowiedzi na pytanie o rezydencję podatkową uprawnionego podmiotu, *de facto* DAO nie pozwala również na przypisanie przychodów (zysków) do danego kraju na podstawie zasady miejsca źródła tego przychodu (zysku). Może to powodować konflikty między krajami, którym uda się zidentyfikować przychód (zysk) z DAO i przypisać go do swojej jurysdykcji, powodując podwójne lub nawet wielokrotne opodatkowanie tego samego przychodu (zysku). Natomiast na gruncie podatku od towarów i usług brak identyfikacji uczestników DAO, a zatem również ich statusu jako podatników tego podatku czy ich miejsca siedziby lub stałego miejsca prowadzenia działalności, nie pozwala na ustalenie charakteru operacji jako B2B albo B2C, co może mieć kolosalne znaczenie dla ustalenia miejsca świadczenia, a zatem miejsca opodatkowania tym podatkiem, jak i podmiotu zobowiązanego.

Wreszcie wyzwanie w zakresie ustalenia kręgu podmiotów zobowiązanych może stanowić natura DAO i zmienność jego uczestników, których krąg może nawet wielokrotnie zmieniać się w ciągu na przykład doby.

Równie trudnym sprawdzianem, tak dla fiskusa, jak i samych podatników, może być dokumentowanie i ewidencjonowanie zdarzeń podatkowych związanych z DAO.

Powyżej wskazano jedynie wybrane i bardzo ogólne przykłady zagadnień, z którymi mogą zetknąć się z jednej strony podatnicy angażujący się w projekty typu DAO, a z drugiej strony przedstawiciele fiskusa. Interwencja ustawodawcy podatkowego na tym etapie wydaje się przedwczesna, m.in. z uwagi na brak odpowiedniej wiedzy o samym DAO i jego mechanizmach, co może realnie grozić brakiem adekwatnych regulacji. Interwencji takiej nie należy jednak wykluczać w przyszłości. Pewne działania mógłby za to podjąć aparat wykładający prawo podatkowe, np. wydając ogólną interpretację prawa podatkowego. Nie tylko ułatwiłoby to prawidłowe rozliczanie podatków przez podmioty zaangażowane w DAO (uznane za podatników z tego tytułu w Polsce), ale mogłoby – przy odpowiedniej i klarownej konstrukcji – stanowić zachętę dla zagranicznych graczy do opodatkowania z tego tytułu w Polsce. Nie należy też wykluczać, że to fiskus mógłby stworzyć obowiązkowe dla wszystkich DAO lub przystępować do kolejnych DAO. Dzięki temu mógłby pozyskać wiedzę, a nawet wpływ na przebiegające tam procesy. W grę wchodzić może nawet automatyczne rozliczenie podatku. Pomysł ten nie wydaje się większą abstrakcją niż samo DAO.



DAO a prawo karne

Krzysztof Wojdyło

Działanie danego DAO lub inteligentnego kontraktu może okazać się sprzeczne z przepisami prawa obowiązującymi w określonej jurysdykcji. Jak w takich sytuacjach będą stosowane przepisy prawa karnego? Kto ryzykuje w takim przypadku odpowiedzialnością karną?

Prawo karne w dobie internetu

Bardzo dynamiczny rozwój cyberprzestępczości, odnotowywany szczególnie w ostatnich latach, uwidacznia niedoskonałości współczesnego systemu prawa karnego. Przestępstwa w cyberprzestrzeni są często znacznie trudniejsze do wykrycia, mają też często międzynarodowy charakter. To właśnie ta ostatnia okoliczność jest źródłem największych problemów prawnych.

Przestępstwa dokonywane są w cyberprzestrzeni, a więc w autonomicznej przestrzeni wirtualnej, którą trudno z góry przypisać do określonej jurysdykcji. Zastosowanie prawa karnego wymaga tymczasem przypisania danego przestępstwa do określonej jurysdykcji (choćby po to, aby rozstrzygnąć, czy dany czyn jest rzeczywiście karalny, a jeżeli tak, to na jakich zasadach ponoszona jest odpowiedzialność karna). W efekcie regułą w przypadku cyberprzestępstw jest ocena danego przestępstwa równoległe przez pryzmat wielu jurysdykcji, co powoduje znaczącą niepewność u podmiotów prowadzących działalność w internecie.

W obliczu swoistej konkurencji porządków prawnych kluczowe staje się ustalenie kryteriów, które umożliwiają ostateczny wybór jurysdykcji. Przepisy poszczególnych państw różnie określają te kryteria. Jednym z najpopularniejszych kryteriów jest kryterium miejsca popełnienia przestępstwa. Stosuje je również

polski Kodeks karny, który rozstrzyga, że polskie przepisy prawa karnego stosuje się do sprawcy, który popełnił czyn zabroniony na terytorium Rzeczypospolitej Polskiej, jak również na polskim statku wodnym lub powietrznym. Jednocześnie przepisy rozstrzygają, że czyn zabroniony uważa się za popełniony w miejscu, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, albo gdzie skutek stanowiący znamię czynu zabronionego nastąpił lub według zamiaru sprawcy miał nastąpić. Problem polega na tym, że analogiczne przepisy znajdują się w systemach prawnych wielu państw, co w związku z naturą przestępstw internetowych nie eliminuje bynajmniej kolizji jurysdykcji.

Przykładowo portal internetowy świadczący nielegalne usługi może popełniać przestępstwo w państwie, w którym znajduje się infrastruktura tego portalu, ale również w państwie, w którym przebywa osoba korzystająca z portalu. Jeżeli bowiem jednym z kryteriów popełnienia przestępstwa jest wystąpienie skutków tego przestępstwa na terytorium danego państwa, to do popełnienia przestępstwa na terytorium tego państwa nie jest konieczne działanie lub przebywanie sprawcy przestępstwa na jego terytorium.

Powyższe zasady mogą skutkować jeszcze innym efektem, który poważnie utrudnia prowadzenie działalności w internecie. Łatwo można wyobrazić sobie sytuację, w której określona

działalność prowadzona w internecie jest legalna w państwie, w którym zarejestrowany jest operator portalu lub w którym znajduje się infrastruktura techniczna portalu, ale jest nielegalna w państwach, z których pochodzą niektórzy użytkownicy portalu. Operator portalu nadal będzie mógł więc ponosić odpowiedzialność karną według przepisów państw, w których znajdują się odbiorcy portalu, nawet jeżeli w państwie, w którym portal jest zarejestrowany, dana działalność jest legalna.

W takim przypadku powstaje jeszcze trudność z faktycznym pociągnięciem do odpowiedzialności sprawcy przestępstwa, zwłaszcza jeżeli przebywa on w państwie, które nie uznaje danego zachowania za przestępstwo. Ewentualne wydanie sprawcy innemu państwu jest w takich przypadkach regulowane umowami międzynarodowymi. Nieco inaczej jest w przypadku, w którym sprawca posiada jakieś aktywa w państwie, w którym jego zachowanie podlega karze. W takim przypadku sprawca musi liczyć się z ryzykiem sankcji wymierzonych w jego aktywa w danym państwie.

DAO w perspektywie zasad odpowiedzialności karnej

Powyższe trudności mają zastosowanie również w stosunku do DAO oraz inteligentnych kontraktów. W tym przypadku także może dochodzić do konkurencji między jurysdykcjami w zakresie prawnej kwalifikacji określonych działań. Wyobraźmy sobie DAO, które tworzy model zdecentralizowanego kasyna, w ramach którego poszczególni użytkownicy mogą zawierać kontrakty będące rodzajem gier hazardowych. W zależności od jurysdykcji działalność organizowana z wykorzystaniem takiego DAO może być dozwolona lub traktowana jako przestępstwo. Patrząc z tej perspektywy, DAO jest zbliżone do innych przedsięwzięć organizowanych w cyberprzestrzeni.

Niewątpliwym wyróżnikiem DAO w kontekście odpowiedzialności karnej są za to trudności z przypisaniem ewentualnej odpowiedzialności karnej konkretnemu podmiotowi. W bardziej tradycyjnych organizacjach za prowadzenie nielegalnej działalności mogą zasadniczo odpowiadać członkowie organów tych podmiotów. Konstrukcja wielu DAO nie przewiduje jednak istnienia żadnych organów. DAO jest autonomicznym algorytmem funkcjonującym w rozproszonej sieci. To właśnie algorytm, a nie konkretna osoba realizuje ewentualne znamiona czynu zabronionego. Tymczasem odpowiedzialność karną – zasadniczo – mogą ponosić osoby, a nie abstrakcyjne byty w postaci algorytmu. Wskazana właściwość DAO niewątpliwie utrudnia egzekucję przepisów prawa karnego. Wbrew pozorom nie czyni jej jednak całkowicie niemożliwą.

Kto odpowiada za DAO?

W związku z brakiem organów DAO oraz niemożliwością przypisania DAO zdolności prawnej oraz zdolności sądowej powstanie naturalna potrzeba poszukiwania innych podmiotów, które mogą potencjalnie ponosić odpowiedzialność za niezgodne z prawem działania realizowane z wykorzystaniem DAO.

Wróćmy na chwilę do przykładu z grami hazardowymi. Załóżmy, że w określonej jurysdykcji odpowiedni przepis prawa karnego rozstrzyga, że organizowanie gier hazardowych jest przestępstwem. Działaniem, które determinuje przestępstwo, jest w tym przypadku „organizowanie” gier. Tak rozumiane znamie czynu zabronionego wypełnia przede wszystkim działanie bezosobowego algorytmu. Należy mieć jednak na uwadze, że większość systemów prawa karnego rozpoznaje różne formy popełnienia przestępstwa. Odpowiedzialności karnej nie musi podlegać wyłącznie bezpośredni sprawca realizujący znamiona

czynu zabronionego. W tym kontekście szczególnie istotna wydaje się możliwość przypisania odpowiedzialności karnej pomocnikowi oraz osobie, która przygotowuje przestępstwo. Różne systemy prawne będą zapewne różnie definiować te role. Dla przykładu polski system prawa rozumie przez przygotowanie m.in. czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do dokonania przestępstwa. Z kolei pomocnictwo może polegać np. na dostarczeniu narzędzia ułatwiającego popełnienie przestępstwa.

Oczywiście pociągnięcie konkretnej osoby do odpowiedzialności z tytułu przygotowania lub pomocnictwa będzie wymagało spełnienia szeregu wymagań oraz będzie uzależnione od specyfiki określonego DAO. Nie można jednak z góry wykluczyć takiej możliwości. Mając na uwadze naturę DAO, należy przyjąć, że szczególnie narażeni na ewentualną odpowiedzialność mogą być twórcy algorytmów DAO oraz osoby zaangażowane w pełnienie roli wyroczni. W określonych sytuacjach nie można

też wykluczyć ewentualnej odpowiedzialności posiadaczy tokenów DAO oraz jego użytkowników.

Opierając się na obserwacjach związanych z pierwszymi DAO, można przyjąć, że szczególne ryzyka prawne mogą wiązać się z przeprowadzeniem ICO (patrz niżej). Gromadzenie środków na rozwój DAO oraz emisja ewentualnych tokenów może implikować konieczność stosowania przepisów o publicznym oferowaniu instrumentów finansowych. Nawet jeżeli osoby organizujące ICO funkcjonują w jurysdykcji, w której zbiórka jest dozwolona, nie można wykluczyć, że ICO zostanie uznane za przestępstwo w innych jurysdykcjach, w których dane ICO będzie dostępne. Na szczególną uwagę zasługują w tym zakresie restrykcyjne regulacje amerykańskiego rynku kapitałowego.

Prawne aspekty Initial Coin Offerings oraz Token Crowdsales

Jacek Czarnecki

Wiele projektów rozwijanych w oparciu o publiczne blockchaine, jak Bitcoin lub Ethereum, to fascynujące rozwiązania technologiczne. Jednym z aspektów ich rozwoju jest potrzeba pozyskania środków na ten cel. Ostatnie miesiące pokazują dynamiczny wzrost zainteresowania nowymi metodami pozyskiwania środków na rozwój projektów związanych z technologią blockchaina: *Initial Coin Offerings* (ICO), znane również jako *Coin* lub *Token Crowdsales*.

ICO

Twórcom projektów blockchainowych nie-rzadko najłatwiej pozyskać środki na ich rozwój w otoczeniu, które najlepiej rozumie rozwijane projekty czy usługi, a potencjalnie należy również do grona przyszłych klientów.

Nic zatem dziwnego, że wiele z takich projektów pozyskuje finansowanie w drodze ICO, czyli wydawania określonego (krypto)tokena na danym publicznym blockchainie (najczęściej Ethereum) i jego sprzedaży każdemu zainteresowanemu. Zbycie wyemitowanych tokenów następuje zazwyczaj za posiadające wymierną ekonomiczną wartość kryptowaluty: bitcoiny czy ethery (natywna jednostka sieci Ethereum).

ICO może zostać przeprowadzone zarówno przez DAO, jak i przez bardziej tradycyjne podmioty. Te ostatnie mogą prowadzić klasyczną działalność gospodarczą, nawet luźno związaną z technologią blockchaina. Cel ICO jest jednak uniwersalny: zdobycie środków finansowych na potrzeby rozwoju danego projektu.

Proces ICO może być o wiele łatwiejszy, tańszy i bardziej efektywny niż przeprowadzenie tradycyjnych działań na rzecz zebrania finansowania. O jego skuteczności niech świadczy przykład The DAO, gdzie w zamian za wydanie specjalnych tokenów The DAO pozyskało ethery o wartości ok. 150 milionów dolarów.

Kolejną zaletą ICO jest możliwość elastycznego ukształtowania cech sprzedawanego tokena. Może on mieć różne cechy.

1. **Uprawnienia decyzyjne.** Czasami token nabywany w drodze ICO niesie określone uprawnienia dla jego posiadacza, które nie mają charakteru ściśle finansowego. Może to być np. uprawnienie do głosowania (wiążącego lub nie) w sprawach ważnych

dla danego projektu, co zbliża je do uprawnień posiadanych przez wspólników w tradycyjnych spółkach. Nierzadko token odgrywa sporą rolę w rozwijanej w ramach danego projektu zdecentralizowanej aplikacji (Dapp) i może dawać posiadaczowi dostęp do usług czy produktów oferowanych w jej ramach.

2. **Quasi-instrumenty finansowe.** Charakterystyka niektórych tokenów sprawia, że pełnią one funkcje zbliżone do tradycyjnych instrumentów finansowych. Niektóre z tokenów mają charakter zbliżony do instrumentów udziałowych, ponieważ z ich posiadaniem wiąże się np. uprawnienie do partycypacji w przyszłych zyskach wygenerowanych przez projekt. Inne tokeny, czerpiąc z konstrukcji instrumentów dłużnych, dają prawo do zwrotu określonej wartości po spełnieniu się określonych warunków. Wiele z tokenów będzie miało charakter mieszany, czyli będzie łączyć niektóre cechy instrumentu finansowego z umożliwieniem dostępu do danych usług.
3. **Inne.** Wraz z rozwojem technologii blockchaina i podobnych rozwiązań możemy spodziewać się powstawania kolejnych rodzajów tokenów. Nierzadko intuicyjnie staramy się porównywać prawa wynikające z tokena z pieniądzem albo instrumentem finansowym, jak chociażby papier wartościowy. Mylące może być również samo pojęcie „token”, które sugeruje istnienie jakiegoś nośnika. Tymczasem tokeny są w zasadzie zapisami w bazie danych i mogą służyć do różnych celów. Mogą reprezentować bardzo różne rodzaje wartości. W praktyce nie jest zatem możliwe stworzenie wyczerpującego katalogu rodzajów tokenów.

Z punkty widzenia osoby biorącej udział w ICO istotny jest również potencjał inwestycyjny nabywanych tokenów. Tokeny mogą bowiem zazwyczaj podlegać obrotowi, np. na giełdach kryptowalut. Nierzadko ich kurs cechuje się wysoką zmiennością, co zachęca do działań spekulacyjnych.

Co więcej, udane projekty pozwalają osiągnąć wysoką stopę zwrotu z wirtualnej inwestycji. Przykładem może być ether, który w pierwszej fazie *Ether Sale* był zbywany po kursie 1 ETH / 0,0005 BTC, podczas gdy w połowie marca 2016 r. osiągnął kurs ok. 1 ETH / 0,0345 BTC. Oczywiście drugą stroną medalu jest nadzwyczajne ryzyko związane z inwestycjami w ICO.

Jak wynika z powyższych rozważań, tokeny zbywane w ramach ICO lub podobnej akcji mogą mieć bardzo różną charakterystykę. Możliwość kształtowania uprawnień wiążących się z posiadaniem danego tokena jest wręcz dowolna i zależy od umiejętnego posługiwania się kodem programistycznym. Sprawia to, że bardzo trudne staje się prawne ujęcie kolejnych faz życia tokena: wygenerowania, zbywania i posiadania tokenów.

Charakterystyka prawna tokenu

Próba zastosowania istniejących regulacji dotyczących publicznego obrotu instrumentami finansowymi do ICO będzie w dużej mierze uzależniona od odpowiedzi na pytanie, czy dany token ma cechy instrumentu finansowego zgodnie z obowiązującą definicją prawną.

Udzielenie takiej odpowiedzi będzie każdorazowo wymagało analizy szerokiego katalogu instrumentów finansowych zawartego w art. 2 ustawy o obrocie instrumentami finansowymi. O tym, jak trudne może okazać się to zadanie, może świadczyć próba ustalenia, czy prawa wynikające z tokena mogą być uznane za prawa wynikające z papierów wartościowych,

a co za tym idzie, czy token mógłby zostać uznany za jeden z rodzajów papierów wartościowych.

Na marginesie warto zauważyć, że token zazwyczaj zostanie uznany za prawo majątkowe. Kodeks cywilny posługuje się bardzo szerokim pojęciem praw majątkowych, uznając je w art. 44 za rodzaj mienia (obok własności). Nierzadko tokeny, jakkolwiek pozbawione substratu materialnego, będą posiadały określoną i wymierną wartość. Należałoby je zatem zakwalifikować jako rodzaj dobra niematerialnego, będącego mieniem w rozumieniu Kodeksu cywilnego oraz mogącego stanowić przedmiot stosunków cywilnoprawnych.

Punktem wyjścia do przeprowadzenia oceny statusu prawnego tokena będzie analiza ogólnych przepisów dotyczących papierów wartościowych w Kodeksie cywilnym. Na podstawie art. 921⁶ k.c. można stwierdzić, że papier wartościowy charakteryzuje się następującymi podstawowymi cechami:

- ma formę dokumentu,
- wynika z niego zobowiązanie danego dłużnika,
- jego posiadanie jest konieczne do skutecznego żądania wykonania zobowiązania przez dłużnika.

Odkładając na bok szczególną charakterystykę tych papierów wartościowych, które w oparciu o przepisy szczególne mogą posiadać formę zdematerializowaną, wydaje się, że przeszkodą do zakwalifikowania danego tokenu jako papieru wartościowego w powyższym rozumieniu będzie wymóg, aby papier wartościowy był w formie dokumentu. Od niedawna obowiązuje jednak w Kodeksie cywilnym definicja legalna dokumentu jako „nośnika informacji umożliwiającego zapoznanie się z jej treścią”. W związku z tym powstają wątpliwości, czy token – zazwyczaj zapis w rozproszonej bazie

danych – będzie mógł zostać uznany za taki nośnik informacji.

Kwestia, czy z tokena wynika zobowiązanie danego dłużnika oraz czy jego posiadanie jest konieczne do skutecznego żądania wykonania zobowiązania przez dłużnika, również będzie wywoływała szereg kontrowersji. Konstrukcja instytucji papieru wartościowego opiera się na relacji obligacyjnej pomiędzy różnymi podmiotami. Token nie zawsze będzie miał taki charakter.

Przepisy nie zawsze pozwolą definitywnie ustalić, czy dany token jest instrumentem finansowym. Nierzadko konieczna będzie podstawowa analiza na temat fundamentalnych przesłanek definicji danego instrumentu finansowego, co jednak nie gwarantuje osiągnięcia jednoznacznych wniosków. Wobec tego podmioty, które będą chciały przeprowadzić ICO, powinny mieć świadomość tych wątpliwości i uwzględnić w swych działaniach ewentualne ryzyka prawne z tym związane.

Zagadnienia prawne związane z ICO

Z prawnego punktu widzenia ICO wywołuje skojarzenia z bardziej (oferta publiczna papierów wartościowych) lub mniej (crowdfunding) tradycyjnymi metodami pozyskiwania finansowania przez podmioty gospodarcze. Ponieważ nie ma szczególnych regulacji prawnych dotyczących zbierania środków finansowych w drodze ICO, należy zastanawiać się nad ewentualnym stosowaniem instrumentów prawnych należących do różnych obszarów prawa.

Po pierwsze powstaje pytanie, czy o ICO oraz zbywaniu w ich ramach tokenów można mówić w kontekście regulacji prawnych dotyczących oferowania i obrotu instrumentami finansowymi. Nie bez powodu termin „ICO” nawiązuje do pojęcia „IPO” (*initial public offering*, pierwsza oferta publiczna). W praktyce ICO

wykazuje wiele podobieństw do pozyskiwania środków finansowych w drodze oferty publicznej instrumentów finansowych.

W toku stosowania regulacji obrotu instrumentami finansowymi należy mieć na uwadze specyfikę ICO. Te regulacje mają na celu między innymi zapewnić efektywność rynku. Służą temu liczne obowiązki informacyjne, którymi obciążone są podmioty działające w tym obszarze. Innym celem regulacji jest ochrona inwestora.

Specyfika ICO, zwłaszcza dokonywanego za pośrednictwem DAO, polega jednak często na jawności kodu będącego ich podstawą. Oznacza to, że kod programistyczny, który określa zasady przeprowadzenia ICO, a także sposób funkcjonowania zbywanych tokenów i uprawnień, jakie się z nimi wiążą, jest dostępny dla każdego zainteresowanego. W praktyce zatem potencjalny „inwestor” (nabywca tokenów) może z góry zweryfikować zasady przedsięwzięcia, w którym chce wziąć udział.

Z drugiej strony występuje bariera w postaci konieczności posiadania wiedzy technicznej w celu zrozumienia kodu. Powoduje to powstanie sytuacji, w której inwestor ma dostęp do wszelkich istotnych informacji, jednak może nie mieć możliwości ich sprawdzenia. Możemy mieć zatem do czynienia ze specyficzną asymetrią informacyjną. Podobne problemy stoją przed inwestorami dokonującymi inwestycji w skomplikowane strukturyzowane instrumenty finansowe, aczkolwiek w ich przypadku próbują przyjąć w sukurs regulacje rynku kapitałowego. Szczególny charakter ICO sprawia jednak, że powstaje konieczność weryfikacji roli, jakie pełnią obecne regulacje.

Po drugie można się zastanawiać, ile wspólnego ma ICO z pozyskiwaniem tradycyjnych środków pieniężnych poprzez fundusze inwe-

stycyjne. Tu znów można odwołać się do przykładu The DAO, którego rolą było w uproszczeniu zebranie puli środków oraz ich inwestowanie w określone projekty. Ten model określano jako „zdecentralizowany fundusz *venture capital*”.

Choć przykład The DAO automatycznie wywoływał skojarzenia z funduszami inwestycyjnymi, powstaje pytanie, czy przepisy ich dotyczące mogą znaleźć zastosowanie również w sytuacjach niekonwencjonalnego wirtualnego zbierania wartości majątkowych w celu ich dalszego wspólnego inwestowania. Ekonomiczne modele niektórych podmiotów inicjujących ICO będą powodowały powstawanie tego typu wątpliwości. Kolejną kwestią jest praktyczne stosowanie odpowiednich przepisów. Jak bowiem stosować je np. w stosunku do zdecentralizowanej struktury, jaką jest DAO?

Oczywiście ICO i zbywane w ich ramach tokeny będą budzić kontrowersje również na gruncie innych regulacji. W zależności bowiem od charakterystyki danego tokena będzie można uznać go za różnego rodzaju instrumenty prawne. Przykładowo uznanie za pieniądź elektroniczny będzie wiązało się z określonymi konsekwencjami regulacyjnymi dla podmiotu (np. inicjatora ICO), który zostanie uznany za wydawcę pieniądza elektronicznego.

Innego rodzaju wątpliwości prawne będą wiązały się z celem, dla którego dany podmiot pozyskuje środki. Jednym przykładem są wspomniane fundusze inwestycyjne. Jeżeli zaś będą one miały charakter zbliżony do depozytów, z których będą następnie udzielane pożyczki, taka działalność ma charakter depozytowo-

kredytowy, co do zasady regulacyjnie zastrzeżony dla banków.

Czy należy spodziewać się interwencji ustawodawcy lub regulatora?

Choć obecnie ICO mają charakter niszowy wobec skali innych metod pozyskiwania finansowania na rynkach finansowych, już teraz w ich drodze zdobywane są dziesiątki milionów dolarów. Trudno powiedzieć, czy publiczna sprzedaż tokenów w tej formie będzie zyskiwała na znaczeniu w tempie, który zwróci uwagę organów regulacyjnych. Obecna dynamika rozwoju tego typu projektów jest jednak znacząca.

Działania ustawodawcy lub nadzorcy mogą być utrudnione ze względu na ponadnarodowy charakter ICO. Organizacja takiego przedsięwzięcia oraz wzięcie w nim udziału wymaga właściwie wyłącznie dostępu do internetu. Samo ICO odbywa się w sieci, przez co nie rzadko trudne jest określenie powiązań z jakąkolwiek jurysdykcją (przede wszystkim w sytuacji organizowania ICO przez DAO).

Nie można wykluczyć, że ICO i podobnymi metodami pozyskiwania finansowania zainteresuje się główny nurt sektora finansowego. W takim przypadku reakcja władz publicznych będzie zapewne nieodzowna. Jednak także w przypadku równoległego rozwoju ICO oraz publicznej sprzedaży tokenów poza regulowanym rynkiem finansowym można z czasem spodziewać się zainteresowania tymi zjawiskami ze strony ustawodawcy i organów regulacyjnych.



Zaawansowana cyfryzacja, czyli odkrywanie użytecznej kryptografii

Piotr Rutkowski

Coraz bardziej przekonujemy się do korzyści ze stosowania technologii cyfrowych. Przedsiębiorcy decydujący się na wdrożenie innowacyjnych technologii, by uzyskać przewagę konkurencyjną, przeważnie muszą przełamywać zastane schematy i bariery, ale w ostatnich latach wzrosło przekonanie o niewykorzystanym potencjale cyfryzacji, a tym samym motywacja, by próbować nowych sposobów na biznes.

Wiadomo, że platformy handlu elektronicznego znacząco poprawiły skuteczność tradycyjnych relacji klient – dostawca. Dzięki automatyzacji, robotyce, narzędziom analizy dużych zbiorów danych (big data), łączeniu w rozległych sieciach czujników i sterowników (internet rzeczy) powstają nowe możliwości kontroli kosztów i zwiększania zysków we wszelkich ogniwach łańcucha wartości przedsiębiorstw.

Szczególnie istotna, żeby nie powiedzieć przełomowa dla obrotu gospodarczego stała się możliwość wprowadzenia systemów płatności elektronicznych. Pomimo że płatności są kluczowym procesem w gospodarce, to są zdominowane na rynku pieniądza przez sektor bankowy. Nie było więc szczególnych powodów, by w innych sektorach biznesu zgłębiać technologiczne kwestie systemów płatności. Tym bardziej, że techniki zabezpieczenia poufności systemów transakcyjnych tradycyjnie traktowano jako wiedzę wymagającą ochrony. Ponadto zaawansowana kryptografia jest wciąż poddana restrykcyjnym rządowym reżimom kontrolnym.

Kryptografia w służbie biznesu

Tymczasem cyfryzacja systemów płatności stała się możliwa, przede wszystkim dzięki zastosowaniu technik kryptograficznych. Pierwotnym celem kryptografii jest zapewnienie

bezpiecznej łączności. Nadawca wysłał do odbiorcy wiadomość, której nikt postronny nie jest w stanie odszyfrować ani zinterpretować, nawet jeżeli może przekazywać podsłuchać. Kiedy nadawca i odbiorca mogą dzielić fizyczny kanał łączności, ten cel można osiągnąć, stosując klasyczne techniki kryptografii klucza publicznego. W rzeczywistych warunkach, kiedy używamy publicznej sieci, internetu, wielu niekoniecznie zabezpieczonych i nie zawsze w pełni sprawnych serwerów pośredniczących, taka luksusowa możliwość zdarza się rzadko, a jeżeli jest wykonalna, to jest też kosztowna. Dlatego kryptologia zajmuje się zagadnieniami matematycznymi i technicznymi, wykraczającymi bardzo daleko poza opracowanie algorytmów do szyfrowania wiadomości. Poza oczywistymi ogólnymi aspektami bezpieczeństwa, takimi jak zapewnienie poufności poprzez szyfrowanie czy uwierzytelnianie dostępu, odpowiednio zestawione protokoły algorytmów kryptograficznych mogą odpowiadać za wypełnianie najróżniejszych wymogów złożonych i rozbudowanych systemów komunikacji, w tym również systemów płatności. Wynikało to też z konieczności opracowywania dla rozległych sieci bezpiecznych, w tym również wygodnych systemów dystrybucji kluczy oraz przypisywania uprawnień. Zabezpieczenia może wymagać nie tylko treść wiadomości i prywatność nadawcy i odbiorcy, ale też dane

dotyczące topologii sieci, serwerów pośredniczących, lokalizacji nadawcy, używanych przez niego urządzeń mobilnych. Kryptologia, szukając rozwiązań dla różnych oczekiwań, dała w związku z tym narzędzia do skutecznego łączenia niektórych tak pozornie sprzecznych oczekiwań jak sprawdzanie tożsamości i anonimowość.

Wymagania użytkowe i techniczne w systemach płatności bywają specyficzne dla różnych koncepcji biznesowych kart płatniczych, transakcji w sklepach internetowych, mikropłatności, pieniądza elektronicznego, rozliczeń międzybankowych. Dla każdego z systemów należy wprowadzić rozwiązania gwarantujące ochronę przed fałszerstwem, ryzykiem dublowania transakcji, nadużyciami ze strony sklepu, praniem brudnych pieniędzy czy wyludzeniami.

Kwestią konwencji jest, czy płacący ma się rejestrować w systemie, czy pozostawać anonimowy, tak jak zwykłych transakcjach płatności monetami lub banknotami papierowymi. W płatnościach elektronicznych kwestią konwencji jest też moment przepływu pieniądza pomiędzy płacącym, pośrednikiem, bankiem płacącego, bankiem odbiorcy, odbiorcą oraz dostawcą towaru lub usługi.

Anonimowość (technicznie powinniśmy mówić raczej o pseudoanonimowości) rzadko jest celem samym w sobie. W transakcjach biznesowych zwykle preferowana jest gwarancja rozliczalności. Równocześnie jednak wszelkie ogniwa transakcji z zasady powinny dysponować wyłącznie taką informacją, która jest im niezbędna do podjęcia decyzji. Inaczej system nie zyskałby zaufania użytkowników.

Nowe sposoby na płacenie

Można przyjąć, że wstępne podstawy dla nowoczesnych koncepcji systemów płatności elektronicznych mógł stworzyć schemat

tzew. ślepego podpisu elektronicznego opisany matematycznie przez Chauma w 1982 r. Oznacza on potwierdzenie transakcji podpisem z dodatkowym wymaganiem, że podpisujący nie dysponuje żadną informacją na temat podpisywanej wiadomości ani na temat samego podpisu. Można to zilustrować podpisywaniem z opaską na oczach dokumentu przyniesionego na biurko w zamkniętej kopercie i przekazania go dalej w następnej zamkniętej kopercie. Opisy tego rodzaju systemów stopniowo się rozwijały. W połowie lat dziewięćdziesiątych Camenisch, Piveteau, Stadler i Maurer opublikowali kilka artykułów o systemach anonimowych kont bankowych. Jedną z konkluzji ówczesnych publikacji było stwierdzenie, że wprowadzenie w szerszej skali anonimowych systemów płatności wymaga rozproszonego przetwarzania ogromnych baz danych, a tym samym mocy obliczeniowych i zdolności przesyłu, których wtedy jeszcze w powszechnym użyciu nie było.

Stało się to technicznie wykonalne stosunkowo niedawno. Pragnący zachować *nomen omen* anonimowość Satoshi Nakamoto opracował w 2008 r. założenia wirtualnego pieniądza Bitcoin opartego o rozproszony system przetwarzania rejestrów (*distributed ledger*), znany szerzej jako technologia blockchain.

Trudno jednoznacznie zdiagnozować, na ile Bitcoin – swoisty światowy poligon dla technologii blockchain – sprawdził się już jako rozwiązanie dla powszechnego użytku. Można uznać, że korzystanie z Bitcoina wymaga od konsumenta pewnego rodzaju obycia z nowościami technicznymi, w tym wykonania pewnych czynności przygotowawczych, a przede wszystkim zaufania, że mamy do czynienia z czymś bezpiecznym i legalnym. Dla wielu osób to nazbyt skomplikowane. Nie obyło się też bez przypadków wykorzystywania atrybutu

anonimowości transakcji Bitcoin przez przestępców. Z drugiej jednak strony jest przynajmniej kilka powodów, dla których technologia blockchain zaczęła być traktowana poważnie w zastosowaniach profesjonalnych, które zapewne ją upowszechnią.

- Technologia blockchain jest systemem otwartym, który okazał się na razie dosyć odporny na ataki hakerskie. Znane przypadki naruszeń cyberbezpieczeństwa Bitcoina dotyczyły nie samej technologii blockchain, ale przełamania zabezpieczeń innych elementów systemów IT i oprogramowania. Inaczej mówiąc, technologię blockchain można określić jako bezpieczną, zakładając staranność w unikaniu błędów projektowania systemu, w rodzaju tych, które wykorzystano w głośnym przypadku ataku na eksperymentalny projekt crowdfundingowy The DAO w czerwcu 2016 r.
- Jednostkowe koszty obsługi transakcji są dużo niższe niż w tradycyjnym systemie bankowym, co wzbudziło już zainteresowanie tradycyjnego sektora bankowego i kapitałowego.
- Zakres zastosowań tego rodzaju protokołów kryptograficznych wykracza daleko poza potrzeby sektora usług finansowych, obejmując najróżniejsze rodzaje prostych systemów transakcyjnych (inteligentne kontrakty), co z kolei inspiruje pomysły na nowe sposoby organizacji przedsiębiorstw.

Blockchain dla wszystkich

Technologia blockchain może być platformą do konstruowania bardzo różnych systemów transakcyjnych, od całkowicie rozproszonych jak Bitcoin, do wydzielonych z funkcjami scentralizowanego zarządzania. Dla każdego z zastosowań należy rozważać stosowne czynniki

ryzyka i środki zaradcze. Duża odporność i stabilność Bitcoina ma bezpośredni statystyczny związek z całkowitą decentralizacją tego systemu, w którym za zgodą użytkowników nie ma ośrodków zarządzania.

Inaczej jest w systemach wydzielonych, które chciałyby wdrażać biznes i banki. Najbardziej doceniany bywa tam atrybut rozliczalności, oparty o bezpieczny dostęp do współdzielonych zbiorów danych (rejestrów). Właśnie to przyczynia się do obniżenia kosztów działalności przedsiębiorstw, które stały się chyba najlepszą pożywką dla koncepcji wdrażania inteligentnych kontraktów czy DAO.

Praktyczne komercyjne lub rządowe zastosowania technologii blockchain są często mieszanką funkcji zdecentralizowanych i scentralizowanych. Czynniki ryzyka i środki zaradcze bywają też ważone pozamatematycznymi racjami optymalizacji funkcji kryptograficznych. Można np. założyć, że tak bywa w rządowych zastosowaniach usług sektora publicznego.

Zdiagnozowanie czynników ryzyka może się wiązać z koniecznością podejmowania dodatkowych technicznych środków ochrony, np. w formie wielostopniowych schematów podpisów elektronicznych chroniących określone serwery, wprowadzenia procedur testów penetracyjnych itp. Na pewno przy każdym wdrożeniu warto rozpatrywać specyficzne czynniki ryzyka i dostosowywać je do uwarunkowań cyberbezpieczeństwa dla konkretnego przedsiębiorcy lub określonych zastosowań.

Użyteczność technologii blockchain, w tym ocena jej bezpieczeństwa, definitywnie przestała być teoretyczna. Na przykład zarządzający bezpieczeństwem amerykańskich federalnych agencji rządowych Departament Bezpieczeństwa Krajowego (DHS) ogłosił niedawno przyznanie kilku grantów konkursowych na

wdrożenia technologii blockchain w systemach zarządzania tożsamością i ochroną prywatności.

Właściwie każda z „wielkiej czwórki” firm konsultingowych oraz najważniejsi gracze na światowym rynku integratorów systemów ICT prezentują obecnie autorskie rozwiązania systemów technologii blockchain do wykorzystania w biznesie. Równie istotne są inicjatywy podejmowane w sektorze bankowym. Zamiast bronić się przed wymykającym się spod ich kontroli Bitcoinem, banki same pracują nad wdrożeniami, które zreorganizują infrastrukturę i zasady funkcjonowania usług finansowych, ubezpieczeń transakcji, depozytów, pożyczek, papierów wartościowych, zarządzania kapitałem, inwestycjami, pełnomocnictwem czy aktywami. Profesjonalne zastosowania wewnątrzbankowe z pewnością zaowocują również nowymi produktami dla klientów, ale zapewne już w formie nie tak „niezależnej” jak Bitcoin.

Można zauważyć, że powtarza się mechanizm znany z historii sektora telekomunikacji. W 2004 r., kiedy technologie internetu stały się już powszechnie dostępne, na rynku usług telekomunikacyjnych pojawiły się niezależne oferty tanich głosowych połączeń międzyna-

rodowych poprzez internet (w technologii nazywanej VoIP). Naruszyło to status quo kosztownych rozliczeń dawnych monopolistów telekomunikacyjnych, właścicieli infrastruktury kabli międzynarodowych. To było dla starych telekomów trudne, ponieważ większość infrastruktury była przystosowana do tradycyjnego systemu rozliczeń, gdzie taryfa była funkcją odległości. Niezależne giełdy minut VoIP funkcjonowały do czasu, gdy wielkie telekomy same nie zmobilizowały się do nowego systemu rozliczeń, już bezpowrotnie tańszych. Protokoły komunikacyjne opracowane z myślą o rozwoju internetu przyczyniły się do rozwoju konkurencji i spadku cen. Obecnie sektor telekomunikacji stoi przed tym samym wyzwaniem co inne, próbujące opracować strategię zastosowania technologii blockchain. Ma też przy tym własne wyzwania związane z systemami billingowymi, roamingiem międzynarodowym, a także zupełnie nowymi obszarami usług, które próbuje oferować swym abonentom. Technologie blockchain mogą zatem posłużyć nie tylko zmianie organizacji przedsiębiorstw, ale również przebudowie struktury rynku.



Wnioski

Ogromny potencjał technologii blockchain

Innowacje powstające dzięki zastosowaniu technologii blockchaina, takie jak inteligentne kontrakty i DAO, mogą wpłynąć na przyszłość znanych nam modeli biznesowych oraz struktur ekonomicznych i społecznych w sposób podobny lub nawet dalej idący niż internet. DAO oraz inteligentne kontrakty mogą doprowadzić do rozwoju struktur, w których wymiana dóbr, idei oraz treści będzie w dużej mierze możliwa bez pośredników, przy wykorzystaniu rozproszonej sieci. Z jednej strony otwiera to szansę na tworzenie zupełnie nowych, bardziej efektywnych modeli działania gospodarki. Z drugiej strony nowe technologie mogą okazać się katastrofalne dla tradycyjnych struktur gospodarczych opartych na modelu pośrednictwa. Dotyczy to w szczególności np. sektora finansowego.

Blockchain nie powinien być ograniczany do Bitcoina

Niezwykle istotne jest zrozumienie technologii blockchain i kierunków jej rozwoju. Technologia blockchaina nie należy np. postrzegać wyłącznie przez pryzmat Bitcoina. Może to prowadzić do błędnych i szkodliwych decyzji legislacyjnych. Już teraz widać, że zastosowanie blockchaina wykroczy daleko poza wąsko rozumiane rozwiązania transakcyjno-płatnicze.

Potencjał dla sektora publicznego

Instytucje publiczne powinny starać się zrozumieć zmiany technologiczne i czerpać w tym zakresie dobre wzorce z zewnątrz. Zastosowania technologii blockchaina mogą zostać z powodzeniem użyte w procesie cyfryzacji pań-

stwa. W tym kontekście wymienia się najczęściej rejestry publiczne, systemy do głosowania, pobór podatków, kontrolę wydatków publicznych i ochronę infrastruktury krytycznej. Już obecnie obserwujemy, że w programach rządowych bierze się pod uwagę potencjał technologii blockchaina. Należy wspierać takie inicjatywy, które jednak dla swojego powodzenia potrzebują działań edukacyjnych oraz wsparcia badań naukowych poświęconych technologii blockchain.

Fenomen inteligentnych kontraktów oraz DAO z perspektywy prawa

Fenomen nowych rozwiązań tworzonych w ramach technologii blockchain wynika m.in. z ich następujących cech:

- a. **Autonomiczny charakter.** Określone działania mające znaczenie z perspektywy prawa (np. przeniesienie określonego dobra cyfrowego) są w przypadku inteligentnych kontraktów oraz DAO realizowane w sposób zautomatyzowany. Działania te są wynikiem realizacji kodu będącego podstawą danego kontraktu. Tradycyjne systemy prawa przypisują tymczasem poszczególne działania określonym podmiotom, a nie abstrakcyjnym algorytmom.
- b. **Abstrakcyjny charakter.** Inteligentne kontrakty oraz DAO istnieją w cyberprzestrzeni jako algorytm. Do prawidłowego działania, tj. organizowania zdarzeń w cyberprzestrzeni, nie potrzebują zasadniczo jakichkolwiek tradycyjnych struktur prawnych. Można wyobrazić sobie, że struktury gospodarcze organizowane tradycyjnie przez podmioty prawa (np. spółki), takie jak

gielny, publiczne rejestry działają z powodzeniem wyłącznie w formie algorytmu.

- c. **Globalny charakter.** Inteligentne kontrakty oraz DAO funkcjonują w rozproszonej sieci, której nie da się przypisać do konkretnego, tradycyjnie rozumianego miejsca w przestrzeni. Można powiedzieć, że DAO czy inteligentny kontrakt jest „wszędzie”. Tymczasem tradycyjne systemy prawa zawsze dążą do przypisania zjawisk prawnych do konkretnej jurysdykcji.
- d. **Brak centralnego podmiotu odpowiedzialnego.** W przypadku DAO bardzo trudno jest ustalić podmiot/osobę, która jest odpowiedzialna za jego funkcjonowanie. Nie ma centralnych organów reprezentujących DAO. Nawet odpowiedzialność twórców algorytmu, w oparciu o który działa DAO, jest ograniczona, gdyż po stworzeniu algorytmu tracą oni w dużej mierze kontrolę nad jego funkcjonowaniem.

Najtrudniejsze zagadnienia prawne

Następujące zagadnienia prawne wydają się w tej chwili stanowić największą przeszkodę w dalszym rozwoju inteligentnych kontraktów oraz DAO:

- a. **Brak podmiotowości prawnej DAO.** DAO oraz inteligentne kontrakty mogą realizować skomplikowane struktury prawnogospodarcze, analogiczne do struktur realizowanych przez tradycyjne podmioty prawa. W odróżnieniu jednak od podmiotów tradycyjnych nie mają one podmiotowości prawnej. Są dla prawa transparentne, co oznacza, że DAO z perspektywy prawa to w zasadzie wszyscy jego uczestnicy. Taka sytuacja jest bardzo niepraktyczna, szczególnie w tych przypadkach, w których zachodzi konieczność interakcji DAO z podmiotami zewnętrznymi. Tak będzie w szczególności w przypadku konieczności

nawiązania relacji DAO z kontrahentem zewnętrznym. Transparentność prawna DAO jest też olbrzymią przeszkodą w ustalaniu obowiązków podatkowych w związku z działaniami realizowanymi z wykorzystaniem DAO oraz inteligentnych kontraktów.

- b. **Brak zdolności sądowej DAO.** Chociaż DAO mogą być wykorzystywane do organizowania bardzo złożonej wymiany gospodarczej, nie mogą być stroną w postępowaniu sądowym. Powoduje to szereg praktycznych trudności, które mogą zniechęcić do wchodzenia w relacje prawne z DAO, choć te relacje mogą być niekiedy niezbędne do ich prawidłowego funkcjonowania (np. relacje z kontrahentami dostarczającymi informacje niezbędne do działania DAO lub podmiotami rozwijającymi kod DAO). Wizja pozywania wszystkich użytkowników DAO jest zarówno niepraktyczna, jak i w zasadzie niemożliwa do realizacji.
- c. **Niepewność prawna.** Z uwagi na zdecentralizowany charakter DAO oraz inteligentnych kontraktów bardzo trudno jest z góry ustalić, przez pryzmat jakiej jurysdykcji należy oceniać działania realizowane z wykorzystaniem określonego DAO lub inteligentnego kontraktu. Ma to bardzo istotne znaczenie z perspektywy przepisów prawa karnego oraz ryzyk prawnych podmiotów zaangażowanych w tworzenie DAO (np. twórców algorytmu). Nie sposób jednoznacznie ocenić, czy działania tych osób nie naruszają przepisów prawa karnego określonej jurysdykcji. Okoliczność ta może być istotną przeszkodą w rozwoju technologii blockchain.
- d. **Podatki.** DAO, jako podmiot całkowicie cyfrowy oraz zdecentralizowany, ma niejasny status na gruncie prawa podatkowego.

Możliwa kwalifikacja DAO jako wspólnego przedsięwzięcia nie odpowiada na wszystkie wyzwania związane z DAO. Interwencja ustawodawcy podatkowego na tym etapie wydaje się przedwczesna, m.in. z uwagi na brak odpowiedniej wiedzy o samym DAO i jego mechanizmach, co może realnie grozić brakiem adekwatnych regulacji. Interwencji takiej nie należy jednak wykluczać w przyszłości. Pewne działania mogłby za to podjąć aparat wykładający prawo podatkowe, np. wydając ogólną interpretację prawa podatkowego. Nie tylko ułatwiłoby to prawidłowe rozliczanie podatków przez podmioty zaangażowane w DAO (uznane za podatników z tego tytułu w Polsce), ale mogłoby – przy odpowiedniej i klarownej konstrukcji – stanowić zachętę dla zagranicznych graczy do opodatkowania z tego tytułu w Polsce.

- e. **Niejasny status regulacyjny ICO.** Coraz popularniejsze jest pozyskiwanie finansowania przez projekty oparte na technologii blockchain w drodze ICO. Ze względu na liczne wątpliwości prawne w wielu krajach (przede wszystkim związane ze stosowaniem regulacji dotyczących obrotu instrumentami finansowymi) widoczny jest trend poszukiwania jurysdykcji, która zapewni stabilny porządek prawny i przewidywalne reguły dla zainteresowanych podmiotów, a także otwarte podejście organów publicznych do innowacji.

Konieczne są aktywne działania

Wspomniane powyżej wyzwania prawne mogą skutecznie sparaliżować dalszy rozwój technologii blockchain. Dostosowanie systemu prawa do wyzwań stawianych przez inteligentne kontrakty staje się zatem koniecznością, jeżeli zależy nam na dalszym rozwoju tej technologii. Prawnicy powinni dołożyć starań, by zrozumieć tę technologię i umożliwić jej stosowanie.

Zakładamy, że w tym zakresie możliwe są rozwiązania krótkoterminowe oraz długoterminowe.

- a. **Rozwiązania krótkoterminowe.** Niezbędne są względnie proste rozwiązania krótkoterminowe, które zapewnią bezpieczeństwo prawne i podatkowe. Chodzi na przykład o jasne określenie skutków regulacyjnych i podatkowych udziału w ICO. Można również rozważyć promowanie tworzenia prowizorycznych tradycyjnych podmiotów prawnych (np. fundacji czy spółek), które pełniłyby funkcję łącznika pomiędzy tradycyjnym systemem prawnym a blockchainem. Takie podmioty mogłyby przynajmniej częściowo zaradzić trudnościom związanym z brakiem podmiotowości prawnej DAO oraz niemożliwością identyfikowania stron stosunków gospodarczych na potrzeby podatkowe.
- b. **Rozwiązania długoterminowe.** W dalszej kolejności potrzebne są rozwiązania długoterminowe, które będą znacznie lepiej odpowiadać naturze DAO. Możliwe są bardzo różne scenariusze. Wydaje się, że nieunikniona będzie zmiana tradycyjnego paradygmatu osobowości prawnej. Ta instytucja mogłaby zostać uelastyczniona i np. stosowana na żądanie (po spełnieniu określonych kryteriów). Dalszy rozwój technologii blockchain będzie wymagał wsparcia ze strony państwa. Rozwój niektórych technologii blockchain bez wyklarowania ich statusu prawnego będzie kreował dla ich twórców zbyt duże ryzyko prawne (np. na gruncie prawa podatkowego oraz prawa karnego). Z dużym prawdopodobieństwem należy założyć, że ceną za przychyłność państwa będą próby poddania DAO oraz inteligentnych kontraktów kontroli przez tradycyjnie rozumiane państwa i ich porządki prawne. Państwu będzie zależało na tym, żeby DAO i inteligentne kontrakty

nie funkcjonowały w regulacyjnej próżni, która grozi anarchią. W związku z tym należy spodziewać się nowych pomysłów w zakresie technik umożliwiających ingerencję państwa w DAO lub inteligentny kontrakt. Przykładowo można sobie wyobrazić, że państwa będą gotowe uznać podmiotowość prawną DAO, ale pod warunkiem zastosowania w danym DAO rozwiązania, które pozwoli na ingerencję państwa w kod danego DAO (np. w celu egzekucji określonego porządku prawnego). Takie rozwiązania byłyby trudne do zaakceptowania dla wielu zwolenników blockchaina, upatrujących w tej technologii niepowtarzalnej szansy na stworzenie gospodarki w pełni wolnej od kontroli oraz ingerencji państwa. Jest to jednak być może jedyny kierunek, który umożliwi dalszy rozwój technologii blockchain.

Technologia blockchain to szansa dla polskiej gospodarki

Choć postęp technologiczny jest niezwykle dynamiczny, wciąż znajdujemy się na wstępnym etapie rozwoju inteligentnych kontraktów i DAO. Sprawia to, że państwa takie jak Polska mają szansę stać się liderami rozwoju innowacji w tym obszarze. Jest to sytuacja unikatowa, bo w przypadku wielu innych rodzajów nowych technologii Polska nie ma i w krótkiej perspektywie nie będzie miała zasobów, by

skutecznie konkurować z najbardziej rozwiniętymi gospodarkami. W przypadku technologii blockchain wielką szansą Polski jest znakomita baza w postaci jednej z najlepszych na świecie kadr IT, która stanowi naturalne zaplecze dla rozwoju tych technologii. Potrzebne jest wsparcie państwa, zarówno w obszarze badań naukowych, jak i dla innowacyjnych przedsiębiorców.

Technologia blockchain wymaga radykalnej zmiany w zakresie stosowania prawa

Inteligentne kontrakty oraz DAO przenoszą prawo z przestrzeni języka naturalnego do przestrzeni algorytmu. Z tej perspektywy jest to jedna z najbardziej doniosłych rewolucji w dziejach prawa. Wraz z rozwojem technologii blockchain tworzenie oraz stosowanie prawa będzie wymagało zupełnie nowych umiejętności, w szczególności umiejętności sprawnego i płynnego przechodzenia z poziomu języka naturalnego na poziom kodu i odwrotnie. Rozwój technologii blockchain będzie w ogromnej mierze warunkowany nabywaniem tych nowych umiejętności przez środowiska prawnicze i informatyczne, które w coraz większym stopniu będą musiały współpracować ze sobą w procesach tworzenia oraz stosowania prawa.



Autorzy



Jacek Czarnecki jest młodszym prawnikiem w praktyce prawa nowych technologii kancelarii Wardyński i Wspólnicy. Zajmuje się regulacjami dotyczącymi technologii finansowych (w tym technologii blockchaina i cyfrowymi walutami), crowdfundingiem, usługami zaufania, prawem telekomunikacyjnym, prawem ochrony danych osobowych, prawnymi aspektami internetu, prawem cywilnym i prawem spółek handlowych.

E-mail: jacek.czarnecki@wardynski.com.pl



Maciej Jędrzejczyk od 2011 roku związany jest z firmą IBM w ramach Strategic Outsourcing. Architekt IT odpowiedzialny za rozwiązania IaaS oraz Workplace Engineering dla zachodnioeuropejskich klientów. Kryptoentuzjasta i umiarkowany zwolennik technologii Blockchain. Zawsze na rozdrożach między prawem, biznesem, badaniami naukowymi i informatyką. Zamiłowany amator historii, kartografii, podróżowania i nauki języków obcych.

E-mail: maciej_jedrzejczyk@pl.ibm.com



Agnieszka Kraińska jest radcą prawnym w kancelarii Wardyński i Wspólnicy. Specjalizuje się w zagadnieniach dotyczących prawa międzynarodowego, prawa Unii Europejskiej, postępowań przed Komisją Europejską i Trybunałem Sprawiedliwości Unii Europejskiej.

E-mail: agnieszka.krainska@wardynski.com.pl



Rafał Kuchta jest aplikantem adwokackim w praktyce prawa nowych technologii kancelarii Wardyński i Wspólnicy. Zajmuje się nowymi rozwiązaniami płatniczymi, crowdfundingiem, prawem telekomunikacyjnym, ochroną danych osobowych oraz e-commerce, w szczególności w zakresie doradztwa regulacyjnego oraz związanego z umowami.

E-mail: rafal.kuchta@wardynski.com.pl



Karolina Marzantowicz stoi pomiędzy światem informatyki, innowacji biznesowych i psychologii. Działa jak katalizator i pobudza ciekawość pomagając przedsiębiorstwom w adaptacji szybko zmieniających się technologii. Reprezentuje IBM jako mówca i znawca tematu w wydarzeniach publicznych w Polsce i na świecie. Pasjonatka transformacji cyfrowej. W IBM pełni rolę architekta i doradcy dla klientów sektora bankowego w Europie. Pracuje w branży IT od 1994 roku. Jestem członkiem Akademii Technologii IBM. Prywatnie mama trójki dzieci, zakochana w górach od zawsze.

E-mail: karolina.marzantowicz@pl.ibm.com



Joanna Prokurat jest doradcą podatkowym w praktyce podatkowej kancelarii Wardyński i Wspólnicy. Odpowiada również za obszar crowdfundingu, finansowania nowych technologii, gamingu oraz prac badawczych w praktyce prawa nowych technologii. Doradza w sprawach dotyczących polskiego i międzynarodowego prawa podatkowego. Specjalizuje się w doradztwie w zakresie podatku dochodowego od osób prawnych oraz podatku od towarów i usług, międzynarodowego planowania podatkowego i optymalizacji podatkowej oraz podatku transakcyjnego. Świadczy usługi doradztwa podatkowego w odniesieniu do podatku dochodowego od osób fizycznych oraz ubezpieczeń społecznych. Doradza w zakresie podatku od gier. Świadczy usługi ukierunkowane zarówno na optymalizację opodatkowania, jak i ograniczenie ryzyk podatkowych. Prowadzi przeglądy podatkowe (*tax reviews*), w tym przeglądy typu *due diligence*, oraz przygotowuje analizy podatkowe dla firm inwestujących w Polsce.

E-mail: joanna.prokurat@wardynski.com.pl



Piotr Rutkowski jest doradcą kancelarii kancelarii Wardyński i Wspólnicy ds. nowych technologii. Zajmuje się uwarunkowaniami prawnymi, regulacyjnymi i technologicznymi innowacyjnych sektorów gospodarki. Prowadzi firmę konsultingową Rotel, specjalizując się w problematyce strategii i regulacji rynku telekomunikacyjnego, zastosowaniach nowych technologii, bezpieczeństwie, ochronie infrastruktury krytycznej, zarządzaniu ryzykiem oraz współpracy sektora prywatnego i publicznego. Doradzał wielu firmom sektora telekomunikacji. Był też zatrudniany jako ekspert przez administrację tączności, Sejm, instytucje międzynarodowe. Jest jednym ze współtwórców systemu prawnego dla sektora telekomunikacji w Polsce. Jest też założycielem i wiceprezesem fundacji Instytut Mikromakro, think-tanku promującego strategiczne myślenie o państwie.

E-mail: piotr.rutkowski@wardynski.com.pl



Krzysztof Wojdyło jest adwokatem, partnerem kancelarii Wardyński i Wspólnicy odpowiedzialnym za praktykę prawa nowych technologii. Działa również w praktyce postępowań regulacyjnych oraz usług płatniczych. Zajmuje się regulacjami dotyczącymi elektronicznych instrumentów płatniczych, crowdfundingu, komercjalizacji nowych technologii, telekomunikacji, robotyki, obrotu wierzytelnościami i przeciwdziałania praniu brudnych pieniędzy. Uczestniczy w dużych i nowatorskich projektach z zakresu szeroko rozumianych nowych technologii. Regularnie doradza zarówno start-upom, jak i dużym podmiotom z sektora nowych technologii. Jest autorem lub współautorem publikacji dotyczących między innymi crowdfundingu, robotyki, wirtualnych walut oraz nowych technologii w sektorze usług finansowych. Publikuje m.in. w „Monitorze Prawa Bankowego”. Wielokrotnie występował jako wykładowca na konferencjach oraz seminariach, w tym w ramach konferencji International Bar Association. Prowadzi również szkolenia dla przedstawicieli start-upów. Jest koordynatorem grupy roboczej ds. regulacji działającej w ramach Koalicji na rzecz Polskich Innowacji.

E-mail: krzysztof.wojdylo@wardynski.com.pl

Praktyka prawa nowych technologii

Dla nas nowe technologie to przede wszystkim nowe wyzwania prawne. W wielu przypadkach musimy zmagać się z wątpliwościami dotyczącymi kwalifikacji prawnej innowacyjnych produktów lub usług albo wręcz z brakiem odpowiednich regulacji. Zapewnienie klientom bezpieczeństwa prawnego w takich okolicznościach wymaga od prawników doświadczenia, kreatywności i rozumienia otoczenia biznesowego.

Dlatego stworzyliśmy w kancelarii interdyscyplinarną praktykę prawa nowych technologii, która skupia wysokiej klasy prawników, specjalistów w wybranych dziedzinach prawa. Wspierają nas współpracujący z kancelarią eksperci dysponujący szeroką wiedzą techniczną.

Nasza firma stworzyła program skierowany do start-upów z branży technologicznej. Bieżące wsparcie tych firm pozwala naszym prawnikom mieć stały kontakt z nowymi technologiami i wyzwaniami prawnymi, które się z nimi wiążą. Nasza firma koordynuje prace grupy regula-

cyjnej w ramach [Koalicji na rzecz Polskich Innowacji](#), gdzie nasi prawnicy pracują nad rozwiązaniami udoskonalającymi regulacje dotyczące nowych technologii (np. przepisy o komercjalizacji wiedzy, regulacje dotyczące przedmiotów podwójnego zastosowania lub crowdfundingu).

Staramy się na bieżąco reagować na potrzeby naszych klientów, tworząc wysoce wyspecjalizowane usługi prawne adresowane do poszczególnych segmentów rynku nowych technologii. Świadczymy kompleksowe doradztwo regulacyjne, podatkowe oraz transakcyjne. Nasze dotychczasowe doświadczenia pozwoliły na zidentyfikowanie następujących obszarów naszej praktyki: biomedycyna i nowoczesna żywność, crowdfunding, cyberbezpieczeństwo, e-commerce, finansowanie nowych technologii, gaming, nowe rozwiązania płatnicze, nowe technologie w pozyskiwaniu energii, ochrona prywatności, prace badawcze, projekty PPP, przemysł kreatywny, technologie informacyjne, telekomunikacja, usługi zaufania.

KONTAKT



Anna Pompe
advokat, wspólnik

E-mail: anna.pompe@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00



Krzysztof Wojdyło
advokat, partner

E-mail: krzysztof.wojdylo@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00



Joanna Prokurat
doradca podatkowy

E-mail: joanna.prokurat@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00



Piotr Rutkowski
doradca ds. nowych technologii

E-mail: piotr.rutkowski@wardynski.com.pl
Tel.: 22 437 82 00, 22 537 82 00

O kancelarii

Kancelaria Wardyński i Wspólnicy została założona w 1988 roku. Czerpiemy z najlepszych tradycji kancelarii adwokackich w Polsce. Skupiamy się na biznesowych potrzebach naszych klientów, pomagając im znaleźć skuteczne i praktyczne rozwiązanie najtrudniejszych problemów prawnych.

Firma jest szczególnie ceniona przez klientów i konkurencję za swoje usługi w dziedzinie sporów, transakcji, własności intelektualnej, nieruchomości i reprivatyzacji.

Obecnie w firmie jest ponad 100 prawników świadczących obsługę prawną w języku polskim, angielskim, francuskim, niemieckim, hiszpańskim, rosyjskim, czeskim i koreańskim. Nasze biura znajdują się w Warszawie, Krakowie, Poznaniu i Wrocławiu.

Klientom doradzamy w następujących dziedzinach: bankowość i finansowanie projektów, *compliance*, dochodzenie trudnych wierzytelności, doradztwo dla klientów indywidualnych, fuzje i przejęcia, infrastruktura, instytucje finansowe, kontrakty w obrocie profesjonalnym, *life science*, nieruchomości

i inwestycje budowlane, nowe technologie, obsługa klientów z sektora rolnictwa, obsługa korporacyjna, ochrona danych osobowych, ochrona zdrowia, outsourcing, podatki, pomoc publiczna, postępowania sądowe i arbitrażowe, prawo energetyczne, prawo europejskie, prawo karne, prawo konkurencji, prawo lotnicze, prawo ochrony środowiska, prawo pracy, prawo sportowe, prawo upadłościowe, *private equity*, reprivatyzacja, restrukturyzacja, rynki kapitałowe, sprzedaż detaliczna i sieci sprzedaży, transport, ubezpieczenia, usługi płatnicze, własność intelektualna, zamówienia publiczne i partnerstwo publiczno-prywatne.

Dzielimy się wiedzą i doświadczeniem za pośrednictwem portalu dla prawników i przedsiębiorców (www.codozasady.pl), firmowego Rocznika, a także publikacji z serii „Prawo w praktyce”. Jesteśmy też wydawcą pierwszej polskojęzycznej aplikacji o tematyce prawnej na urządzenia mobilne (Wardyński+). Aplikację można pobrać nieodpłatnie w App Store i Google Play.

www.wardynski.com.pl

www.codozasady.pl

Wardyński+

Wardyński i Wspólnicy
Al. Ujazdowskie 10
00-478 Warszawa

Tel.: 22 437 82 00, 22 537 82 00

Faks: 22 437 82 01, 22 537 82 01

E-mail: warsaw@wardynski.com.pl ●