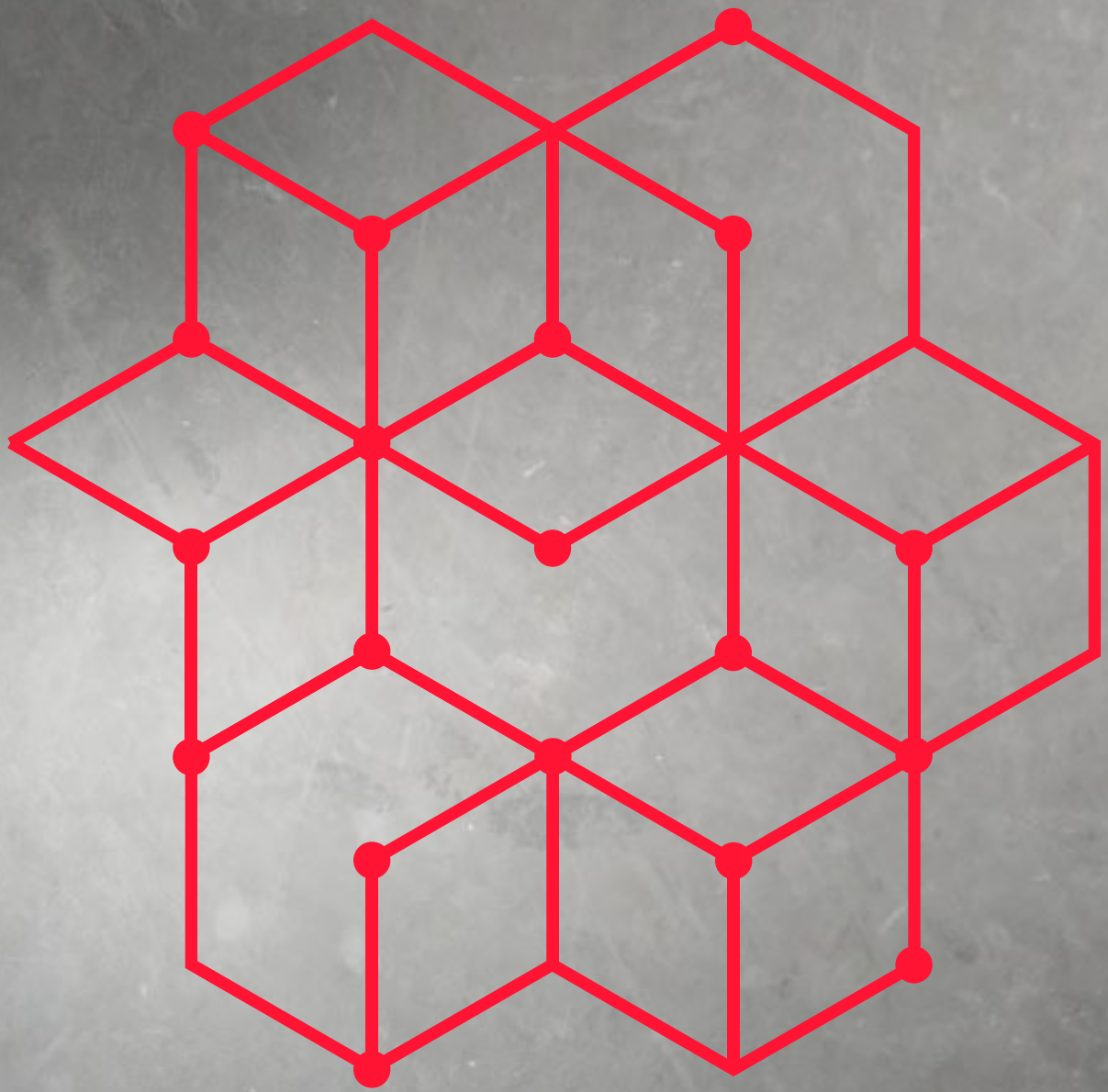
BLOCKCHAIN

w Polsce



MOŻLIWOŚCI I ZASTOSOWANIA

PIIT

SPIS TREŚCI

SŁOWO WSTĘPU

Polska Izba Informatyki i Telekomunikacji realizuje swoją misję – współtworzenie fundamentów cyfrowego rozwoju Polski, podejmując wiele działań których celem jest rzetelne promowanie cyfrowych innowacji. Jednym z nich jest niniejszy raport, przygotowany przez ekspertów Izby, pod kierunkiem Marcina Chruściela, przewodniczącego działającego w Izbie Komitetu Fintech. Liczę na to, że znajdziecie w nim państwo wiele inspiracji dotyczących praktycznego zastosowania technologii blockchain, bo to właśnie mądre zastosowania są źródłem wartości technologicznych innowacji.

Borys Stokalski
Prezes PIIT

W otaczającym nas świecie odkrycie technologii blockchain jest tym czym było wynalezienie komputera do dokonywania skomplikowanych obliczeń. Od tego momentu nastąpił rozkwit usług bankowych i rozwój bankowości. Dziś blockchain szykuje nam kolejną przejażdżkę rollercosterem w przyszłość. Zmieni się dosłownie wszystko – od prostych operacji po globalne zaawansowane procesy rozliczeniowe. Doszliśmy do wniosku w Komitecie Fintech, którym mam przyjemność kierować w PIIT, że potrzebne jest rzetelne opisanie technologii tak, aby blockchain z tytułów nagłówków gazet i artykułów w Internecie trafił na listę projektów transformujących wiele obszarów Państwa firm. Gdzie i jak? Zapraszamy do lektury o tym co już zrobili Ci, którzy zrozumieli przewagę nowej technologii...

Marcin Chruściel
Przewodniczący Komitetu Fintech przy PIIT
Dyrektor Orange Finanse

Polska Izba Informatyki i Telekomunikacji

Kim jesteśmy?

PIIT to platforma firm działających na rzecz cyfrowej transformacji gospodarki i modernizacji państwa. Współtworzymy fundamenty cyfrowego rozwoju, realizując następujące działania:

- opiniujemy akty prawne istotne z punktu widzenia firm teleinformatycznych
- współtworzymy w konsultacjach i grupach roboczych warunki do uzgodnień sektorowych dotyczących wspólnych stanowisk oraz nowych inicjatyw branży (poprzez działalność komitetów, grup roboczych, animowanie prac członków nad konkretnymi zagadnieniami)
- budujemy trwałe relacje z administracją publiczną, poprzez organizowanie spotkań oraz inicjowanie nowych, wspólnych projektów
- reprezentujemy interesy polskich firm teleinformatycznych na poziomie europejskim, poprzez organizację DIGITALEUROPE

Nasze cele

1. Sprzyjające warunki dla rozwoju przemysłu teleinformatycznego
2. Racjonalne regulacje i inicjatywy wspierające wdrażanie cyfrowych innowacji
3. Partnerska współpraca przemysłu teleinformatycznego i administracji publicznej

Chcesz nas bliżej poznać?

Zadzwoń: 22 628 22 60, 691 119 555
Napisz: sekretariat@piit.org.pl

Polska Izba Informatyki i Telekomunikacji
Al. Jerozolimskie 136 (IX piętro), Eurocentrum Alfa
02-305 Warszawa

WPROWADZENIE

Od kilku lat można zaobserwować rosnące zainteresowanie biznesu i sektora publicznego technologią blockchain lub rozproszonych rejestrów (DLT[1]). PIIT, organizacja będąca platformą firm działających na rzecz cyfrowej transformacji gospodarki i modernizacji państwa, publikuje niniejszy raport stawiając sobie za cel przedstawienie praktycznej i eksperckiej informacji na temat tej szybko rozwijającej się dziedziny.

Raport ma służyć jako:

- Inspiracja dla firm i organizacji, które zaciekawione są możliwościami technologii blockchain i zastanawiają się, czy ich pomysły na jej wykorzystanie są w ogóle możliwe. Raport zawiera wytłumaczenie czym jest blockchain i jakie powinny być kryteria wyboru tej technologii oraz wytłumaczenie co czyni ją w tym kontekście lepszą od wykorzystywanych obecnie tradycyjnych systemów.
- Źródło zaleceń dla tych, którzy widzą, że zastosowanie technologii blockchain jest możliwe (bo, na przykład, opisane przez nas zastosowanie jest analogiczne). Raport zawiera praktyczne informacje na temat zalet i ograniczeń istniejących platform oraz wskazówki, jak podejść do rozpoczęcia projektu.
- Źródło informacji na temat wdrożonych zastosowań, ze szczególnym naciskiem na specyfikę rynku polskiego. Oprócz konkretnych rozwiązań, pokazujemy także potencjalne zastosowania, jakie widzimy w przyszłości, w tym rozwiązania wymagające współpracy wielu podmiotów w danej branży.
- Źródło ogólnych informacji o funkcjonowaniu systemów opartych o blockchain w ujęciu polskich uregulowań i prawne odniesienie do przykładów zastosowań zawartych w raporcie.

PIIT jest źródłem informacji na temat technologii blockchain oraz przestrzenią do kontaktu firm i ekspertów zrzeszonych w Izbie, udostępniającymi swoje oferty i usługi, a innymi podmiotami zainteresowanymi poznaniem, rozwijaniem czy też biznesowym zastosowaniem rozwiązań opartych o blockchain.

Raport adresuje dwie dodatkowe kwestie. Pierwszą z nich jest silne kojarzenie technologii blockchain z Bitcoinem i innymi kryptowalutami. Kryptowaluty często wzbudzają podejrzenia wśród obywateli i decydentów ze względu na występujące asocjacje z transakcjami kryminalnymi i „ciemną stroną" Internetu. Niniejszy raport celowo nie skupia się na kryptowalutach i koncentruje się przede wszystkim na biznesowych zastosowaniach blockchain. Dokument jedynie odnotowuje zainteresowanie banków centralnych i regulatorów rynku finansowego w Polsce i na świecie kwestią walut cyfrowych. Drugą kwestią adresowaną w Raporcie jest trudność w komunikacji tematu ze względu na znaczącą liczbę nowych terminów i skomplikowanych zagadnień technicznych związanych z technologią blockchain. W odpowiedzi na ten problem, raport zawiera krótki opis kluczowych technologii z odniesieniami do istniejących źródeł informacji uzupełniony leksykonem najważniejszych pojęć.

1 Terminy blockchain i rejestr rozproszony używane są często zamiennie, choć istnieją miedzy nimi pewne różnice. W niniejszym raporcie skupiamy się na technologii blockchain.

CZYM JEST BLOCKCHAIN?

BITCOIN I KRYPTOWALUTY

Pierwszym praktycznym wdrożeniem systemu blockchain był Bitcoin. Bitcoin to także kryptowaluta, czyli forma gotówki elektronicznej, którą mogą obracać uczestnicy sieci, bez pośredników, centralnego emitenta i administratora systemu. W przypadku sieci Bitcoin konsensus oparty jest na algorytmie „dowodu wykonania pracy" (Proof of Work, w skrócie PoW) który wymaga od uczestników zatwierdzających i dodających bloki do łańcucha wykazania się, że zainwestowały znaczną moc obliczeniową zużywając kosztowny zasób, jakim jest energia elektryczna. Ten kto zdobędzie prawo do stworzenia nowego bloku otrzymuje nagrodę w postaci nowo wyemitowanych monet Bitcoin.

Bitcoin pokazał, że można zbudować globalną, zdecentralizowaną platformę wymiany wartości pomiędzy milionami uczestników, ale nie został alternatywną platformą płatniczą z kilku powodów: braku regulacji, niskiej wydajności (mierzonej w ilości transakcji na sekundę), zmienności notowań w stosunku do tradycyjnych walut i ogromnego zużycia energii potrzebnej, by sieć Bitcoin mogła właściwie funkcjonować.

Od roku 2009, czyli momentu pierwszej transakcji Bitcoina, pojawiły się dziesiątki kryptowalut. Jednak obszarem zainteresowania tego raportu jest potencjał zastosowania technologii blockchain w biznesie i w sektorze publicznym, a nie kryptowaluty. Zainteresowanych kryptowalutami odsyłamy do następujących źródeł informacji na ich temat:

- K. Piech (red.), 2017, Podstawy korzystania z walut cyfrowych,
- A. Antonopoulos, Mastering Bitcoin 2nd Edition - Programming the Open Blockchain.

CZYM JEST BLOCKCHAIN?

Dzisiaj, większość systemów przetwarzających dane opartych jest o zcentralizowane platformy informatyczne zlokalizowane w ramach jednej organizacji lub opartych o rozwiązania chmurowe. Jeżeli proces biznesowy wymaga interakcji pomiędzy wieloma podmiotami, dodawane są systemy sieciowe i komunikacyjne, aby te interakcje umożliwić. Scentralizowane systemy mogą być źródłem pojedynczego punktu awarii, są podatne na cyberataki, a dane w poszczególnych systemach są często niezsynchronizowane, nieaktualne lub po prostu niedokładne. Zwiększa to koszty i złożoność systemów, a uczestnicy procesu biznesowego muszą często polegać na zaufanych pośrednikach pełniących rolę arbitra zatwierdzającego transakcje lub weryfikującego pochodzenie i prawdziwość danych. Mimo, że często potrzeba przejrzystości i zaufania jest niezbędna, zbudowanie i utrzymanie sieci biznesowej spełniającej te wymagania jest trudne.

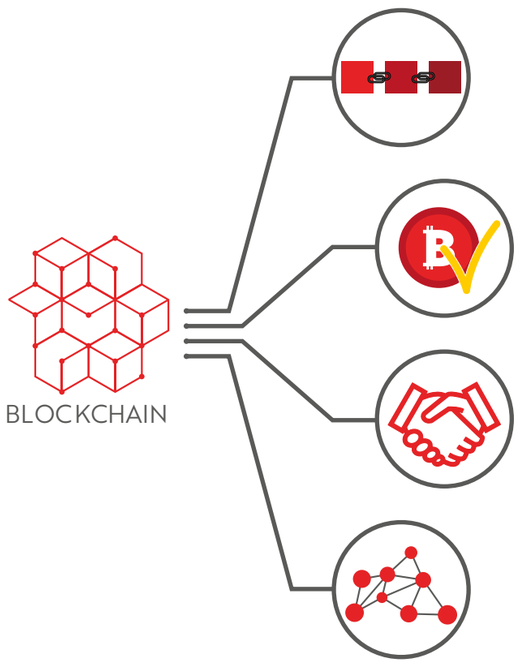
Jako kontrast do powyższej sytuacji, wyobraźmy sobie system opierający się na sieci baz danych, które umożliwiają wszystkim uczestnikom, na równych prawach, efektywne i bezpieczne zapisywanie, rozpowszechnianie i przechowywanie informacji. Dodatkowo, to system mogący działać poprawnie bez centralnego zarządcy lub administratora, w którym pełna historia danych jest zawsze dostępna, a raz zapisane informacje nie mogą być zmienione. Innymi słowy, jest to system zaprojektowany w taki sposób, że informacje przechowywane i komunikowane za pośrednictwem sieci mają bardzo wysoki poziom wiarygodności i bezpieczeństwa, a uczestnicy sieci mają transparentny dostęp do wspólnego, zaufanego źródła informacji. Tak można najprościej opisać system oparty o technologię blockchain.

W praktyce blockchain to rozproszona, współdzielona i zaufana baza danych, zarządzana przez sieć komputerów, które działają według ustalonych z góry zasad zwanych protokołem blockchain. Każdy uczestnik sieci ma swoją kopię bazy, działa na równych prawach, a także może inicjować i weryfikować zmiany. Każdy ma wgląd do bazy danych, ale nikt jej nie kontroluje, natomiast wszystkie zmiany odbywają się na zasadach konsensusu wymuszonego przez protokół i w niektórych przypadkach system nagród za aktywny udział w sieci. Blockchain działa autonomicznie, bez zcentralizowanego nadzoru.

Nazwa blockchain, czyli łańcuch bloków, pochodzi od sposobu, w jakim dane są zorganizowane. Jest to wydłużająca się lista połączonych ze sobą bloków, w których zgrupowana jest określona ilość zmian w formie transakcji. Każdy nowy blok jest dołączany do końca łańcucha i zawiera, między innymi, znacznik czasu, który określa, kiedy został stworzony, a także odnośnik do poprzedniego bloku. Całość zabezpieczona jest przy wykorzystaniu kryptografii. Zmiana danych transakcji zawartej wcześniej w którymkolwiek bloku wymagałaby modyfikacji wszystkich następujących po nim bloków, przez co zmiany w zapisach historycznych są praktycznie niewykonalne ze względu na trudność związaną z przeliczeniem zawartości bloków. Poza tym, każda nieupoważniona zmiana byłaby natychmiast zauważona przez uczestników sieci.

Z biegiem lat termin „blockchain" zaczął odnosić się potocznie do systemów mających wszystkie lub tylko niektóre cechy opisane powyżej. Dziś istnieje ogromna różnorodność systemów opartych na technologii blockchain. By ułatwić zrozumienie, czym jest dany blockchain, dodawane są przymiotniki: publiczny, prywatny, zdecentralizowany, z ograniczonym lub nieograniczonym dostępem, itd. Bardziej szczegółowy opis typów sieci i opisy najpopularniejszych platform znajdują się w rozdziale Technologia.

Podsumowując, blockchain to:



Rozproszona baza danych w formie łańcucha bloków, które zawierają historię wszystkich zweryfikowanych i zaakceptowanych przez wszystkich zmian (transakcji).

Zasady tworzenia i weryfikacji transakcji, które odzwierciadlają zmiany.

Zasady konsensusu, które decentralizują kontrolę nad łańcuchem bloków, w niektórych przypadkach wiążący się z system nagród.

Rozproszona sieć łącząca równorzędnych uczestników działających według tych samych zasad (często określana jako sieć P2P - Peer-to-Peer, czyli „osoba do osoby").

BLOCKCHAIN W BIZNESIE

Blockchain to nowa technologia, która ma potencjał, by zasadniczo zmienić sposób, w jakim partnerzy działający w połączonym cyfrowo ekosystemie dzielą się informacjami i jakich używają reguł biznesowych. Technologia umożliwia tworzenie zupełnie nowej klasy aplikacji rozproszonych i będzie miała ogromne znaczenie dla innowacji w obszarze modeli oraz procesów biznesowych.

Korzyści związane z wykorzystania technologii blockchain wynikają z cech, które odróżniają ją od tradycyjnych rozwiązań:

- **Niezmienność i integralność danych** – w sieci blockchain nie można zmodyfikować potwierdzonych transakcji, co rozwiązuje jedną z głównych trudności w projektowaniu i działaniu systemów informatycznych. Blockchain może być postrzegany jako jedyna wersja prawdy o danych akceptowana przez wszystkich uczestników ekosystemu.
- **Pełność i trwałość danych** – dopóki blockchain pozostaje aktywny, dostępne są wszystkie wprowadzone do niego dane ponieważ każdy węzeł systemu ma pełną kopię łańcucha bloków, to w naturalny sposób eliminuje pojedyncze punkty awarii i konieczność zapewnienia redundancji systemu.
- **Bezpieczeństwo danych** – wykorzystanie technik kryptograficznych i autentykacji (uwierzytelniania), daje wyższy poziom bezpieczeństwa niż tradycyjne rozwiązania.
- **Decentralizacja konsensusu** – dodanie nowych danych do bazy blockchain wymaga zgody wszystkich uczestników sieci, co eliminuje potrzebę zaufanych pośredników i umożliwia uczestnikom procesów zaimplementowanych na systemie blockchain bezpośrednie działania miedzy sobą.
- **Audytowalność** – blockchain zapewnia integralność, niezmienność i transparentność zapisanych na nim danych, umożliwiając precyzyjne audyty zarejestrowanych transakcji.
- **Eliminacja problemu podwójnego wydatkowania** – blockchain rozwiązał długotrwały problem wielokrotnego wysłania tych samych danych w rozproszonych sieciach transakcyjnych, eliminując potrzebę korzystania z centralnych podmiotów rozliczeniowych.
- **Automatyzacja** – możliwość optymalizacji procesów, poprzez usunięcie pośredników i konieczności centralnego procesowania danych, a także eliminację ręcznych interwencji, często związanych z hierarchicznymi organizacjami. Tego typu automatyzacja będzie się wiązać się z obniżką kosztów.
- **Innowacje** – technologia blockchain może być podstawą do budowania całkowicie nowych modeli biznesowych i ekosystemów, a także tworzenia nowych łańcuchów wartości.

SMART CONTRACT'Y W NOWYCH MODELACH BIZNESOWYCH

Koncepcja smart contract'ów, określanych również jako inteligentne kontrakty, nie jest nowa, ale to właśnie blockchain, a dokładnie platforma Ethereum, umożliwiła ich tworzenie i właściwe funkcjonowanie w cyfrowym świecie. W roku 2018, dzięki kolejnym platformom, smart contract'y uzyskały technologiczny potencjał do dynamicznego rozwoju.

Zgodnie z tradycyjnym ujęciem, umowa określa zasady dostarczenia produktów lub usług za określoną cenę, uzgodnione pomiędzy sprzedającym i kupującym. smart contract pozwala na zaangażowanie wielu stron transakcji w jednym lub wielu systemach rozliczeniowych, działających w ramach transparentnego modelu rozliczeń, dzięki czemu wszystkie strony mają poczucie pełnego komfortu w zakresie działania nawet bardzo złożonych reguł takiej elektronicznej umowy.

W przyszłości smart contract'y mogą zmienić lub wprowadzić nowe modele biznesowe w wielu branżach, zmniejszą się bowiem bariery tworzenia bardziej złożonych umów w postaci elektronicznej i jednocześnie zostaną dostarczone rozwiązania do ich natychmiastowej wykonalności. Na kolejnym etapie rozwoju technologii powstaną prawdziwie inteligentnie „myślące" umowy, które będą dostosowywały własne reguły w czasie, m.in. na podstawie analizy zmiennych dostarczonych przez sztuczną inteligencję. Kolejny etap rozwoju inteligencji umów pozwoli na wykrywanie luk i błędów, których szybkie eliminowanie będzie podnosiło konkurencyjność i efektywność danego ekosystemu lub modelu biznesowego firmy.

Kilka przykładów możliwości wykorzystania smart contract'ów w praktyce:

- **Ubezpieczenia** – koszty ubezpieczenia samochodu rozliczane w czasie rzeczywistym, uzależnione m.in. od tego jak bezpiecznie prowadzimy samochód i od tego, jaki średni poziom bezpieczeństwa uzyskujemy w porównaniu do pozostałych ubezpieczonych kierowców.
- **Nieruchomości** – automatyczne zatwierdzenie notarialne zmiany własności, gdy tylko zostaną spełnione wszystkie warunki ustalone przez strony (np. zapłata uzgodnionej sumy).
- **Telekomunikacja** – abonament za usługi telekomunikacyjne pomniejszony o wartość danych wycenionych rynkowo i udostępnionych przez klienta w celu ich odsprzedaży, po podziale prowizji pomiędzy dostawcą usług telekomunikacyjnych, klientem i innymi stronami umowy.

Używając smart contract'ów możemy zmienić nasz model działania i sposób zaangażowania klientów. Klient może stać się partnerem w biznesie i wspólnie z nami czynnie budować wartość wspólnej inicjatywy, z którą będzie się utożsamiał, ponieważ jego zaangażowanie będzie miało znaczny wpływ na jakość i cenę usług. W tym nowym modelu sterowanym przez smart contract'y klient zmienia się z odbiorcy usług na współtwórcę całego ekosystemu. Jeśli smart contract'y staną się powszechne, może okazać się, że ich rozumienie stanie się niezbędne do budowy oferty nowych usług, opartych o współpracę wszystkich stron umowy.

NA CO ZWRACAĆ UWAGĘ PRZY WDROŻENIACH SYSTEMÓW OPARTYCH NA BLOCKCHAIN

Blockchain oferuje wiele atrakcyjnych funkcji i możliwości, ma jednak pewne ograniczenia. Ich zrozumienie ma istotne znaczenie dla identyfikacji obszarów zastosowań i ustalania priorytetów inwestycyjnych. W dalszej części raportu zamieszczamy wybrane przykłady użycia, poniżej zamieszczamy listę potencjalnych barier które zaobserwowaliśmy na tym etapie rozwoju technologii:

Wydajność i skalowalność – intensywność obliczeniowa i potrzebna do synchronizacji danych w sieciach blockchain może ograniczać skalowalność i powodować opóźnienia w przetwarzaniu transakcji. Większość platform blockchain ma znacząco niższą wydajność niż tradycyjne systemy transakcyjne.

Kwestie prawne i regulacyjne – niewiele aspektów używania technologii blockchain jest dziś formalnie uregulowanych. Firmy wdrażające systemy oparte o blockchain powinny na bieżąco śledzić zmiany i postanowienia w tym obszarze.

Bezpieczeństwo – w przypadku zastosowań biznesowych, w szczególności tych opartych na sieciach prywatnych, istnieje zwiększone ryzyko ataku hackerskiego (na przykład przejęcia kluczy prywatnych) lub wypływu danych dostarczanych z systemów zewnętrznych, takich jak czujniki IoT.

Interoperacyjność – brak standardów i ciągła ewolucja platform oraz systemów może być czynnikiem ograniczającym szeroką adopcję. Blockchain można porównać do prostej tabeli, i jako taki nie nadaje się do przechowywania dużej ilości danych. Powoduje to konieczność współdziałania z zewnętrznymi bazami danych.

Ograniczony zakres danych – niezmienialny zapis ogranicza zakres danych, jakie mogą być zapisywane w sieci blockchain (na przykład dane osobowe, które zgodnie z RODO muszą być usunięcie na żądanie użytkownika).

Zarządzanie – w przypadku użycia sieci prywatnych niektóre funkcje sieci blockchain będą delegowane do określonych podmiotów, co będzie wymagało wypracowania nowych reguł współpracy biznesowej.

INWESTYCJE W TECHNOLOGIĘ BLOCKCHAIN

Systematycznie rośnie poziom inwestycji w technologię blockchain i DLT. Zgodnie z danymi IDC, w 2018 r. poziom inwestycji w technologię blockchain osiągnie poziom 1,5 miliarda dolarów, rosnąc do 2022 r. w tempie ponad 70%[2] rocznie. Rosną wydatki, zarówno w kategorii tradycyjnego finansowania (IPO oraz wczesne zaangażowanie VC, w tym finansowanie przez aniołów biznesu), jak i finansowania alternatywnego w postaci ICO.

2 *www.idc.com/getdoc.jsp?containerId=prUS44150518*

ICO

Initial Coin Offering (w skrócie ICO[3]) jest metodą pozyskiwania kapitału poprzez sprzedaż określonego zasobu tokenów cyfrowych wraz z obietnicą, że tokeny te będą wykorzystywane jako narzędzie dające dostęp do usług oferowanych przez daną platformę lub będą stanowiły elektroniczny odpowiednik papieru wartościowego (na przykład w formie udziału w przedsięwzięciu lub prawa do części zysku). Koncepcja tokenu opisana jest szerzej w części Technologia.

Aby daną zbiórkę móc określić mianem ICO, musi ona spełniać kilka podstawowych kryteriów:

TOKENY CYFROWE

zbierający fundusze generuje specjalne tokeny cyfrowe, które są potem oferowane kupującym (w formie oferty zamkniętej lub publicznej)

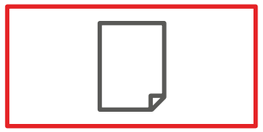
BRAK POŚREDNIKÓW

zbiórka odbywa się w ramach zdecentralizowanej sieci, bez udziału pośrednika w postaci zaufanej strony trzeciej (tę rolę pełni Smart Contract)

SPRZEDAŻ ELEKTRONICZNA

sprzedaż tokenów odbywa się wyłącznie w systemie elektronicznym, bez sprzedaży bezpośredniej lub stacjonarnej

WHITEPAPER



oferujący przekazuje informacje o projekcie w tzw. whitepaperze, który pełni funkcję oferty dla potencjalnych nabywców

ICO jako mechanizm zbierania środków powstał z myślą o projektach opartych na technologii blockchain (w tym kryptowalutowych), jednak jego potencjalne wykorzystanie jest znacznie szersze. ICO może być wykorzystywane również przez twórców projektów niezwiązanych bezpośrednio z technologią blockchain, w których jednak pewna forma tokenu cyfrowego może mieć zastosowanie.

Z punktu widzenia organizatorów zbiórek, ICO ma kilka ważnych zalet, które sprawiają, że mechanizm ten może być alternatywą dla tradycyjnych metod pozyskiwania kapitału. Do głównych zalet ICO należą m.in.:

- **Koszty** – niższy koszt pozyskiwanego kapitału, w stosunku do tradycyjnych metod (kredyty bankowe, fundusze inwestycyjne, IPO).
- **Elastyczność** – możliwość elastycznego dobierania warunków finansowania – to organizator zbiórki określa warunki i przedstawia ofertę potencjalnym kupującym.
- **Klienci** – budowanie sieci lojalnych użytkowników rozwiązania – nabywcy tokenów są bardziej związani z daną usługą i często sami promują ją w swojej sieci kontaktów.

ICO może być skutecznym sposobem na rozwój projektów, cechujących się występowaniem efektu sieciowego[4]. Tego typu projekty osiągają większe korzyści z przeprowadzonej zbiórki ICO, ponieważ uzyskują jednocześnie kapitał na rozwój oraz użytkowników.

3 W różnych opracowaniach można także zetknąć się z następującym nazewnictwem: token sales, Initial Coin Public Offering, Initial Token Offering, Initial Crypto-Token Offering, czy Initial Token Sales.

4 W rozwiązaniach cechujących się występowaniem efektu sieciowego korzyści dla użytkowników są tym większe, im większa jest liczba jego użytkowników. Dobrym przykładem działania tego zjawiska są media społecznościowe, np. Facebook.

ICO może służyć nie tylko finansowaniu projektów start-upowych, ale również bardziej dojrzałych rozwiązań. Tego typu projekty są dobrze przyjmowane przez nabywców tokenów, ponieważ dużym problemem zbiórek ICO jest niska wiarygodność sprzedających tokeny (w przypadku bardziej dojrzałych projektów, ich wiarygodność jest znacząco wyższa). Dodatkowo, ICO może być również łączone ze standardowymi metodami finansowania.

Organizując własne ICO należy być świadomym wielu potencjalnych ryzyk, które mogą spowodować niepowodzenie projektu. Bardzo istotnym aspektem jest bezpieczeństwo, ponieważ zbiórki ICO często padają ofiarą ataków hackerskich. Każdy organizator zbiórki ICO powinien również pamiętać o kwestiach prawnych i podatkowych, które muszą zostać spełnione, aby zbiórka była legalna. W związku z tym, zasadne jest skorzystanie z profesjonalnego wsparcia ze strony wyspecjalizowanych kancelarii prawnych oraz doradców, w tym m.in. od cyberbezpieczeństwa.

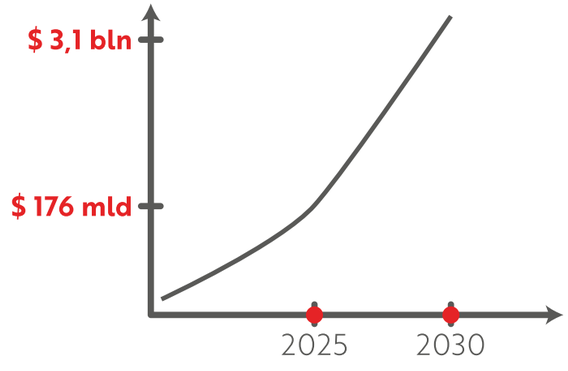
PRZYSZŁOŚĆ BLOCKCHAIN – KIERUNKI ROZWOJU

Przydatność i zalety technologii blockchain są obecnie pilotowane, a gotowe wdrożenia pojawiają w większości sektorów gospodarki: finansach, ubezpieczeniach, handlu detalicznym, przemyśle, opiece zdrowotnej oraz sektorze publicznym. Wczesne projekty i analizy pokazują znaczące możliwości zwiększenia efektywności i usprawniania systemów transakcyjnych, procesów śledzenia aktywów i ich audytowania oraz zarządzaniem danymi.

W 2017 roku firma analityczna Gartner, wykorzystując nową metodologię przewidywania wartości, określiła globalną wartość dodaną wynikająca z innowacji związanych z technologią blockchain na ponad 176 miliardów dolarów do 2025 roku, i przewiduje, że przekroczy ona 3,1 biliona dolarów do 2030 roku[5].

Z punktu widzenia technologicznego blockchain jest jeszcze na wczesnym etapie rozwoju, ale jego zmiany następują niezwykle dynamicznie. Każdy miesiąc przynosi wiadomości o powstaniu nowych platform, które przełamują kolejne bariery skalowalności i wydajności, przy jednoczesnym obniżeniu kosztów eksploatacji.

Rynek czeka jeszcze główna faza konsolidacji, ale już teraz są pierwsze przykłady łączenia się platform prywatnych z sieciami publicznymi i pojawiają się pierwsze przejęcia oraz fuzje firm. Nie powinno to zniechęcać do eksperymentowania i wdrażania systemów. Ważną cechą technologii blockchain jest to, że w znaczący sposób ułatwia integrację i przenośność systemów.



5 Gartner, *Forecast: Blockchain Business Value, Worldwide, 2017-2030*

Parlament Europejski dostrzegł doniosłość tematu i przyjął w październiku 2018 roku rezolucję w sprawie technologii rozproszonego rejestru i łańcuchów bloków, która w ostatnim paragrafie podsumowuje ją następująco:

PE podkreśla, że Unia ma wielką szansę, by stać się światowym liderem w sektorze technologii DLT oraz wiarygodnym podmiotem uczestniczącym w rozwoju tej technologii i kształtowaniu rynków na całym świecie we współpracy z naszymi międzynarodowymi partnerami.

REKOMENDACJE

Liderzy poszczególnych funkcji w firmach, takich jak informatyka, finanse, zasoby ludzkie i zaopatrzenie, a także decydenci w administracji publicznej powinni zaznajomić się z doświadczeniami pierwszych projektów pilotażowych i wdrożeniowych, aby ocenić przydatność technologii blockchain do własnych aplikacji i procesów. W dalszej części raportu prezentujemy przykłady zastosowań, które będą mogły służyć jako wzorce do własnych rozwiązań. Przykładowa mapa drogowa działań może zawierać:

1. poznanie charakterystyk platform i różnic pomiędzy sieciami publicznymi i prywatnymi,
2. identyfikację procesów biznesowych które dziś sprawiają najwięcej kłopotów lub są kosztowne w utrzymaniu pod kątem optymalizacji przy wykorzystaniu technologii blockchain,
3. podjęcie pilotażowych wdrożeń i ich oceny pod względem zwrotu poniesionych inwestycji oraz oceny ryzyka w tym uwarunkowań prawnych i regulacyjnych,
4. wyszukanie i pozyskanie potencjalnych partnerów do wdrożenia pierwszych systemów rozproszonych.

Cytując za Harvard Business Review:

Technologią, która najprawdopodobniej zmieni kolejną dekadę biznesu jest blockchain, a nie sieci społecznościowe, big data, chmura, robotyka, czy nawet sztuczna inteligencja[6].

6 D. Tapscott, A. Tapscott, 2016, *The Impact of the Blockchain Goes Beyond Financial Services*

PODSTAWOWE KONCEPCJE TECHNOLOGII BLOCKCHAIN

Technologia blockchain istnieje już od 10 lat i jest szeroko opisana. W tej części raportu pomijamy podstawy takie jak transakcja, blok, sieć rozproszona itd. Zamieszczamy natomiast krótkie opisy najważniejszych według nas elementów architektury: kryptografii, zasad konsensusu oraz tematów takich jak open source, rodzaje sieci, skalowalność i wydajność, tokeny, smart contract'y (inteligentne kontrakty). Opisujemy też najpopularniejsze platformy.

Więcej informacji na temat podstaw technologii blockchain można znaleźć w następujących źródłach:

- Wikipedia – hasło: Blockchain
- Antonopoulos, Mastering Bitcoin 2nd Edition - Programming the Open Blockchain,
- Antonopoulos, Mastering Ethereum: Building Smart Contracts and DApps 1st Edition.

KRYPTOGRAFIA UŻYWANA W SYSTEMACH BLOCKCHAIN

Kryptografia, a w szczególności kryptografia asymetryczna i jej użycie do składania i weryfikacji podpisów cyfrowych, oraz wykorzystanie funkcji skrótu (ang. hash) leżą u podstaw technologii blockchain i są szeroko wykorzystywane w procesie inicjowania, walidacji i zatwierdzania transakcji, budowaniu bloków oraz dodawaniu bloków do łańcucha. Paradoksalnie, szyfrowanie nie jest zazwyczaj stosowane w systemach blockchain, bo jedną z jego cech jest transparentność, choć oczywiście są zastosowania, w których szyfrowanie danych zapisywanych w blokach może być pożądane.

W kryptografii asymetrycznej mamy do czynienia z parą powiązanych ze sobą matematycznie kluczy, kluczem publicznym i kluczem prywatnym. Klucz publiczny może być udostępniony każdemu, a odpowiadający mu klucz prywatny powinien być przez właściciela trzymany w tajemnicy. Dane zaszyfrowane za pomocą klucza publicznego można rozszyfrować tylko przy pomocy odpowiadającego mu klucza prywatnego. Dane zaszyfrowane przy pomocy klucza prywatnego mogą być rozszyfrowane przez każdego, kto ma odpowiadający mu klucz publiczny.

Funkcja skrótu to funkcja, która przyporządkowuje dowolnie dużej wiadomości krótką, zwykle posiadającą stały rozmiar unikalną wartość, która stanowi coś w rodzaju elektronicznego „odcisku palca" tej wiadomości. Funkcja skrótu ma te cechy, że jest łatwo ją obliczyć, ale praktycznie niemożliwe jest odtworzenie oryginalnej wiadomości na podstawie skrótu (jednokierunkowość) oraz że skrót danej wiadomości będzie unikalny (odporność na kolizje).

Powyższe techniki wykorzystuje się by zapewnić:

- **unikalność** – każda wiadomość elektroniczna posiada unikalny podpis cyfrowy ściśle związany z tą wiadomością
- **integralność** – jakakolwiek zmiana w treści wiadomości podpisanej cyfrowo unieważnia podpis
- **niezaprzeczalność** – tylko osoba posiadająca klucz prywatny może wygenerować podpis pod wiadomością
- **uwierzytelnianie** – odbiorca wiadomości może ustalić jego pochodzenie poprzez potwierdzenie tożsamości nadawcy
- **poufność** – szyfrowanie wiadomości zabezpiecza ją przed podsłuchem i fałszerstwem

Więcej informacji na temat kryptografii i funkcji skrótu można znaleźć w następujących źródłach:

- K. Bartyzel, Kryptografia asymetryczna i jej zastosowanie w algorytmach komunikacji
- Wikipedia – hasło: Kryptografia klucza publicznego
- Wikipedia – hasło: Public-key cryptography
- Wikipedia – hasło: Funkcja skrótu
- Wikipedia – hasło: Hash function

ZASADY KONSENSUSU

Konsensus jest najważniejszym elementem każdej sieci blockchainowej. Jest to sposób, w jakim wszystkie węzły w sieci podejmują decyzję o tym, czy konkretna operacja (np. przesłanie informacji lub tokenów) może być zaakceptowana i dodana do bloku danych i w związku z czym niepodważalna. Konsensus jest zaszyty w oprogramowaniu i nie wymaga fizycznych osób ani instytucji do jego osiagniecia. Od konsensusu zależy nie tylko, jak bardzo bezpieczna będzie dana sieć blockchainowa, ale również jak szybko będzie mogła ona zatwierdzać kolejne operacje i ile to będzie kosztować jej użytkowników.

Sposób osiągania konsensusu w sieciach blockchainowych stanowi wciąż główny problem w zakresie osiągania stanu optymalnego, rozumianego jako maksymalne bezpieczeństwo sieci przy jednocześnie możliwie jak najniższych kosztach i jak najwyższej prędkości zatwierdzania bloków (inaczej wydajności sieci). Obecnie najpopularniejszymi sposobami osiągania konsensusu są:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Delegated Proof of Stake (DPoS)
- Proof of Authority (PoA)

Proof of Work to najstarsza metoda, wykorzystana w sieci Bitcoin. W tym typie sieci wszystkie węzły mają możliwość zatwierdzenia kolejnego bloku danych, a prawdopodobieństwo dodania kolejnego bloku przez węzeł rośnie w momencie, gdy dostarcza on więcej mocy (określonej przez twórcę Bitcoina jako praca). W związku z tym cała sieć wymaga dostarczenia bardzo dużej ilości energii elektrycznej, która jest następnie zamieniana na moc komputerów zamykających bloki danych. To prowadzi do wysokich kosztów utrzymania tego typu sieci. Dodatkowo, konieczność zatwierdzania każdego bloku przez wszystkich użytkowników znacząco spowalnia cały proces i powoduje, że sieć jest mniej efektywna od standardowych, scentralizowanych rozwiązań. W związku z tym charakteryzuje się znacznie mniejszą możliwością skalowania.

Proof of Stake to model konsensusu, który można porównać do praw majątkowych z tytułu udziałów w spółce kapitałowej. Nagroda za zatwierdzenie bloku jest rozdysponowana zgodnie z liczbą posiadanych tokenów. W związku z tym, nie ma konieczności podłączania do sieci tak dużej mocy obliczeniowej, jak w przypadku Proof of Work, dzięki czemu cały system jest znacznie tańszy.

Dodatkowo, sieci oparte o konsensus Proof of Stake są bardziej efektywne i dzięki temu mają większy potencjał skalowalności. Niemniej należy pamiętać o tym, że od pewnego momentu możliwości skalowania tych sieci spadają, przede wszystkim z powodu rosnącej liczby węzłów zatwierdzających.

Delegated Proof of Stake to modyfikacja PoS, polegająca na tym, że użytkownicy sieci głosują na jednostki, które w ich ocenie będą najlepiej zatwierdzały bloki danych. Głosowanie odbywa się przy zatwierdzaniu każdego kolejnego bloku i kończy się w momencie, gdy uda się osiągnąć satysfakcjonującą liczbę węzłów zatwierdzających. Dzięki takiej konstrukcji oraz mechanizmowi rankingowemu, jednostki zatwierdzające bardziej dbają o jakość operacji dodawanych do bloku, niż w standardowym PoS. Koszty działania są również znacząco niższe niż w przypadku PoW. Podobnie jednak jak PoS, również delegowana wersja tego konsensusu musi mierzyć się z problemem zbytnio rozbudowanej sieci jednostek potwierdzających operacje, ograniczających wydajność całej sieci. Dodatkowo, sieci delegowane mogą być częściej wstrzymywane w wyniku braku wymaganej liczby wybranych węzłów zatwierdzających.

Proof of Authority bazuje z kolei na odmiennym podejściu. W ramach tego konsensusu istnieją z góry wyznaczone węzły nadzorujące, które stale zajmują się autoryzowaniem operacji. Tego typu sieci wymagają centralnego nadzoru, ponieważ w ich przypadku liczba węzłów powinna być dostosowywana do wielkości samej sieci (w przypadku pozostałych metod konsensusu odbywa się to często w wyniku porozumienia uczestników sieci). Ważne jest przy tym bezpieczeństwo, które spada wraz ze zmniejszającą się liczbą węzłów oraz ich koncentracją (węzły skoncentrowane w jednym miejscu, np. wspólnej serwerowni są znacznie bardziej narażone na skuteczny atak niż jednostki rozproszone). Dzięki temu jednak, sieci te są bardzo wydajne oraz pozwalają na skalowanie do dużych rozmiarów.

Tabela poniżej prezentuje podsumowanie najważniejszych cech opisanych typów konsensusu. Należy jednak podkreślić, że każda z tych sieci ma swoje wady i zalety, a wybór konkretnego rodzaju konsensusu powinien być podjęty po szczegółowej analizie potrzeb związanych z danym systemem.

	BEZPIECZEŃSTWO	WYDAJNOŚĆ I SKALOWALNOŚĆ	KOSZTY	WYKORZYSTANIE
PoW	●●● Wysokie w przypadku rozbudowanych sieci	●○○ ●○○ Niska wydajność i bardzo ograniczona skalowalność	●●● Bardzo wysokie (głównie z powodu kosztów energii elektrycznej)	Sieci publiczne, wykorzystujące kryptowaluty
PoS	●●○ Niższe niż w PoW, zależne od dywersyfikacji tokenów (rośnie wraz z dużą dywersyfikacją)	●●○ ●●○ Wyższa niż w przypadku PoW, jednak ograniczona od pewnego momentu rozwoju	●●○ Niższe niż w PoW	Sieci publiczne lub hybrydowe
DPoW	●●● Wyższe niż w przypadku PoS	●●○ ●●○ Wyższa niż w przypadku PoW, jednak ograniczona od pewnego momentu rozwoju	●●○ Niższe niż w PoW	Sieci publiczne lub hybrydowe
PoA	Zależne od liczby jednostek nadzorujących sieć (rośnie wraz z liczbą tych jednostek)	●●● ●●● Bardzo wysoka wydajność i skalowalność zależna od nakładów na sprzęt	●●○ Niższe niż w PoW, zależne od liczby jednostek nadzorujących sieć	Sieci prywatne

Warto jeszcze przyjrzeć się problemowi jednoczesnego zapewnienia jak najwyższego bezpieczeństwa sieci oraz jej wydajności. Bezpieczeństwo sieci blockchainowych rośnie wraz z liczbą węzłów autoryzujących operacje. Im większa liczba węzłów, tym dłużej trwa weryfikacja każdej kolejnej operacji. To oznacza, że sieć zawierająca więcej węzłów będzie zatwierdzała mniej operacji. W związku z tym, każde zwiększenie bezpieczeństwa lub wydajności będzie się odbywało kosztem drugiego parametru. Istnieją sposoby na eliminowanie tej negatywnej tendencji, jednak jak na razie nie ma takiej możliwości.

Cały czas trwają intensywne poszukiwania w kierunku znalezienia takiej metody konsensusu, w której wydajność i bezpieczeństwo sieci będą na najwyższym poziomie. Kilka projektów już dziś z sukcesem testuje tzw. metody mieszane np. projekt Zilliqua stosuje autorską metodę konsensusu PoW, zmodyfikowanego w taki sposób, że węzły są grupowane w ramach mniejszych sieci, które są następnie wybierane losowo do potwierdzania transakcji w kolejnych blokach.

OPEN SOURCE I JEGO ZNACZENIE DLA ROZWOJU TECHNOLOGII BLOCKCHAIN

Open source zdobywa coraz większą popularność wśród twórców nowych rozwiązań programistycznych. Coraz częściej kod jest udostępniany publicznie nie tylko przez niezależnych twórców rozwiązań non-profit, ale również przez globalne firmy informatyczne.

Kod wystawiony na widok publiczny jest bardzo szybko sprawdzany przez jego użytkowników, w celu ustalenia luk w zabezpieczeniach oraz potencjalnych usterek. Kod open source jest również często obiektem weryfikacji prowadzonej przez niezależnych audytorów oraz tzw. white hat (termin określający hackerów, których zadaniem jest legalne odszukiwanie luk i testowanie zabezpieczeń komputerowych). Tak szeroka weryfikacja kodu znacząco zwiększa bezpieczeństwo oraz niezawodność oprogramowania.

Użytkownicy oprogramowania typu open source mogą w prosty sposób modyfikować je do swoich zmieniających się potrzeb. Również nowi użytkownicy systemu mogą włączyć się w tworzenie modyfikacji, sprawiając, że oprogramowanie zaspokaja nowe potrzeby, których twórcy pierwotnie nie zaobserwowali. Skraca to również czas aktualizacji oprogramowania i umożliwia szybsze reagowanie na zmiany potrzebnych funkcjonalności.

Oprogramowanie, którego kod jest wystawiony na widok publiczny przyciąga do siebie grupę użytkowników, którzy mogą łączyć swoje siły w celu stworzenia większych oraz bezpieczniejszych modyfikacji danego oprogramowania. Użytkownicy, którzy są zaangażowani we współtworzenie kodu, są znaczeni bardziej przywiązani do danego oprogramowania oraz zaczynają się specjalizować w obsłudze tego konkretnego rozwiązania. Zwiększa to przywiązanie użytkowników do wykorzystywanego oprogramowania i wydłuża jego cykl życia.

Większość twórców rozwiązań opartych na technologii blockchain wykorzystuje powyższe możliwości oraz upublicznia swój kod programistom z całego świata. W sieciach publicznych jest to standardem, głównie ze względu na niski poziom zaufania. Za tego typu rozwiązaniami stoją najczęściej niewielkie i nieznane zespoły programistów, dlatego zbiorowa weryfikacja i ocena kodu pozwala uzyskać potwierdzenie wiarygodności danego projektu.

Znaczenie open source jest również bardzo istotne w przypadku sieci prywatnych oraz hybrydowych. Najbardziej podkreślaną zaletą sieci blockchainowych jest ich bezpieczeństwo, dlatego tego typu sieci muszą być w szczególności odporne na ataki z zewnątrz. W ich przypadku kod jest upubliczniany, w celu weryfikacji jego bezpieczeństwa przez niezależnych programistów i audytorów. Dodatkowo, rozwiązania te przybierają najczęściej formę platform, które mogą być wykorzystywane przez wielu różnych użytkowników, bez konieczności tworzenia rozwiązań „szytych na miarę", na rzecz personalizacji. W tym przypadku, włączenie nowych grup użytkowników we współtworzenie kodu pozwala lepiej dostosować rozwiązanie do ich potrzeb.

RODZAJE SIECI

Istnieją trzy zasadnicze rodzaje sieci blockchainowych:

PUBLICZNA

Główną cechą charakterystyczną sieci publicznej jest to, że może się do niej podłączyć każdy, a sama sieć działa w zdecentralizowany, autonomiczny sposób. Brak jest jakiejkolwiek jednostki nadzorującej, a wszystkie decyzje dotyczące rozwoju tej sieci podejmowane są przez jej użytkowników.

PRYWATNA

Przeciwieństwem sieci publicznej jest sieć prywatna, tworzona najczęściej na potrzeby zamkniętej organizacji, przedsiębiorstwa lub grupy takich podmiotów. Dostęp do niej mają tylko konkretne jednostki, a polityka sieci jest kształtowana przez jednostkę nadzorującą.

HYBRYDOWA (publiczno-prywatna)

Połączeniem obu typów jest sieć hybrydowa. Jest to szczególny typ sieci prywatnej, która ma własną politykę zarządzania siecią i dostęp mają do niej tylko uprawnione jednostki. W przeciwieństwie jednak do całkowicie publicznej sieci, systemy hybrydowe wykorzystują często infrastrukturę sieci publicznej, np. w celu rozliczeń pomiędzy użytkownikami.

Więcej na temat rodzajów sieci:
K. Piech (red.), Leksykon pojęć na temat technologii blockchin i kryptowalut

POPULARNE PLATFORMY

Wraz z coraz większym rozwojem oraz kolejnymi wdrożeniami technologii blockchain, popularność zdobywają platformy typu open source. Ich sukces opiera się w głównej mierze na elastyczności, z jaką mogą być implementowane w celu zaspokojenia różnych potrzeb biznesowych oraz wielkości społeczności programistów, zaangażowanych w jej rozwój. Dodatkowo platforma, która może zostać wdrożona efektywnie jako rozwiązanie pewnego problemu biznesowego musi zapewniać odpowiednią wydajność sieci oraz skalowalność. Więcej na ten temat w części *Skalowalność i wydajność*.

Obecnie jednymi z najczęściej wykorzystywanymi platformami bazującymi na technologii blockchain i używanymi do wdrożenia smart contract'ów i rozproszonych aplikacji są:

HYPERLEDGER FABRIC to standard architektury blockchainowej, rozwijanej w ramach projektów Hyperledger, zarządzanych przez Linux Foundation. Wersja Fabric umożliwia tworzenie własnych aplikacji korzystających z sieci niepublicznych. Dodatkowo, umożliwia on również tworzenie oraz działanie smart contract'ów. Celem samego projektu Hyperledger jest wspólne rozwijanie rozwiązań opartych na technologii rozproszonych rejestrów, poprzez zrzeszenie współpracujących ze sobą organizacji i firm komercyjnych. Więcej informacji na temat Hyperledger Fabric dostępnych jest pod tym adresem.

ETHEREUM to obecnie najpopularniejsza platforma do tworzenia aplikacji opartych na technologii blockchain, umożliwiająca tworzenie aplikacji w ramach sieci publicznej lub prywatnej (w tym przypadku działa raczej jako sieć hybrydowa, ponieważ zamknięte grono użytkowników korzysta z publicznej sieci do zatwierdzania operacji). W związku z tym, że aplikacje tworzone na platformie Ethereum korzystają z publicznej sieci jednostek zatwierdzających, koszty funkcjonowania zależą od rynkowej ceny gasu (jednostki rozliczeniowej). Więcej informacji na temat platformy Ethereum dostępnych jest pod tym adresem.

Rozwijane są również inne platformy, które mają duży potencjał:

EOS to platforma do tworzenia zdecentralizowanych aplikacji, bazująca na konsensusie DPoS. Dzięki temu koszty funkcjonowania aplikacji w sieci opartej o ten rodzaj protokołu są niższe niż w standardowych sieciach opartych na PoW. Ze względu na wady konsensusu DPoS oraz faktu, że EOS jest siecią publiczną, rozwiązanie to nie powinno być stosowane w zamkniętych systemach wymagających wysokiego poziomu bezpieczeństwa i poufności danych. Z drugiej jednak strony ma duży potencjał, jeśli chodzi o wykorzystanie w ogólnodostępnych aplikacjach blockchainowych. Więcej informacji na temat platformy EOS dostępnych jest w White Paper projektu.

IOTA to platforma przeznaczona do integracji urządzeń w ramach sieci Internet of Things (Internetu Rzeczy). W ramach systemu IOTA, każda pojedyncza transakcja formuje nowy blok i weryfikuje się sama. Weryfikacja transakcji odbywa się na podstawie uproszczonego PoW. Dzięki takiemu mechanizmowi działania, koszt transakcji jest praktycznie pomijany. W związku z tym, IOTA może być bardziej skalowalnym systemem niż tradycyjne sieci blockchainowe. Więcej informacji na temat platformy IOTA dostępnych jest pod tym adresem.

Przykładem konsolidacji platform jest fuzja firm Chain i Lightyear (części komercyjnej firmy Stellar Development Foundation). Nowa firma będzie oferowała narzędzia, produkty i usługi ułatwiające korzystanie z transgranicznego systemu płatności Stellar i wykorzystanie ich przez przedsiębiorstwa oraz instytucje finansowe. Produkty firmy Chain – takie jak rejestr rozproszony w chmurze Sequence, a także narzędzie do budowania prywatnych sieci blockchain Chain Core będą częścią portfolio produktów Interstellar. Celem jest stworzenie platformy, w której aktywa finansowe będą mogły być płynnie przenoszone pomiędzy publiczną siecią Stellar, a prywatnymi sieciami zarządzanymi przez firmy. Więcej informacji można znaleźć na tej stronie.

Firmy, które chcą przetestować lub wdrożyć rozwiązania oparte o blockchain bez konieczności ponoszenia kosztów związanych z implementacją platformy i szukania wewnętrznych lub zewnętrznych deweloperów, na których zapotrzebowanie rynkowe jest ogromne, mają alternatywę w postaci platform oferowanych w chmurze (BaaS – Blockchain as a Service). Wśród firm oferujących tego typu usługę są potentaci, tacy jak Microsoft, IBM, Amazon, SAP, Hewlett Packard, czy Oracle. Platformy dostępne w chmurze to między innymi Ethereum Enterprise, Hyperledger i Corda. Mniejsze firmy, takie jak Chain, że swoim produktem Sequence, również oferują swoje usługi w chmurze. Computerworld ocenia, że rozwiązania blockchain wygenerują do 2023 r. łączne przychody w wysokości ponad 10 miliardów dolarów[7].

7 L. Mearian, *Blockchain to generate more than $10.6B in revenue by 2023*

SKALOWALNOŚĆ I WYDAJNOŚĆ

Obecne systemy finansowe rutynowo obsługują tysiące transakcji na sekundę. Na przykład, system VISA przetwarza 2000 transakcji na sekundę, a w okresach szczytowego ruchu może obsłużyć ponad 50 000 transakcji na sekundę.

Publiczne sieci oparte na konsensusie Proof of Work mają znacznie niższą wydajność. Na przykład Bitcoin obsługuje około 6 transakcji na sekundę, a sieć Ethereum około 15 transakcji na sekundę. Jest to znacznie poniżej typowych wymagań biznesowych. Dlatego trwają intensywne prace by zwiększyć efektywność sieci blockchain. Nie może to jednak odbywać się kosztem zmniejszenia wiarygodności tych sieci.

Alternatywą jest zastosowanie sieci hybrydowych lub prywatnych. Na przykład, platforma Hyperledger Fabric jest w stanie przetwarzać kilka tysięcy transakcji na sekundę.

Drugim czynnikiem który ogranicza platformy blockchain to wzrost wielkości bazy danych wynikający z podstawowej cechy, jaką jest niezmienialność (bloki są ciągle dodawane do łańcucha i nie mogą być z niego usunięte). Tu również pomaga stosowanie sieci prywatnych lub hybrydowych, co ogranicza wolumen zapisywanych danych do tych niezbędnych dla danego zastosowania biznesowego.

Więcej informacji na temat skalowalności i wydajności systemów blockchain można znaleźć na tej stronie.

TOKENY

Token jest jednostką wartości zapisaną cyfrowo w bazie danych blockchain. W ramach opracowanych zasad działania konkretnej bazy danych blockchain, tokenom może zostać nadana wartość, dlatego też często tokeny są nazywane potocznie wirtualną walutą. Te zasady to:

- policzalna, ograniczona i niezmienna liczba tokenów, które istnieją w każdej bazie danych blockchain;
- możliwość przechowywania poszczególnych jednostek lub ich części w bazie danych blockchain i możliwość ich przenoszenia przez osoby lub urządzenia IoT, dysponujące kluczami prywatnymi do kont na których są zdeponowane;
- dzięki odpowiednim zasadom potwierdzania (konsensusu) brak jest możliwości wystąpienia sytuacji, w których token zostanie zatwierdzony w tym samym czasie w wielu zdublowanych transakcjach;
- podzielność tokena do dowolnej liczby zer po przecinku umożliwia mikro rozliczenia, na przykład płatności za sekundę pracy sieci o minimalnej mocy.

Dzięki tym cechom, które były możliwe do zaprogramowania w blockchain, token staje się niepodważalnym nośnikiem wartości, stosowanym w wielu bardzo różnych modelach biznesowych, w których zasady dystrybucji, inflacji, czy pozyskania („wydobywania") nadają indywidualną charakterystykę poszczególnym projektom, których wartość tokeny reprezentują.

Rozróżniamy następujące kategorie tokenów:

- **Przechowywanie wartości** – do tej grupy zalicza się m.in. Bitcoin (BTC). Ze względu na to, że w perspektywie długookresowej BTC jest jednostką, której wartość wzrasta systematycznie w czasie i jednocześnie Bitcoin jest zabezpieczony przez największą moc obliczeniową komputerów w porównaniu do innych walut cyfrowych.
- **Personalizowanie wartości** – do tej kategorii zaliczamy tokeny, które nadają wartość usługom świadczonym przez konkretne osoby np. muzyków, artystów, czy youtuberów. Gdy za pomocą tych tokenów realizowana jest płatność za usługi konkretnych osób, grupy osób, organizacji lub instytucji, rynkowa wartość tokenów jest odpowiednikiem atrakcyjności usług lub popularności usług personalnych.
- **Tokeny akcyjne, udziałowe** – są odpowiednikiem akcji giełdowych i mogą mieć w ramach koncepcji wbudowane rozwiązania wypłaty dywidendy czy głosowania akcjonariuszy.
- **Tokeny inwestycyjne** – są zabezpieczone depozytem wartości materialnych, np. złota, surowców, nieruchomości i stanowią odwzorowanie ich wartości. Szczególnym typem tego rodzaju tokenów są tzw. stablecoin'y, które odwzorowują 1 do 1 wartość danej waluty, np. USD.
- **Tokeny użytkowe** – są to tokeny niezbędne do zakupu oprogramowania lub usług opartych o technologię blockchain. Przykładowo, jeśli dana sieć blockchain oferuje przechowywanie danych w modelu rozproszonym, to token jest niezbędny do utrzymania tych danych w sieci. Z kolei, jeśli sieć oferuje budowanie smart contract'ów, to token służy do płatności za ich tworzenie i obsługę.
- **Tokeny bezwartościowe** – aby lista była kompletna, należy wspomnieć i o tym typie tokenów, które nie reprezentują sobą żadnej wartości. Szczególnie duża liczba tokenów nie reprezentujących sobą żadnej wartości pojawiła się przy okazji ICO (Initial Coin Offering). Tokeny te w początkowej fazie stanowiły narzędzie do zebrania pieniędzy od inwestorów, ale ostatecznie nie służyły do niczego, nie została określona w żaden sposób ich wartość użytkowa w kolejnych etapach. Wartość tych tokenów nieuchronnie zmierza do osiągnięcia zera. Nawet jeśli koncepcja biznesowa powiedzie się, to jednak taki token może finalnie nie mieć żadnej wartości.

Warto podkreślić, że tokeny są najbardziej newralgicznym i często budzącym kontrowersję elementem technologii blockchain. Możliwość ich szybkiego przesyłania, wymiany, przechowywania w sposób wysoce poufny, stojąca za nimi wielka liczba możliwości budowania różnorodnych koncepcji biznesowych powoduje, że obok bardzo obiecujących biznesowo modeli występują też takie, które można zdecydowanie nazwać oszustwami.

Domena przenoszenia wartości i zarządzania gospodarką pieniądza zarezerwowana dotychczas dla państw, bankowości, budzi skrajne nastroje i powoduje, że decyzje rządów i instytucji często są skrajnie odmienne. Jedne kraje chcą regulować rynek, inne chcą zakazać posiadania i wymiany tokenów, a kolejne chcą tworzyć możliwie przyjazne środowisko dla rozwoju tej technologii, licząc na napływ wielkiego kapitału, a jeszcze inne twierdzą, że blockchain jest technologią z potencjałem, ale może istnieć bez tokenów. Są to bardzo gorące tematy w dyskusjach specjalistów z wielu branż, nowa rzeczywistość Internet of Value buduje się właśnie na naszych oczach.

SMART CONTRACT'Y W TECHONOLOGII BLOCKCHAIN

Czym jest smart contract?

Koncepcja smart contract'ów powstała jeszcze w latach 90-tych poprzedniego stulecia, ale dopiero pierwsze wdrożenia technologii blockchain umożliwiły ich praktyczne zastosowanie

Smart contract (inteligentny kontrakt) to kod komputerowy zawierający zestaw reguł biznesowych, na które umówiły się strony zawierające kontrakt, uruchamiany na blockchainie. Smart contract zapisywany jest na blockchaine, więc nie może być zmieniony lub odwołany. Kiedy spełnione zostaną ustalone wcześniej warunki, kontrakt jest automatycznie i nieodwołalnie wykonany. Mechanizm ten obejmuje aktywa cyfrowe i co najmniej dwie strony transakcji. Aktywa należące do jednej strony są automatycznie redystrybuowane zgodnie z regułami kontraktu, czyli kontrakt inicjuje jedną lub więcej transakcji, które zapisywane są na blockchainie i zmieniają jego stan.

Termin „smart contract" jest trochę niefortunny, gdyż odzwierciedla on tylko reguły zapisane przez programistów na podstawie dostępnych w danym czasie informacji i może zawierać błędy. Taki kontrakt nie jest też dziś uznawany za umowę prawną i nie może być kontestowany na drodze prawnej, na przykład przed sądem. Bardziej adekwatną nazwą mogła by być „umowa".

Oczekuje się, że w przyszłości smart contract'y staną się umowami prawnymi, ale najpierw technologia leżąca u ich podstaw musi stać się bardziej dojrzała, a jej adopcja bardziej powszechna. Muszą też zostać przyjęte odpowiednie standardy prawne i regulacyjne.

Jak działa smart contract?

Każdy węzeł w sieci blockchain ma uruchomiony program, który zawiera wirtualną maszynę – wewnętrzy „komputer" który potrafi wykonać instrukcje zawarte w kodzie opisującym smart contract. W momencie, gdy spełnione zostaną warunki kontraktu, węzły wykonują go i tworzą transakcje, które poddawane są zasadom akceptacji według ustalonych dla danego blockchaina reguł konsensusu. Raz uruchomiony, smart contract nie może zostać zatrzymany, a zmiany na blockchainie z niego wynikające będą nieodwracalne (wyjątki opisane są w sekcji *Ryzyka i zagrożenia*).

W niektórych przypadkach smart contract'y wykorzystują dane spoza sieci blockchain. W takich przypadkach wdrażane są zewnętrzne programy, zwane „oracle" (wyrocznia), które stanowią łącznik pomiędzy blockchainem a innymi systemami.

Korzyści ze smart contract'ów

Smart contract'y wykorzystują wszystkie zalety technologii blockchain: niezmienialność danych, bezpieczeństwo, odporność na błędy i ataki, transparentność, współdzielenie, rozproszenie, eliminacja pośredników.

Dodatkowo inteligentne kontrakty umożliwiają następujące korzyści:

- uproszczenie i automatyzację procesów
- obniżkę kosztów
- gwarancję wyników, eliminację potrzeby weryfikacji
- możliwość tworzenia organizacji autonomicznych, nie wymagających hierarchicznej struktury zarzadzania

Ryzyka i zagrożenia

Smart contract'y nie są narzędziem idealnym i istnieją rzeczywiste ryzyka związane z ich używaniem w powiazaniu z technologią blockchain.

Poniżej opisane są najważniejsze ryzyka.

Czynnik ludzki
Programy opisujące inteligentne kontrakty pisane są przez ludzi i mogą zawierać błędy, czasami o katastrofalnych skutkach. Kontrakt jest zapisywany na blockchainie więc nie może być zmieniony, ponadto będzie widoczny dla każdego uczestnika sieci. Nie można założyć, ze wszyscy uczestnicy sieci są uczciwi, są wśród nich hakerzy, którzy mogą wykorzystać słabości w kodzie, a raz uruchomiony inteligentny kontrakt nie może zostać zatrzymany i zmiany na blockchainie z niego wynikające będą nieodwracalne. Najbardziej spektakularnym przykładem wykorzystania błędu w kodzie inteligentnego kontraktu była sprawa „The DAO" z 2016 roku na sieci Ethereum, kiedy doszło do kradzieży 56 milionów dolarów.

Jakość danych
Fakt, że dane na blockchainie nie mogą by zmienione nie oznacza, że są one poprawne. Podobnie jest z danymi zewnętrznymi dostarczonymi poprzez program „oracle". W przypadku pojawienia się niepoprawnych danych inteligentny kontrakt będzie opierał się na fałszywych przesłankach, co doprowadzi do niepożądanego wyniku.

Wysokie koszty wdrożenia
By zabezpieczyć się przed ryzykiem wykorzystania błędu w kodzie, musi on zostać wyczerpująco przetestowany co wiąże się z wysokimi kosztami.

Wysokie koszty wykonania
Smart contract może zawierać skomplikowaną logikę biznesową i wykonanie wymaganych obliczeń może wiązać się dużymi kosztami. Mogą pojawić się też nieskończone pętle w źle napisanym kodzie. Niektóre systemy wdrażają mechanizmy, które ograniczają to ryzyko. W sieci Ethereum trzeba za wykonanie inteligentnego kontaktu płacić i deklarowany jest maksymalny dopuszczalny wydatek związany z taką transakcją (gas – paliwo). W przypadku przekroczenia tej zadeklarowanej kwoty, wykonanie inteligentnego kontraktu zostaje przerwane, a jego częściowe wyniki nie są rejestrowane na blockchainie.

Niepewny status prawny
Obecnie inteligentne kontrakty nie są regulowane przez agencje rządowe i nie stanowią umowy prawnej w powszechnym rozumieniu.

Dodatkowe źródła informacji:

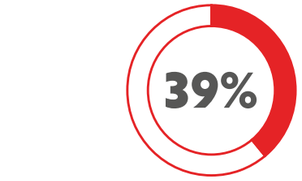
- Wikipedia – hasło: smart contract
- Antonopoulos, Mastering Ethereum: Building Smart Contracts and DApps 1st Edition

SPIS TREŚCI

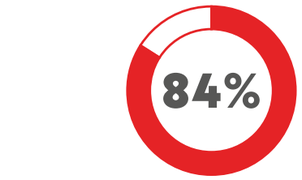
WSTĘP

W ciągu ostatnich dwóch lat można zaobserwować rosnące zainteresowanie praktycznymi zastosowaniami technologii blockchain w biznesie. Potwierdzają to badania rynkowe przeprowadzone ostatnio przez czołowe firmy analityczne.

Z badania Deloitte z 2018 r., które objęło ponad 1000 menedżerów wykonawczych czołowych firm z Ameryki Północnej, Europy Zachodniej i Chin wynika, że 39% procent z nich zainwestuje w tym roku ponad 5 milionów dolarów w technologię blockchain (65% zainwestuje ponad 1 milion dolarów), a 84% z nich myśli, że blockchain jest już wystarczająco skalowalny i znajdzie zastosowanie w głównym nurcie biznesu[8].



chce zainwestować ponad $5 mln w technologię blockchain



twierdzi, że blockchain znajdzie zastosowanie w biznesie

Z kolei tegoroczne badanie rynkowe IBM wśród 147 operatorów telekomunikacyjnych pokazuje, że 36% z nich planuje wdrożenie lub wdraża blockchain, 41% uważa, że blockchain pomoże w realizacji strategii spójności danych, a 46% chce użyć blockchain do realizacji nowych modeli biznesowych[9].

36% planuje wdrożenie

41% uważa blockchcain za pomocny

46% chce wykorzystać do modeli biznesowych

8 Breaking blockchain open. Deloitte’s 2018 global blockchain survey

9 Reimagining telecommunications with blockchains. From concept to reality. - IBM Institute for Business Value

Na świecie powstają rozwiązania oparte na blockchainie dla przedsiębiorstw z różnych gałęzi gospodarki. Można je sklasyfikować w następujący sposób:

→ Usprawnienie systemów transakcyjnych

Blockchain służy do tworzenia, zatwierdzania oraz do udostępniania informacji o transakcjach. Blockchain potencjalnie eliminuje pośredników, ręczną walidację danych, konieczność potwierdzeń oraz rozliczeń i tym samym usprawnia, przyspiesza i zmniejsza koszty przetwarzania transakcji. Poprzez użycie technologii blockchain, firmy powiązane biznesowo zyskują natychmiastowy dostęp do zaufanych, bezpiecznych i aktualnych danych. Przetwarzanie transakcji można dodatkowo przyspieszyć i zautomatyzować przez wykorzystanie smart contract'ów.

Zastosowania:

- rozliczenia między podmiotami biznesowymi
- bezpośrednia dystrybucja treści cyfrowych
- wykrywanie oszustw w procesach finansowych
- zarządzanie usługami udostępnionymi w chmurze
- zarzadzanie płatnościami, w tym mikropłatnościami
- e-commerce

Główne branże: finanse, bankowość, spedycja, przemysł, sprzedaż detaliczna on-line, ubezpieczenia, dystrybucja muzyki, filmów i publikacji, usługi chmurowe, działalność charytatywna, NGO.

→ Śledzenie aktywów i audytowanie danych

Blockchain zapewnia niezmienialny i niezaprzeczalny zapis danych. Te cechy mogą być wykorzystane przez różne firmy, by zredukować zbędne czynności związane weryfikacją nieautoryzowanych lub nieprawidłowych operacji oraz potwierdzaniem pochodzenia i prawdziwości danych.

Zastosowania:

- zarządzanie łańcuchem dostaw
- potwierdzanie zgodności z regulacjami
- wykrywanie fałszerstw i podróbek
- wsparcie dla programów lojalnościowych
- zarzadzanie własnością intelektualną
- e-commerce

Główne branże: farmaceutyka, sprzedaż detaliczna, rolnictwo, dobra luksusowe, sektor publiczny (w tym regulatorzy), hotele i podróże, organy ścigania, bezpieczeństwo, rozrywka.

→ Zarządzanie danymi

Blockchain jest rejestrem elektronicznym, dlatego jednym z podstawowych jego zastosowań jest zapewnienie bezpiecznego dostępu do danych węzłom sieci. Ze względu na rozproszoną architekturę, blockchain może działać w ekosystemach biznesowych łączących różnorodne przedsiębiorstwa, które potrzebują dzielić się danymi. W przypadku użycia tradycyjnych systemów jest to trudne ze względu na rozbieżne standardy i modele danych. W tym sensie blockchain może być wykorzystany do zarządzania danymi podstawowymi, a jego zastosowanie może w znaczący sposób obniżyć koszty integracji systemów.

Zastosowania:

- zarządzanie danymi publicznymi (akty notarialne, dane osobowe, itd.)
- zarządzanie danymi medycznymi
- zarządzanie tożsamością
- potwierdzanie kwalifikacji

Główne branże: służba zdrowia, sektor publiczny, administracja, przemysł, usługi prawne, finanse, bezpieczeństwo, organy ścigania.

W dalszej część prezentowane są wybrane przykłady rozwiązań, które są aktualnie wykorzystywane bądź rozwijane przez firmy w Polsce i na świecie.

1. TRWAŁY NOŚNIK

Opis przypadku i problemu do rozwiązania

Istnieją regulacje prawne w UE wymagające, aby firma dostarczała klientowi określone informacje na piśmie, na papierze lub na innym trwałym nośniku.

Koncepcja trwałego nośnika została po raz pierwszy wprowadzona w UE przez dyrektywę 97/7 dotyczącą sprzedaży na odległość. Od tego czasu trwały nośnik pojawił się także w innych dyrektywach Parlamentu Europejskiego:

- dyrektywa 2002/65 – dotycząca sprzedaży konsumentom usług finansowych na odległość
- dyrektywa 2007/64 – w sprawie usług płatniczych w ramach rynku wewnętrznego
- dyrektywa 2008/48 – w sprawie umów o kredyt konsumencki
- dyrektywa 2011/83 – w sprawie praw konsumentów

W związku z postępującą na rynku cyfryzacją procesów biznesowych w przedsiębiorstwach, w tym w komunikacji z klientem, wymagania implementacji trwałego nośnika dotykają coraz większej liczby firm.

Pozostanie przy fizycznych nośnikach informacji tj. papier, CD-ROM, USB jest możliwe, ale dla przedsiębiorstw działających w dużej skali nieefektywne kosztowo, pogarszające doświadczenia klienta oczekującego pełnej zdalnej obsługi i hamujące rozwój nowych modeli biznesowych online.

Blockchain jest technologią umożliwiającą tworzenie w pełni zautomatyzowanych rozwiązań do implementacji trwałego nośnika informacji.

Tradycyjne podejście do rozwiązania

W tradycyjnym podejściu dokumenty są przekazywane w wersji papierowej. Klient musi fizycznie je otrzymać oraz w pewnych okolicznościach potwierdzić to własnoręcznie. W przypadku zawierania umów zdalnych praktyką jest korzystanie z firm kurierskich pośredniczących w wymianie dokumentów pomiędzy przedsiębiorstwem a klientem. Dokumentacja publiczna, jak na przykład regulamin, jest najczęściej wysyłana pocztą w formie fizycznej.

Główni uczestnicy procesu:

- **Przedsiębiorstwo** – firma publikująca dokumenty wpadające w reżim prawny trwałego nośnika (np. bank, operator telekomunikacyjny)
- **Klient** – osoba mająca relacje z przedsiębiorstwem, realizowane za pomocą dokumentów wpadających w reżim prawny trwałego nośnika (np. osoba zawierająca online umowę na usługi telekomunikacyjne)
- **Pośrednik** – podmiot pośredniczący w przekazywaniu dokumentów w wersji trwałej pomiędzy przedsiębiorstwem a klientem (np. firma kurierska)

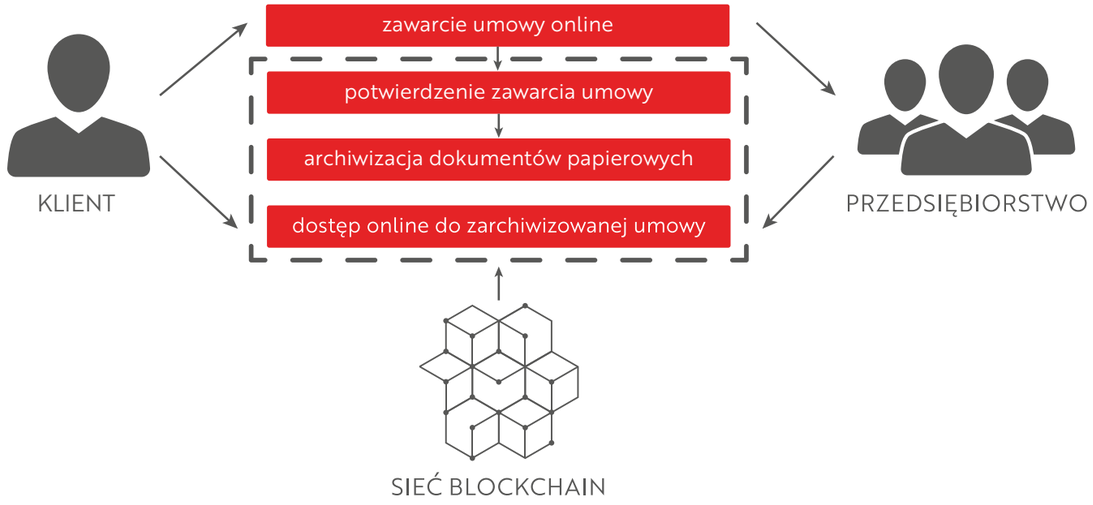
Rys. Proces przekazywania dokumentów podczas zawierania umowy zdalnej – wersja tradycyjna

Rozwiązanie oparte o blockchain

W podejściu z wykorzystaniem blockchaina nie ma potrzeby tworzenia fizycznych (np. papierowych) wersji dokumentów.

Główni uczestnicy procesu:

- **Przedsiębiorstwo** – firma publikująca dokumenty wpadające w reżim prawny trwałego nośnika (np. bank, operator telekomunikacyjny)
- **Klient** – osoba mająca relacje z przedsiębiorstwem realizowane za pomocą dokumentów wpadających w reżim prawny trwałego nośnika (np. osoba zawierająca online umowę na usługi telekomunikacyjne)
- (opcjonalnie) **Zaufana strona trzecia** – podmiot uczestniczący w procesie przekazywania dokumentów elektronicznych potwierdzający poprawność procesu



Rys. Proces przekazywania dokumentów podczas zawierania umowy zdalnej – wersja Blockchain

Rozwiązania mogą być tworzone o sieć prywatną konsorcjalną, tworzoną przez podmioty współpracujące ze sobą dla celów realizacji trwałego nośnika. Dodatkowym elementem poprawiającym bezpieczeństwo i wiarygodności rozwiązania może być zaangażowanie w proces tzw. zaufanej strony trzeciej - podmiotu, który partycypuje w infrastrukturze blockchain, ale nie jest uczestnikiem relacji biznesowych pomiędzy przedsiębiorstwem a klientem.

Na rynku istnieje już kilka koncepcji trwałego nośnika opartego o blockchain. Proponowane rozwiązania można podzielić na kilka kategorii ze względu na pewne charakterystyczne cechy.

OTWARTE OPROGRAMOWANIE	ZAMKNIĘTE OPROGRAMOWANIE
Rozwiązania wykorzystujące otwarty kod silnika blockchain dają gwarancję, co do zakresu funkcjonalności oferowanych przez narzędzie.	Wykorzystanie zamkniętego kodu silnika blockchain wprowadza wymóg audytów rozwiązania, ponieważ istnieje ryzyko, iż taki węzeł poza deklarowanymi funkcjonalnościami posiada też jakieś właściwości ukryte.

OTWARTY BLOCKCHAIN	ZAMKNIĘTY BLOCKCHAIN
Publiczny blockchain eliminuje instytucje zaufane, ale niestety nie daje żadnych gwarancji co do czasu życia danej sieci. Dla przykładu, skompletowanie w pełni funkcjonalnego węzła popularnej sieci Ethereum zajmuje już ponad 1TB miejsca na dysku i rośnie w zastraszającym tempie. Nietrudno zatem wyobrazić sobie sytuację, w której liczba pełnych węzłów ulegnie gwałtownej redukcji lub całkowitej eliminacji. W przypadku otwartej sieci blockchain nie ma gwarancji co do długości życia takiej sieci a przypomnieć należy, że dla trwałego zapisu dokumentów to musi być co najmniej 10 lat.	Wykorzystanie zamkniętej sieci blockchain wymaga odwołania się do zaufanej strony trzeciej. Bez niej mogłoby dojść do tak zwanej zmowy przedsiębiorstw, które razem miałyby techniczne możliwości podmiany całej sieci. W blockchainie, poza węzłami zaufanymi, znajdują się tylko węzły z sieci walidacji dokumentów. To sieć sama zarządza dostępem i najczęściej będzie uniemożliwiać podłączanie się z zewnątrz. Takie podejście podnosi bezpieczeństwo rozwiązania. Do rozważenia jest jeszcze koncepcja hybrydowa. Przy prywatnej sieci blockchain z węzłami zaufanymi, udostępniamy węzeł klientom i umożliwiamy im podłączenie. Konstruując to w ten sposób, że tylko rozpoznani klienci otrzymują swoje klucze niezbędne do partycypacji w sieci blockchain, dalej zachowujemy prywatność, pomimo otwarcia na szersze grono uczestników.

DOKUMENTY ZAPISANE POZA BLOCKCHAIN	DOKUMENTY ZAPISANE W BLOCKCHAIN
Zapisywanie w blockchain tylko skrótów dokumentów wymagać będzie dodatkowo mechanizmów typu backup. Trwały nośnik to nie tylko niezmienność treści dokumentu ale również dostęp do samego dokumentu. Aby więc dostęp do plików był zapewniony przez wymagany czas, należy je również zapisać na przykład na serwerach strony zaufanej i udostępnić klientom poprzez wybrany kanał. Posługiwanie się funkcjami skrótu jest zgodne z RODO, ponieważ nie da się wywnioskować danych osobowych i treści dokumentu, mając do dyspozycji jedynie jego skrót.	Zapisanie całych plików w blockchain daje pełną funkcjonalność trwałego nośnika i nie jest już potrzebny dodatkowy backup. Niestety, utrudniony jest przez to dostęp do plików. Należy udostępnić klientom specjalne narzędzie, przez które będą mogli skompletować oczekiwane pliki. Zapis tego typu wzbudza też kontrowersje ze względu na bezpieczeństwo przechowywania danych poza infrastrukturą przedsiębiorstwa. Co więcej, aktualne przepisy RODO precyzują okoliczności, w których niezbędne jest usunięcie pewnych danych wrażliwych, natomiast dane zapisane w blockchain są już nieusuwalne.

Rozwiązania alternatywne

Najprostszym rozwiązaniem trwałego nośnika jest fizyczne przekazanie pliku podpisanego elektronicznie przez przedsiębiorcę. Można tego dokonać wysyłając plik w wiadomości e-mail do klienta. To podejście niesie za sobą jednak duże niebezpieczeństwo, gdyż stwarza okazję podmiotom o złej woli do tego, by „przemycić" klientom wrogie oprogramowanie. Wiadomo powszechnie, że wysyłanie załączników to nie jest najlepszy pomysł. Regulator uważa, iż dokumenty nie będą musiały być fizycznie przekazywane klientom, jeżeli potrafimy udowodnić, że są nieusuwalne oraz pozostają dostępne dla klienta także po zakończeniu umowy. Funkcjonalność nieusuwalności przyjęło się przypisywać macierzom WORM (ang. write once read many), które pozwalają zapisać plik tylko raz, bez możliwości skasowania lub podmiany.

Innym rozwiązaniem może być podejście hybrydowe, w którym pliki przechowywane są w macierzy WORM, a skróty dokumentów w sieci blockchain.

Zalety i wady rozwiązań blockchainowego w stosunku do rozwiązań alternatywnych:

MACIERZ WORM

ZALETY/SZANSE	WADY/RYZYKA
• Hardwarowa pewność niezmienności zapisu. • Możliwość zapewnienia bezpieczeństwa poprzez redundancję danych. • Wysoka wydajność macierzy.	• Brak rozwiązania problemu skutecznego dostarczenia informacji do odbiorcy – wymaga organizacyjnego lub softwarowego dostarczenia informacji o dokumencie. • Poleganie na instytucjach zaufania publicznego hostujących/udostępniających dane. • Odbiorcy nie posiadają u siebie kopii dokumentu dostarczonego w sposób trwały. • Brak wiedzy, czy takie macierze mogą stanowić dokument dowodowy w przypadku sporów. • Problematyczne możliwości realizacji „prawa do bycia zapomnianym" (GDPR).

CENTRALNE ARCHIWUM PROWADZONE PRZEZ ZAUFANĄ STRONĘ TRZECIĄ

ZALETY/SZANSE	WADY/RYZYKA
• Uregulowany stan prawny. • Możliwość działania w obszarze UE z wykorzystaniem bezpiecznych metod szyfrowania i podpisu (eIDAS - Electronic Identification and Trust Services Regulation)	• Brak rozwiązania problemu skutecznego dostarczenia informacji do odbiorcy – wymaga organizacyjnego lub softwarowego dostarczenia informacji o dokumencie. • Poleganie na instytucjach zaufania publicznego hostujących lub udostępniających dane. • Spore wymagania sieciowe i wydajnościowe przy dużej skali dokumentów.

DOKUMENTY ZAPISYWANE W CENTRALNYM ARCHIWUM, A ICH SKRÓTY W SIECI PUBLICZNEJ

ZALETY/SZANSE	WADY/RYZYKA
• Korzystanie z uznanego standardu lub frameworka. • Niewielkie obciążenie sieci – publikowane tylko skróty.	• Brak rozproszenia sieci – tylko węzły publikatorów i ewentualnie replikacja do dodatkowych podmiotów. • Fizyczne dokumenty przechowywane w centralnym repozytorium. • Rozwiązanie de-facto wymusza wprowadzenie zaufanej strony trzeciej - niewiele różni się od rozwiązania z centralnym archiwum.

DOKUMENTY ZAPISYWANE W BLOKACH BLOCKCHAIN

ZALETY/SZANSE	WADY/RYZYKA
• Możliwość rozproszenia sieci i pojawienie się wielu węzłów. • Dokumenty są faktycznie dystrybuowane do uczestników sieci w blokach blockchainowych. • Brak konieczności tworzenia dodatkowego mechanizmu dostarczania informacji o dokumencie.	• Korzystanie z prywatego frameworka blockchain rozwijanego przez niewielką firmę. • Duże ryzyko wydajnościowe z powodu umieszczania całych dokumentów w blokach. • Problematyczne możliwości realizacji „prawa do bycia zapomnianym" (RODO) – dokumenty z danymi osobowymi w blokach.

ROZWIĄZANIE HYBRYDOWE – DOKUMENTY PRZECHOWYWANE W RÓŻNYCH TECHNOLOGIACH W ZALEŻNOŚCI OD KONTEKSTU

ZALETY/SZANSE	WADY/RYZYKA
• Rozwiązanie pozwala część dokumentów publicznych (takich jak regulaminy) przechowywać bezpośrednio w blockchain. • Dokumenty zawierające dane wrażliwe ze względu na RODO nie są zapisywane w blockchain i są zapisywane albo na macierzach WORM bezpośrednio w instytucji albo na serwerach strony zaufanej. • Obie te metody uniemożliwiają instytucji samodzielnego usunięcia dokumentu. Dokument może jednak zostać usunięty na żądanie klienta.	• Z uwagi na rozmiar redundancji sieci, może być problematyczne przechowywanie wszystkich dokumentów w blockchain. • Blockchain uniemożliwia usuwanie z niego wcześniej zapisanych danych, dlatego też należy bardzo uważnie umieszczać w nim informacje.

Wszystkie nowe rozwiązania problemu trwałego nośnika nie mają w pełni uregulowanego stanu prawnego.

2. E-GŁOSOWANIE (E-VOTING)

Opis przypadku i problemu do rozwiązania

Akcjonariusze spółek publicznych, co do zasady, są uprawnieni do podejmowania decyzji w sprawach spółek, których są właścicielami. Prawo to mogą realizować poprzez uczestnictwo w walnych zgromadzeniach (WZ) spółek, w tym poprzez prowadzenie dyskusji w sprawach objętych porządkiem obrad WZ, zadawanie pytań Zarządowi spółki, jednak przede wszystkim poprzez głosowanie nad projektami uchwał lub zgłaszanie własnych projektów. Uprawnienia te wynikają wprost z zapisów Kodeksu spółek handlowych związanych z funkcjonowaniem instytucji Walnego Zgromadzenia, które to jednocześnie regulują cały obszar związany z organizacją WZ oraz podejmowaniem uchwał w trakcie jego trwania. Niedługo do prawa krajowego zaimplementowane zostaną przepisy dyrektywy Parlamentu Europejskiego i Rady (EU) 2017/828 z dnia 17 maja 2017 r. zmieniającej dyrektywę 2007/36/WE w zakresie zachęcania akcjonariuszy do długoterminowego zaangażowania (SRDII), co powinno wpłynąć na zwiększenie zainteresowania akcjonariuszy mniejszościowych aktywnym decydowaniem o przyszłości spółek publicznych w Polsce.

Obecnie walne zgromadzenia odbywają się w sposób wymagający fizycznej obecności inwestora, co z kolei oznacza szereg wyzwań. Do najistotniejszych zaliczyć należy konieczność przybycia na miejsce i poniesienia związanych z tym kosztów dojazdu oraz konieczność poświęcenia odpowiedniej ilości czasu, w związku z częstymi przerwami w obradach,

które mogą trwać nawet kilka lub kilkanaście dni. W efekcie, jak wynika z Ogólnopolskiego Badania Inwestorów OBI 2017, niespełna 4% inwestorów indywidualnych uczestniczy w walnych zgromadzeniach spółek giełdowych[10]. Jako główny powód inwestorzy wskazują brak czasu (43,2%) oraz poczucie braku rzeczywistego wpływu na przebieg walnego zgromadzenia (29,7%). Kolejne powody, które są wskazywane, to brak zainteresowania, wysokie koszty dojazdu, brak możliwości udziału on-line oraz złożoność i niezrozumiałość procedur i obowiązujących przepisów. Patrząc globalnie można wyciągnąć wniosek, że istotna większość barier w procesie aktywizacji drobnych akcjonariuszy jest związana z brakiem możliwości organizacji i przeprowadzenia walnych zgromadzeń wyłącznie w sposób zdalny, tzn. bez konieczności fizycznej obecności w miejscu obrad.

Prawo już obecnie dopuszcza możliwość głosowania zdalnego, bez konieczności fizycznej obecności na walnym zgromadzeniu (co wynika z art. 406^5 pkt 3 Kodeksu spółek handlowych, zgodnie z którym udział w walnym zgromadzeniu przy wykorzystaniu komunikacji elektronicznej może polegać na osobistym lub przy pomocy pełnomocnika wykonywaniu prawa głosu przed lub w trakcie walnego zgromadzenia), niemniej złożoność związana zarówno z samym głosowaniem, jak również z zapewnieniem kontaktu pomiędzy emitentem a akcjonariuszami powoduje, że w praktyce nie powstało żadne rozwiązanie pozwalające na organizację tego procesu.

Krajowy Depozyt jako spółka oparta na technologii, z silnymi kompetencjami IT oraz zapleczem badawczo-rozwojowym, dostrzega istotny potencjał technologii rozproszonych rejestrów, w tym technologii blockchain, w dostarczaniu nowej jakości usług finansowych dzięki możliwości współpracy wielu podmiotów. W związku z tym oraz biorąc pod uwagę kluczową rolę KDPW w kształtowaniu usług dla rynku papierów wartościowych, Krajowy Depozyt uruchomił projekt eVoting (eVoting), który poza rozpoznaniem technologii blockchain pozwala na zamodelowanie procesu zdalnego udziału i głosowania na WZ, przy zapewnieniu wysokiego stopnia zaufania pomiędzy poszczególnymi interesariuszami procesu. Rozwiązanie przede wszystkim ma za zadanie zbudowanie zaufania inwestora, co do tego że jego głos zostanie skutecznie wykonany oraz zaufania emitenta, że głos akcjonariusza jest oddany przez właściwą osobę z prawidłową liczbą akcji, a całość jest przeprowadzona w sposób niezaprzeczalny. Dodatkowo, celem jest także wyeliminowanie większości barier wskazywanych przez inwestorów, co dodatkowo może podnieść poziom świadomości inwestowania na ryku kapitałowym.

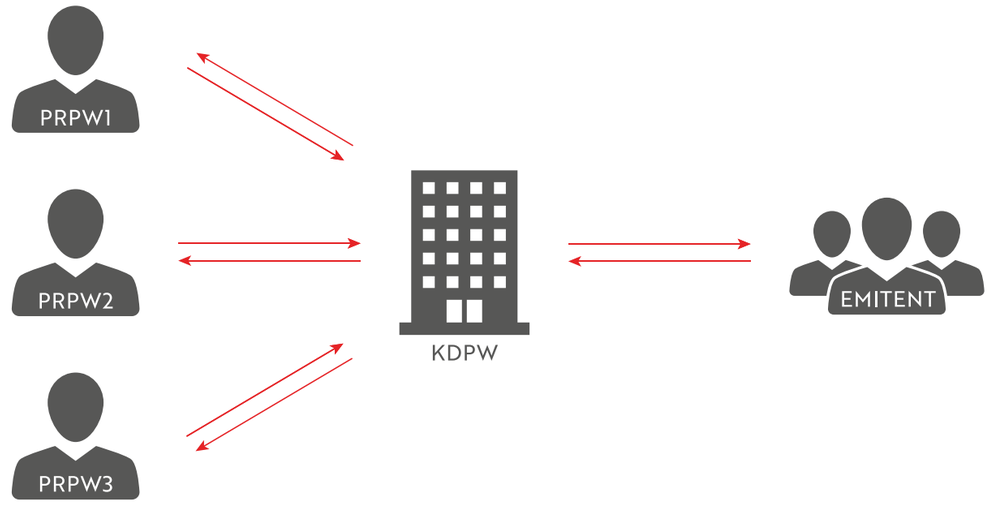
Tradycyjne podejście do rozwiązania

Proces WZ realizowany jest obecnie na bazie przepisów KSH w sposób fizyczny. Inwestor, by wziąć udział w WZ musi uzyskać zaświadczenie o prawie uczestnictwa w WZ od podmiotu, w którym prowadzi swój rachunek papierów wartościowych. Na podstawie wydanych zaświadczeń podmiot prowadzący rachunki papierów wartościowych sporządza wykaz uprawnionych do udziału w WZ. Wykaz trafia do Emitenta poprzez system KDPW. Inwestor przybywając na WZ uwierzytelnia się z wykorzystaniem dokumentu tożsamości. Przebieg WZ jest protokołowany fizycznie przez notariusza.

10 Stowarzyszenie Inwestorów Indywidualnych, Wyniki Ogólnopolskiego Badania Inwestorów OBI 2017

Główni uczestnicy procesu:

- Emitent – spółka publiczna, której akcje są rejestrowane w KDPW.
- PRPW – podmioty prowadzące rachunki papierów wartościowych dla inwestorów (firmy inwestycyjne, banki).
- KDPW – centralny depozyt papierów wartościowych, podmiot odpowiedzialny m.in. za obsługę realizacji zobowiązań Emitenta wobec uprawnionych z papierów wartościowych.
- Inwestor – akcjonariusz Emitenta, posiadacz rachunku papierów wartościowych w wybranym PRPW.
- Pełnomocnik – osoba realizująca prawo głosu zgodnie z wolą swojego mocodawcy, którym jest Inwestor.
- Nadzorca – podmiot nadzorujący prawidłowość funkcjonowania procesu organizacji i obsługi Walnych Zgromadzeń w spółkach publicznych.



Rys. Architektura rozwiązania (obejmuje jedynie obszar wspierany obecnie przez rozwiązania systemowe, bez uwzględnienia uczestników procesu, którzy komunikują się jedynie poza systemowo).

Główne problemy wyzwania w tradycyjnym podejściu:

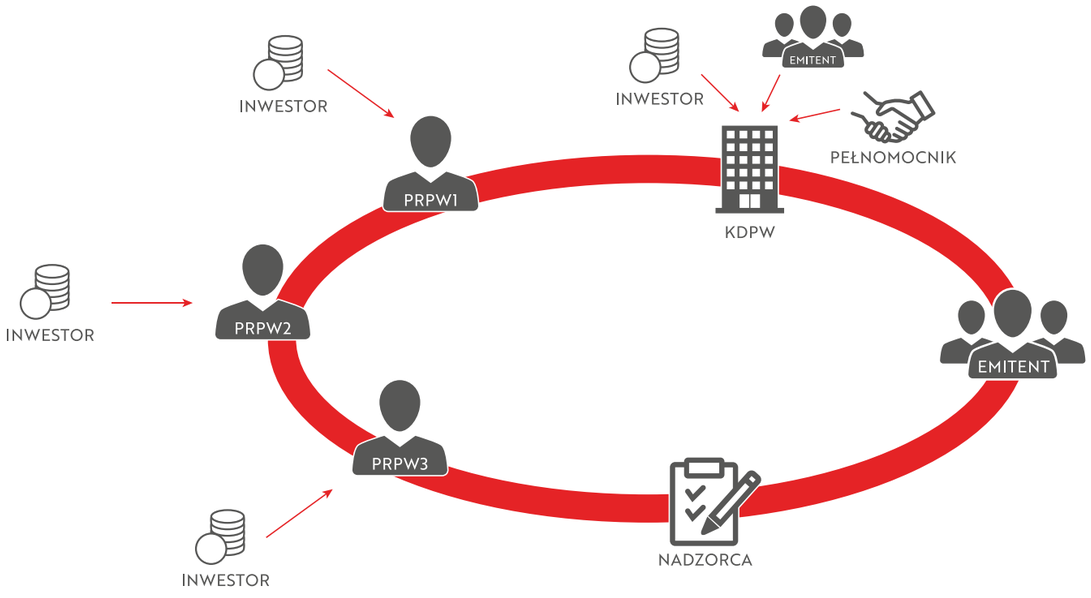
- Przygotowanie i zorganizowanie WZ przez Emitenta jest procesem bardzo złożonym, przez co również kosztownym i czasochłonnym,
- Brakuje łatwo dostępnej i jednolitej informacji o Walnych Zgromadzeniach (WZ),
- Procedury związane z udziałem i głosowaniem na WZ są z perspektywy Inwestorów niejasne, złożone i zbyt sformalizowane,
- Uczestnictwo w WZ wymaga fizycznej obecności, co generuje pośrednie i bezpośrednie koszty po stronie Inwestora,
- Niedogodne terminy oraz częste przerwy paraliżują przebieg WZ i podnoszą koszty zarówno organizacji WZ przez Emitenta, jak i uczestnictwa Inwestora,
- Centralizacja informacji o uprawnionych do udziału w WZ stwarza ryzyko zaburzenia całego procesu, w przypadku awarii systemu centralnego.

Rozwiązanie oparte o blockchain

Proces zdalnego udziału i głosowania na WZ realizowany jest w obrębie rozproszonej sieci blockchain, opartej na modelu tzw. permissioned blockchain. Podmioty takie jak PRPW, KDPW, Organy Nadzorcze, tworzą wspólną sieć węzłów, w ramach której realizowany jest pełen proces obsługi WZ. Pozostali uczestnicy uzyskują dostęp do systemu poprzez infrastrukturę właściwych podmiotów, które są w stanie dokonać uwierzytelnienia i autoryzacji ich dostępu do danych funkcji w ramach zgromadzenia.

Główni uczestnicy procesu:

W ramach rozwiązania opartego o blockchain przewiduje się uczestnictwo tych samych Uczestników, którzy występują w obecnym procesie, przy czym przewiduje się zmianę charakteru partycypacji w kierunku przekształcania się części z nich w infrastrukturę wspierającą proces i zapewniającą dostęp pozostałym Uczestnikom do sieci w sposób gwarantujący odpowiedni poziom uwierzytelnienia.



Rys. Architektura rozwiązania opartego o blockchain

Główne korzyści wynikające z wykorzystania technologii blockchain:

- Wpisanie się rozwiązania w założenia i cel dyrektywy 2007/36/WE w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym (Shareholders' Rights Directive) oraz dyrektywy Parlamentu Europejskiego i Rady (EU) 2017/828 z dnia 17 maja 2017 r. zmieniającej dyrektywę 2007/36/WE w zakresie zachęcania akcjonariuszy do długoterminowego zaangażowania.
- Przeprowadzenie całości procesu, począwszy od ogłoszenia o zwołaniu walnego zgromadzenia, poprzez ustalenie uprawnionych, głosowanie i potwierdzanie sposobu głosowanie do publikacji wyników WZ w sposób niezaprzeczalny, z wykorzystaniem elektronicznych środków komunikacji.
- Zniesienie konieczności fizycznej obecności Inwestora na WZ, przez co potencjalne zwiększenie aktywności Inwestorów i ich zaangażowania w sprawy Emitenta.
- Zmniejszenie kosztów organizacji WZ,
- Zmniejszenie kosztów udziału w WZ po stornie Inwestora,
- Możliwość integracji usług związanych z udziałem i głosowaniem na WZ bezpośrednio z usługą prowadzenia rachunku papierów wartościowych przez PRPW,
- Zmniejszenie liczby potencjalnych błędów poprzez automatyzację procesu,
- Minimalizacja ryzyka pojedynczego punktu awarii, poprzez rozproszenie danych w sieci blockchain,
- Zapewnienie możliwości audytu procesu przez Nadzorcę bez konieczności ponoszenia dodatkowych nakładów ze strony pozostałych Uczestników oraz podniesienie bezpieczeństwa procesu poprzez włączenie Nadzorcy do systemu.

3. PLANOWANIE I KONTROLA DOSTAW

Śledzenie pochodzenia oraz warunków, w jakich były transportowane oraz przechowywane produkty jest istotne dla każdego konsumenta. Jednak możliwość zapewnienia dostępu do tych informacji przez producenta oraz przewoźników jest wyzwaniem, którego nadal większość z nich nie jest w stanie zagwarantować.

Od wielu lat, w celu śledzenia i zarządzania łańcuchem dostaw wykorzystuje się czujniki RFID, jednak ich wykorzystywanie przez poszczególne organizacje i przechowywanie danych z nich związanymi w obrębie zcentralizowanych systemów nie gwarantuje ich niepodważalności towarów i może podlegać manipulacjom. Ponadto, samo ich wykorzystywanie wzbudza wiele kontrowersji w kontekście bezpieczeństwa, prywatności a także anonimowości konsumentów.

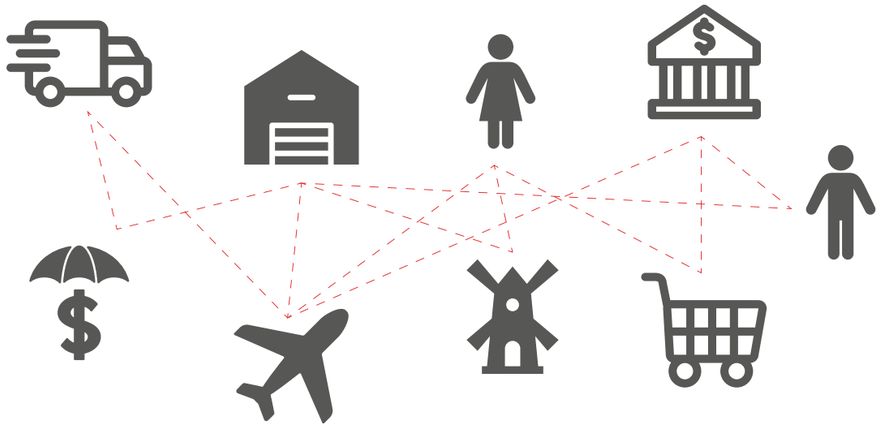
Podmioty, które biorą udział jako uczestnicy w poszczególnych łańcuchach dostaw często odgrywają tam różną rolę, mogą być zarówno producentami, jak i sprzedawcami, a czasem również odpowiadać za magazynowanie lub transport. Ponadto, mnogość uczestników oraz łańcuchów, które nie są ze sobą spięte powoduje, że firmy są zmuszone korzystać z systemów centrów logistycznych, ale również wymieniać się informacjami między sobą, przez co proces zarządzania i przepływu informacji jest niezwykle skomplikowany. W przypadku potrzeby rozwiązania sporów handlowych, podmioty są zmuszone do wyciągnięcia informacji z wielu systemów informatycznych, a następnie ich dokładnej analizy celem zidentyfikowania ich źródła. Są to procesy, które generują wysokie koszty oraz pochłaniają czas.

Główni uczestnicy procesu:

- Producenci – firmy produkujące lub wytwarzające dany towar, mogą to być zarówno farmy, producenci elektroniki, ubrań, samochodów, kopalnie, itp.
- Przewoźnicy – grupa, która może składać się z różnych podkategorii, możemy sklasyfikować tutaj zarówno przewoźników globalnych, włączając w to transport morski oraz powietrzny, jak również regionalnych (np. firmy spedycyjne) i lokalnych (np. kurierzy, poczta).

- Magazyny – podmioty świadczące usługi przechowywania towaru, mogą to być magazyny producentów, przewoźników jak również odbiorcy towaru. Często muszą oni zadbać o odpowiednie warunki przechowywania np. w przypadku żywności lub leków.
- Administracja państwowa – podmioty, których zadaniem jest kontrolowanie przepływu towarów pomiędzy różnymi państwami. Zaliczyć tutaj można np. urzędy celne, które kontrolują ilość oraz rodzaj przesyłanych dóbr oraz odpowiadają za pobieranie należnych opłat.
- Porty i terminale – podmioty odpowiedzialne za przyjmowanie oraz rejestrowanie towarów przesyłanych drogą morską lub lotniczą na szczeblu międzynarodowym oraz krajowym.
- Banki – odpowiadające za rozliczenia pomiędzy podmiotami biorącymi udział w łańcuchu dostaw.
- Ubezpieczyciele – odpowiadający za świadczenie usług związanych z rekompensatą w przypadku utraty towaru, spadku jego jakości lub fałszerstwa.
- Klienci – odbiorcy towaru, zainteresowani szczególnie jego pochodzeniem oraz warunkami, w jakich był on transportowany lub przechowywany. Klientami producentów mogą być zarówno sklepy, odbiorcy hurtowi, jak również klienci detaliczni.

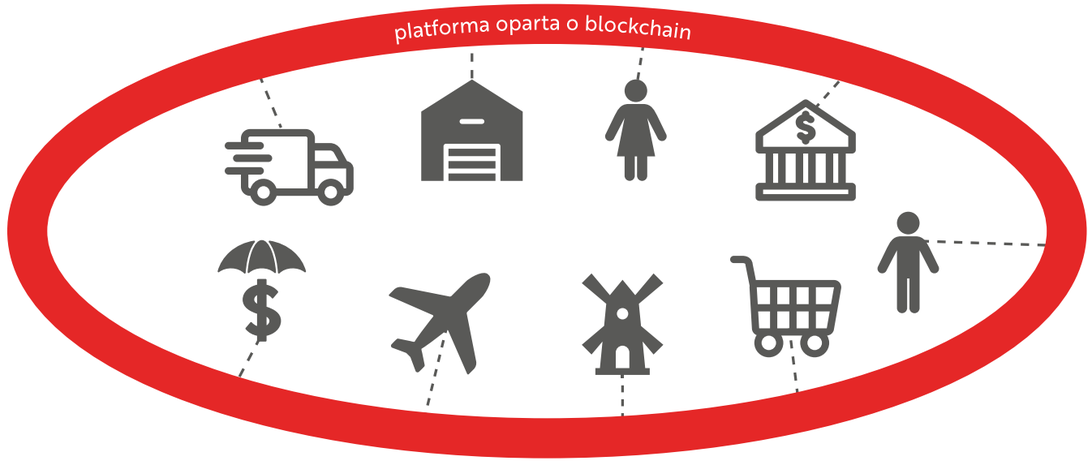
W tradycyjnym podejściu mamy do czynienia z istnieniem wielu systemów informatycznych skomunikowanych ze sobą w różnym stopniu, ale nie uwzględniających wszystkich powyżej opisanych aktorów. Często jeden aktor jest podłączony do kilku sieci informatycznych, gdzie wymienia informacje z innymi. Rozwiązywanie sporów oraz sciąganie należności z ich tytułu może być czasochłonnym procesem, który wymaga zaangażowania dodatkowych zasobów potrzebnych do wykonania zarówno czynności analitycznych, jak również administracyjnych. Ponadto żaden z aktorów nie ma pełnego wglądu w historię danego towaru oraz jego aktualny stan i położenie.



Rys. Schemat procesów wymiany informacji pomiędzy różnymi uczestnikami w łańcuchu dostaw – wersja tradycyjna

W przypadku łańcucha dostaw, nie ma konieczności eliminowania któregokolwiek z uczestników, natomiast istotną zmianą jest tutaj brak konieczności polegania na infrastrukturze IT któregoś z podmiotów. Zamiast tego stworzona może zostać jedna wspólna platforma, nie posiadająca jednego właściciela, co zapewnia zdecentralizowanie informacji w niej zgromadzonych, gwarantując ich niepodważalność i szybką replikację pomiędzy uczestnikami.

Takie podejście zapewnia, że dostęp do informacji jest zdecydowanie uproszczony, a modyfikacja raz wprowadzonych informacji nie może zostać wprowadzona bez wiedzy zainteresowanych. Ponadto, dołączenie do platformy o ujednoliconych standardach dla wszystkich uczestników jest prostsze niż integracja systemów wewnętrznych poszczególnych uczestników pomiędzy sobą.



Rys. Schemat procesu wymiany informacji pomiędzy różnymi uczestnikami w łańcuchu dostaw – wersja Blockchain

3.1. PLANOWANIE I KONTROLA DOSTAW W OBIEGU ŻYWNOŚCI

Opis przypadku i problemu do rozwiązania

Problem skażenia żywności jest niestety wciąż dość powszechnym zjawiskiem, które może mieć zasięg lokalny, regionalny, a nawet globalny. Jeden z przypadków skażenia dotyczący szpinaku, który miał miejsce w Stanach Zjednoczonych, zwrócił uwagę na potrzebę rozwiązania problemu komunikacji oraz możliwości szybkiego lokalizowania potencjalnie zagrożonych partii żywności.

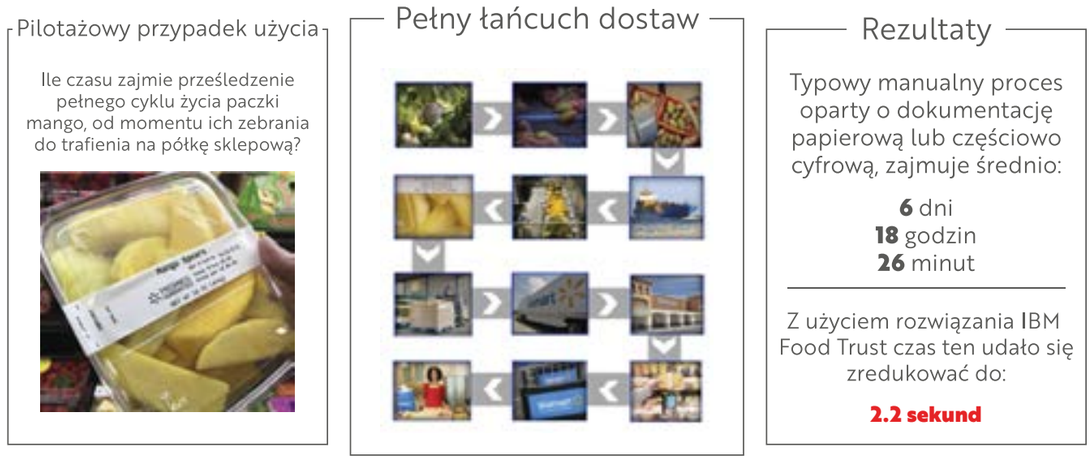
Tradycyjne podejście do rozwiązania

Proces zlokalizowania źródła pochodzenia skażenia oraz zidentyfikowanie wszystkich partii, które mogły mieć kontakt z anomalią trwał kilka tygodni i miał wieloletni wpływ na cały rynek ze względu na konieczność wycofania szpinaku w całym kraju pomimo faktu, że problem dotyczył tylko jednego dostawcy. Wynika to z faktu, że każdy z uczestników ekosystemu tj. producenci, dostawcy, przewoźnicy, magazyny oraz sprzedawcy prowadzą własne rejestry, które często są ze sobą niespójnie i wymagają czasochłonnej analizy w celu zidentyfikowania kompletnego cyklu życia poszczególnych produktów.

Źródło: Materiały IBM

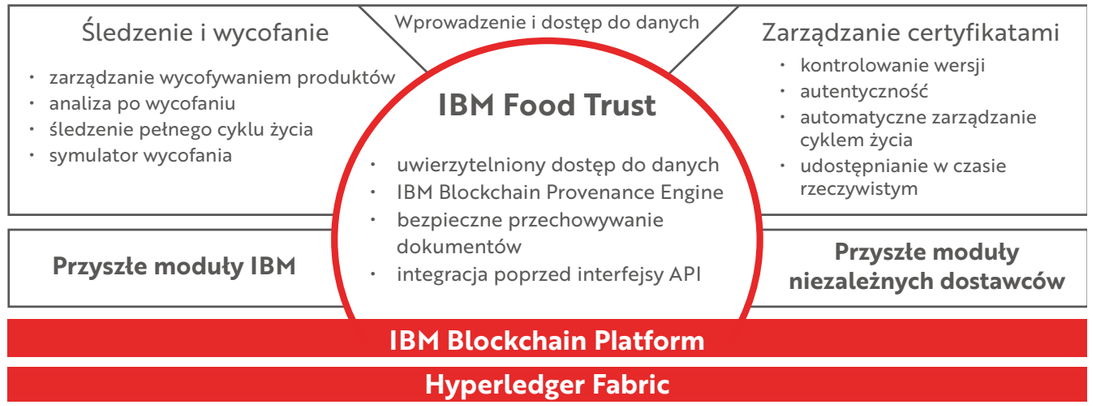
Rozwiązanie oparte o blockchain

Przykładowe rozwiązanie oparte o blockchain zostało opracowane przez firmę IBM. W 2017 roku Walmart wraz z IBM przeprowadził projekt pilotażowy rozwiązania opartego o blockchain, które miało pomóc w rozwiązaniu problemu identyfikacji źródeł kontaminacji. Dzięki wspólnemu rejestrowi prowadzonemu przez wszystkich uczestników utworzonego ekosystemu, udało się skrócić czas potrzebny na przeanalizowanie całego cyklu życia owoców mango od momentu ich zebrania, przez obróbkę, transport, magazyn, aż do półki sklepowej. Kilka tygodni analizy zostało zredukowane do kilku sekund.



Źródło: Materiały IBM

Od połowy 2018 roku rozwiązanie przeszło do fazy produkcyjnej umożliwiając integrację kolejnych organizacji zainteresowanych rejestrowaniem cyklu życia poszczególnych produktów, celem łatwiejszej identyfikacji anomalii oraz szybkiego reagowania w przypadku wykrycia skażenia.



Źródło: Materiały IBM

3.2. PLANOWANIE I KONTROLA DOSTAW W TRANSPORCIE MIĘDZYNARODOWYM

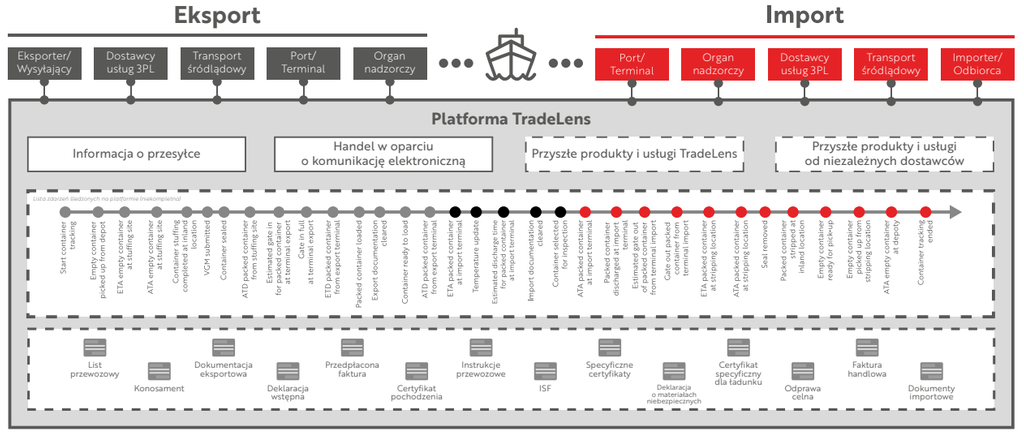
Opis przypadku i problemu do rozwiązania

Wartość transportowanych na świecie dóbr szacuje się obecne na około 16 bilionów dolarów rocznie, przy czym rozmiary i koszty obsługi tego transportu rosną z roku na rok. Biorąc pod uwagę, że około 80% dóbr przewożonych jest z wykorzystaniem transportu morskiego, należy dostrzec, jak ważną rolę odgrywa on w całym ekosystemie oraz jak znaczne oszczędności może przynieść obniżenie kosztów obsługi transportu. Z przeprowadzonych badań wynika, że nawet 20% wydatków ponoszonych na transport jest generowane przez samą tylko obsługę dokumentacji.

Tradycyjne podejście do rozwiązania

W chwili obecnej prawie wszystkie procesy związane z obsługą transportu wykonywane są manualnie, a dokumentacja przekazywana pomiędzy poszczególnymi organizacjami nadal obsługiwana jest w formie papierowej.

Transport pojedynczego kontenera z towarami od eksportera do lokalizacji docelowej może angażować nawet ponad 30 organizacji i wymiany ponad 200 komunikatów pomiędzy nimi. Poniższy schemat obrazuje ten proces, przy czym nie wyczerpuje w sposób kompleksowy ilości możliwych interakcji.

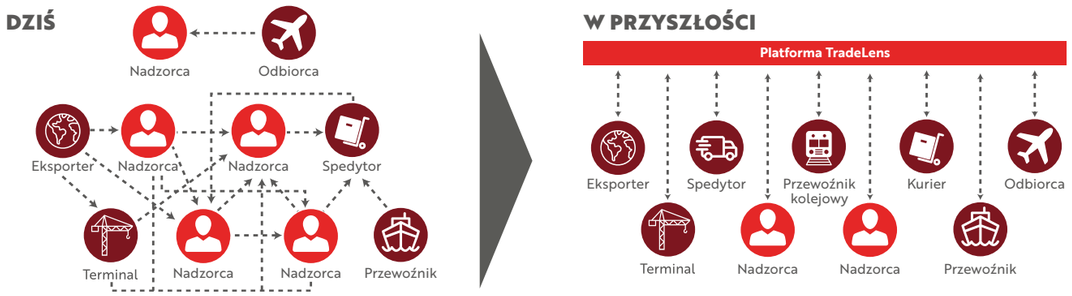


Źródło: www.danskehavne.dk/wp-content/uploads/2018/04/Thomas-Bagge.pdf

Złożoność tego procesu oraz obieg dokumentacji w formie papierowej, powodował jego częstą duplikację oraz brak integralności, a co za tym idzie generował znaczne koszty w przypadku rozwiązywania potencjalnych sporów, czy dochodzenia swoich praw lub reklamacji dotyczących transportu.

Rozwiązanie oparte o blockchain

Przykładowe rozwiązania oparte o blockchain opracowała firma IBM dla Maersk. Platforma TradeLens umożliwia obsługę handlu międzynarodowego za pomocą jednej aplikacji dla wszystkich uczestników ekosystemu. Gwarantuje wspólny punkt widzenia oraz łatwą do weryfikacji i niezaprzeczalną dokumentację w formie elektronicznej, przechowywaną w zdecentralizowanej sieci blockchain, której uczestnikami są między innymi przewoźnicy morscy, porty morskie, urzędy celne, kurierzy oraz dostawcy.



Źródło: https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/

Umożliwienie wymiany informacji oraz obsługi transportu z poziomu wspólnej platformy pozwoliło znacznie obniżyć koszty administracyjne oraz związane z wymianą dokumentacji na szczeblu międzynarodowym. Ponadto, udało się zminimalizować ryzyko związane z błędami, brakiem dokumentów lub podpisów oraz idące za tym interwencje i rozstrzyganie sporów.

4. ELEKTRONICZNA DOKUMENTACJA MEDYCZNA PACJENTÓW

Opis przypadku i problemu do rozwiązania

Historia zdrowia pacjentów jest rozproszona. Ośrodki medyczne, które gromadzą dane pacjenta w wersji elektronicznej wykorzystują je jedynie na własne potrzeby, bez możliwości przekazania tych danych do innych ośrodków, z których korzysta pacjent. W przypadku potrzeby przekazania informacji o historii pacjenta do innego ośrodka, pacjent zazwyczaj potrzebuje pozyskać takie dane w wersji papierowej i przekazać je osobiście.

Problemy:

- Brak ciągłości informacji o pacjencie – lekarze obsługujący pacjenta bazują tylko na wywiadzie i ograniczonej historii dostępnej w ramach danego ośrodka co może wpływać na jakość diagnozy i podejmowanych decyzji o metodach leczenia
- Rozproszone dane o pacjentach – w związku z rozproszeniem informacji o pacjentach, utrudniony jest proces śledzenia zmian zdrowotnych wśród grup społecznych i podejmowania właściwych systemowych działań profilaktycznych
- Rozproszone dane o efektach leczenia – brak możliwości zebrania informacji o metodach leczenia wybieranych przez lekarzy i ich efektach utrudnia śledzenie efektowności metod leczenia jednostek chorobowych w różnych grupach pacjentów
- Brak dostępu do danych zanonimizowanych przez ośrodki badawcze – spowalnia proces rozwoju medycyny

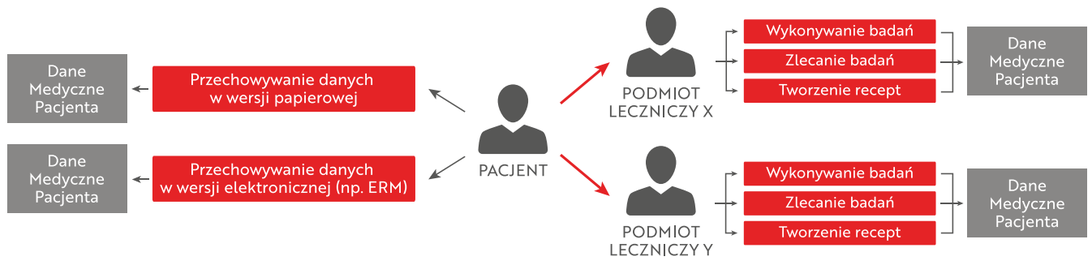
Rozwiązanie powyższych problemów mogłoby przynieść wymierne efekty dla społeczeństwa i gospodarki, poprzez ogólną poprawę kondycji zdrowotnej społeczeństwa, wydłużenie czasu aktywności zawodowej obywateli, zmniejszenie kosztów opieki zdrowotnej i usprawnienie rozliczeń w służbie zdrowia.

Tradycyjne podejście do rozwiązania

W trakcie życia pacjenta powstaje wiele dokumentów opisujących jego stan zdrowia, przebyte choroby, podejmowane metody leczenia, wyniki badań itp. Aktualnie jedynym ośrodkiem, który ma pełną wiedzę o tym jest sam pacjent. Z powodu korzystania przez pacjenta z usług różnych podmiotów leczniczych dokumentacja medyczna pacjenta jest rozproszona. Skutkuje to tym, że lekarz podejmujący leczenie pacjenta bazuje na jego aktualnym stanie i badaniach, a wiedzę historyczną ma ograniczoną jedynie do tego, co zawarte jest w systemach podmiotu, dla którego pracuje. Aby uzupełnić tę wiedzę, pacjent musi sam dbać je archiwizować i dostarczać informacje nt. wcześniejszego leczenia. Dodatkowo pacjent nie wie, kto konkretnie miał dostęp do jego danych medycznych, zwłaszcza gdy te dane były przekazywane w postaci dokumentacji papierowej.

Główni uczestnicy procesu:

- Pacjent – osoba korzystająca ze świadczeń zdrowotnych realizowanych przez podmioty lecznicze
- Podmiot Leczniczy – podmiot wykonujący działalność leczniczą, m.in. ośrodki zdrowia, praktyka indywidulana (lekarska, pielęgniarska, rehabilitacyjna, itd.)



Rys. Dane medyczne pacjenta w procesie tradycyjnym

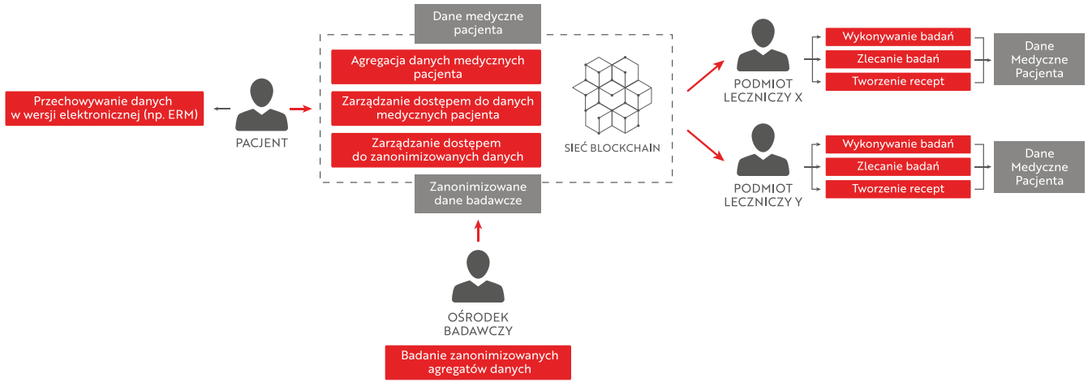
Rozwiązanie oparte o blockchain

W rozwiązaniu opartym o blockchain dane pacjenta są agregowane, przechowywane i dystrybuowane pod nadzorem smart contract'ów. Rekordy medyczne tworzone przez wszystkie podmioty lecznicze trafiają do własnej „bazy danych" pacjenta.

Dostęp do zgromadzonych danych jest kontrolowany przez samego pacjenta, który decyduje, czy dany podmiot leczniczy może mieć do nich dostęp i w jakim zakresie (np. tylko dane związane z urazami ortopedycznymi, lub z wyłączeniem historii chorób zakaźnych). Dodatkową możliwością jaką stwarza to rozwiązanie jest możliwość udostępniania zanonimizowanych i zagregowanych danych ośrodkom zajmującym się badaniami.

Główni uczestnicy procesu:

- Pacjent – osoba korzystająca ze świadczeń zdrowotnych realizowanych przez podmioty lecznicze.
- Podmiot Leczniczy – podmiot wykonujący działalność leczniczą, m.in. ośrodki zdrowia, praktyka indywidulana (lekarska, pielęgniarska, rehabilitacyjna, itd.).
- Ośrodek badawczy – podmiot wykonujący prace badawcze wykorzystując zagregowane dane medyczne.



Rys. Dane medyczne pacjenta w procesie opartym o rozwiązanie blockchain

Blockchain może umożliwić kompleksową, interoperacyjną i bezpieczną wymianę danych medycznych, w której pacjenci są ostatecznymi właścicielami swojej elektronicznej dokumentacji medycznej.

Elektroniczna dokumentacja medyczna oparta na blockchain może umożliwić różnym przedstawicielom opieki zdrowotnej, takim jak lekarze, szpitale, laboratoria, farmaceuci i ubezpieczyciele, zażądanie pozwolenia na dostęp do dokumentacji medycznej i korzystanie z niej. Każda taka interakcja jest kontrolowana, przejrzysta i bezpieczna, a także rejestrowana jako transakcja w sieci blockchain.

Korzyści:

- zebranie informacji w jednym miejscu
- kompleksowy wgląd we wszystkie swoje dane przez pacjenta
- możliwość zarządzania dostępem do danych przez pacjenta
- błyskawiczny dostęp do danych między różnymi placówkami medycznymi
- możliwość wykorzystania danych do celów statystycznych

Wyzwania:

- dane bardzo wrażliwe, konieczność zapewnienia bezpieczeństwa danych
- bardzo duża ilość różnorodnych danych, możliwe problemy wydajnościowe sieci
- konieczność „wyposażenia" pacjentów w oprogramowanie zapewniające bezpieczny i wydajny dostęp do sieci lub zarządzania własnym węzłem
- rozwiązanie problemów związanych z osiągnięciem konsensusu w takiej sieci

Proponowane rozwiązanie jest dużym wyzwaniem operacyjnym, nie tylko na rynku polskim. Wynika to przede wszystkim z konieczności partycypowania wielu podmiotów w takim przedsięwzięciu. Ważną rolę w realizacji takiego rozwiązania miałby też regulator, który mógłbym umożliwić i wesprzeć zmiany, które w konsekwencji przyniosłyby wymierną korzyść dla państwa.

Technologia blockchain może szybciej znaleźć swoje miejsce w polskiej opiece medycznej w wybranych zastosowaniach, tj. w ramach wcześniej opisywanego przykładu trwałego nośnika, gdzie blockchain uniemożliwi ingerencję w dane i zapewni ich pełną audytowalność placówkom medycznym. Takie rozwiązanie jest aktualnie opracowywane m.in. przez Atende.

5. ZAPOBIEGANIE KRADZIEŻY TELEFONÓW

Kradzież telefonu jest częstym przypadkiem. Telefon może by skradziony użytkownikowi lub w trakcie przesyłki (transport, magazyn, itd.). Skradzione telefony są blokowane przez operatorów po zgłoszeniu kradzieży i skradziony telefon nie może być wykorzystany w sieci macierzystej. Niestety, informacja o kradzieży przekazywana jest do innych operatorów z opóźnieniem (lub w ogóle) i skradziony telefon może być w tych sieciach wykorzystany.

W teorii, dostępny rejestr używany przez większość operatorów do blokowania skradzionych telefonów mógłby zniechęcić złodziei. Mógłby też być wykorzystany przez ubezpieczycieli, by zautomatyzować wypłaty odszkodowań i obniżyć koszty obsługi polis ubezpieczeniowych.

Obecne podejście do rozwiązania

GSMA utrzymuje system znany jako Międzynarodowa Baza Identyfikacji Sprzętu Mobilnego (IMEI DB), która jest globalną centralną bazą danych zawierającą podstawowe informacje o zakresach numerów seryjnych (IMEI) milionów urządzeń mobilnych (np. telefonów komórkowych, przenośnych kart danych, itp.), które są używane w sieciach komórkowych na całym świecie. Numer IMEI to 15-cyfrowy numer używany do identyfikacji urządzenia w sieci komórkowej. W bazie jest też centralny rejestr identyfikacyjny sprzętu (CEIR), który działa jako system służący operatorom sieci do udostępniania swoich czarnych list (list zablokowanych IMEI urządzeń zgłoszonych jako skradzione lub zgubione). Ta baza danych może służyć innym operatorom, by odmawiały świadczenia usługi urządzeniom na czarnej liście. Niestety, dostęp do tego systemu jest ograniczony, a strony udostępnione publicznie nie zawsze pokazują aktualne dane lub są w ogóle niedostępne.

Główni uczestnicy w procesie:

- Operatorzy
- GSMA

Główne wyzwania:

1. Ręczne procesy powodujące błędy i opóźnienia w procesowaniu zgłoszeń kradzieży.

→ Blokowanie urządzenia nie jest natychmiastowe i może być wykonane wyłącznie przez operatora macierzystego.

→ Aktualizacja globalnej bazy danych robiona jest przez operatorów okresowo, na przykład poprzez dzienne wysyłanie czarnych list do GSMA.

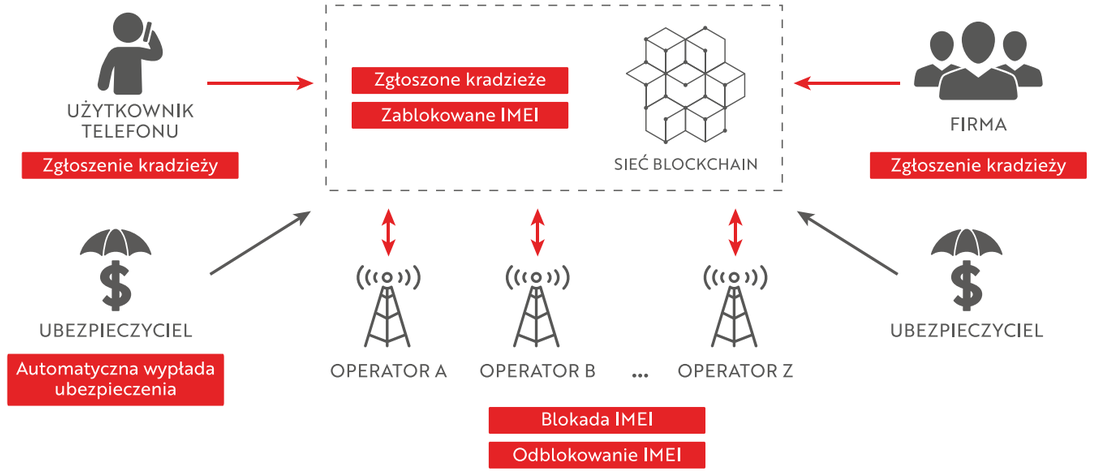
2. Rozwiązanie jest uzależnione od jakości i dostępności globalnej bazy danych.

→ Blokowanie urządzeń z czarnej listy jest możliwe tylko wtedy, gdy wszyscy operatorzy regularnie pobierają najnowszą, zaktualizowaną globalną bazę danych, na przykład od GSMA.

3. Brak możliwości wdrożenia prostego mechanizmu korzystania z informacji przez strony trzecie, np. policję lub ubezpieczycieli.

4. Brak możliwości korzystania z informacji przez użytkowników końcowych by sprawdzić status blokady lub sprawdzić, czy nabywany używany telefon nie znajduje się na czarnej liście.

Rozwiązanie oparte o blockchain



Rys. Proces przekazywania informacji i zapobiegania używania skradzionych telefonów – wersja blockchain

Użytkownik zgłasza kradzież telefonu. Operator macierzysty blokuje IMEI, a informacja na temat skradzionego telefonu umieszczana jest na blockchainie. Jeżeli ktoś spróbuje zadzwonić u innego operatora z telefonu z danym IMEI, będzie możliwość natychmiastowego sprawdzenia czy nie był on wcześniej zgłoszony jako skradziony. Dostęp do systemu będą mogli mieć opcjonalnie ubezpieczyciele lub policja. System będzie umożliwiał poinformowanie macierzystego operatora o odnalezieniu telefonu w celu jego odblokowania.

Aktorzy w procesie:

- operatorzy
- użytkownicy końcowi
- ubezpieczyciele
- policja

Korzyści z zastosowania technologii blockchain:

1. Każdy uprawniony uczestnik systemu będzie mógł zgłosić kradzież telefonu komórkowego.

2. Natychmiastowa informacja o zablokowaniu zgłoszonego skradzionego urządzenia dostępna jest dla wszystkich korzystających z systemu.

3. Możliwość sprawdzenia statusu urządzenia przez wszystkich uczestniczących operatorów.

4. Możliwość wykorzystania inteligentnych kontraktów (smart contracts):

→ Do automatycznego informowania zainteresowanych o zmianie statusu urządzenia (np. odnalezienie urządzenia i jego odblokowanie).

→ Automatyzacji procesu wypłacania odszkodowania przez ubezpieczycieli.

5. Ograniczenia ilości kradzieży poprzez nieuchronność zblokowania urządzenia.

6. Możliwość kierowania klientów na zakup nowej słuchawki.

Źródło: Telemanagement Forum, Program Catalyst, 2018.

6. PRZECIWDZIAŁANIE OSZUSTWOM FAKTORINGOWYM TYPU "DUBLOWANY FACTORING"

Opis przypadku i problemu do rozwiązania

We włoskim obrocie gospodarczym popularną usługą oferowaną przez banki jest faktoring. Jedne z najdłuższych w Europie terminy płatności oraz zatory płatnicze[11] powodują, że uczestnicy rynku chętnie przedstawiają wystawiane przez siebie dokumenty sprzedaży do obsługi faktoringowej w celu poprawienia płynności finansowej.

Powszechność finansowania wierzytelności przez banki ma również inny aspekt – oszustwa finansowe na bazie fałszywych faktur, fałszywych kontrahentów lub przedstawienia tej samej wierzytelności do kilku faktorów. Są to wymierne zagrożenia, w szczególności tam, gdzie wymiana informacji pomiędzy uczestnikami rynku (instytucjami finansowymi, wierzycielami i płatnikami) jest utrudniona lub niemożliwa z tytułu wielkości rynku i wolności obrotu gospodarczego. Oszustwa związane ze zdublowanym faktoringiem są powszechne i oszuści próbują pozyskać środki z tytułu przedstawienia tej samej faktury wielu bankom.

Rozwiązanie oparte o technologię blockchain potencjalnie może wyeliminować utrudnienia, pozwolić na większą przejrzystość i wymianę informacji.

11 European Payment Report 2018

Tradycyjne podejście do rozwiązania

Proces obsługi dokumentów przez instytucje finansowe od momentu otrzymania dokumentacji do momentu uruchomienia środków zajmuje zazwyczaj między 2 a 4 tygodnie.

Głównym wyzwaniem są:

- czas spędzony nad sprawdzaniem wiarygodności przedstawionej wierzytelności
- sprawdzenie, czy wierzytelność nie została wcześniej lub równocześnie przedstawiona do finansowania lub sfinansowana (częściowo lub w całości) w innym banku
- niejednorodny sposób komunikacji pomiędzy bankami finansującymi
- brak transparentności danych oraz niechęć do dzielenia się pełnymi zestawami danych

Rozwiązanie oparte o blockchain

Przykładowe rozwiązanie oparte o blockchain opracowała firma GFT. Wdrożone rozwiązanie oparte jest o architekturę DLT zapewnia:

- pełną historię wierzytelności zgłoszonych do systemu przez zapytania od uczestników,
- pełen dostęp do ograniczonego, lecz unikalnego modelu danych o wierzytelnościach (identyfikator faktury, numer identyfikacji podatkowej, data wystawienia),
- integralność i bezpieczeństwo danych,
- redukcja czasu potrzebnego do sprawdzenia wierzytelności,
- możliwy dalszy rozwój rozwiązania i implementacja kolejnych funkcjonalności związanych np. z kalkulacją ryzyka, historią kredytową, sekurytyzacją wierzytelności.

Rozwiązanie zbudowane w oparciu o węzeł DLT jest udostępnione w prywatnej infrastrukturze operatora usługi z dostępem do systemu oferowanemu przez web interface dla operatorów, interface SCP do wymiany danych oraz umożliwia uruchomienie własnego węzła po stronie uczestników usługi przy zachowaniu identycznej funkcjonalności.

Użytkownicy mają dostęp do następujących informacji zbudowanych w oparciu o swoje zapytania kierowane i utrzymywane w rejestrze:

- unikalny klucz zbudowany w oparciu o dane wierzytelności
- zrealizowany procent finansowania wierzytelności
- komunikat o ryzyku związanym z wierzytelnością.

Korzyści:

- uregulowanie obiegu informacji i sformalizowanie modelu danych
- eliminacja ryzyka związanego z możliwościami oszustw typu „podwójny faktoring" dla uczestników systemu
- redukcja czasu związanego z decyzją o finansowaniu z 2-4 tygodni do 24h-48h
- podstawa do uruchomiania kolejnych usług na bazie historycznych danych

Wyzwania:

- zbudowanie „masy" faktorantów, faktorów i potencjalnie dłużników chcących uczestniczyć w inicjatywie,
- moderacja ryzyka operatora usługi – teoretycznie mogłaby to być sieć w pełni automatyzująca p2p kontrakty o wykup wierzytelności,
- moderacja ryzyka wydajnościowego – pełne dane faktury przekazywane przez sieć blockchain.

7. ZDECENTRALIZOWANA DYSTRYBUCJA TREŚCI CYFROWYCH

Opis przypadku i problemu do rozwiązania

Studia produkcyjne i sieci mediowe (w tym dostawcy treści w modelu OTT, tacy jak Netflix i Amazon) finansują produkcję treści, a treści te podążają następnie tradycyjną ścieżką dystrybucji – od studia i wydawcy do użytkownika końcowego jednym z predefiniowanych kanałów: TV (kablową, naziemną, satelitarną) lub przez Internet (strona internetowa lub dedykowana aplikacja na komputer bądź urządzenie mobilne).

Dostawcy treści wciąż opierają się na idei „scentralizowanej" agregacji i dystrybucji. Aby znaleźć się w dystrybucji, twórcy treści muszą minąć pewną liczbę „odźwiernych". Decyzje dotyczące tego, jaka treść jest oferowana, kiedy jest oferowana, ceny i drogi dystrybucji, są hierarchiczne i zazwyczaj narzucone przez sieci dystrybucyjne.

Blockchain umożliwia zrealizowanie zdecentralizowanego modelu dystrybucji treści i likwidację barier dla twórców w dystrybucji i konsumentów w dostępie.

Tradycyjne podejście do rozwiązania

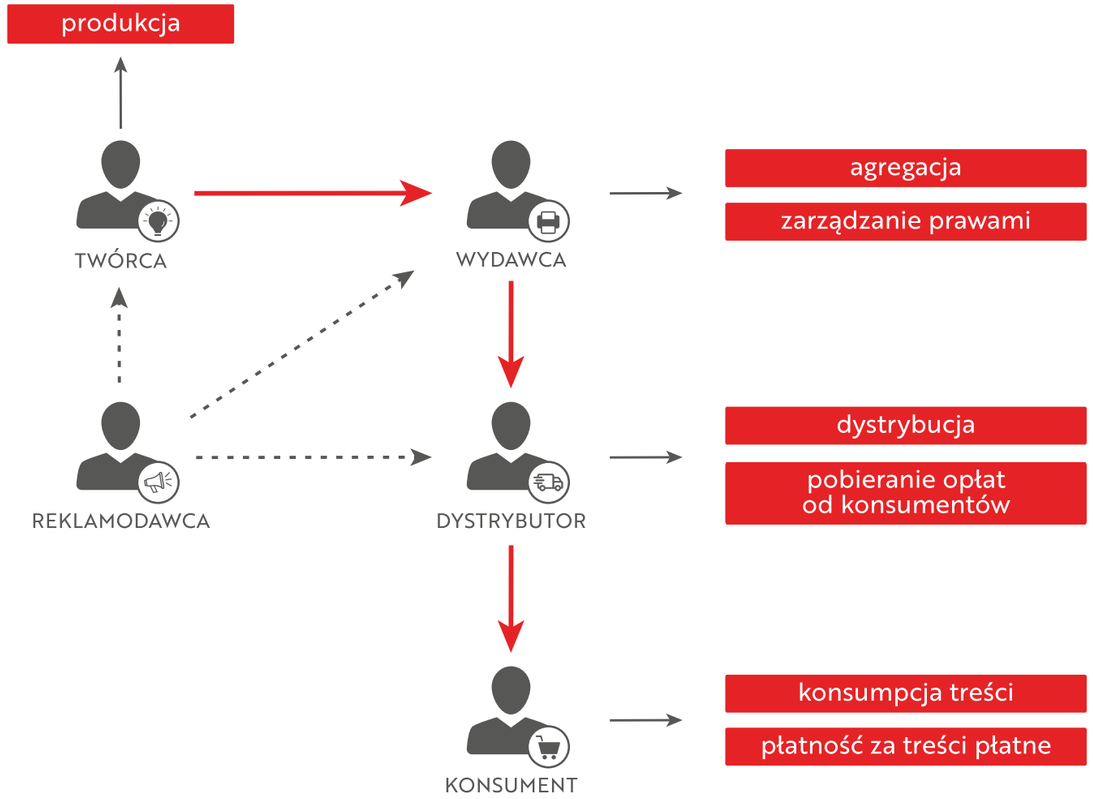
W tradycyjnym modelu, punktem wejścia dla twórcy są wydawcy zajmujący się agregacją treści, zarządzaniem prawami i umowami z dystrybutorami. Dystrybutorzy działający na różnym poziomie zajmują się dalszą dystrybucją treści, aż do poziomu lokalnych dystrybutorów i nadawców. Opłaty od konsumentów, wracają ścieżką zwrotną aż do twórcy. Serwisy internetowe tj. Netflix skracają i przyspieszają ścieżkę dystrybucji, ale nadal pozostają bariery dla twórców i konsumentów.

Główni uczestnicy procesu:

- Twórca – osoba lub firma zajmująca się produkcją treści np. produkcją wideo
- Wydawca – firma pozyskująca treści od producentów, agregująca je, sprzedająca Dystrybutorom prawa do dalszej dystrybucji posiadanych treści
- Dystrybutor – firma pozyskująca treści od Wydawcy i zajmująca się ich sprzedażą do klienta końcowego lub kolejnych dystrybutorów
- Konsument – osoba oglądająca treści, płacąca za ich oglądanie
- Reklamodawcy – firmy plasujące (poprzez agencje) treści reklamowe. Treści te mogą być dołączane na różnym etapie dystrybucji, wpływając na cenę kosztową dla klienta końcowego (w efekcie mogą także pojawić się treści w pełni sponsorowane przez reklamy).

W świecie zdecentralizowanej dystrybucji mediów cyfrowych opartej o blockchain, relacje pomiędzy interesariuszami są regulowane przez smart contract'y.

Twórcy mogą udostępniać swoje produkcje bezpośrednio w sieci definiując dodatkowe zasady w postaci smart contract'ów np. cenę dla dystrybutora (np. niższa cena za zakup praw na odtworzenie treści x 1000), cenę dla klienta końcowego, gotowość do łączenia z reklamami itp. Dzięki decentralizacji, twórcy nie będą musieli przekonywać wydawców czy dystrybutorów, by ich treści pojawiły się w dystrybucji. Zmniejszają się bariery wejścia do dystrybucji, choć nadal pozostaje kwestia dotarcia do klienta końcowego.



Rys. Proces dystrybucji treści cyfrowych w modelu tradycyjnym

W systemie opartym o blockchain każdy podmiot może pełnić rolę dystrybutora, który tworzy serwisy i aplikacje do dystrybucji moderowanych treści udostępnionych przez twórców. Nowe „kanały TV" mogą pojawić się w całkowicie zdecentralizowany sposób poprzez agregację treści udostępnionych w sieci, np. kanały e-sport, wydarzeń na żywo, fantasy, sci-fi, itp. Te kanały mogą być konfigurowane przez każdego i dołączane przez twórców treści.

Dystrybucją bezpośrednio do klienta końcowego mogą też zajmować się sami twórcy, przy czym zasady na jakich oferują swoje treści, są jasno określone i znane wszystkim uczestnikom, w tym wyspecjalizowanym dystrybutorom.

Konsument uiszcza opłatę za dostęp do treści w sieci blockchain, a ona zajmuje się automatycznym rozdziałem przychodów zgodnie z wcześniej zdefiniowanymi zasadami. Wszyscy interesariusze otrzymują przychody bezpośrednio z sieci – nie ma już rozliczeń w tradycyjnej ścieżce dystrybutor → wydawca → twórca. Pieniądze trafiają do wszystkich odbiorców w tym samym czasie i bez zwłoki.

Reklamodawcy udostępniają treści reklamowe w sieci definiując dodatkowe zasady dla ich ekspozycji w postaci smart contract'ów, tj. profil odbiorcy, cenę jaką są skłonni zapłacić za obejrzenie reklamy, kategorię treści z jakimi może pojawić się reklama. Konsument może z kolei sam decydować, czy chce obejrzeć reklamę otrzymując w zamian tańsze lub bezpłatne treści.

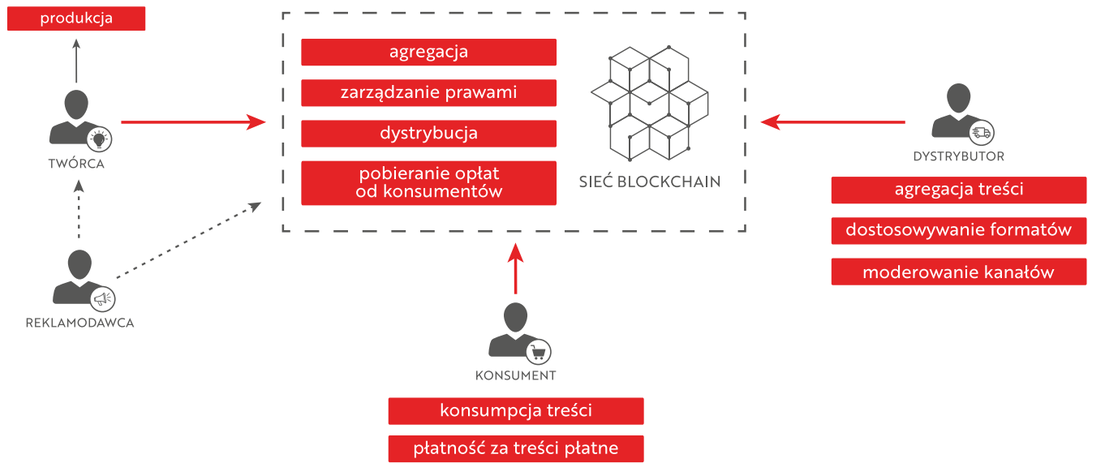
Główni uczestnicy procesu:

- Twórca – osoba lub firma zajmująca się produkcją treści np. produkcją wideo,
- Konsument – osoba oglądająca treści, płacąca za ich oglądanie,
- Reklamodawcy – firmy plasujące (poprzez agencje) treści reklamowe,
- Dystrybutor – firma agregująca treści umieszczone w sieci i udostępniająca je poprzez własne witryny i aplikacje, dokonująca adaptacji formatów dla konsumentów.

Technologia Blockchain ma możliwość zrewolucjonizowania modelu biznesowego branży rozrywkowej poprzez przełamanie pseudo-monopolu, zastępując scentralizowany i zhierarchizowany model siecią peer-to-peer.

Dodatkową zaletą dystrybucji przez blockchain jest pełna przejrzystość historii produkcji i ich wyników finansowych. Dla twórców z dobrą historią, daje to większe możliwości pozyskiwania funduszy, a dla inwestorów minimalizuje ryzyko nietrafnych inwestycji.

Nie jest wykluczone równoległe funkcjonowanie wielu rozproszonych sieci dystrybucji treści, np. odrębnych dla w pełni komercyjnych podmiotów (aktualnie biorących udział w scentralizowanym procesie dystrybucji) oraz dla treści tworzonych przez niezależnych twórców. W każdym wypadku udostępnienie treści przez sieci blockchain umożliwi ich szerszą dystrybucję oraz większe szanse dla konsumentów dotarcia do nich.



Rys. Proces dystrybucji treści w modelu zdecentralizowanym opartym o Blockchain

8. ROBOTIC PROCESS AUTOMATION WSPIERANE TECHNOLOGIĄ BLOCKCHAIN

Opis przypadku i problemu do rozwiązania

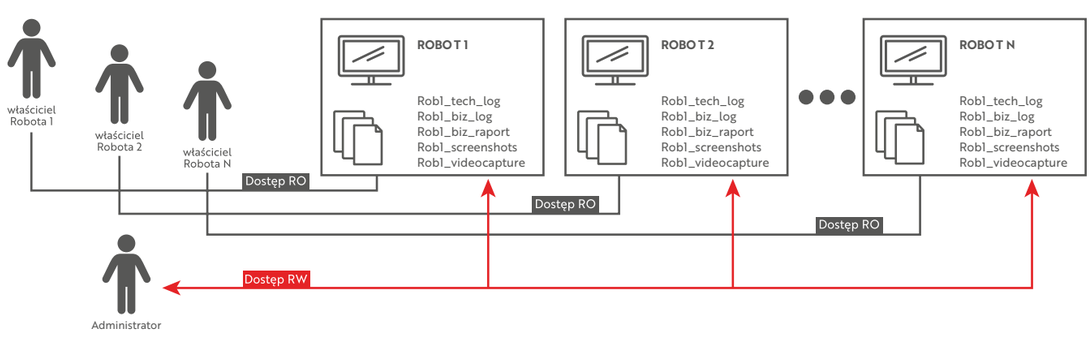
Zrobotyzowana Automatyzacja Procesów (ang. Robotic Process Automation – RPA) to nowa, rewolucyjna dziedzina informatyki znajdująca swoje zastosowanie w świecie procesów biznesowych. Idea Software'owego Robota polega na realizowaniu operacji (które w konwencjonalnym ujęciu pracy wykonuje pracownik) przez zaprogramowany algorytm. W efekcie działania takiego algorytmu otrzymujemy konkretny oczekiwany efekt procesu

biznesowego (przeprocesowaną sprawę, zaksięgowaną fakturę, itp.). W praktyce wszystkie procesy, które można opisać algorytmem działania, mogą zostać zautomatyzowane z wykorzystaniem Robotic Process Automation. Robot operuje na interface użytkownika – realizuje takie same czynności co człowiek np. wprowadza dane do formularzy, przełącza się pomiędzy aplikacjami biznesowymi, przenosi dane pomiędzy nimi. W sposób programowy wykorzystuje wszystkie urządzenia peryferyjne potrzebne do działania – klawiaturę, myszkę etc.

W przypadku realizacji procesów operujących na danych, które uznawane są przez daną organizację za krytyczne, niezbędne jest zapewnienie bezpieczeństwa tych danych. Uniemożliwienie modyfikacji danych poprzez zastosowanie mechanizmów audytowalności działań w procesie pozwala znacznie ograniczyć ryzyko operacyjne danego procesu biznesowego.

Tradycyjne podejście do rozwiązania

Właściwa i dojrzała implementacja Robotic Process Automation zapewnia minimalny, niezbędny poziom audytowalności działań poprzez zastosowanie logów technicznych z działania robota, logów biznesowych przeprocesowanych spraw, raportów zawierających informacje pozwalające stwierdzić jak dana sprawa została zrealizowana. Z punktu widzenia użytkownika systemu klasy RPA (częstokroć rolę tą reprezentuje właściciel lub operator procesu) efekty działań robota software'owego mogą zostać zaprezentowane w postaci zrzutów ekranów bądź fragmentów filmów z przeprowadzonych operacji w systemie, w którym operuje robot.

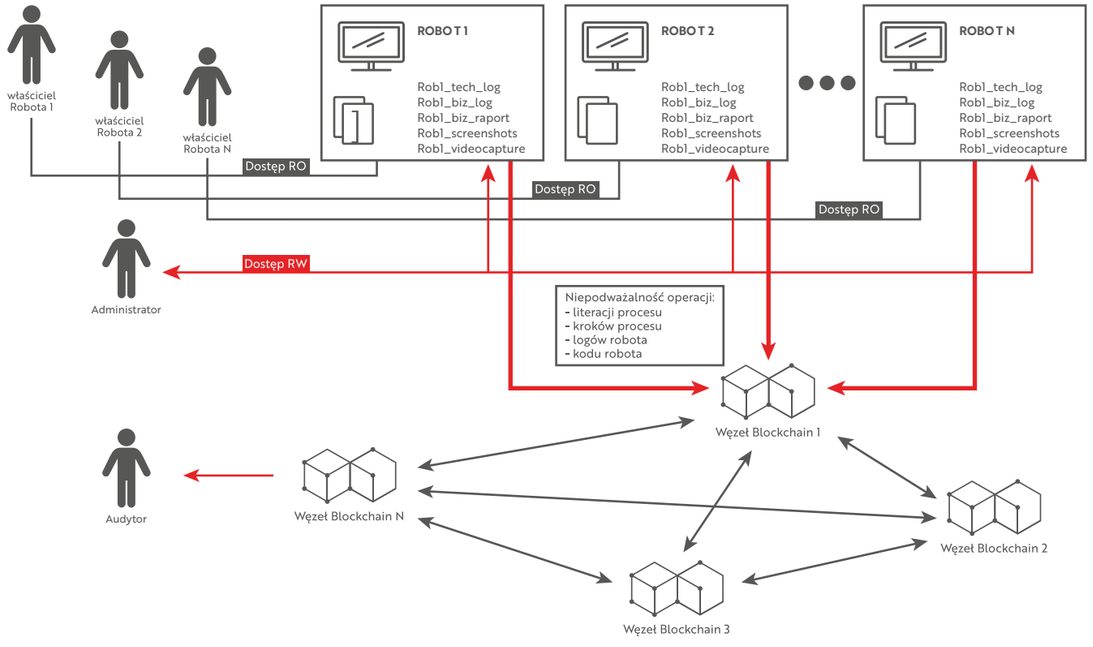


Przedstawione powyżej rozwiązania, pomimo swoich zalet, nie posiadają bardzo istotnej cechy jaką jest niezaprzeczalność danych. Z punktu widzenia audytu zautomatyzowanego procesu, dane mogą zostać zmienione na poziomie administracyjnym – zarówno w obszarze administracji infrastrukturą i systemami IT, jak i administracji procesem.

Rozwiązanie oparte o blockchain

Zastosowanie technologii blockchain w technologii Robotic Process Automation jest wielowymiarowe. Pierwszym miejscem, w którym bezpieczeństwo automatyzacji procesów biznesowych może zostać znacznie zwiększone jest zabezpieczenie kolejnych iteracji wykonania procesu lub też pojedynczych kroków danego procesu. Jeśli przeprocesowana sprawa będzie stosownie logowana, a następnie logi zostaną potwierdzone z wykorzystaniem technologii blockchain, wyeliminowana zostaje możliwość manipulacji faktem jej przeprocesowania. Jeśli krytyczne z punktu widzenia biznesu jest zapewnienie niezaprzeczalności konkretnego elementu procesu np. wykonania przelewu, wysłania dokumentu do organu regulacyjnego, itp., również w takim przypadku istnieje możliwość potwierdzenia takiego faktu. Należy zaznaczyć, że takie ostemplowanie zawiera w sobie informacje o dacie i czasie stemplowania. Posiadając zatem niezmienialny skrót wykonanego procesu bądź konkretnego kroku procesu, zawierający dodatkowo informacje o czasie stemplowania, jesteśmy w posiadaniu niezaprzeczalnego dowodu wykonania danej czynności w czasie.

Innym obszarem, w którym robotyzacja może zostać wykorzystana jest zabezpieczenie samego kodu robota. Paczka wdrożona do silnika robotyzacji, która zawiera informacje o tym, jak cały proces ma być wykonywany, jest w dojrzałych implementacjach objęta procesem Release Management'u. Jest to podejście znane z typowego procesu wytwórczego oprogramowania. Zmiany kodu robota odkładane są w systemach zarządzania wersjami, a samo wdrożenie produkcyjne nowych wydań realizowane jest bardzo często w sposób nieautomatyczny przez administratorów systemów IT. Zastosowanie blockchain w tym obszarze znacząco podnosi poziom zabezpieczenia kodu robota. Poprzez stemplowanie wersji kodu ograniczona zostaje do minimum podatność na niepotwierdzone modyfikacje w kodzie robota.



Korzyści:

- Zapewnienie niezaprzeczalności wykonania iteracji procesu oraz konkretnych kroków procesu
- Zabezpieczenie opisu procesu (kodu robota) przed nieautoryzowanymi zmianami
- Centralizacja informacji o wykonanych czynnościach w zautomatyzowanym procesie
- Automatyczne znakowanie czasem

Wyzwania:

- Zapewnienie uzgodnionej struktury danych wprowadzanych do łańcucha blockchain
- Zapewnienie infrastruktury IT (budowa bądź wykupienie stosownej usługi)

9. PŁATNOŚCI I ROZLICZENIA MIĘDZYBANKOWE Z WYKORZYSTANIEM SIECI RIPPLE

Opis przypadku i problemu do rozwiązania

Systemy płatności służą do rozliczania transakcji finansowych poprzez przekazywanie wartości pieniężnej i obejmują instytucje, procedury, standardy i technologie, które umożliwiają taką wymianę. Systemy płatności są wykorzystywane zamiast bezpośredniej wymiany gotówki w transakcjach krajowych i międzynarodowych i są utrzymywane przez banki i inne instytucje finansowe.

Systemy płatności mogą być fizyczne lub elektroniczne, a każdy z nich ma swoje własne procedury i protokoły. Standaryzacja pozwoliła niektórym z tych systemów i sieci rozwinąć się na skalę globalną, ale wciąż istnieje wiele systemów wykorzystywanych w danym kraju lub dedykowanych do obsługi konkretnych transakcji finansowych.

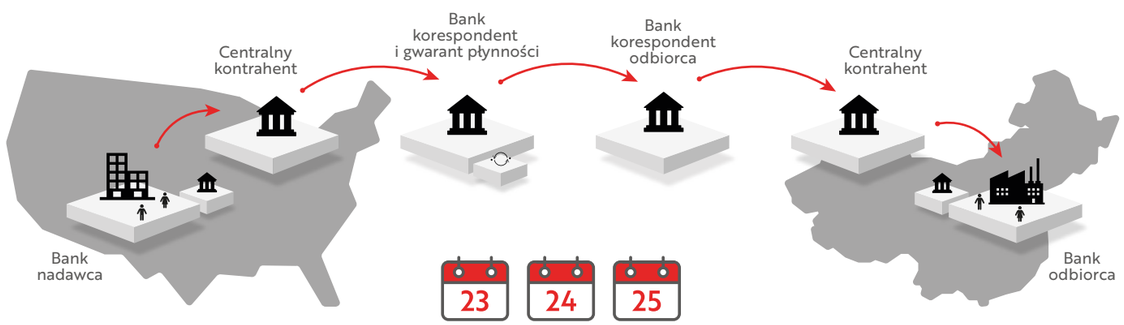
Tradycyjne podejście do rozwiązania

Dzisiejsze systemy płatności i rozliczeń międzybankowych opierają się o technologie wymyślone jeszcze przed istnieniem Internetu. Istnieją systemy płatności wykorzystywane do rozliczania transakcji finansowych związanych z rynkami papierów wartościowych i obligacji, rynkami walutowymi, rynkami instrumentów pochodnych, oraz innymi instrumentami finansowymi. Szczególnymi przypadkami są transfery miedzy instytucjami finansowymi w obrębie jednego kraju z wykorzystaniem systemów rozliczeniowych działających w czasie rzeczywistym RTGS (real-time gross settlement) oraz transfery międzynarodowe korzystające z sieci SWIFT.

Głowni uczestnicy procesu:

- banki i inne instytucje finansowe,
- banki centralne,
- Krajowe Izby Rozliczeniowe,
- międzynarodowe stowarzyszenia np. SWIFT.

Dziś: Międzynarodowe płatności wymagają użycia pośredników



Niski wolumen **Duże wartości** **Powolny** **Płatności okresowe**

Główne wyzwania

- Wysokie opłaty transakcyjne pobierane przez banki i pośredników. WTO (World Trade Organization) ocenia, że w 2017 globalne opłaty transakcyjne sięgały 1,6 tryliona dolarów.
- Prędkość transakcji. Realizacja niektórych typów transferów może zająć 3-5 dni, w trakcie których strony nie mają dostępu do transferowanych aktywów.
- Brak transparentności.
- Podatność na błędy w transmisji, opóźniające rozliczenia.
- Nieprzystosowanie do wymagań współczesnej zglobalizowanej i ucyfrowionej gospodarki.

Rozwiązanie oparte o blockchain

Firma Ripple stworzyła otwarty system oparty na protokole który pozwala na transfery wartości w sieci peer-to-peer. System Ripple umożliwia płatności bezpośrednio między bankami lub innymi instytucjami finansowymi, w różnych sieciach, granicach geograficznych lub walutach.

W systemie Ripple użytkownicy dokonują płatności między sobą, korzystając z transakcji podpisanych kryptograficznie, denominowanych w walutach fiducjarnych, reprezentowanych przez tokeny lub wewnętrznej walucie Ripple (XRP). Ripple wykorzystuje rozproszony rejestr danych przechowujący informacje o wszystkich kontach Ripple. Sieć jest zarządzana przez niezależne serwery walidujące, które stale porównują swoje rekordy transakcji. Serwery mogą należeć do każdego, w tym do banków lub niezależnych instytucji. Prócz banków, walidatorami w sieci Ripple są między innymi MIT (Massachusetts Institute of Technolgy) oraz dostawcy usług internetowych.

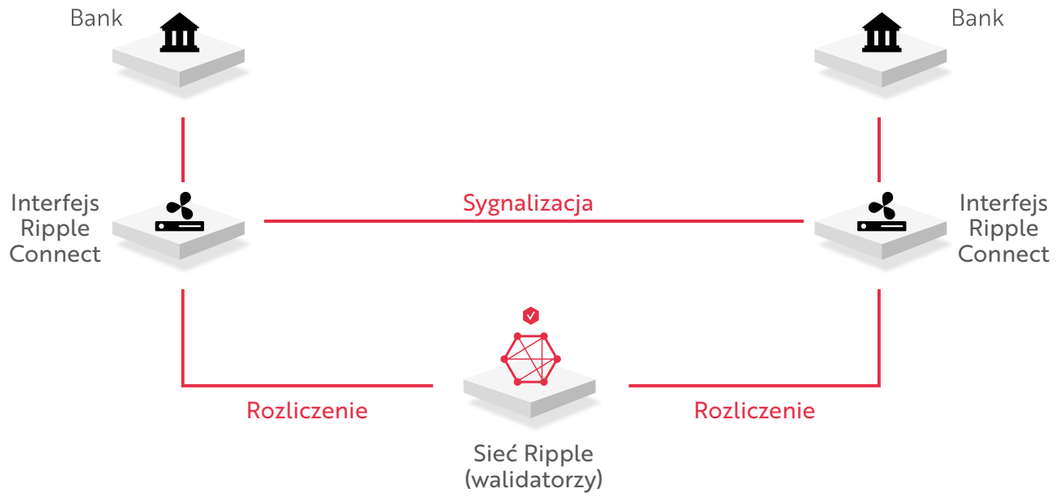
Proces konsensusu jest rozproszony, a celem konsensusu jest, by każdy serwer miał ten sam zestaw transakcji w bieżącej wersji rejestru. Transakcje uzgodnione przez większość uczestników sieci są uważane za zatwierdzone. Jeśli nie ma zgody miedzy uczestnikami, może to oznaczać, że wolumen transakcji jest zbyt wysoki lub opóźnienie w sieci zbyt duże, by proces konsensusu zadziałał. Proces jest ponownie uruchamiany przez węzły w sieci, a każda runda porozumienia zmniejsza spór, aż do osiągnięcia większości.

Ripple umożliwia transakcje w różnych walutach i realizuje je w ciągu 3 do 5 sekund. Konta i transakcje są kryptograficznie zabezpieczone i sprawdzane algorytmicznie. Płatności mogą być autoryzowane tylko przez posiadacza rachunku, a wszystkie płatności są przetwarzane automatycznie, bez żadnych stron trzecich lub pośredników. Płatności są nieodwracalne, a Ripple pobiera opłatę transakcyjną, której celem jest ochrona przed zalaniem sieci przez transakcje generowane przez hakerów.

Korzyści wynikające z korzystania z sieci Ripple

- Prędkość – transakcje realizowane są w ciągu kilku sekund z natychmiastowym rozliczeniem (z wydajnością około 1,5 tysięcy transakcji na sekundę), a nie w dniach.
- Pewność – transakcje są zabezpieczone kryptograficznie, walidowane w procesie konsensusu i są nieodwracalne. Uczestnicy zyskują kompleksową widoczność opłat, statusu i informacji o kliencie.

- Dostępność – każdy bank lub inna instytucja finansowa na świecie może w prosty sposób dołączyć do sieci używając standardowych interface'ów.
- Koszty – Ripple pobiera nominalne opłaty, dużo niższe niż tradycyjne opłaty transakcyjne pobierane przez pośredników w trakcie transferów międzybankowych, co przekłada się na niższe wymogi kapitałowe dla płatności międzynarodowych.



Rys. Architektura rozwiązania opartego o blockchain

Z sieci Ripple korzysta dziś komercyjnie ponad 75 banków i instytucji finansowych w tym Santander Bank, Royal Bank of Scotland, Crédit Agricole, American Express, MoneyGram, MUFG Bank, SBI Remit.

Firma znanego blogera, założyciela Crunchbase, Michaela Arringtona poinformowała pod koniec października 2018 roku, że przetransferowała za pośrednictwem Ripple 50 milionów dolarów. Opłata transakcyjna wyniosła 30 centów, a transakcja została wykonana w 2 sekundy. Tego typu transfery finansowe przy użyciu tradycyjnych metod obciążane są opłatami na poziomie 0,5-2% i trwają 2-3 dni.[12]

12 Bitcoin Exchange Guide News, 2018

PORTFOLIO NASZYCH PROJEKTÓW

IBM Services

- Trwały Nośnik
- Planowanie kontroli dostaw żywności
- Łańcuch dostaw
- Międzynarodowy system płatności międzybankowych

KDPW | Krajowy Depozyt Papierów Wartościowych & IBM

KDPW i IBM Services

- e-Głosowanie

ATENDE

Atende S.A.

- Trwały Nośnik
- Łańcuch dostaw
- Robotic Process Automation
- Blockchain w medycynie

automa & ATENDE

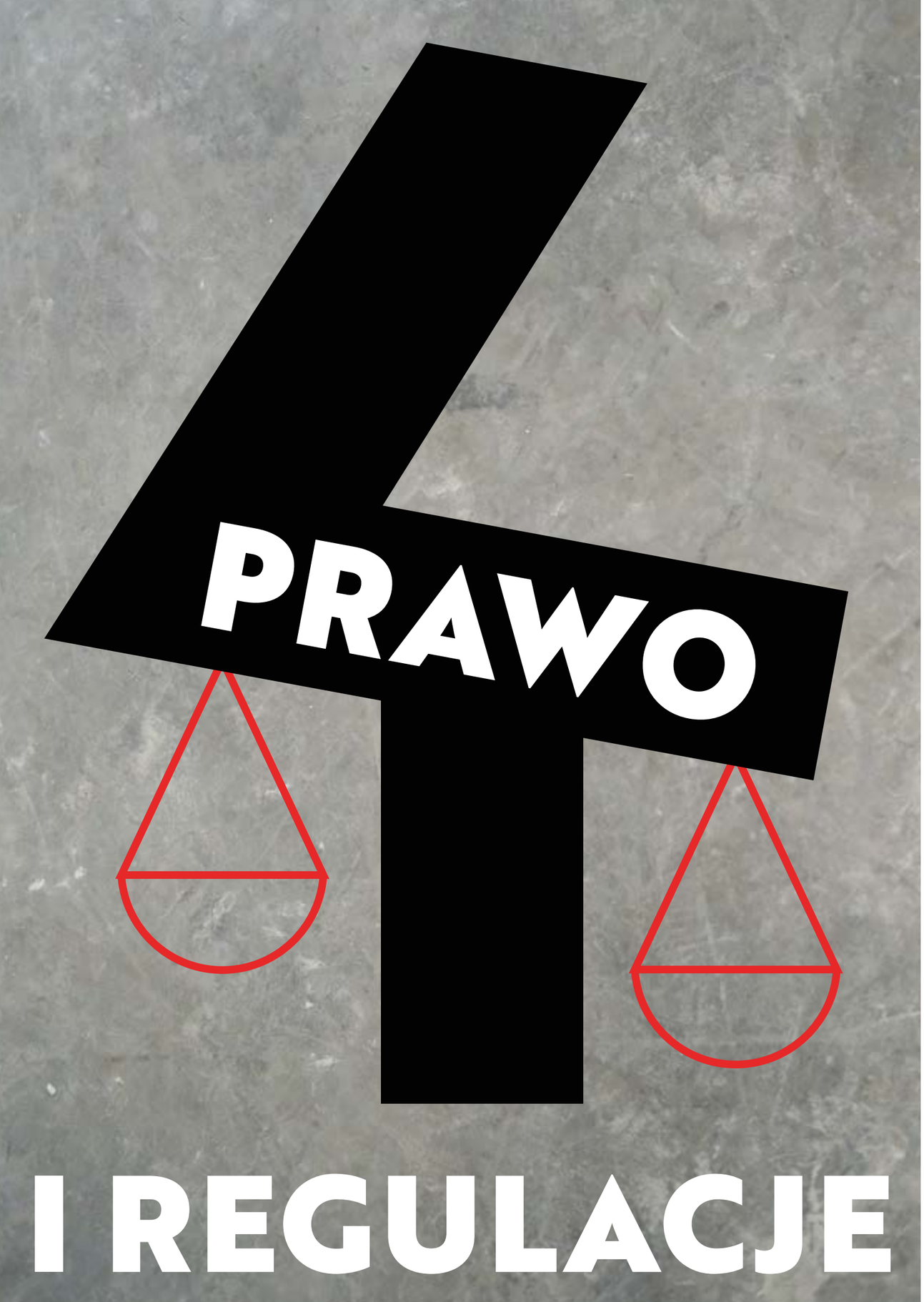
Automa Services i Atende S.A.

- Robotic Process Automation

GFT

GFT Polska

- Faktoring
- Łańcuch dostaw farmaceutycznych



Czy blockchain to tylko modny zwrot, czy też rewolucyjna technologia na miarę nowego Internetu?

Michał Kibil – kancelaria Kibil i Wspólnicy

Niewątpliwie blockchain (łańcuch bloków) to buzzword[13], wykorzystywany powszechnie jako magnes na inwestorów. Pomimo, że większość projektów, w których deklaruje się używanie rozproszonego rejestru nie tylko tego nie wymaga, ale też nierzadko stoi w sprzeczności z istotą blockchaina, konsekwentnie wskazaną technologię próbuje się umieścić w opisach projektów, tylko po to, by zwiększyć zasięg zainteresowania danym pomysłem.

Pomimo powyższego, sama technologia zdaniem większości specjalistów zajmujących się tą tematyką, jest opisywana jako kolejna rewolucja technologiczna, po wynalezieniu e-maila i Internetu.

O rewolucyjnym charakterze blockchaina świadczy w dużej mierze możliwość zastąpienia zaufanej strony trzeciej (takiej jak notariusz, czy urząd) technologią, gwarantującą (przy odpowiednim stopniu rozproszenia rejestru) prawidłowość (zgodność z prawdą) danych wprowadzonych do rejestru poprzez brak możliwości modyfikowania danych raz wprowadzonych, a także, tak długo jak dany blockchain będzie miał użytkowników, kontynuację świadczenia usług świadczonych z jego wykorzystaniem.

Samo rozwiązanie zdecentralizowanych baz danych nie jest innowacyjne. Pierwsze przypadki informacji o transakcjach zapisywanych w identycznych kopiach u wszystkich uczestników handlu miały miejsce już w I w. n.e. To co w blokchainie jest rewolucyjne to algorytm, który poprzez stosowanie stosownych dowodów prawdziwości danych potrafi automatycznie eliminować wpisy, które są niezgodne z kopiami zarejestrowanymi na innych komputerach tworzących łańcuch (tzw. node'ów lub węzłów). Co należy podkreślić, wskazane węzły zapewniają swoim istnieniem spójność systemu oraz ciągłość jego działania.

Wskazany algorytm stworzony przez Satochiego Nakamoto na potrzeby wprowadzenia bitcoina, okazał się na tyle uniwersalny, że w dniu dzisiejszym może być wykorzystywany nie tylko do odnotowywania transakcji kryptowalutowych, ale także do zapisu wszelkiego innego rodzaju danych.

Kod źródłowy pierwszego blockchaina stanowił podstawę tak publicznych (takich jak Ethereum) jak i prywatnych (takich jak Hyperledger) rozproszonych rejestrów. Nowe rejestry uwolniły potencjał zaszyty w tej technologii. Na popularności zyskały w szczególności tzw. inteligentne kontrakty, czyli samowykonywalne umowy rejestrowane w blockchainie, które po ich zakodowaniu eliminują potrzebę występowania czynnika ludzkiego (z chwilą spełnienia warunku zapisanego w kontrakcie, dochodzi do jego automatycznej realizacji), czy też tokeny emitowane przez poszczególnych uczestników systemu, które jak biała kartka papieru, w zależności od tego jak je opiszemy mogą przyjmować charakter instrumentów finansowych (tzw. tokeny security), udziałów (jak ma to miejsce w tzw. DAO, czyli zdecentralizowanych autonomicznych organizacjach), kolejnego środka rozliczeniowego (choć niekoniecznie krytowaluty), czy też mogą odpowiadać jakiemuś uprawnieniu (np. do usługi świadczonej w ramach rozwiązania technologicznego opartego na blockcha-

13 Modny zwrot, którego używanie stało się modne w wyniku jego częstego używania – vide: Collins English Ditionary on-line

inie). Szerzej o charakterystyce tokenów można przeczytać w części raportu przygotowanej przez prof. UO dr hab. Dariusza Szostka z kancelarii Szostek_Bar i Partnerzy pt. *Jaki jest charakter Tokenu?*

Nowe możliwości, jakie przynieśli nam twórcy kolejnych blockchainów, zaowocowały dynamicznym rozrostem projektów z tego obszaru. Jak wskazują raporty, w ciągu ostatnich 10 lat na rynku pojawiło się ponad 80 000 rozwiązań dedykowanych pod blockchain. Jako, że większość z nich potrzebowała finansowania dla developmentu rozwiązania, a środowisko blockchain dysponowało znaczną liczbą kryptowalut akceptowanych przez nie jako środek płatniczy, w świecie blockchaina wykształciła się nieznana dotąd konstrukcja ekonomiczna, jaką jest publiczna emisja tokenów (tzw. ICO tj. Initial Coin Offering). Porównując ICO do tradycyjnych konstrukcji prawnych, można w nim znaleźć cechy crowdfundingu, bądź oferty publicznej (w zależności od charakteru emitowanego tokenu). Jako, że obie instytucje realizowane w tradycyjnym obrocie, zostały prawnie uregulowane (a w przypadku emisji publicznej istnieje także konieczność spełnienia szeregu wymogów takich jak sporządzenie, zatwierdzenie oraz publikacja prospektu emisyjnego), emisje ICO zaczęły być realizowane z dużą ostrożnością, a emitenci zaczęli przywiązywać dużą wagę do weryfikacji, jakie przepisy mogą ich dotyczyć. Szerzej o wyzwania dotyczących emisji ICO pod kątem regulacji finansowych można przeczytać w części raportu przygotowanej przez Tomasza Kalickiego z kancelarii Domański Zakrzewski Palinka pt. Emisja tokenów w Polsce, a wymogi regulacyjne.

Co jest warte odnotowania, obserwując rynek nowych technologii zauważamy coraz większą świadomość prawną nie tylko u osób emitujących tokeny w ramach ICO, ale praktycznie u wszystkich tworzących nowe projekty oparte na blockchainie. Błędnym jest twierdzenie, że świat blockchaina funkcjonuje w próżni prawnej. Są to raczej dwa wzajemnie przenikające się światy, do których należy podejść ze zrozumieniem, jak na siebie wzajemnie wpływają. Nie można ignorować faktu, że w blockchainie coraz częściej pojawiają się autonomiczni aktorzy w postaci smart contrakt'ów[14], którym ciężko przypisać podmiotowość prawną, że ze względów na rozproszenie informacji po poszczególnych węzłach, ciężko zidentyfikować, gdzie faktycznie dochodzi do realizacji usługi opartej na blockchainie oraz że ciężko zidentyfikować suwerena, który mógłby przejąć kontrolę nad tym, co się w tej przestrzeni rozgrywa[15] (w tym ciężko znaleźć sąd, który mógłby rozpoznać ewentualny spór). Nie zwalnia to jednak twórców poszczególnych rozwiązań od gruntownego badania, jakie przepisy mogą wpływać na ich produkty, jakie prawne konstrukcje są możliwe do zastosowania oraz jakie przepisy będą dla nich bezpośrednim zagrożeniem.

Z punktu widzenia rozwiązań tworzonych na blockchainie analizę prawną warto zacząć od obowiązków wynikających z przepisów o świadczeniu usług drogą elektroniczną. Jak wskazuje Jakub Kubalski z kancelarii Domański Zakrzewski Palinka, w części raportu pt. *Czym w ujęciu prawnym jest blockchain?* ich zastosowanie będzie niejako wynikało z samego charakteru blockchaina.

Wdrażając rozwiązania z wykorzystaniem publicznych blockchainów, nierzadko będziemy stawać przed wyzwaniami prawnymi narzucanymi przez tradycyjne regulacje, nieprojektowane z uwzględnieniem tej technologii, takie jak m.in. RODO. Wśród aktualnych wyzwań blockchaina jednym z najistotniejszych jest sposób rozwiązania konfliktu pomiędzy absolutną dostępnością informacji zgromadzonych w rejestrze (tak długo jak będzie funkcjonował chociaż jeden węzeł na którym zapisane są informacje, będzie możliwość zweryfikowania treści wszystkich wpisów, które w danym blockchainie zostały umieszczone) oraz prawa do bycia zapomnianym wynikającym z RODO. Szerzej o niezwykle ciekawym konflikcie jawności wynikającej z istoty blockchaina oraz RODO można przeczytać w artykule dr hab. Jana Byrskiego, Partnera z kancelarii Traple Konarski Podrecki i Wspólnicy pt. *Blockchain a RODO.*

Jako autorzy części prawnej raportu, pozostajemy w przekonaniu, że zainspiruje on Państwa do spoglądania na planowane rozwiązania w obszarze blockchain, systemowo tj. nie tylko w ujęciu biznesowych możliwości technologicznego rozwiązania, ale także z uwzględnieniem jego prawnej złożoności.

Zapraszam do lektury!

14 podobnie mec. Krzysztofa Wojdyło
15 j.w.

Jaki jest charakter tokenu?

prof. UO dr hab. Dariusz Szostek – kancelaria Szostek Bar i Partnerzy

Specyfika tokenów pozwala na ich wykorzystanie zarówno w ramach każdego z rodzajów „inteligentnych kontraktów", ale także poza nimi. Charakter prawny tokenu należy ustalić każdorazowo w oparciu o stosunek prawny, w którym ma być wykorzystany. Wówczas nie tylko bierze się pod uwagę takie czynniki jak prawo właściwe dla umowy, w ramach której token jest wytwarzany i zbywany, lecz również przede wszystkim treść samego kontraktu (z uwzględnieniem obowiązujących przepisów ius cogens i ius dispositivi). Innymi słowy, token jest narzędziem, którego zastosowanie i funkcje są determinowane przez przepisy konkretnej gałęzi prawa (np. przepisy papierów wartościowych).

W ujęciu prawnym token nie jest nowym rewolucyjnym i nieznanym wcześniej instrumentem prawnym. Należałoby raczej traktować go jako nowy nośnik instrumentu prawa. Twierdzenie to opiera się na najnowszych stanowiskach organów nadzoru finansowego. Jako przykład można wskazać raport amerykańskiej Komisji Papierów Wartościowych i Giełd (The Securities and Exchange Commission - SEC) z dnia 25 lipca 2017 r., w którym ostrzega się uczestników rynku, że oferty i sprzedaż aktywów cyfrowych (tokenów) przez „wirtualne" organizacje prowadzone przez przedsiębiorstwa korzystające z technologii DLT (distributed ledger technology) lub technologii bloków, określane m.in. jako ICO (initial coin offering) lub „sprzedaż tokenów", podlegają wymogom federalnego prawa papierów wartościowych. Innymi słowy, tokeny jako narzędzia stają się przedmiotem uwagi krajowych organów nadzoru.

W sprawozdaniu z dochodzenia amerykańskiej SEC z dnia 25 lipca 2017 r.[16] stwierdzono, że tokeny oferowane i sprzedawane przez „wirtualną" organizację zwaną „DAO" są papierami wartościowymi i w związku z tym podlegają federalnemu prawu papierów wartościowych. Raport potwierdza, że emitenci papierów wartościowych rozproszonych lub papierów wartościowych opartych na technologiach blokowych muszą rejestrować oferty i sprzedaż takich papierów, chyba że zastosowanie ma obowiązujące wyłączenie.

W omawianym zakresie interesujące jest stanowisko Singapurskiego Banku Centralnego (Monetary Authority of Singapore – MAS)[17]. Stwierdził on, że tokeny oferowane lub wydawane w Singapurze będą regulowane przez MAS, jeżeli spełniają definicję produktu, określoną w ustawie o papierach wartościowych. W przypadku, kiedy tokeny cyfrowe wchodzą

16 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO
17 MAS clarifies regulatory position on the offer of digital tokens in Singapore

w zakres definicji papierów wartościowych zawartej w Securities and Futures Act (SFA), emitenci takich tokenów mieliby obowiązek złożenia i zarejestrowania prospektu emisyjnego w systemie MAS przed ofertą takich instrumentów finansowych, chyba że zostaliby objęci wyłączeniem. Ponadto platformy ułatwiające obrót wtórny takimi tokenami również musiałyby zostać zatwierdzone lub uznane przez Bank Centralny, odpowiednio jako zatwierdzona giełda lub uznany operator rynku. Należy jednak pamiętać o tym, że rodzaje tokenów cyfrowych oferowanych w Singapurze i w innych krajach znacznie się od siebie różnią.

Na gruncie ogólnoeuropejskim pionierem regulacji związanej z tokenami jest ustawodawstwo białoruskie. Zgodnie z Dekretem Prezydenta Białorusi obowiązującym od 1 stycznia 2018 r., tokeny nie podlegają zgłoszeniu organom państwowym. Operatorzy platform kryptograficznych oraz operatorzy giełd kryptowalut są zobowiązani do zapewnienia dostępności (na rachunkach w bankach Republiki Białorusi) środków pieniężnych w wysokości nie mniejszej niż 1 miliona białoruskich rubli na każdego operatora platformy kryptograficznej i odpowiednio nie mniej niż 200 tysięcy białoruskich rubli na każdego operatora wymiany kryptowalut.

Najnowszą światową regulacją prawną dotyczącą tokenu oraz smart contract'ów jest maltańska ustawa Virtual Financial Assets (VFA) Act[18] z dnia 5 lipca 2018 r. Ustawa ta, w połączeniu z dwiema innymi (Innovative Technology Arrangements and Services Act[19] oraz Malta Digital Innovation Authority Act[20]) reguluje sposób wydawania tokenów, nadzór organów państwowych oraz ochronę uczestników obrotu tokenami. Ze względu jednak na mnogość odmian, token może zostać uznany nie tylko za papier wartościowy, czy instrument finansowy, lecz również za kryptowalutę, bądź znak legitymacyjny.

Jednym z nowych pojęć wprowadzonych w powyżej wymienionych ustawach, a mającym wydatne zastosowanie w związku z technologią blockchain, jest „virtual financial asset" (VFA; wirtualne aktywa finansowe) będące każdą formą zapisu cyfrowego, używanego jako cyfrowy środek wymiany, jednostka rozliczeniowa lub przechowanie wartości, ale niebędąca jednocześnie ani pieniądzem elektronicznym, ani instrumentem finansowym, ani wirtualnym tokenem. Każdy jednak emitent VFA przed dopuszczeniem takich aktywów na rynek maltański, musi przedstawić tzw. „Whitepaper", zbliżoną do prospektu emisyjnego dokumentację, zawierającą szereg informacji o charakterze emitenta oraz technologii DLT i produktu. Ze względu na zapewnienie koniecznego bezpieczeństwa uczestnikom obrotu, wprowadzono także wymóg złożenia wniosku o licencję do odpowiedniego organu państwowego (Malta Financial Services Authority), co więcej jedynie za pośrednictwem odpowiedniego zarejestrowanego podmiotu, zwanego agentem (pośrednikiem) VFA. Od takiego podmiotu wymaga się wykazania, że wnioskodawca jest właściwą osobą do świadczenia danych usług VFA oraz, że będzie spełniał i przestrzegał wymogów przepisów maltańskiego prawa.

Nie jest to jednak jedyny organ administracji publicznej biorący udział w całym procesie licencyjnym. Utworzono bowiem nowy organ - Malta Digital Innovation Authority (MDIA), pełniącego rolę urzędu nadzoru innowacji cyfrowych. Podstawowym zadaniem tego organu jest kontrola kodów źródłowych smart contract'ów, od którego zależy wydanie decyzji o przyznaniu licencji. Podobne badanie kodu źródłowego dotyczy też DAO, pragnących

18 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1, dostęp w dniu 8 listopada 2018 r.
19 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1, dostęp w dniu 8 listopada 2018 r.
20 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1, dostęp w dniu 8 listopada 2018 r.

funkcjonować legalnie na terytorium Malty.

Wspomniana powyżej licencja jest elementem niezbędnym dla prowadzenia działalności związanej z branżą blockchain, bez niej będzie ona bowiem nielegalna.

Z powyżej wspomnianych metod wyraźnie rysuje się konieczność wprowadzenia regulacji na szczeblu krajowym, dotyczącej technologii blockchain także w Polsce. Wydaje się, że pożądanym kierunkiem zmian jest, podobnie jak na Malcie, wprowadzenie państwowego nadzoru oraz odpowiedniej polityki licencyjnej. Można by wykorzystać także zawarte w statucie stanu Vermont[21], konstrukcje domniemań prawnych związanych z zapisem cyfrowym zapisanym w łańcuchu bloków, jeżeli jest powiązany z pisemną deklaracją kwalifikowanego podmiotu uprawnionego do poświadczeń. Co więcej wiąże się z tym także domniemanie autentyczności takiego faktu lub zapisu, jeżeli korzysta on z prawidłowo zastosowanej technologii blockchain.

Nie ma wątpliwości, że powyżej przedstawione uregulowania czynią wskazane państwa pionierami w zakresie branży blockchain. W dużej mierze są to gotowe i sprawdzone rozwiązania, które znalazłyby zastosowanie także w Polsce. W niektórych wypadkach takie regulacje (instytucje) prawne już nawet są stosowane, lecz w wypadku odmiennych sektorów, takich jak chociażby usługi zaufania, konieczne jest ich wdrożenie.

Emisja tokenów w Polsce, a wymogi regulacyjne

Tomasz Kalicki – kancelaria Domański Zakrzewski Palinka

W polskim porządku prawnym nie ma odrębnej regulacji dla wydawania tokenów w ramach ICO. Z perspektywy ww. zaproponowanego dychotomicznego podziału tokenów na tzw. (i) tokeny utility oraz (ii) tokeny security[22], wydaje się, że rozważeniu powinna podlegać przede wszystkim kwestia sprawowania nadzoru przez Komisję Nadzoru Finansowego (KNF) pod kątem kwalifikacji ICO jako oferty publicznej w rozumieniu ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych („ustawa o ofercie"). Ofertą publiczną w rozumieniu ustawy o ofercie, jest udostępnienie, co najmniej 150 osobom na terytorium jednego państwa członkowskiego lub nieoznaczonemu adresatowi w dowolnej formie i w dowolny sposób, informacji o papierach wartościowych i warunkach ich nabycia stanowiących wystarczającą podstawę do podjęcia decyzji o nabyciu tych papierów wartościowych. Oferta publiczna, co do zasady, wiąże się z obowiązkiem wydawcy do udostępnienia do publicznej wiadomości prospektu emisyjnego, zatwierdzonego przez KNF i sporządzonego zgodnie z wymogami prawa[23].

W przypadku tokenów należy w pierwszej kolejności ustalić, czy kwalifikują się one jako instrumenty finansowe w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi („ustawa o obrocie"), a co za tym idzie czy będą miały charakter tokenów security. Tylko takie tokeny, co do zasady, będą bowiem podlegały regulacjom dotyczącym obrotu instrumentami finansowymi. W następnym kroku należy ustalić czy dane tokeny security można zakwalifikować jako papiery wartościowe czy też raczej jako

20 2016 Vermont Statutes Title 12 - Court Procedure Chapter 81 - Conduct Of Trial Subchapter 1: GENERALLY §1913 Blockchain enabling
22 Występują też inne podziały tokenów, jednakże w niniejszym opracowaniu bazujemy na podziale dychotomicznym, odpowiednim w naszej ocenie dla opisu zagadnienia z perspektywy regulacji dotyczących nadzoru nad przeprowadzaniem oferty publicznej.
23 Zgodnie z ustawą o ofercie brak zatwierdzenia prospektu emisyjnego, brak zatwierdzenia memorandum informa-

instrumenty pochodne.

W rozumieniu ustawy o ofercie[24] instrumentami finansowymi są papiery wartościowe czyli:

- akcje, prawa poboru w rozumieniu ustawy z dnia 15 września 2000 r. - Kodeks spółek handlowych („ksh"), prawa do akcji, warranty subskrypcyjne, kwity depozytowe, obligacje, listy zastawne, certyfikaty inwestycyjne i inne zbywalne papiery wartościowe, w tym inkorporujące prawa majątkowe odpowiadające prawom wynikającym z akcji lub z zaciągnięcia długu, wyemitowane na podstawie właściwych przepisów prawa polskiego lub obcego,
- inne zbywalne prawa majątkowe, które powstają w wyniku emisji, inkorporujące uprawnienie do nabycia lub objęcia papierów wartościowych określonych w lit. a) powyżej, lub wykonywane poprzez dokonanie rozliczenia pieniężnego, odnoszące się do papierów wartościowych określonych w lit. a) powyżej, walut, stóp procentowych, stóp zwrotu, towarów oraz innych wskaźników lub mierników (prawa pochodne).

Ponadto do kategorii instrumentów finansowych zalicza się[25] niebędące papierami wartościowymi:

- tytuły uczestnictwa w instytucjach wspólnego inwestowania,
- instrumenty rynku pieniężnego,
- opcje, kontrakty terminowe, swapy, umowy forward na stopę procentową, inne instrumenty pochodne, których instrumentem bazowym jest papier wartościowy, waluta, stopa procentowa, wskaźnik rentowności, uprawnienie do emisji lub inny instrument pochodny, indeks finansowy lub wskaźnik finansowy, które są wykonywane przez dostawę lub rozliczenie pieniężne, z wyłączeniem instrumentów pochodnych, o których mowa w art. 10 rozporządzenia 2017/565,
- opcje, kontrakty terminowe, swapy, umowy forward na stopę procentową oraz inne instrumenty pochodne, których instrumentem bazowym jest towar i które są wykonywane przez rozliczenie pieniężne lub mogą być wykonane przez rozliczenie pieniężne według wyboru jednej ze stron,
- opcje, kontrakty terminowe, swapy oraz inne instrumenty pochodne, których instrumentem bazowym jest towar i które mogą być wykonane przez dostawę, pod warunkiem że są dopuszczone do obrotu w systemie obrotu instrumentami finansowymi, z wyłączeniem produktów energetycznych będących przedmiotem obrotu hurtowego na OTF, które muszą być wykonywane przez dostawę,
- niedopuszczone do obrotu w systemie obrotu instrumentami finansowymi opcje, kontrakty terminowe, swapy, umowy forward oraz inne instrumenty pochodne, których instrumentem bazowym jest towar i które mogą być wykonane przez dostawę, a które nie są przeznaczone do celów handlowych i wykazują właściwości innych pochodnych instrumentów finansowych,
- instrumenty pochodne dotyczące przenoszenia ryzyka kredytowego,
- kontrakty na różnicę,
- opcje, kontrakty terminowe, swapy, umowy forward dotyczące stóp procentowych oraz inne instrumenty pochodne odnoszące się do zmian klimatycznych, stawek frachtowych oraz stawek inflacji lub innych oficjalnych danych statystycznych, które są wykonywane przez rozliczenie pieniężne albo mogą być wykonane przez rozliczenie pieniężne według wyboru jednej ze stron, a także instrumenty pochodne, o których mowa w art. 8 rozporządzenia 2017/565, i inne, które wykazują właściwości innych pochodnych instrumentów finansowych,
- uprawnienia do emisji.

Mając na uwadze powyższe można wyróżnić zasadniczo dwie sytuacje:

1. zakres uprawnień związanych z tokenami security odpowiada ww. kategorii instrumentów finansowych niebędących papierami wartościowymi (np. odzwierciedla tylko część uprawnień wynikających z papieru wartościowego lub uzależnia swoją wartość od wartości papieru wartościowego) – w takiej sytuacji emisja tokenów security, jako instrumentów pochodnych nie będących papierami wartościowymi, nie podlega uregulowaniom wynikającym z obowiązku prospektowego (także w przypadku publikuji informacji na temat możliwości nabycia tokenu security na stronie internetowej, gdyż emitent kieruje w ten sposób ofertę do nieograniczonego grona odbiorców). Nie wyklucza to jednak konieczności dochowania obowiązków związanych z oferowaniem lub obrotem instrumentami finansowymi wskazanych w ustawie o obrocie;
2. zakres uprawnień związanych z tokenami security odpowiada wprost papierom wartościowym, będąc w gruncie rzeczy cyfrową formą zapisu tych papierów wartościowych[26] lub odpowiada części uprawnień z papieru wartościowego podlegającym regulacjom ustawy o ofercie – w takiej sytuacji emisja tokenów security podlega, co do zasady, uregulowaniom wynikającym z obowiązku prospektowego. KNF nie sprawuje nadzoru nad tworzeniem[27] tokenów security niebędących papierami wartościowymi, a kwalifikującymi się jako instrumenty pochodne[28].

Ze względu na skalę części ICO na uwagę zasługuje możliwość skorzystania z wyjątku określonego wart. 7 ust 8a ustawy o ofercie, tj. braku obowiązku udostępnienia do publicznej wiadomości prospektu emisyjnego, pod warunkiem udostępnienie dokumentu zawierającego co najmniej podstawowe informacje o emitencie papieru wartościowego, warunkach i zasadach oferty, ze wskazaniem oferowanych papierów wartościowych, celach emisji, na które mają być przeznaczone środki uzyskane z emisji papieru wartościowego, istotnych czynnikach ryzyka oraz oświadczenie emitenta o odpowiedzialności za informacje zawarte w tym dokumencie, w przypadku oferty publicznej, w wyniku której zakładane wpływy brutto emitenta lub sprzedającego na terytorium UE, liczone według ich ceny emisyjnej lub ceny sprzedaży z dnia jej ustalenia, stanowią nie mniej niż 100 tys. EUR i mniej niż 1 mln EUR i wraz z wpływami, które emitent lub sprzedający zamierzał uzyskać z tytułu takich ofert publicznych takich papierów wartościowych, dokonanych w okresie poprzednich 12 miesięcy, nie będą mniejsze niż 100 tys. EUR i będą mniejsze niż 1 mln EUR. Zwolnienie z obowiązku prospektowego nie wyklucza konieczności wypełnienia przez podmiot wydający tokeny security innych obowiązków wynikających m.in.

cyjnego i zaniedbanie innych obowiązków związanych z publicznym oferowaniem papierów wartościowych zagrożone są karą grzywny do 10 mln PLN albo karze pozbawienia wolności do lat 2, albo obu tym karom łącznie. Dodatkowo, w myśl Kodeksu karnego, kto w dokumentacji związanej z obrotem papierami wartościowymi, rozpowszechnia nieprawdziwe informacje lub przemilcza informacje o stanie majątkowym oferenta, mające istotne znaczenie dla nabycia, zbycia papierów wartościowych, podwyższenia albo obniżenia wkładu, podlega karze pozbawienia wolności do lat 3.

24 Artykuł 2 ust. 1 pkt 1) w zw. z art. 3 ust. 1 pkt a) i b) ustawy o obrocie.

25 Artykuł 2 ust. 1 pkt 2) ustawy o obrocie.

26 Poza zakresem niniejszego zwięzłego opracowania pozostaje złożona kwestia formy wymaganej dla niektórych rodzajów papierów wartościowych oraz kwestie tzw. dematerializacji papierów wartościowych.

27 Nie wyklucza to konieczności spełnienia obowiązków wynikających z innych przepisów, w szczególności wskazanych na końcu niniejszej części.

28 Przez instrumenty pochodne rozumie się prawa majątkowe, które są powiązane z papierami wartościowymi lub których cena rynkowa zależy bezpośrednio lub pośrednio od ceny lub wartości papierów wartościowych, o których mowa w art. 3 pkt 1 lit. a) ustawy o obrocie, oraz inne prawa majątkowe, których cena rynkowa bezpośrednio lub pośrednio zależy od kształtowania się ceny rynkowej walut obcych lub od zmiany wysokości stóp procentowych.

z ustawy o ofercie, np. obowiązków informacyjnych.

Powyższe stanowi ogólne podsumowanie związane z nadzorem KNF nad ICO, które mogą stanowić ofertę publiczną. Poza zakres niniejszego opracowania wykraczają takie kwestie jak m.in.: zasady działania platform crowdfundingowych, dopuszczanie instrumentów finansowych do obrotu zorganizowanego, obowiązek posiadania licencji na działalność firmy inwestycyjnej w zakresie oferowania instrumentów finansowych oraz przyjmowania i przekazywania zleceń, zezwolenie na organizację obrotu na instrumentach finansowych w sposób spełniający przesłanki uznania za system obrotu, o którym mowa w ustawie o obrocie, obowiązki wynikające z Markets in Financial Instruments Directive (MiFID II) oraz Alternative Investment Fund Managers Directive (AIFMD), regulacje dotyczące przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, ryzyko obejścia zakazu określonego w art. 171 ust. 1 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe czy też spełnienie obowiązków wynikających z powszechnie obowiązujących przepisów prawa. Wyżej wskazane regulacje także powinny być brane pod uwagę przez podmioty przeprowadzające i uczestniczące w ICO[29].

Czym w ujęciu prawnym jest blockchain?

Jakub Kubalski – kancelaria Domański Zakrzewski Palinka

Blockchain jako umowa ramowa

Pod koniec czerwca 1948 roku rozpoczęła się blokada wwozu towarów do Berlina Zachodniego. W ślad za tymi wydarzeniami, państwa zachodnie rozpoczęły jedną z największych operacji przerzutu towarów w nowożytnej historii. Operacja ta wymagała ustandaryzowania formatu wymiany danych o zamówieniach na wielką skalę[30].

Stanowiło to podwalinę do opracowania w latach 70-tych ubiegłego stulecia rozmaitych standardów tzw. EDI (Electronic Data Interchange), czyli systemów wymiany informacji o możliwościach dostawców i potrzebach zamawiających – w ramach łańcucha dostaw. Co istotne, wymiana tych informacji odbywała się bez udziału człowieka. Udział ludzkiego operatora był wymagany na wstępie – przy określaniu warunków brzegowych zamówienia.

Systemy EDI funkcjonują nadal i co bardziej istotne – nie są one kontrowersyjne z punktu widzenia prawa cywilnego. W standardowym systemie EDI, strony umowy – użytkownicy systemu EDI składają odpowiednio oświadczenia, że zgadzają się na konkretne warunki brzegowe umowy poprzez określenie zakresu cen, wolumenu towarów itp. Kolejno, punkty styku systemu EDI mają „dowolność" w składaniu zamówień, ofert[31] i ich realizacji. Rozwiązanie to jest analogiczne do umów ramowych i zawieranych na ich podstawie zamówieniach.

Blockchain w najbardziej ogólnym rozumieniu[32] może funkcjonować jak wcześniej opisane systemy EDI – użytkownicy systemu określają warunki brzegowe transakcji zapisywanych w blokach, zaś oprogramowanie klienckie składa odpowiednie zamówienia, oferty. Przykładem takiego systemu mogą być platformy handlowe służące do sprzedaży energii elektrycznej wytwarzanej w gospodarstwach domowych.

Blockchain jako usługa świadczona drogą elektroniczną

Dostęp do systemów EDI uzyskuje się od skonkretyzowanego podmiotu – z reguły strony umowy ramowej bądź od zewnętrznego dostawcy. Użytkownicy w tym zakresie zawierają umowę o świadczenie usług[33] z dostawcą rozwiązania EDI. Przedmiotem tej umowy jest świadczenie usługi umożliwiającej dostęp do systemu i składanie zamówień, ofert.

Blockchain jest co do zasady zdecentralizowanym sposobem gromadzenia informacji o transakcjach w blokach i łańcuchu bloku. Jest to swoista baza danych. Natomiast dostęp do tej bazy danych jest wszakże pewnego rodzaju świadczeniem - usługą świadczoną drogą elektroniczną. I w tym względzie zasady dostępu do łańcucha bloków, rejestrowania transakcji mogą być ujęte w regulaminie świadczenia usług drogą elektroniczną.

Podstawowym jednak pytaniem w tym względzie jest: kto ma być usługodawcą w ramach systemu blockchain? Istnieje możliwość argumentacji, że taka umowa powinna być zawierana z dostawcą rozwiązania informatycznego zapewniającego dostęp do łańcucha bloków. Z drugiej jednak strony system dostępu do blockchain jest oparty o zasady sieci peer-to-peer, co z kolei może powodować wątpliwości, czy taka umowa nie powinna być zawarta z poszczególnymi użytkownikami systemu.

Co więcej, usługa ta może mieć za przedmiot przetwarzanie danych w chmurze. W tym względzie, zastosowanie znajdzie m.in. ustawa o krajowym systemie cyberbezpieczeństwa oraz Ogólne Rozporządzenie o Ochronie Danych Osobowych (tzw. RODO). Reżimy te nakładają rozmaite obowiązki na podmioty świadczące usług przetwarzania w chmurze. Z tego powodu, należałoby zbadać konkretne przypadki systemów opartych na blockchain – pod względem świadczenia usług drogą elektroniczną.

Oprogramowanie Open source w systemach opartych o blockchain

Każde rozwiązanie IT, w tym systemy oparte o blockchain, może być oparte o oprogramowanie open source. Ważne jest jednak, aby znać konsekwencje takiego rozwiązania – a te są opisane w warunkach licencyjnych oprogramowania open source.

Niejednokrotnie, wzorce licencji open source, w tym jeden z bardziej popularnych - GNU/GPL, nakładają na licencjobiorcę pewne obowiązki. Najbardziej istotnym z nich jest obowiązek udostępniania programu w wersji zmienionej, czy oryginalnej na takich samych zasadach, na jakich uzyskano prawo do korzystania z oprogramowania.

Nie chodzi tu jednak o zobowiązanie do rozpowszechniania oprogramowania, lecz o narzucenie warunków tej samej licencji, gdy pierwotny licencjobiorca zdecyduje się na rozpowszechnianie oryginalnego lub zmienionego oprogramowania. Przy rozpowszechnianiu oprogramowania należy ponadto dołączać kod źródłowy, z należycie opisanymi zmianami, które pierwotny licencjobiorca dokonał (wskazanie na zmianę oraz datę). Do każdego egzemplarza takiego oprogramowania powinno się dołączać treść licencji, z której licencjobiorca korzystał.

Przy opracowaniu założeń systemu opartego na łańcuchu bloków z wykorzystaniem oprogramowania open source warto rozważyć powyższe konsekwencje płynące z warunków licencji open source i ewentualnie wdrożyć środki zapobiegające niepożądanym skutkom. Takim środkiem może być rozdział kodu – tak aby była pewność która część systemu jest objęta warunkami licencji open source, a która ma być przedmiotem warunków licencyj-

29 Niniejsze opracowanie odnosi się do obecnego stanu prawnego i nie bierze pod uwagę planowanych zmian w prawie, po których wejściu w życie część konkluzji wymagać będzie aktualizacji.

30 Wymiana danych, co ciekawe odbywała się drogą elektroniczną – za pośrednictwem prymitywnych modemów.

31 Kodeks cywilny określa minimalne treściowe warunki oferty przedsiębiorcy – art. 661 §2 Kodeksu cywilnego.

32 Nie uwzględniając kryptowalut jako przedmiotów świadczeń w stosunkach cywilnoprawnych. W tym przedmiocie mogą mieć zastosowanie dodatkowe względy – zob. zwłaszcza: M. Michna *Bitcoin jako przedmiot stosunków cywilnoprawnych*, Warszawa 2018

33 Wymogi prawne co do treści regulaminu usługi świadczonej droga elektroniczną określone są w art. 8 ustawy oświadczeniu usług drogą elektroniczną.

nych określonych dowolnie przez podmiot uprawniony do autorskich praw majątkowych.

Blockchain a RODO

Dr hab. Jan Byrski – kancelaria Traple Konarski Podrecki i Wspólnicy
Karol Juraszczyk – kancelaria Traple Konarski Podrecki i Wspólnicy

Zyskująca na popularności technologia rejestrów rozproszonych (z ang. distributed ledger technology, DLT) opartych o łańcuch bloków (blockchain) rodzi szereg pytań i wątpliwości. Dotyczą one m.in. zapewnienia, aby rozwiązania czy projekty oparte o tę technologię były zgodne z wymogami wynikającymi z Ogólnego Rozporządzenia o Ochronie Danych (RODO), które ma zastosowanie od 25 maja 2018 r. Trzeba przy tym podkreślić, że technologia rejestrów rozproszonych może być wykorzystywana w wielu różnych konfiguracjach i – jak to zwykle bywa – specyfika danego przypadku oraz szczegóły rozwiązania decydować będą niejednokrotnie o jego kwalifikacji prawnej.

Poniżej wskazano na wybrane problematyczne zagadnienia, które mogą pojawić się w każdym nowym projekcie opartym o blockchain.

Na wstępie należy ustalić, czy w ramach danego rejestru będą przetwarzane dane osobowe, a więc informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Aby ocenić, czy osoba fizyczna może być bezpośrednio lub pośrednio zidentyfikowana należy wziąć pod uwagę wszelkie racjonalne i prawdopodobne sposoby, które mogą zostać użyte przez administratora danych lub inną osobę w celu zidentyfikowania osoby fizycznej (w przypadku systemów blockchain np. poprzez połączenie publicznego klucza użytkownika z jego adresem IP[34]). Jakkolwiek w ramach systemów opartych o blockchain, dane użytkowników np. dokonujących transakcji mogą być przetwarzane w postaci zaszyfrowanej, to na gruncie RODO takie dane (jako lub dane spseudonimizowane zgodnie z art. 4 pkt 5 RODO, lub zaszyfrowane) również należy traktować jako dane osobowe. W związku z szeroką definicją danych osobowych w wielu rejestrach opartych o blockchain, przewidziane w RODO zasady ochrony prywatności będą miały zatem zastosowanie.

Kolejnym krokiem, w przypadku stwierdzenia, że w ramach systemu blockchain będą przetwarzane dane osobowe, powinno być ustalenie statusów poszczególnych podmiotów występujących w tym systemie. Na gruncie RODO należy określić kto jest administratorem danych (podmiotem, który ustala cele i sposoby przetwarzania danych osobowych), a kto podmiotem przetwarzającym, czyli tzw. procesorem (podmiotem, który przetwarza dane osobowe w imieniu administratora). W niektórych sytuacjach może również dochodzić do sytuacji współadministrowania danymi osobowymi przez dwóch lub więcej administratorów (art. 26 RODO). Na zasadzie pewnej analogii, system oparty na blockchain można porównać do usługi chmury obliczeniowej, w ramach której korzystający z usługi (użytkownicy), decydujący o umieszczeniu w niej danych osobowych, są administratorami danych, a dostawca usługi przetwarzania danych w chmurze obliczeniowej jest procesorem[35]. Zasadnicza różnica polega jednak na tym, że systemy oparte o blockchain z reguły nie posiadają podmiotu centralnie administrującego systemem, a sami użytkownicy również mogą uczestniczyć w jego administrowaniu w charakterze węzłów (ang. nodes; podmiot, który przechowuje lokalnie kopię rejestru) lub „górników" (ang. miners; podmiot, który tworzy nowe bloki i proponuje ich dodanie do łańcucha). Może więc dochodzić do sytuacji, gdy ten sam podmiot (użytkownik), w systemie opartym o blockchain, występować będzie zarówno w roli administratora danych jak i procesora.

Na administratorze danych spoczywa szereg obowiązków wynikających z RODO. W kontekście przetwarzania danych osobowych w rejestrach rozproszonych opartych o blockchain zwraca się szczególną uwagę na problem związany z realizacją prawa do sprostowania danych lub usunięcia danych (prawa do bycia zapomnianym – art. 17 RODO). W istocie rzeczy technologia blockchain ma uniemożliwiać zmiany w zapisach historycznych w rejestrze, w celu zapewnienia odpowiedniego stopnia zaufania użytkowników do danych w nim zawartych. O ile w ramach rejestrów prywatnych[36] (gdzie blockchain może pobierać i udostępniać jedynie zamknięta grupa podmiotów), zmiana lub usunięcie danych z rejestru wydają się możliwe do realizacji (na zasadzie uzgodnień między wszystkimi uczestnikami systemu), to w przypadku rejestrów publicznych, zadośćuczynienie powyższym wymogom może być w praktyce trudne lub niewykonalne. Nie oznacza to jednak, że nie jest możliwe zapewnienie zgodności rozwiązań opartych o blockchain z wymogami RODO. Jednym z proponowanych rozwiązań w tym zakresie jest przechowywanie danych stanowiących dane osobowe poza systemem blockchain, a w jego ramach wyłącznie odnośników (linków) do tych danych. Usunięcie danych osobowych poza systemem (nawet przy zachowaniu odnośników do tych danych w ramach systemu blockchain), mogłoby być uznane za wystarczające dla wykonania żądania usunięcia danych, o ile zajdą to tego przesłanki[37]. Innym dyskutowanym rozwiązaniem jest trwałe usuwanie klucza prywatnego, umożliwiającego odszyfrowanie danych przechowywanych w ramach systemu blockchain w formie zaszyfrowanej[38].

34 Zob. Wyrok TSUE w sprawie C 582/14 Patrick Breyer przeciwko Republice Federalnej Niemiec.
35 Zob. Grupa Robocza Art. 29 w Opinii z dn. 1 czerwca 2012 r. w sprawie przetwarzania danych w chmurze obliczeniowej (WP 196)
36 Zob. K. Piech (red.), *Leksykon pojęć na temat technologii blockchain i kryptowalut*
37 J. Bacon, J. David Michels, Ch. Millard, J. Singh, Blockchain Demistified, Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017
38 Ibidem.

LEK·SY·KON

rzeczownik

– uporządkowany zbiór objaśnionych wyrazów i terminów jednego języka, dotyczących określonej dziedziny

A

Adres

Adresy używane są do wysyłania i przyjmowania transakcji w sieci blockchain. Adres działa w sposób analogiczny do numeru konta bankowego i może być udostępniany publicznie. Adresy kryptowalutowe są najczęściej ciągiem znaków alfanumerycznych (np. 1BvBMSEYstWetTFn5Au4m4GFg7xJaNVN2) i mogą być przedstawiane jako skanowalne kody QR.

AML

AML (ang. anti money laundering) to zestaw procedur, regulacji oraz działań ukierunkowanych na przeciwdziałanie praniu brudnych pieniędzy. Główny ciężar wykonywania tych obowiązków spoczywa na instytucjach prywatnych (w szczególności rynku finansowego), które są zobowiązane do wprowadzenia restrykcyjnych procesów weryfikacji źródła pochodzenia środków finansowych oraz śledzenia transakcji.

Architektura sieci

Architektura sieci określa sposoby realizacji przekazu informacji pomiędzy urządzeniami końcowymi. Są trzy podstawowe typy sieci komputerowych: scentralizowana, zdecentralizowana i rozproszona. W zależności od rodzaju sieci, komputery podłączone są w odmienny sposób, który warunkuje możliwości ich wzajemnej komunikacji oraz bezpieczeństwo całej sieci.

Architekturę sieci komputerowej można porównać do instalacji elektrycznej, do której podłączone są urządzenia elektryczne. Każda taka instalacja ma inny sposób działania, w zależności od sposobu połączenia poszczególnych urządzeń pośrednich oraz końcowych.

Atak 51%

Atak na sieć, polegający na przejęciu przez atakującego kontroli nad ustalaniem konsensusu sieci (np. poprzez przejęcie ponad połowy całkowitej mocy obliczeniowej komputerów podłączonych do danej sieci) w celu wytworzenia osobnego łańcucha bloków i zmiany oryginalnych zapisów w utworzonych blokach danych. W przypadku sieci Bitcoin taki atak mógłby spowodować m.in. możliwość podwójnego wydawania tych samych jednostek waluty wirtualnej przez atakującego, zatrzymanie transakcji lub wydobywania bloków.

B

Blok

Pojedynczy element łańcucha danych, składający się z nagłówka (łączącego ten blok z poprzednimi) i właściwych danych, które są w nim zapisywane. Nagłówek składa się ze skrótu, znacznika czasu oraz tzw. korzenia drzewa hash'y (ang. merkle tree root) umożliwiającego weryfikację rodzaju przechowywanych danych. Dzięki temu, że każdy kolejny blok odwołuje się do poprzednich, zmiana jednego bloku w łańcuchu wymagałaby modyfikacji we wszystkich kolejnych blokach, co praktycznie uniemożliwia zmiany w informacjach zapisach w starszych blokach danych. Bloki danych można porównać do dokumentów połączonych w spójny rejestr, w którym każdy kolejny dokument zawiera informacje

o treści poprzednich dokumentów, przez co nieuprawniona zmiana w jednym dokumencie może być wyłapana w dokumentach wydanych później.

Block Explorer

Block explorer, inaczej eksplorator bloków to narzędzie umożliwiające przejrzenie wydobytych bloków oraz listy transakcji, które się w nich znajdują. Eksplorator można porównać do wyszukiwarki, która po wpisaniu odpowiedniego adresu przeszukuje cały łańcuch bloków w poszukiwaniu właściwych informacji.

Blockchain

Blockchain to rozproszona baza danych, która zawiera stale rosnącą ilość informacji (rekordów) pogrupowanych w bloki i powiązanych ze sobą w taki sposób, że każdy następny blok zawiera oznaczenie czasu (timestamp), kiedy został stworzony oraz link do poprzedniego bloku, będący zaszyfrowanym „streszczeniem" (hash) jego zawartości.

Blockchain prywatny

Typ blockchaina, który może pobierać i udostępniać jedynie wybrana grupa podmiotów. Prywatny blockchain wykorzystywany jest, gdy sieć biznesowa zawiera poufne dane lub gdy regulacje prawne nie pozwalają poszczególnym członkom na korzystanie z blockchaina publicznego.

Blockchain publiczny

Typ blockchaina, który umożliwia pobranie dowolnego fragmentu lub całości bazy danych oraz udostępnianie kopii innym węzłom (NOD'om). Najczęściej wykorzystywany w systemach kryptowalutowych.

D

Darknet

Darknet to część Internetu, której nie można przeglądać przy użyciu popularnych wyszukiwarek. Jest to sieć tworzona i rozwijana autonomicznie przez społeczność internautów, którzy podłączają do sieci serwery pośredniczące. Idea działania darknetu jest zbliżona do funkcjonowania sieci Bitcoin, ponieważ nie ma żadnego scentralizowanego podmiotu, który zarządzałby tego typu siecią.

Distributed Ledger Technology

Technologia rozproszonego rejestru (ang. Distributed Ledger Technology, DLT) to technologia rozproszonej bazy danych, której rejestry są replikowane, współdzielone i zsynchronizowane w ramach konsensusu różnych osób, firm czy instytucji. W przeciwieństwie do technologii blockchain, dane w ramach DLT utrzymywane są w formie ciągłej bez podziału na bloki. W związku z tym konsensus może być osiągnięty przez ograniczoną liczbę użytkowników. DLT jest wykorzystywana najczęściej w sieciach prywatnych, w ramach których nie ma potrzeby angażowania dużej liczby rozproszonych jednostek potwierdzających.

Dowód wykonania pracy

Dowód wykonania pracy (ang. Proof of Work) to mechanizm osiągania konsensusu w sieciach zdecentralizowanych. Dowód wykonania pracy wymaga od węzła zatwierdzającego blok transakcji znalezienie rozwiązania równania, którego wynik musi mieć wartość niższą niż aktualna wartość trudności. Im większa jest moc obliczeniowa węzłów zatwierdzających, tym wyższa jest trudność równania. W związku z tym, rozwój oraz wzrost bezpieczeństwa sieci wymaga zwiększenia mocy obliczeniowej komputerów do niej podłączonych. Dowód wykonania pracy jest podstawowym mechanizmem wykorzystywanym m.in. w sieci Bitcoin.

E

Enterprise Ethereum Alliance (EEA)

Enterprise Ethereum Alliance (EEA) to organizacja mają na celu łączenie ekspertów w zakresie platformy Ethereum z największymi firmami świata, start-upami, uczelniami wyższymi oraz dostawcami technologii. Podstawowym celem organizacji jest stworzenie standardu dla korporacyjnych łańcuchów danych opartych na Ethereum. EEA wspiera również popularyzację technologii blockchain poprzez organizację spotkań, warsztatów i wydarzeń edukacyjnych.

G

Giełda Kryptowalut

Giełda kryptowalut to platforma, umożliwiająca wymianę jednostek pieniądza fiducjarnego (np. euro, dolar amerykański) na jednostki kryptowaluty lub wymianę różnych rodzajów kryptowalut. Działają podobnie jak giełdy lub kantory, ponieważ umożliwiają nie ufającym sobie osobom na dokonywanie transakcji wymiany kryptowalut.

H

Hash

Hash (pol. skrót) to krótki ciąg znaków przyporządkowany do dowolnie dużego zbioru danych za pomocą funkcji mieszającej (haszującej). Główną przewagą skrótów jest wygoda stosowania, ponieważ zamiast dużych ilości danych, można użyć stosunkowo krótkiego ciągu znaków. Hash można porównać do losowego kodu, który jest przyporządkowany do danej informacji i przechowywany oddzielnie w celu ukrycia treści informacji przed osobami niepowołanymi.

Funkcja skrótu

Funkcja skrótu, znana również jako funkcja haszująca lub funkcja mieszająca, przyporządkowuje dowolnie dużej liczbie krótszą wartość. Wartość skrótu ma zawsze stały rozmiar (liczbę znaków). Dzięki temu, że wartość jest dobierana losowo, nie da się odczytać informacji zapisanej w taki sposób za pomocą samego hash'u. Najpopularniejszym wykorzystaniem funkcji skrótu poza zastosowaniami technologii blockchain jest podpis elektroniczny.

Szybkość hashowania

Szybkość hashowania (ang. hash rate) to liczba hash'y, która może zostać obliczona

w określonym czasie (najczęściej sekundy). Miara ta określa efektywność i zyskowność wydobywania kolejnych bloków.

Hyperledger

Hyperledger to projekt typu open source, zainicjowany i zarządzany przez Linux Foundation, którego celem jest wspólne rozwijanie rozwiązań opartych na technologii rozproszonych rejestrów. Projekt funkcjonuje na zasadzie zrzeszenia (federacji) współpracujących ze sobą organizacji i firm komercyjnych.

I

ICO

Metoda pozyskiwania kapitału poprzez sprzedaż określonego zasobu tokenów cyfrowych, dające ich posiadaczom prawo majątkowe (tokeny udziałowe albo w formie instrumentów finansowych) lub wiążące się z obietnicą, że tokeny te będą wykorzystywane jako narzędzie dające dostęp do usług oferowanych przez daną platformę (tokeny użytkowe). ICO w swojej formule podobne jest to pierwszej oferty publicznej (ang. Initial Public Offering – IPO), wiąże się jednak ze zdecydowanie mniejszymi wymogami regulacyjnymi w większości krajów świata.

Hard Cap

Hard cap w przypadku zbiórek ICO to maksymalny pułap środków finansowych, jaki oczekują zebrać organizatorzy danej zbiórki. W momencie, kiedy wartość zebranych środków osiągnie hard cap, zbiórka zostaje zakończona.

Soft Cap

Soft cap w przypadku zbiórek ICO to minimalny pułap środków finansowych, którego osiągnięcie powoduje wykonalność zbiórki. Oznacza to, że zbiórka musi osiągnąć ten poziom, aby organizatorzy otrzymali jakiekolwiek środki. W przypadku, gdy w z góry określonym czasie, dana zbiórka nie osiągnie poziomu minimalnego, przesłane przez uczestników zbiórki środki trafiają z powrotem na ich konto.

Pre-sale

Faza procesu ICO, podczas której podmiot pozyskujący środki oferuje ograniczoną pulę tokenów cyfrowych, sprzedawanych na specjalnych warunkach, najczęściej korzystniejszych niż w fazie zasadniczej zbiórki. Głównym celem przedsprzedaży jest zbadanie popytu potencjalnych inwestorów na oferowane tokeny oraz ustalenie ostatecznej ceny, po jakiej będą one sprzedawane w fazie zasadniczej.

Whitepaper

Podstawowy dokument w procesie ICO zawierający szczegóły techniczne na temat projektu, aktualne dane rynkowe, cele projektu, a także wymagania dla nabywców dotyczące nabycia i używania tokenów. W środowisku inwestorów ICO jest standardem, stanowiąc podstawę dla decyzji o nabyciu tokenów. Whitepaper można porównać do biznes planu, prezentowanego potencjalnym inwestorom przez osoby pragnące pozyskać środki na działalność.

Inteligentny Kontrakt (Smart Contract)

Inteligentny kontrakt (ang. smart contract) to cyfrowy odpowiednik umowy zapisanej w łańcuchu danych, zawierającej warunki świadczeń pomiędzy stronami tej umowy. Ważnym atutem inteligentnych kontraktów jest to, że uruchamiają się automatycznie po zaistnieniu określonych w umowie warunków. Dzięki temu po zapisaniu warunków w blockchainie, żadna ze stron nie może zmienić warunków takiego kontraktu, ani uchylić się od jego wypełnienia. Inteligentny kontrakt można porównać do banku oferującego usługę akredytywy, z tym, że w tym przypadku rolę pośrednika zabezpieczającego całą transakcję pełni algorytm inteligentnego kontraktu.

K

Know Your Customer (KYC)

Poznaj swojego klienta (ang. know your customer), w skrócie KYC, jest to procedura należytej staranności, którą muszą przeprowadzać określone prawnie podmioty, w celu właściwego zidentyfikowania swoich klientów. KYC, oprócz funkcji identyfikacji, ma również na celu śledzenie transakcji dokonywanych przez klienta w ramach serwisu lub platformy. Głównym zadaniem KYC jest redukcja ryzyka prania pieniędzy, a także finansowania terroryzmu i innych nielegalnych działań.

Konsensus

Konsensus (ang. consensus) to automatyczny proces uzgadniania zgodności operacji w danej sieci blockchainowej pomiędzy jej użytkownikami, bez konieczności zaangażowania centralnej jednostki lub zaufanej strony trzeciej. Konsensus musi zostać każdorazowo osiągnięty, zanim blok zostanie dodany do łańcucha danych. Najbardziej znanym sposobem osiągania konsensusu jest Proof of Work.

Kryptografia asymetryczna

Kryptografia asymetryczna to rodzaj kryptografii, w którym wykorzystuje się zestaw dwóch lub więcej powiązanych ze sobą kluczy, tzw. kluczy publicznych i prywatnych. Kryptografia asymetryczna zakłada operacje jednokierunkowe. Zgodnie z tym, w jedną stronę łatwo jest wykonać jakieś działanie, w drugą stronę jest to natomiast trudne lub niemal niemożliwe. Taka sytuacja występuje m.in. w funkcji haszującej. Dzięki takiej formule, zaszyfrowana wiadomość jest prawie niemożliwa do odczytania przez osobę nieuprawnioną.

Klucz Prywatny

Klucz prywatny to kod, umożliwiający odczytanie wiadomości zaszyfrowanej według algorytmu RSA (jeden z algorytmów szyfrowania asymetrycznego). Można go porównać do indywidualnego hasła, którym logujemy się do swojego konta.

Klucz Publiczny

Klucz publiczny to kod, który jest wysyłany wraz z wiadomością zaszyfrowaną według algorytmu RSA (jeden z algorytmów szyfrowania asymetrycznego). Sam klucz publiczny, w odróżnieniu od klucza prywatnego, służy do szyfrowania wiadomości.

Można go porównać do unikalnego kodu wiadomości, na podstawie którego jej odbiorca jest w stanie określić, czy wiadomość, którą otrzymał pochodzi od właściwego nadawcy.

Kryptowaluta

Kryptowaluta (ang. cryptocurrency) to forma aktywu cyfrowego opartego na algorytmach matematycznych i kryptograficznych, które automatycznie regulują tworzenie nowych jednostek danej kryptowaluty oraz weryfikację ich przesyłania pomiędzy użytkownikami danej sieci. Funkcjonowanie kryptowalut jest niezależne od banków centralnych oraz organów rządowych. Pierwszą i jednocześnie najpopularniejszą kryptowalutą jest bitcoin.

Bitcoin

Bitcoin (skrót giełdowy BTC) to pierwsza i najpopularniejsza kryptowaluta, uruchomiona w 2009 r. przez Satoshi Nakamoto. Bitcoin wykorzystuje do ustalania konsensusu algorytm Proof of Work.

Bitcoin Cash

Bitcoin Cash (skrót giełdowy BCH) to kryptowaluta, która powstała w 2017 r. w wyniku rozłamu społeczności Bitcoina. Konflikt wśród użytkowników dotyczył sposobu skalowania i rozwoju całej sieci. Podstawowe parametry Bitcoin Cash są identyczne jak w przypadku Bitcoina, największą różnicą jest jednak wielkość bloku, który jest znacznie większy w przypadku BCH.

Bitcoin Gold

Bitcoin Gold (skrót giełdowy BTG) to kryptowaluta będąca forkiem Bitcoina. Główną cechą różniącą BTG od bitcoina jest to, że do kopania tej pierwszej kryptowaluty wykorzystuje się koparki wykorzystujących kart graficznych zamiast układów ASIC. 16 maja 2018 r. BTG stał się ofiarą ataku 51%, w wyniku którego dokonano podwójnego wydania jednostek tej kryptowaluty.

Dash

Dash (skrót giełdowy DASH) to kryptowaluta, zapewniająca funkcję Instand Send, czyli natychmiastowego i bezpiecznego blokowania środków przed przetworzeniem ich przez blockchain. Funkcja została stworzona dzięki wprowadzeniu do sieci tzw. Masternode'ów, które działają podobnie do węzłów sieci Bitcoin. Różnią się przede wszystkim tym, że każdy węzeł musi wpłacić zastaw w postaci 1000 DASH, który umożliwia im zarabianie w formie odsetek oraz głosowanie nad zmianami w systemie.

Ether

Ether (skrót giełdowy ETH) to kryptowaluta rozliczeniowa i transakcyjna na platformie Ethereum. Jest to obecnie druga po bitcoinie najpopularniejsza kryptowaluta na świecie.

Ethereum Classic (ETC)

Ethereum Classic (skrót giełdowy ETC) to kryptowaluta będąca forkiem Ethereum, powstałym w wyniku rozłamu społeczności tej platformy. Główną przyczyną sporu, który doprowadził do podziału był atak dokonany na platformę The DAO, skutkujący największą kradzieżą w od początku powstania kryptowalut. Ethereum Classic, w odróżnieniu od Ethereum posiada niezmieniony kod w stosunku do czasów sprzed ataku na The DAO.

IOTA

IOTA (skrót giełdowy MIOTA) to kryptowaluta posiadająca pewne cechy blockchaina, jednak nie oparta o żaden blockchain. Jej głównym przeznaczeniem jest integracja danych i urządzeń w ramach Internetu Rzeczy (IoT). W IOTA każda pojedyncza transakcja formuje nowy blok i weryfikuje się sama. Weryfikacja transakcji odbywa się na podstawie uproszczonego Proof of Work. Dzięki takiemu mechanizmowi działania, koszt transakcji jest praktycznie pomijany. W związku z tym, IOTA może być bardziej skalowalnym systemem niż tradycyjne sieci blockchainowe.

Litecoin (LTC)

Litecoin (skrót giełdowy LTC) to kryptowaluta bardzo podobna do Bitcoina, różniąca się od niego pewnymi parametrami. Głównymi modyfikacjami względem Bitcoina jest to, że algorytm Litecoina przetwarza bloki szybciej, a także dopuszcza większą maksymalną podaż jednostek tej kryptowaluty.

Monero (XMR)

Monero (skrót giełdowy XMR) to kryptowaluta bazująca na formule Bitcoina, poprawiająca jednak pewne jego elementy, takie jak efektywność kopania oraz prywatność transakcji. Same opłaty transakcyjne oraz wielkości bloków w Monero nie są z góry określone, tylko dostosowywane dynamicznie za pomocą algorytmu.

Ripple

Ripple (skrót giełdowy XRP) to kryptowaluta umożliwiająca dokonywanie transakcji w sieci blockchain za pomocą walut fiducjarnych. Ripple nie jest kryptowalutą, którą można kopać, ponieważ cała podaż jest kontrolowana przez firmę, która ją stworzyła. Należy również wspomnieć, że w przypadku Ripple nie istnieją typowe węzły, a rejestry są automatycznie synchronizowane na wielu portfelach posiadaczy tej kryptowaluty. Dzięki temu jednak, transakcje w systemie Ripple są szybsze niż w standardowych sieciach kryptowalutowych.

M

Maszyna Wirtualna

Maszyna wirtualna to plik komputerowy, który funkcjonuje jak rzeczywisty komputer. Jest on wydzielany z systemu, dzięki czemu nie może negatywnie wpłynąć na główny system operacyjny. Pozwala to stworzyć środowisko testowe na potrzeby sprawdzania innych systemów operacyjnychlub oprogramowania, bez konieczności używania dodatkowego sprzętu. Maszynę wirtualną można określić jako komputer utworzony wewnątrz innego komputera.

O

Open Source

Open source to rodzaj kodu komputerowego, który jest udostępniany publicznie. Użytkownicy programu opartego na takim kodzie mogą go dzięki temu modyfikować oraz korzystać z niego przy tworzeniu innych rozwiązań.

P

P2P

P2P (ang. Peer to Peer) to rodzaj sieci, w ramach której użytkownicy przesyłają nawzajem informacje bezpośrednio, bez konieczności wykorzystania centralnego serwera.

Pieniądz cyfrowy (waluta cyfrowa)

Pieniądz cyfrowy (inaczej waluta cyfrowa lub kryptowaluta) to elektroniczne odwzorowanie wartości w świecie wirtualnym, oparte na rozproszonych rejestrach lub sieci blockchain. Jest to cyfrowy odpowiednik pieniędzy rzeczywistych, działających jednak w sieciach wirtualnych oraz najczęściej bez bezpośredniej kontroli instytucji publicznych.

Podpis

Podpis to znak graficzny utrwalony w dokumencie, umożliwiający jednoznaczną identyfikację składającego, składany w celu potwierdzenia oświadczenia zawartego w dokumencie lub jego autentyczność.

Podpis Cyfrowy

Podpis cyfrowy to oparty na mechanizmach kryptograficznych sposób potwierdzania dokumentów oraz wiadomości przesyłanych drogą elektroniczną. Właściwie nadany podpis cyfrowy pozwala na jednoznaczną identyfikację składającego oraz potwierdza, że podpisany przez niego dokument został dostarczony w formie niezmodyfikowanej.

Podwójny wydatek

Podwójny wydatek (ang. double-spending) to sytuacja, w której schemat płatności elektronicznych umożliwia wielokrotne wydanie tej samej jednostki płatniczej (tokena). Spowodowane jest to możliwością zduplikowania tego samego pliku odpowiedzialnego za dany token cyfrowy. Mechanizmy osiągania konsensusu obecne w większości sieci blockchainowych umożliwiających przesyłanie wartości pomiędzy użytkownikami sieci, nastawione są na eliminację tego zjawiska.

Potwierdzenie

Potwierdzenie (ang. confirmation) to czynność akceptacji i wpisania do bloku danej transakcji. Każde dodatkowe potwierdzenie obniża ryzyko podwójnego wydatku oraz zwiększa wiarygodność danej transakcji. Najczęściej odbiorca przesłanych informacji lub tokenów wymaga określonej liczby potwierdzeń, aby zaakceptować daną transakcję. Średni czas potwierdzenia transakcji zależy od efektywności danej sieci blockchainowej.

Problem bizantyjskich generałów

Problem bizantyjskich generałów to problem obecny w sieciach komputerowych, polegający na braku możliwości ustalenia właściwej decyzji przez różne jednostki (węzły). Objawia się, gdy wiele współpracujących ze sobą węzłów podaje różne rekomendacje, a system nie jest w stanie określić, które z nich należy przyjąć za prawdziwe i uwzględnić w ramach całościowej decyzji o działaniu, a które należy uznać za nieprawdziwe i odrzucić. Algorytm ustalania konsensusu stosowany w prawidłowo działających sieciach blockchainowych eliminuje ten problem, umożliwiając osiągnięcie porozumienia pomiędzy węzłami sieci.

Proof of Authority

Proof of Authority, w skrócie PoA, to mechanizm osiągania konsensusu w sieciach blockchainowych, w którym występują wyznaczone węzły nadzorujące, zajmujące się autoryzowaniem transakcji w ramach sieci. W przeciwieństwie do Proof of Work, gdzie każda transakcja potwierdzana jest przez wszystkich uczestników sieci, w PoA występuje ograniczona liczba węzłów nadzorujących. Dzięki temu sieć działa szybciej, przy zachowaniu wysokiego poziomu bezpieczeństwa.

Proof of Stake

Proof of Stake, w skrócie PoS, to mechanizm osiągania konsensusu w sieciach blockchainowych, w którym nagroda za wykopanie bloku jest rozdysponowana pomiędzy górników w zależności od liczby posiadanych przez nich jednostek tokenów. Dzięki temu eliminowana jest potrzeba wykorzystania dużej mocy obliczeniowej do wykopania każdego kolejnego bloku.

Przechowanie danych

→ Przechowanie danych to czynność zabezpieczania i gromadzenia uporządkowanych zbiorów informacji (danych).

Off-line

→ Off-line to sposób przechowywania danych w miejscu, które nie posiada dostępu do Internetu. Może to być miejsce na dysku komputera lub zapis w postaci fizycznej (np. Na kartce papieru, zapamiętane przez człowieka).

On-line

On-line to sposób przechowywania danych w miejscu wirtualnym, np. w wirtualnej chmurze. Dzięki temu właściciel danych ma do nich dostęp z różnych urzadzeń podłaczonych do Internetu.

R

Rejestr

→ Rejestr to miejsce, w którym przechowywane są dane oraz informacje dotyczące danego systemu.

Bez-tokenowy

→ Rejestr bez-tokenowy (ang. tokenless token) to rozproszony rejestr, który do funkcjonowania oraz potwierdzania transakcji nie potrzebuje żadnego natywnego tokena lub kryptowaluty.

Bez Zezwolenia

→ Rejestr Blockchain bez zezwolenia (ang. permissionless blockchain) to typ sieci blockchainowej, do której może się podłączyć każdy, bez konieczności uzyskania zezwolenia na dostęp

Zcentralizowany

Rejestr scentralizowany to rodzaj bazy danych, w której występuje jedna centralna jednostka, w ramach której są gromadzone wszystkie dane w ramach danej sieci.

Zdecentralizowany

Rejestr zdecentralizowany to rodzaj rozproszonej bazy danych, w ramach której pewne węzły mają charakter super-węzłów gromadzących i przetwarzających dane w ramach mniejszej grupy podłączonych urządzeń. Super węzły nie mają charakteru scentralizowanych jednostek.

Z Zezwoleniem

Rejestr Blockchain z zezwoleniem (ang. permissioned blockchain) to typ sieci blockchainowej, do której mogą się podłączyć tylko użytkownicy, którzy otrzymali do niej dostęp. W tych sieciach dodawanie nowego bloku autoryzowane jest tylko przez zaufane węzły.

Rozwidlenie

Rozwidlenie (ang. fork) to sytuacja, w której dana sieć blockchainowa dzieli się na dwa rodzaje, różniące się od siebie zasadami działania lub historią transakcji, w wyniku czego użytkownicy pierwotnej sieci decydują, które z nowych rozwiązań zaakceptują i będą dalej wspierać.

Miękkie

Miękkie rozwidlenie (ang. soft fork) polega na uściśleniu reguł panujących w danej sieci blockchainowej. W wyniku tego procesu niezaktualizowane węzły dalej akceptują bloki według nowych reguł, natomiast te zaktualizowane mogą nie akceptować części nowych bloków, niezgodnych z uściśloną regułą.

Twarde

Twarde rozwidlenie (ang. hard fork) polega na wprowadzeniu nowych zasad w ramach danej sieci blockchainowej. Może być rozumiany jako rozszerzenie zasad. W wyniki aktualizacji, węzły działające według starych zasad nie będą akceptowały nowych bloków tworzonych według nowych reguł. Często twarde rozwidlenie jest skutkiem konfliktu wśród użytkowników sieci.

S

SHA-256

Secure Hash Algoritm, w skrócie SHA w wersji 256, to standard szyfrowania kryptograficznego, wykorzystywany w sieci Bitcoin oraz innych systemach opartych na konsensusie. Technologia ta chroni również portfele tokenów oraz jest wykorzystywana w podpisie elektronicznym.

Sieć rozproszona

Sieć rozproszona (ang. distributed web) to zbiór niezależnych urządzeń komputerowych, połączonych w jedną, spójną strukturę. Komputery połączone w tego typu sieci mogą prowadzić komunikację P2P, bez konieczności wykorzystywania centralnego serwera. W ramach sieci rozproszonej zasoby są współdzielone pomiędzy wszystkimi komputerami, dzięki czemu wszystkie operacje pomiędzy użytkownikami są transparentne i bezpieczne.

Solidity

Solidity to język programowania, wykorzystywany do tworzenia smart contractów oraz zdecentralizowanych aplikacji na platformie Ethereum lub w ramach innych sieci blockchainowych.

Szyfrowanie

Szyfrowanie to proces przekształcania danych lub tekstu czytelnego dla człowieka albo wykorzystywanych przez niego urządzeń w formę niezrozumiałych znaków, w celu ukrycia ich zawartości przed osobami, które nie są uprawnione do ich odczytania. Szyfrowanie przeprowadza się przy użyciu specjalnych funkcji matematycznych, zwanych także kryptograficznymi algorytmami szyfrującymi.

T

Testnet

Testnet to testowa wersja sieci blockchainowej, z której korzystają deweloperzy tworzący nowe rozwiązania lub sprawdzający je pod kątem bezpieczeństwa i efektywności. Dzięki temu, że jest to wersja testowa, wszelkie błędy i wprowadzone zmiany nie mają wpływu na realnych użytkowników.

The DAO

The DAO to projekt informatyczny, którego celem jest stworzenie w pełni zdecentralizowanej autonomicznej organizacji (DAO). Aby sfinansować projekt, jego twórcy zorganizowali jedną z największych zbiórek ICO w historii. Projekt jest jednak znany przede wszystkim z tego, że był celem największego ataku hackerskiego w dotychczasowej historii rynku ICO, w wyniku którego 1/3 zebranych środków wypłynęła na zewnętrzne konta hackerów.

Token cyfrowy

Token cyfrowy to jednostka użytkowa w ramach sieci blockchain. Tokeny mogą być wykorzystywane jako jednostki rozliczeniowe, jako sposób płatności (kryptowaluty), prawo do głosowania w społeczności użytkowników danej sieci lub nawet warunek dostępu do tej sieci. Mogą być również generowane i następnie sprzedawane w ramach zbiórek ICO. W rzeczywistym świecie ich odpowiednikiem są żetony, które również mogą pełnić różnorodne funkcje, w zależności od systemu, w jakim funkcjonują.

Tożsamość Cyfrowa

Tożsamość cyfrowa to zestaw danych, które w sposób jednoznaczny identyfikują podmiot posługujący się taką tożsamością. Zawiera dane i podpis wystawcy tejże tożsamości, co odgrywa kluczową rolę w uwiarygodnieniu informacji przez trzecią stronę. W świecie wirtualnym pełni taką samą funkcję jak zwykła tożsamość w świecie realnym.

Transakcja

Transakcja to każda aktualizacja łańcucha bloków lub rozproszonych rejestrów. Jest to

więc zapis informacji o przesłaniu danych pomiędzy użytkownikami w ramach tych sieci.

W

Waluta FIAT

Waluta fiducjarna (ang. fiat money), znana również w środowisku kryptowalutowym jako waluta FIAT, to pieniądz nie mający pokrycia w aktywach materialnych (np. złoto), opierający się jedynie na zaufaniu do emitenta tego pieniądza. Za pieniądz fiducjarny można uznać wszystkie powszechnie uznawane waluty krajowe, takie jak dolar amerykański, euro, czy polski złoty.

Węzeł

Węzeł (ang. node) to komputer podłączony do sieci blockchain lub rozproszonych rejestrów. W zależności od przyjętego modelu konsensusu pełni różne role. Najczęściej wykorzystywany jest do kopania kryptowalut i zatwierdzania transakcji w bloku danych. W wielu sieciach każdy podłączony do nich węzeł posiada pełną kopię całego rejestru lub łańcucha bloków.

Z

Zaufana trzecia strona

Zaufana trzecia strona (ang. trusted third party) to podmiot, który autoryzuje i dba o bezpieczeństwo transakcji lub wymiany danych pomiędzy dwoma innymi podmiotami. Najczęściej zaufanymi stronami trzecimi są instytucje publiczne lub certyfikowane instytucje, których wiarygodność została potwierdzona przez inny uznany podmiot.

Zdecentralizowana Aplikacja

Zdecentralizowana aplikacja (ang. decentralized application, w skrócie Dapp) to rodzaj aplikacji, opartej na zdecentralizowanej sieci blockchain. Z punktu widzenia użytkownika aplikacja ta nie różni się niczym od standardowej wersji opartej na centralnym serwerze. Jednak dzięki rozproszeniu danych, zapewnia mu większą prywatność, poprzez odebranie możliwości ingerowania twórcy aplikacji w informacje wymieniane pomiędzy użytkownikami.

Zdecentralizowana Autonomiczna Organizacja

Zdecentralizowana Autonomiczna Organizacja (ang. decentralized autonomous organisation, w skrócie DAO) to rodzaj organizacji wirtualnej, która może działać bez jakiejkolwiek ludzkiej aktywności. DAO działa na podstawie z góry przyjętych zasad i założeń, które zapewniają jej pełną transparentnosc oraz eliminację możliwości czerpania nieuprawnionych korzyści przez dowolnego członka organizacji.

Znacznik czasu

Znacznik czasu (ang. timestamp) to dowód istnienia określonej informacji lub pliku w określonym momencie czasu. Można go porównać do pieczątki z datownikiem, wykorzystywanej przy oznaczaniu daty wpłynięcia dokumentu (np. pisma do urzędu).

AUTORZY

Dziękuję członkom grupy roboczej Blockchain za ich ekspercką wiedzę i pomoc w różnych aspektach naszych prac oraz autorom za kontrybucje, które stały się częścią raportu.

Rafał Dziedzic
Orange Polska S.A.
Kierownik Grupy Roboczej Blockchain PIIT

Jan Byrski
Traple Konarski Podrecki i Wspólnicy

Michał Gałagus
Polska Izba Informatyki i Telekomunikacji

Zdzisław Groch
Asseco Poland

Karol Juraszczyk
Traple Konarski Podrecki i Wspólnicy

Piotr Jurowiec
StratoFactory

Tomasz Kalicki
Kancelaria Domański Zakrzewski Palinka

Piotr Kania
GFT Poland Sp. z o.o.

Michał Kibil
Kancelaria Kibil i Wspólnicy

AUTORZY

Jakub Kubalski
Kancelaria Domański Zakrzewski Palinka

Michał Legumina
Atende S.A.

Andrzej Słomczewski
Orange Polska S.A.

Dariusz Szostek
Szostek_Bar i Partnerzy

Patryk Walaszczyk
IBM Services

Rafał Wawrzyniak
Krajowy Depozyt Papierów Wartościowych

Klaudia Borowiec
oprawa graficzna
+48 507 368 311
klaudiaborowiec@hotmail.com