Government
Office for Science

Distributed Ledger Technology: beyond block chain

A report by the UK Government Chief Scientific Adviser

Wyzwania cyfryzacyjne: brytyjskie doświadczenia, polskie aspiracje

Cyfryzacja jako proces adaptacji jednostek i procesów administracji publicznej, biznesu oraz całej gospodarki do nowych realiów technologicznych jest kluczowym wyzwaniem dla rządu i administracji. Rozważnie prowadzona spójna i oparta na empirycznych danych strategia cyfryzacji jest warunkiem sukcesu. W realiach dynamicznie zmieniających się technologii, dostosowanie do tempa zmian jest szczególnie trudne. Dlatego ważne jest prowadzenie systematycznych badań, gromadzenie danych oraz wczesne testowanie nowych zjawisk.

Raport „Technologia rozproszonych rejestrów - więcej niż blockchain" to efekt wspólnego wysiłku brytyjskiej administracji publicznej, środowisk naukowych i akademickich, a także biznesu. Raport przedstawia technologię blockchain/DLT, prezentuje potencjał jej zastosowań w administracji publicznej oraz kluczowych sektorach gospodarki. Dokument oparty na testach i pilotażowych wdrożeniach, przy wsparciu praktyków technologii blockchain/DLT, określa bezpieczne ramy wdrożeniowe dla administracji oraz gospodarki i wyznacza bezpieczną trasę jej adaptacji, poprzez sformułowanie rekomendacji.

W cyfrowej ekonomii, w której nieustanna zmiana jest normą, technologia jest wyzwaniem. Dokumenty tego rodzaju odgrywają ważną rolę semaforów, ułatwiających nawigację, a w efekcie, szybsze wdrożenie z korzyścią dla gospodarki i państwa.

Instytut badawczy NASK przy współpracy z FinTech Poland przygotował tłumaczenie tego ważnego dokumentu na język polski, by administracja publiczna i sektory strategiczne mogły nie tylko zapoznać się z tematem blockchain/DLT, lecz także poznać sprawdzony, efektywny sposób, w jaki administracja brytyjska wspiera rozwój innowacyjnych technologii.

Wierzymy, że lektura raportu pomoże w przygotowaniach do stworzenia we współpracy z Rządem RP i administracją własnego raportu na ten temat, w opartego na wnioskach z badań, testów i pilotażowych wdrożeniach. Raport taki wesprze rozwój nowej technologii transakcyjnej w Polsce oraz przyczyni się do budowania pozycji Polski jako regionalnego centrum wschodzących technologii transakcyjnych. NASK i FinTech Poland wraz z partnerami podjęli intensywne prace, służące realizacji takiego zamierzenia.

Zespół NASK i FinTech Poland

Technologie DLT:
więcej niż łańcuchy bloków

Sprawozdanie głównego doradcy naukowego rządu brytyjskiego

Tłumaczenie na język polski: Zespół NASK we współpracy z Magdą Borowik, Dyrektor Programu Blockchain, FinTech Poland

Spis treści

Raportowi towarzyszy krótki film, który można obejrzeć na: ***https://youtu.be/4sm5LNqL5j0***

Przedmowa:

Postęp ludzkości wyznacza rozwój nowych technologii, które odblokowują ludzką pomysłowość.

W przypadku technologii rozproszonych rejestrów możemy być świadkami jednej z tych potencjalnych eksplozji twórczego potencjału, katalizującego wyjątkowo wysoki poziom innowacyjności. Może się okazać, że ta technologia zwiększy zaufanie do szerokiej gamy usług. Byliśmy już świadkami jak open data zrewolucjonizowała relacje obywateli z państwem. Podobnie przejrzystość w tych technologiach pozwoli zreformować nasze rynki finansowe, łańcuch dostaw, usługi między przedsiębiorstwami oraz usługi konsumenckie, jak również rejestry publiczne.

Wiemy, że staniemy przed ogromnymi wyzwaniami, gdy rozproszone rejestry (ang. Distributed Ledgers) rozwiną się i odmienią sposób w jaki myślimy i w jaki przechowujemy dane. Wielka Brytania znajduje się w wyjątkowej sytuacji, która pozwala podjąć te wyzwania i pomóc zwiększyć korzyści dla brytyjskich usług publicznych i gospodarki. Wielka Brytania osiągnęła już możliwości cyfrowe na najwyższym światowym poziomie, świadczy innowacyjne usługi finansowe, posiada silne zaplecze badawcze oraz ciągle powiększające się doświadczenie sektora publicznego. Niezmiernie istotne jest, że nasze kluczowe aktywa, w tym Instytut im. Alana Turinga, Instytut Open Data oraz Digital Catapult, współpracują z sektorem prywatnym i międzynarodowymi partnerami, aby uwolnić pełen potencjał tej technologii.

Dlatego jesteśmy zadowoleni, że będziemy wspólnie prowadzić działania w tym zakresie i mamy nadzieję na współpracę z innymi departamentami w zakresie wykorzystania szansy, jak również zrozumienia jak możemy ją wykorzystać na korzyść brytyjskiego społeczeństwa i gospodarki.

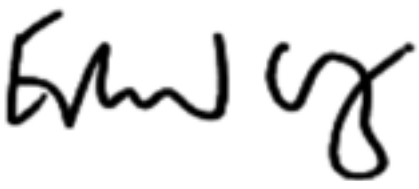
Matthew Hancock

Minister w kancelarii premiera i w Paymaster General

i

Ed Vaizey

Minister Kultury i Gospodarki Cyfrowej



Streszczenie i zalecenia

WSTĘP

Algorytmy umożliwiające stworzenie rozproszonych rejestrów są potężne, stanowią przełomową innowację, która modyfikuje sposób dostarczania usług publicznych i prywatnych oraz zwiększa wydajność dzięki szerokiej gamie aplikacji.

Już od czasów starożytnych rejestry stanowiły kluczowy element handlu. Używano ich do zapisywania różnych rzeczy, głównie aktywów takich jak pieniądze i mienie. Informacje utrwalano na glinianych tabliczkach, później papirusie, pergaminie i papierze. Jednak w całym tym okresie jedyną znaczącą innowacją była komputeryzacja, która początkowo polegała na przeniesieniu danych z papieru na bajty. Teraz, po raz pierwszy, algorytmy umożliwiają wspólne stworzenie cyfrowych rozproszonych rejestrów, posiadających właściwości i możliwości wykraczające daleko poza tradycyjne wersje papierowe.

Rozproszony rejestr jest zasadniczo rozproszoną bazą danych, zdecentralizowanym rejestrem transakcyjnym który może być udostępniany za pośrednictwem sieci internetowej wielu lokalizacjom, regionom lub instytucjom. Dzięki temu wszyscy zainteresowani mogą mieć identyczną kopię tego rejestru. Wszelkie zmiany w rejestrze znajdują odzwierciedlenie we wszystkich kopiach w ciągu kilku minut, lub w niektórych przypadkach nawet sekund. Zasoby mogą być finansowe, prawne, fizyczne lub elektroniczne. Bezpieczeństwo i dokładność danych transakcyjnych przechowywanych w rejestrze są zabezpieczone kryptograficznie, poprzez użycie kluczy cyfrowych i podpisów elektronicznych po to, by kontrolować uprawnienia do korzystania z danych zasobów w ramach współdzielonego rejestru. Wpisy mogą być aktualizowane przez jednego, kilku lub wszystkich użytkowników, zgodnie z ustalonymi w protokole zasadami.

U podstaw tej technologii leży «blockchain», który został wymyślony w 2008 roku na potrzeby wirtualnej waluty Bitcoin. Algorytmy blockchaina umożliwiają grupowanie transakcji bitcoinowych w bloki, które następnie dołączane są chronologicznie do łańcucha już istniejących bloków przy użyciu podpisów kryptograficznych. Rejestr (blockchain) bitcoina ma charakter rozproszony i jest skonstruowany w taki sposób, że każdy mógł dodać blok transakcji, jeśli tylko potrafi rozwiązać nową kryptograficzną zagadkę wydobywając każdy nowy blok. Zachętą do takiego działania jest obecnie nagroda w postaci 12,5 bitcoina, dla każdego, kto rozwiąże zagadkę wyznaczoną dla każdego bloku. Każdy, kto posiada dostęp do internetu oraz wystarczającą moc obliczeniową by rozwiązywać kryptograficzne łamigłówki może weryfikować nowo pojawiające się w rejestrze transakcje. Osoby inwestujące w sieć bitcoina moc obliczeniową nazywamy „górnikami" *(1)*. Analogia do słownictwa górniczego wynika z tego, że proces wydobywania bitcoinów jest energochłonny z racji wymaganej dużej mocy obliczeniowej. Oszacowano, że energia zużywana na wydobycie bloków transakcji w sieci bitcoin może przekraczać 1GW i może być porównywalna ze zużyciem energii elektrycznej w Irlandii.

Bitcoin jest internetową walutą. W świecie realnym pieniądze są uwierzytelniane na podstawie wyglądu i cech charakterystycznych, a w przypadku banknotów numerami seryjnymi bądź innymi zabezpieczeniami. Jednak w przypadku pieniędzy nie posiadamy wspólnego rejestru, w którym zapisujemy przeprowadzane transakcje, dlatego pojawiają się problemy z fałszerstwami zarówno monet jak i banknotów. W przypadku bitcoina wspólny rejestr transakcji zapewnia przejrzystość i autentyczność transakcji. Zarówno fizyczne monety jak i bitcoiny muszą być bezpiecznie przechowywane odpowiednio w realnych lub wirtualnych portfelach – i jeśli nie są objęte właściwą ochroną, mogą zostać skradzione. Główną różnicą pomiędzy tradycyjną walutą a bitcoinami jest to, że emisją tej pierwszej zajmują się banki centralne, zaś ta druga emitowana jest w uzgodnionych ilościach przez globalne, rozproszone, oparte na współpracy przedsięwzięcie, jakim jest bitcoin. Pieniądz jako środek wymiany i handlu funkcjonuje od tysięcy lat i w tym kontekście widać związek pomiędzy muszelkami kauri, wybijanymi groszami i walutą bitcoin.

Jednak ten raport nie jest o walucie bitcoin, tylko o technologiach algorytmicznych, które umożliwiają wykorzystanie bitcoinów i ich mocy do przekształcenia rozproszonych rejestrów w narzędzia do rejestrowania zabezpieczonych transakcji o ogromnym zasięgu. Dlatego podstawowe założenie technologii blockchain może być zmodyfikowane w taki sposób, aby uwzględniać przepisy prawa, inteligentne kontrakty (ang. smart contracts), cyfrowe podpisy oraz szereg innych nowych cyfrowych narzędzi.

Technologie rejestrów rozproszonych mają ogromny potencjał, który może pomóc rządom pobierać podatki, zapewniać korzyści, dystrybuować świadczenia, prowadzić rejestry nieruchomości, dbać o łańcuch dostaw towarów i generalnie zapewnić spójność rejestrów i usług rządowych. W państwowej służbie zdrowia technologia podnosi jakość opieki zdrowotnej poprzez polepszenie i uwierzytelnianie świadczenia usług oraz poprzez udostępnianie danych w bezpieczny sposób z zachowaniem ścisłych reguł. Dla konsumenta tych wszystkich usług technologia oferuje potencjał, stosownie do okoliczno-

ści, który dla indywidualnych konsumentów umożliwiający kontrolowanie dostępu do własnej dokumentacji i wiedzę o tym, kto miał do niej dostęp.

Obecne metody zarządzania danymi, w szczególności danymi personalnymi, zazwyczaj wymagają przestarzałych systemów teleinformatycznych znajdujących się w obrębie jednej instytucji. Do nich dodaje się szereg systemów sieciowych i komunikacyjnych, by utrzymywać kontakt ze światem zewnętrznym, co zwiększa koszty i rodzi komplikacje. Wysoce scentralizowane systemy niosą za sobą duże koszty w przypadku awarii w jednym punkcie systemu. Mogą być również podatne na cyberataki, a dane są często niezsynchronizowane, nieaktualne lub po prostu obciążone błędem.

Natomiast rozproszone rejestry są z natury trudniejszym celem ataku, ponieważ zamiast pojedynczej bazy danych mamy wiele współdzielonych kopii tej samej bazy danych, dlatego by atak zakończył się sukcesem należałoby zaatakować wszystkie kopie na wszystkich węzłach sieci jednocześnie. Technologia rozproszonych rejestrów transakcji jest również odporna na nieautoryzowane zmiany lub ingerencje złośliwego oprogramowania, ponieważ uczestnicy sieci natychmiast wychwycą niespójność w jednej z części rozproszonego rejestru.

Dodatkowo, dzięki metodom, za pomocą których informacje są zabezpieczone i uaktualniane, uczestnicy mogą udostępniać dane i mieć pewność, że w danym momencie wszystkie kopie rejestru pasują do siebie – są identyczne.

Jednak nie oznacza to, że rozproszone rejestry są odporne na cyberataki, ponieważ w zasadzie każdy, kto znajdzie sposób, by legalnie zmodyfikować jedną kopię, będzie automatycznie wprowadzał zmiany we wszystkich kopiach rejestru. Dlatego zapewnienie bezpieczeństwa rozproszonych rejestrów jest ważnym zadaniem i częścią ogólnego wyzwania zapewnienia bezpieczeństwa cyfrowej infrastrukturze, od której zależne są współczesne społeczeństwa.

Rządy zaczynają stosować technologie rozproszonych rejestrów, by prowadzić swoją działalność. Rząd Estonii od kilku lat eksperymentuje z technologią rozproszonych rejestrów używając technologii KSI (Keyless Signature Infrastructure), opracowanej przez estońską firmę Guardtime.

Technologia KSI pozwala obywatelom weryfikować integralność swoich danych w rządowych bazach danych, ale nie pozwala na przeprowadzenie nielegalnych działań wewnątrz rządowych sieci. Zapewnienie obywatelom, że ich dane są bezpiecznie i precyzyjnie przechowywane pomogło Estonii uruchomić usługi cyfrowe, takie jak elektroniczny rejestr przedsiębiorców i e-Podatki. Wprowadzenie tych usług zmniejszyło obciążenia administracyjne spoczywające na państwie i obywatelach. Estonia jest w grupie „Digital 5", która zrzesza takie państwa jak Wielka Brytania, Izrael, Nowa Zelandia i Korea Południowa. Wielka Brytania ma możliwość uczenia się od państw członkowskich Digital 5 i innych rządów mających takie same poglądy na temat wdrożenia technologii blockchain i jej podobnych.

Przedsiębiorcy szybko docenili te możliwości. Rozproszone rejestry mogą zapewnić nowe sposoby informowania o własności i miejscu wytworzenia towarów oraz własności intelektualnej. Na przykład firma Everledger udostępniła rozproszony rejestr, umożliwiający monitorowanie transakcji i rejestrowanie własności diamentów. Na rynku z wysokim poziomem fałszerstw, rozproszone rejestry uniemożliwią wprowadzanie na rynek „krwawych diamentów" i przyczynią się do zmniejszenia liczby oszustw.

Informowanie polityków i opinii publicznej o znaczeniu tych nowych technologii jest niezmiernie ważne i stanowi jeden z najistotniejszych przekazów niniejszego raportu. Pierwszą trudnością w tej komunikacji jest silne powiązanie technologii blockchain z kryptowalutą bitcoin, która nie ma najlepszej opinii. Wśród obywateli i polityków bitcoin budzi podejrzenia ze względu na związek tej kryptowaluty z nielegalnymi transakcjami oraz sklepami internetowymi w ukrytej sieci, takimi jak nieistniejący już Silk Road. Mimo to, cyfrowe kryptowaluty cieszą się zainteresowaniem banków centralnych i rządowych departamentów finansowych na całym świecie. Jest tak dlatego, że elektroniczna dystrybucja cyfrowych środków pieniężnych oferuje potencjalne korzyści ekonomiczne i w przeciwieństwie do fizycznych pieniędzy, umożliwia permanentną kontrolę prowadzonych transakcji.

Drugim utrudnieniem jest zbyt skomplikowana terminologia. Została ona wyjaśniona na końcu niniejszego opracowania przez Simona Taylora.

Jednym z takich określeń jest słowo „rozproszony", które może prowadzić do błędnego przekonania, że jeśli coś jest rozproszone, zatem nie jest kontrolowane lub nie ma właściciela. Odpowiedź brzmi: i tak i nie, ponieważ zależy to od konstrukcji rejestru. W praktyce istnieje szeroka gama rozproszonych rejestrów, z różnymi poziomami centralizacji i rodzajami kontroli dostępu. Wszystko po to, aby zaspokoić różne potrzeby biznesowe. Mogą to być rejestry otwarte, nei wymagające pozwolenia na przystąpienie „unpermissioned", które mają charakter otwarty, co oznacza, że każdy może wprowadzać dane, a rejestry nie są niczyją własnością; lub rejestry należące do jednego lub kilku właścicieli, wymagające zezwolenia na przystąpienie (ang. permis-

sioned), którzy jako jedyni mogą dopuszczać nowe węzły, dodawać rekordy i weryfikować zawartość rejestru.

Naszym kluczowym przesłaniem jest to, że dzięki pełnemu zrozumieniu technologii, administracja publiczna i sektor prywatny mogą wybrać taki rodzaj rejestru, który najbardziej pasuje do ich potrzeb, równoważący bezpieczeństwo i centralny nadzór z wygodą i możliwością udostępniania danych między instytucjami i osobami prywatnymi.

Jak w przypadku większości nowych technologii, pełen zakres przyszłych zastosowań i nadużyć jest słabo zarysowany. W przypadku każdej nowej technologii pytanie nie brzmi: czy technologia jest sama w sobie dobra czy zła, tylko: jakie jest jej zastosowanie oraz jak ją stosować i jakie zabezpieczenia wybrać.

By pomóc znaleźć odpowiedź na powyższe pytania, brytyjski Government Office of Science powołał grupę ekspertów reprezentujących rząd, środowisko biznesowe i naukowe, aby ocenili możliwości wykorzystania rozproszonych rejestrów w sektorze rządowym i prywatnym, a także określili jakie działania powinny zostać podjęte, by ułatwić wykorzystanie potencjału technologii rozproszonych rejestrów i uniknąć ewentualnych szkód. Celem było również wyjaśnienie opinii publicznej i politykom terminologii i przedstawienie im koncepcji i dowodów, które pomogą podjąć decyzję, w jakim obszarze działanie jest konieczne i jak najlepiej je wdrożyć.

Podsumowując, technologia rozproszonych rejestrów zapewnia rządowi ramy, dzięki którym można ograniczyć nadużycia, korupcję, błędy i koszty procesów papierowych. Ma również potencjał, by na nowo określić współpracę pomiędzy rządem a obywatelem w zakresie udostępniania danych, transparentności i zaufania. Podobnie w przypadku sektora prywatnego.

Niniejsze sprawozdanie ustanawia osiem głównych rekomendacji dla naszych działań. Są one ujęte w formie podsumowania kluczowych punktów omówionych w siedmiu rozdziałach, które dotyczą: koncepcji, technologii, zarządzania, prywatność i bezpieczeństwa, zagrożeń, zastosowań i globalnych perspektyw. Rozdziały zostały napisane przez ekspertów z dziedziny technologii rozproszonych rejestrów językiem, który powinien być zrozumiały dla laików. Jestem niezmiernie wdzięczny autorom za wskazówki i przemyślane sugestie.

Mark Walport, Chief Scientific Adviser to HM Government, grudzień 2015

KONCEPCJA

Rozproszone rejestry oferują rządowi oraz innym organizacjom z sektora publicznego i prywatnego szereg korzyści. Jak wskazuje nazwa, rejestry mogą być bardzo szeroko rozproszone w ściśle kontrolowany sposób. Są one bardzo wydajne, ponieważ zmiany dokonywane przez uczestnika z niezbędnymi uprawnieniami do modyfikacji rejestru są natychmiast widoczne we wszystkich jego kopiach. Nieautoryzowane zmiany mogą być równie skutecznie odrzucone, dlatego uszkodzenie rejestru jest niezwykle trudne. Jednak rozproszone rejestry nie powinny być traktowane jako cel sam w sobie. Potencjał może być w pełni wykorzystany dopiero wówczas, gdy rejestry powiązane są z innymi aplikacjami, takimi jak inteligentne kontrakty (ang. smart contracts)

Pierwszy zadaniem rządu w zakresie wspierania rozwoju rozproszonych rejestrów jest opracowanie jasnej koncepcji, w jaki sposób ta technologia może ulepszyć realizację zadań rządu oraz umożliwi dostarczenie usług obywatelom. Następnie rząd powinien przystąpić do wdrożenia technologii pozyskując rozwiązania rozproszonych rejestrów tam gdzie mają one zastosowanie. W ten sposób rząd może wspierać i wpływać na rozwój działalności gospodarczej w tym sektorze, w tym nowych i rozwijających się firm, a także większych przedsiębiorstw działających na rynku już od dawna.

Takie działania sprawią, że w przyszłości dostarczanie usług administracji państwowej stanie się bardziej osobiste, skuteczniejsze i natychmiastowe. Tam, gdzie jest to uzasadnione, obywatele powinni mieć możliwość sygnalizowania swoich własnych potrzeb poprzez udział w inteligentnych kontraktach. Wdrożenie rozproszonych rejestrów z wbudowanymi inteligentnymi kontraktami powinno znacząco wpłynąć na zwiększenie oszczędności finansowych, odpowiedzialności i przejrzystości.

Brytyjski Government Digital Service tworzy właśnie cyfrową platformę, której zadaniem będzie dostarczanie rządowych usług, wśród których są również rozproszone rejestry.

Zalecenie 1:

Uważamy, że rząd powinien:

- *Zapewnić koordynatora ze strony ministerstwa, który zadba, by rząd opracował koncepcję, wybrał kierownictwo oraz platformę rządową dla technologii rozproszonych rejestrów. W przypadku Wielkiej Brytanii prace prowadzone były przez Government Data Service jako specjalistę od rozproszonych rejestrów wspólnie z Działem Gospodarki Cyfrowej funkcjonującym w ramach Departamentu Kultury, Mediów i Sportu (DCMS Digital Economy Unit) zajmującym się komunikacją z rządem. Do współpracy zaproszono także Dział Biznesu, Innowacji i Umiejętności.*
- *Powołany zespół projektowy powinien wspólnie opracować profesjonalny harmonogram oraz za-*

rys działań, wykorzystując rekomendacje zawarte w niniejszym raporcie. Podejmując się realizacji tworzenia platformy e-administracji zaleca się ścisłą współpracę z innymi rządowymi departamentami, przemysłem oraz środowiskiem naukowym. Należy także rozważyć powołanie eksperckiej grupy doradczej.

TECHNOLOGIA

Technologia rozproszonych rejestrów jest wciąż na wczesnym etapie rozwoju. Rozwój technologii blockchain jest jedynie pierwszym, niemniej jednak bardzo ważnym krokiem ku rewolucji, jaką jest wdrożenie technologii rozproszonych rejestrów, które mogłyby zmienić sposób kierowania organizacjami z sektora publicznego i prywatnego. Można dostosować technologię tak, aby „legalne" zmiany w rejestrach mogły być wprowadzane w zasadzie przez każdego (ang. unpermissioned ledger), lub jedynie przez ograniczoną liczbę osób lub nawet pojedynczą osobę posiadającą uprawnienia (ang. permissioned ledger). Na potrzeby rządu rejestry z ograniczoną liczbą osób uprawnionych do wprowadzania zmian są najprawdopodobniej lepsze niż rejestry otwarte oparte na modelu bitcoina, ponieważ posiadają jednego lub kilku właścicieli danych, którzy wyznaczają zasady komu wolno a komu nie wolno korzystać z systemu. Rozproszone rejestry mają również tę zaletę, że wiele kwestii związanych za zarządzaniem bezpieczeństwem schodzi na drugi plan, co powoduje, że system jest prostszy i tańszy w użyciu.

Trzeba uporać się z wieloma nierozwiązanymi jeszcze problemami zanim będzie można w pełni wykorzystać potencjał technologii rozproszonych rejestrów i innych podobnych technologii, m.in. rozstrzygnięciem kwestii prywatności, bezpieczeństwa, wydajności i skalowalności. Istnieje również szeroki wachlarz możliwości rozwoju algorytmów, które wzbogacą rejestry o inteligentne kontrakty, podpisy i inne aplikacje. Dzięki nim zwiększy się zakres wykorzystywania i wartość rejestrów. Ta dziedzina rozwija się niezwykle dynamicznie, dlatego niektóre z wymienionych wyżej problemów są już analizowane, a w niektórych przypadkach problematyczne kwestie zostały już rozwiązane. Jeśli rząd będzie czekać na idealne rozwiązanie, wówczas straci szansę na kształtowanie i wdrożenie technologii, która zapewni maksymalne korzyści dla sektora publicznego, a Wielka Brytania może stracić szansę na korzyści ekonomiczne.

Oprócz zapewnienia, że technologia jest niezawodna i skalowalna, musimy zrozumieć etyczne i społeczne konsekwencje różnych wariantów zastosowań, kosztów finansowych oraz korzyści z wykorzystania technologii. Jeśli chodzi o badania i rozwój, Wielka Brytania jest na dobrej pozycji, jednak nie możemy uznać tego za rzecz oczywistą, ponieważ istnieje duże zainteresowanie i konkurencja w dziedzinie rozwoju technologii rozproszonych rejestrów na całym świecie.

Ważną rolę odgrywają rady ds. naukowych, wspierające badania na uniwersytetach i w nowo powstałym Instytucie im. Alana Turinga. Istotne jest również, by firmy inwestowały w badania i rozwój, a także podejmowały wspólne publiczno-prywatne inwestycje mające na celu rozwiązanie problemów związanych z bezpieczeństwem, prywatnością i rozwojem standardów. Dotyczy to wszystkich obszarów, gdzie korzyści rynkowe zostaną osiągnięte raczej dzięki współpracy niż konkurencji.

Istniejące inwestycje realizowane przez rząd i sektor prywatny to: Digital Catapult, Future Cities Catapult i Open Data Institute. Do tego wymienić należy również stowarzyszenie, takie jak Whitechapel Think Tank, które stanowi centralny punkt dla prowadzenia dyskusji i dzielenia się pomysłami.

Oznacza to, że Wielka Brytania jest w dobrej sytuacji, która pozwala prowadzić badania nad rejestrami oraz testy wydajności. Istnieje jednak niebezpieczeństwo, że taki plan działania nie da maksymalnych korzyści, dlatego są silne argumenty za tym, że środowiska zajmujące się badaniami i rozwojem w sektorach publicznych i prywatnych powinny się same zorganizować w taki sposób, który zachęci do współpracy, gdy jest to korzystne oraz do rywalizacji, dzięki której powstaną najbardziej twórcze badania.Kolejne dwie rekomendacje mają na celu zachęcenie do dalszych badań i ustalenia możliwości Wielkiej Brytanii w zakresie eksperymentowania z różnymi rozwiązaniami:

Zalecenie 2:

Środowisko naukowe Wielkiej Brytanii powinno inwestować w badania, które zapewnią, że rozproszone rejestry są skalowalne i bezpieczne, oraz zagwarantują, że ich zawartość jest poprawna. Rejestry muszą wykazywać wysoką wydajność, działanie z niewielkim opóźnieniem, dostosowane do dziedziny, w ramach której technologia została wdrożona. Rejestry muszą być energooszczędne. Nowo powstały Instytut Alana Turinga, współpracujący z takimi stowarzyszeniami jak Whitechapel Think Tank, mógłby odgrywać ważną rolę koordynując prace badawczo-rozwojowe instytucji z sektora prywatnego i publicznego, które będą zainteresowane technologią rozproszonych rejestrów i pokrewnych. Z kolei sektor prywatny powinien rozważyć inwestowanie w Instytut Alana Turinga, by wesprzeć przedsięwzięcia przed fazą komercjalizacji, które ułatwią nowe działania komercyjne. Dotyczy to działań w oczywistych obszarach, takich jak kryptografia i cyberbezpieczeństwo, ale także rozwoju nowych rodzajów algorytmów.

Zalecenie 3:

Rząd mógłby również wspierać tworzenie demonstratorów rozproszonych rejestrów na potrzeby lokalnych samorządów, co pozwoli zebrać wszystkie elementy potrzebne do testowania technologii i jej działania. Innovate UK wykorzystało współpracę z miastami przy pracach nad rozwojem demonstratora dla miast.

ZARZĄDZANIE

Efektywne zarządzanie i rozporządzenia są kluczem do pomyślnego wdrożenia rozproszonych rejestrów. Zarządzanie obejmuje zasady opracowane przez właścicieli i osoby zarejestrowane w rejestrze, którzy chronią swoich prywatnych interesów. Musi być to uzupełnione o rozporządzenie lub akt prawny stanowiący ramę prawną, ustanowioną przez organ zewnętrzny, w celu ochrony interesów społeczeństwa. Rząd stanowi prawo i tworzy ramy dla regulacji, samodzielnie lub we współpracy z innymi rządami, i zazwyczaj wyznacza organ regulacyjny odpowiedzialny przed rządem, który podejmuje się realizacji prac.

W świecie cyfrowym są dwa zestawy przepisów i norm, które regulują działanie cyfrowych technologii. Pierwszy to klasyczny zestaw przepisów zapewniony przez ramy legislacyjne, normy prawne i przepisy.

Drugi to zestaw zasad, który określa działanie algorytmów zakodowanych przez oprogramowanie. Oba są niezwykle ważne.

Pomyślna implementacja rozproszonego rejestru będzie wymagać połączenia właściwego zarządzania, chroniącego zarejestrowanych i interesariuszy, z przepisami gwarantującymi, że system jest odporny na ryzyko systemowe lub działalność przestępczą. Wyzwaniem jest zachowanie równowagi pomiędzy ochroną interesów zarejestrowanych w systemie a szerszym interesem społecznym przy jednoczesnym uniknięciu ograniczania innowacji przez zbyt sztywne struktury.

Istnieje również możliwość skorzystania z potencjalnych oddziaływań pomiędzy normami prawnymi i technicznymi. Na przykład, można wpływać na regulacje publiczne poprzez połączenie norm prawnych i technicznych, a nie jak obecnie jedynie przez kodeksy prawne. W istocie normy techniczne mogą być wykorzystywane w celu zapewnienia zgodności z kodeksem prawnym, a działając w ten sposób zmniejsza się koszty związane ze sprawdzeniem zgodności z przepisami prawnymi.

Określenie optymalnej równowagi pomiędzy zarządzaniem a przepisami oraz pomiędzy kodeksami prawnymi i technicznymi, wymaga niezwykłych umiejętności, a co za tym idzie rodzi potrzebę podjęcia współpracy pomiędzy prawnikami, matematykami i ekspertami IT w celu rozwiązania wielu kluczowych kwestii, które są przedstawione w rozdziale 3.

Zalecenie 4:

Rząd musi rozważyć jak wprowadzić w życie ramy regulacyjne dla technologii rozproszonych rejestrów. Przepisy będą musiały ewoluować równolegle do rozwoju nowych wdrożeń i zastosowań technologii. Poza tym rząd powinien rozważyć jak osiągnąć cele regulacyjne wykorzystując zarówno normy techniczne jak i prawne. Na gruncie brytyjskim tymi kwestiami zajął się Dział Cyfrowej Gospodarki (DCMS Digital Economy Unit).

BEZPIECZEŃSTWO I PRYWATNOŚĆ

Przestępcy nie włamują się już do pancernych sejfów i bankowych skarbców. Obecnie pieniądze mają również formę cyfrową, ale ona z kolei bywa podatna na działania hackerów. Kryptograficzne kody cyfrowego świata są wyjątkowo trudne do złamania, ale można dokonać włamania. Można do tego wykorzystać człowieka, który może przypadkowo lub celowo udostępnić hasło, lub celowo tworzone tzw. tylne drzwi w oprogramowaniu (backdoory), również te wynikające z niezamierzonej niedoskonałości kodu. Sprzęt wykorzystany do hostowania rozproszonych rejestrów również może posiadać luki w bezpieczeństwie, dlatego trzeba zwrócić uwagę także na odporność i zabezpieczenia sprzętu.

W przypadku bitcoinów, wirtualne portfele przechowujące kryptowalutę okazały się podatne na kradzież – jednak rejestr sam w sobie jest odporny, choć w zasadzie mógłby okazać się podatny, gdyby hipotetycznie, ponad 50% komputerów asygnujących moc obliczeniową do wydobycia bloków rejestru transakcji bitcoin a wpadło w ręce pojedynczego cyberprzestępcy lub cyberprzestępczej organizacji.

Przekroczenie 51% mocy obliczeniowej mogłoby skutkować kontrolą wersji stosowanego przez węzły wydobywcze oprogramowania a w efekcie, obowiązującej rzeczywistości transakcyjnej w rejestrze.

W rzeczywistości, ogromna przewaga rozproszonych rejestrów polega na tym, że są one relatywnie wysoce odporne na ataki.

Jednak liczy się nie tylko integralność rejestru. Ochrona prywatności i poufność informacji są również kluczowymi kwestiami. W zależności od rodzaju rejestru może on przechowywać poufne osobiste dane wrażliwe, dotyczące finansów, spraw rodzinnych lub zdrowotnych. Technologie rozproszonych rejestrów zapewniają dużo większe bezpieczeństwo dla danych niż obecne stoso-

wane bazy. Jest to jednak kolejny obszar, który wymaga wciąż wielu analiz.

Bezpieczeństwo i ochrona prywatności to kolejne dziedziny, w których rząd powinien odegrać ważną rolę, dlatego nasza kolejna rekomendacja brzmi:

Zalecenie 5:

Rząd musi współpracować z ośrodkami akademickimi i przemysłem w celu zapewnienia, że opracowane normy zapewniają integralność, bezpieczeństwo i prywatność rozproszonych rejestrów i ich zawartości. Normy muszą znaleźć odzwierciedlenie zarówno w przepisach jak i wytycznych dla oprogramowania.

Dla każdego konkretnego przypadku zastosowania technologii, użytkownicy administracji rządowej i sektora prywatnego, w stosownych przypadkach, powinni przeprowadzić ocenę ryzyka, by wskazać istotne zagrożenia. Na gruncie brytyjskim zajmują się tym eksperci z Centrum Ochrony Infrastruktury Narodowej (ang. Centre for the Protection of National Infrastructure) oraz z CESG (ang. Communications-Electronics Security Group), którzy doradzają w zakresie zapewnienia integralności, bezpieczeństwa i prywatności rozproszonych rejestrów. Tak jak pisaliśmy w zaleceniu 2., nowo powstały Instytut Alana Turinga, współpracujący z takimi stowarzyszeniami jak Whitechapel Think Tank oraz z CESG, mógłby odgrywać ważną rolę koordynując działania instytucji badawczo-rozwojowych z sektora prywatnego i publicznego.

Nie należy zapominać, że wraz z upływem czasu sprzęt oraz oprogramowanie „starzeją się", pojawia się lepsza technologia a cyberprzestępcy uczą się nowych "sztuczek". Dlatego już na etapie projektowym należy założyć, że systemy z długim okresem żywotności powinny mieć możliwość łatwej aktualizacji elementów sprzętowych i oprogramowania. Ponadto, w ramach testowania nowych implementacji, ważne jest, aby przeprowadzać testy penetracyjne, zarówno na poziomie systemu jak i użytkowników.

ZAUFANIE I WSPÓŁDZIAŁANIE

W rozdziale 7. dotyczącym globalnych perspektyw zaznaczono, że zaufanie jest oszacowaniem ryzyka pomiędzy dwoma osobami lub większą liczbą osób, organizacji lub narodów.

W cyberprzestrzeni, zaufanie opiera się na dwóch podstawowych kwestiach: konieczność udowodnienia, że jest się daną osobą (uwierzytelnianie) oraz wykazanie się koniecznymi uprawnieniami do uzyskania tego, o co się pyta (autoryzacja). W odpowiedzi druga strona udowadnia, że dostarcza usługi lub produkty w bezpieczny, efektywny i niezawodny sposób.

Uwierzytelnianie i identyfikacja są ze sobą powiązane, ale nie oznaczają tego samego. Uwierzytelnianie nie wskazuje twojej tożsamości, tylko udowadnia, że posiadasz token nierozerwalnie związany z twoją tożsamością, na przykład numer PIN związany z kartą kredytową lub debetową, lub odcisk palca przypisany do twojego paszportu biometrycznego lub innego dokumentu. Podobnie, przekazując token do uwierzytelnienia, musimy mieć pewność, że dajemy go właściwej osobie lub instytucji. Dlatego jest niezmiernie ważne, aby instytucje zapewniły swoim użytkownikom uwierzytelnienie, bez względu na to czy są to pojedyncze osoby, inne instytucje czy rząd.

Szansą w cyfrowym środowisku jest wykorzystywanie i stworzenie bardziej rozbudowanych i niezawodnych narzędzi do zarządzania tożsamością, które zapewnią uwierzytelnienie chroniąc jednocześnie prywatność. Jednym z takich systemów jest infrastruktura klucza publicznego (PKI) opierająca się na standardach kryptograficznych zwanych X.509. Organizacje używające PKI mogą się zrzeszyć w celu zapewnienia, współdzielenia lub ewentualnie uproszczenia zasad bezpiecznego dostarczania usług i produktów. Kolejnym ważnym międzynarodowym standardem do identyfikacji jest Rejestr Organizacji Prawnych, który może pomóc uwierzytelnić organizacje w odróżnieniu do osób fizycznych.

Innym istotnych elementem bezpiecznego uwierzytelnienia przez indywidualnych użytkowników jest użycie smartfonów jako de facto zaufanego urządzenia należącego do użytkownika. Współczesne smartfony posiadając istotne funkcje zabezpieczające, jakie jak moduł TPM (ang. Trusted Platform Module), który zabezpiecza cyfrowe certyfikaty i klucze kryptograficzne do uwierzytelniania, szyfrowania i podpisywania, oraz Zaufane Środowisko Wykonawcze (ang. Trusted Execution Environment) i Zaufany Interfejs Użytkownika (ang. Trusted User Interface), z których każdy jest odporny na ingerencję złośliwego oprogramowania.

Dyskusja o uwierzytelnieniu pokazuje, że w celu zwiększenia możliwości rozproszonych rejestrów, muszą one być kompatybilne z innymi rejestrami. Jednak zwiększenie potencjału interoperacyjności wykracza daleko poza interoperacyjność uwierzytelniania – wymaga to ustaleń dotyczących interoperacyjności danych, polityki oraz skutecznego wdrożenia standardów międzynarodowych.

Zalecenie 6:

To zalecenie jest połączone z Zaleceniem 5. Rząd musi współpracować ze środowiskiem naukowym i przemysłem w celu zapewnienia, że dla osób fizycznych i organizacji zostaną wdrożone najbardziej skuteczne i użyteczne protokoły identyfikacji i uwierzytelnienia. Podjęte działania muszą iść w parze z rozwojem i wdrażaniem standardów międzynarodowych.

NIEPEWNA PRZYSZŁOŚĆ – KILKA MOŻLIWYCH PRZYPADKÓW UŻYCIA REJESTRÓW DLA RZĄDU

Rozproszone rejestry mogą mieć destrukcyjny wpływ. Ich zdolność przetwarzania odbywa się w czasie rzeczywistym, są zabezpieczone przed ingerencją osób trzecich i generują niskie koszty. Mają zastosowanie dla wielu usług i branż, takich jak usługi finansowe, branża nieruchomości, opieka zdrowotna i zarządzanie tożsamością. Mogą stanowić podstawę rozwoju innowacji sprzętowych i oprogramowania, takich jak inteligentne kontrakty i Internet Rzeczy. Co więcej, leżące u ich podstaw idee rozwiązań typu open source, transparentności i otwartej, sieciowej społeczności mogą być bardzo uciążliwe dla wielu sektorów.

Dzięki szerokiemu gronu interesariuszy, usług i funkcji, rząd powinien podjąć wiele różnorodnych działań. Wdrożenie rozproszonych rejestrów, podobnie jak każdej innej innowacji, stwarza niebezpieczeństwo dla tych, którym nie uda się lub nie są w stanie dostosować się do zaistniałych zmian. W szczególności, mogą stać się zagrożeniem dla takich instytucji jak banki i jednostki administracji państwowej, czyli dla tych którzy pośredniczą w wymianie dóbr oraz tych, którzy tworzą i utrzymują działające systemy regulacyjne. Wiele z podjętych działań będzie ulepszonych przez innowacje powstałe dzięki rozproszonym rejestrom, inne okażą się wyzwaniem.

Ostatecznie, najlepszym sposobem rozwoju technologii jest użycie jej w praktyce. Grupa ekspertów, która pracowała nad niniejszym raportem, opracowała kilka przykładów możliwych zastosowań omawianej technologii przez rząd brytyjski (zostały one omówione w rozdziale 6):

- *ochrona infrastruktury krytycznej przed cyberatakami*
- *zmniejszenie kosztów operacyjnych i śledzenie uprawnień do udzielenia wsparcia socjalnego, oferując jednocześnie większe społeczne włączenie finansowe*
- *przejrzystość i możliwość monitorowania, w jaki sposób wydawane są środki na pomoc międzynarodową*
- *wytworzenie możliwości dla wzrostu gospodarczego, wsparcie dla małych i średnich przedsiębiorstw, wzrost zatrudnienia*
- *ograniczenie oszustw podatkowych*

Każdy z tych przykładów zawiera propozycję zastosowania rozproszonych rejestrów, przedstawia zalety i ocenę stopnia zaawansowania technologii.

Niniejszy raport przedstawia jedynie niewielki fragment możliwych zastosowań, ale wierzymy, że jest dobrym punktem wyjścia, dzięki któremu rząd będzie mógł rozpocząć pilotażowy projekt wdrażania technologii w poszczególnych jednostkach administracji. Dlatego w naszym końcowym zestawie rekomendacji opowiadamy się za zastosowaniem technologii rozproszonych rejestrów i wykorzystaniem ich do rozwoju potencjału rządu.

Zalecenie 7:

Zrozumienie całego potencjału drzemiącego w rozproszonych rejestrach wymaga nie tylko przeprowadzenia badań, ale także zastosowania technologii w prawdziwych życiu. Rząd powinien przeprowadzić testy rozproszonych rejestrów w celu oceny przydatności tej technologii w sektorze publicznym.

Test powinny być realizowane w podobny sposób jak badania kliniczne. Ważne jest, żeby były raportowane i oceniane w celu zapewnienia jednolitości i osiągnięcia maksymalnej dyscypliny w czasie przeprowadzania testów. Wyniki i wnioski powinny znaleźć się w harmonogramie działań proponowanym w Zaleceniu 1.

Naszym zdaniem badania mogłyby być kontynuowane w następujących obszarach: ochrona krajowej infrastruktury, zmniejszenie tarć na rynku dla małych i średnich przedsiębiorstw, podział środków z ministerstw. W czasie przygotowywania niniejszego raportu spotkaliśmy jedynie niewielką liczbę urzędników, którzy dogłębnie analizowali możliwości wykorzystania technologii rozproszonych rejestrów przez administrację rządową. Rekomendujemy, aby te osoby były mocno wspierane i zachęcane do podejmowania kolejnych kroków w celu nawiązania współpracy między resortami rządowymi a koordynatorem, wdrażającym technologię rejestrów rozproszonych, którym na gruncie brytyjskim jest Government Digital Service.

Zalecenie 8:

Podobnie jak wyznaczenie odgórnego kierownictwa i koordynacji, istnieje także potrzeba budowania kompetencji i umiejętności w administracji państwowej. Proponujemy utworzyć międzyresortową grupę specjalistów, łączących środowiska analityczne i polityczne,

którzy stworzą i opracują możliwe przypadki użycia oraz utworzą centrum wiedzy i doświadczenia w administracji publicznej. Koordynatorem tego przedsięwzięcia na gruncie brytyjskim powinien być Government Digital Service i Data Science Partnership razem z Office for National Statistics (brytyjski organ administracji rządowej zajmujący się zbieraniem i udostępnianiem informacji statystycznych z zakresu gospodarki i demografii na poziomie narodowym, regionalnym i lokalnym) oraz Kancelarią Rządu. Jest to ważne dla rządu, by stymulować działania sektora biznesowego, działając jako klient, który zamawia rozwiązania wykorzystujące technologię rozproszonych rejestrów.

WNIOSKI – GLOBALNA PERSPEKTYWA

Wielka Brytania nie jest jedynym państwem, które dostrzega jak ważne są technologie rozproszonych rejestrów. Inne państwa, małe i duże, szybko wdrażają rozproszone rejestry – przykład Estonii pokazuje jak szybko może się rozwijać mały kraj, którego przywódcy mają świadomość skuteczności cyfrowych rozwiązań. Wielka Brytania potrzebuje jeszcze czasu, by stanąć w czołówce – w rzeczywistości jest to konieczne ze względu na znaczenie sektora finansowego i usług dla gospodarki Wielkiej Brytanii.

W rozdziale 7 Patrick Curry, Christopher Sier i Mike Halsall poddali analizie cechy narodów rozwiniętych cyfrowo i stwierdzili, są to:

- *wyedukowane cyfrowo kierownictwo*
- *wyznaczony departament rządowy, który zajmuje się transformacją cyfrową, z uwzględnieniem współpracy narodowej i ścisłej współpracy z wszystkim sektorami przemysłowymi*
- *narodowy plan oparty na współpracy, prowadzony przez sektor przemysłowy z publicznych wydatków inwestycyjnych*
- *posiadający wiedzę technologiczną, wykwalifikowani i doświadczeni urzędnicy wyższego szczebla w każdej rządowej organizacji*
- *inżynierowi i liderzy cyfrowego biznesu jako politycy*

Wciąż jesteśmy na wczesnym etapie nadzwyczajnej rewolucji postindustrialnej napędzanej przez technologię informacyjną. Ta rewolucja przynosi nowe istotne korzyści i ryzyka. Już teraz wiadomo, że pojawienie się technologii rozproszonych rejestrów zakłóci wiele istniejących sposobów prowadzenia działalności gospodarczej.

Najstarsza dokumentacja rachunkowa powstała ponad 5000 lat temu w Babilonie. Wiele glinianych tabliczek przetrwało stanowiąc dowód wczesnej rewolucji technologicznej w dziedzinie rozwoju pisania, liczenia i pieniędzy. Trudno przewidzieć czy zapisy cyfrowe będą miały taką samą trwałość jak gliniane tabliczki. Pewne jest jednak, że wdrożenie technologii rozproszonych rejestrów jest korzystne dla obywateli i gospodarki. Trzeba stawić czoło wielu wyzwaniom, by móc wyciągnąć jak najwięcej korzyści i zminimalizować szkody wynikające z rozwoju technologii informatycznych.

Definicje

Terminologia stosowana w tej nowej dziedzinie wciąż ewoluuje. Często określenia block chain (lub blockchain), rozproszone rejestry i współdzielone rejestry używane są zamiennie. Formalnie przyjęte definicje prawdopodobnie nie zadowolą wszystkich stron, jednak na potrzeby niniejszego raportu przyjęto następujące kluczowe określenia:

1. Block chain to typ bazy danych, która zawiera szereg zapisów zebranych w bloki (trochę jak zestawienie ich na jednym arkuszu papieru). Każdy blok jest podłączony do następnego przy użyciu podpisu kryptograficznego. Łańcuchy bloków, w których zapisana jest chronologiczna ciągłość prowadzonych transakcji stanowią rozproszony rejestr, który może być udostępniany i potwierdzany przez każdego, kto posiada odpowiednie uprawnienia. Jest wiele sposobów na potwierdzenie spójności i aktualności danej wersji rejestru, co powszechnie nazywane jest konsensusem (w przypadku bitcoina proces ten nazywany jest „wydobywaniem") – patrz niżej.

Jeśli uczestnicy tego procesu są zdefiniowani, mamy do czynienia z rejestrem ograniczonym (ang. permissioned ledger). Rejestr otwarty może być potwierdzany przez wszystkich – patrz poniżej.

Prawdziwą nowością technologii blockchain jest to, że nie jest to tylko baza danych – może również ustalać zasady transakcji (logika biznesowa), które są powiązane z samą transakcją.

To odróżnia technologię blockchainów od tradycyjnej bazy danych, w której zasady są często ustalone dla całej bazy danych lub aplikacji, a nie na poziomie transakcji.

2. Rejestry publiczne, dostępne dla wszystkich, takie jak bitcoin, nie mają jednego właściciela – nie mogą być w niczyim posiadaniu. Ideą otwartych rejestrów jest umożliwienie każdemu węzłowi wprowadzania nowych danych do rejestru i pewność, że wszystkie węzły posiadające rejestr mają jego identyczne kopie.

Rejestr jest odporny na cenzurę, co oznacza, że nikt nie może zablokować wprowadzenia transakcji do rejestru. Uczestnicy sieci utrzymują integralność rejestru osiągając konsensus sieciowy odnośnie jego aktualnego stanu – zgadzają się co do obowiązującej aktualnie wersji rzeczywistości transakcyjnej.

Rejestry publiczne mogą być wykorzystane jako światowy rejestr, który nie może być edytowany: na przykład do ogłaszania ostatniej woli i testamentu lub przypisania własności. Jednak stanowią one także wyzwanie dla instytucjonalnych struktur władzy i istniejącego przemysłu, a to może stanowić podstawę do zmian w polityce.

3. Rejestr ograniczony może mieć jednego lub wielu właścicieli. Gdy dodawany jest nowy rekord, integralność takiego rejestru jest sprawdzana w relatywnie ograniczonym procesie dochodzenia do konsensusu. Jest to realizowane przez zaufane węzły/podmioty – na przykład departamenty rządowe lub banki, dzięki czemu utrzymanie wspólnej uzgodnionwj wersji stanu transakcji jest znacznie prostsze niż proces uzgadniania wersji stanu w publicznych rejestrach. Zamknięte rejestry zapewniają wysoce weryfikowalne zestawy danych, ponieważ proces osiągania konsensusu daje w efekcie cyfrowy podpis, który pieczętuje aktualny stan i jest przy tym widoczny dla wszystkich dopisujących do rejestru stron. Wymóg, aby wiele departamentów rządowych potwierdzało rekord, gwarantuje wysoki poziom zaufania do bezpieczeństwa danego rekordu, w przeciwieństwie do obecnej sytuacji, gdy departamenty często udostępniają dane przy użyciu kartki papieru. Ograniczony rejestr jest zazwyczaj dużo szybszy niż publiczny.

4. Rozproszone rejestry są rodzajem bazy danych, która jest rozproszona na wiele miejsc, państw lub instytucji, i zazwyczaj jest publiczna. Zapis bywa najczęściej prowadzony w zapisie ciągłym, zamiast być grupowany w bloki, a nowe dane mogą być wprowadzane tylko wówczas, gdy uczestnicy uzyskają większościową zgodę (podobnie jak w głosowaniach parlamentarnych).

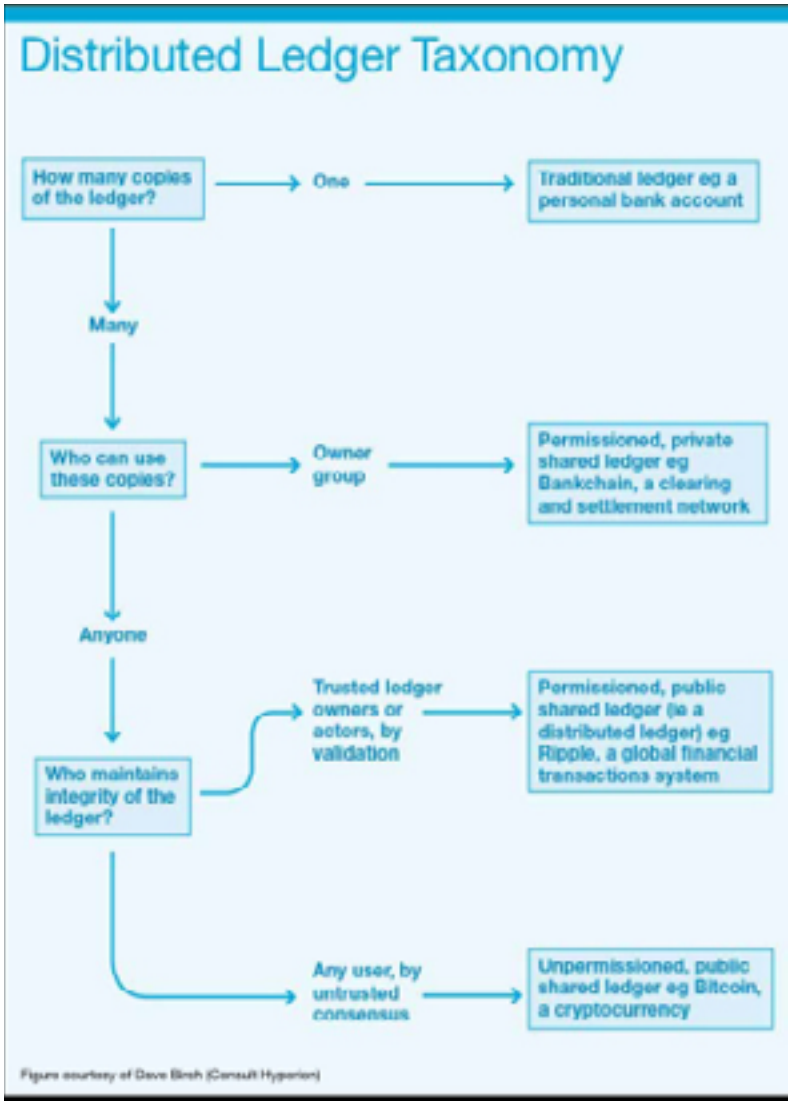
Rejestry rozproszone wymagają większej dozy zaufania do gwarantów i operatorów rejestru. Np. globalny system transakcji finansowych Ripple wybiera grupę stron poświadczających (nazywaną Unique Node Validators – gwaranci unikatowych węzłów), ufając, że nie zmówią się oni w celu oszukania uczestników transakcji. Wybór jest dokonywany spośród maksymalnie 200 znanych, nieznanych i częściowo znanych gwarantów. W ten sposób uzyskuje się wspólny podpis elektroniczny potwierdzający stan transakcyjny, który, jak się uważa, jest mniej odporny na cenzurę niż używany przez bitcoin, ale za to znacząco szybszy i mniej kosztowny energetycznie.

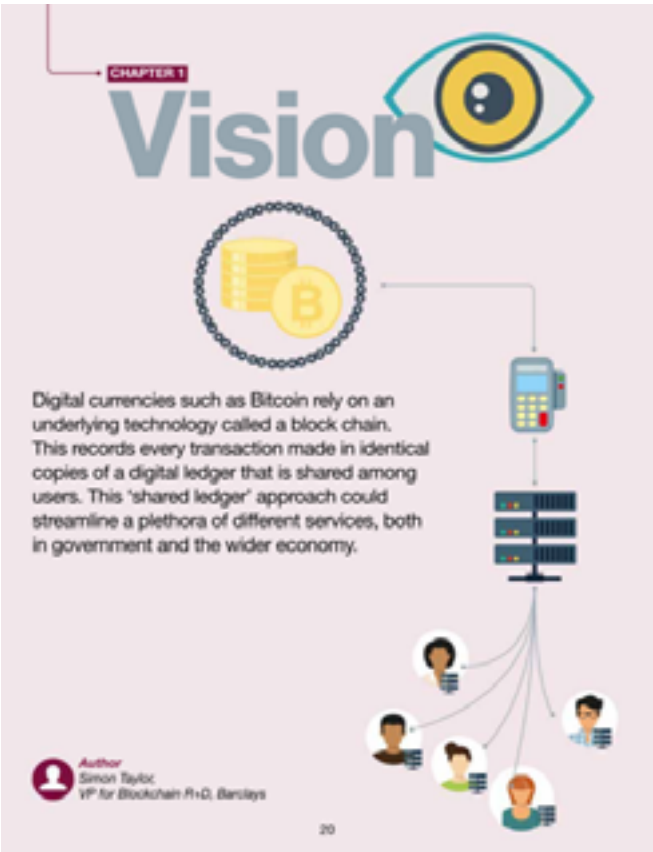
5. Rejestr wspólny to termin ukuty przez Richarda Browna, byłego pracownika IBM, aktualnie głównego specjalistę ds. Technologii w Distributed Ledger Group. Termin ten z reguły odnosi się do jakiejkolwiek bazy danych i aplikacji, używanej wspólnie przez podmioty z jakiejś branży lub konsorcjum lub też jest powszechnie dostępny. Jest to najszerszy, obejmujący najwięcej zjawisk, termin określający technologie z tej grupy.

Rejestr wspólny może korzystać z rejestrów rozproszo-

nych lub blockchainów, jako swojej bazy danych, ale często buduje warstwy uprawnień dla różnych typów użytkowników. W związku z tym termin "rejestr wspólny" może oznaczać wiele różnych wzorów rejestrów i baz danych, dostępnych do pewnego poziomu. Np. branżowy rejestr wspólny może mieć ograniczoną liczbę stałych gwarantów, którym powierza się utrzymywanie rejestru, co może się wiązać ze znaczącymi korzyściami.

6. Inteligentne kontrakty są umowami, których warunki są zapisane w języku komputerowym zamiast w prawniczym. Inteligentne kontrakty mogą być sporządzone przez systemy komputerowe, takie jak odpowiedni system rozproszonego rejestru. Potencjalne korzyści z zastosowania inteligentnych kontraktów obejmują: niskie koszty zawierania, wykonania i egzekwowania umowy. Potencjalne ryzyko to zależność od systemu komputerowego, który realizuje umowę. Na tym etapie, zagrożenia i korzyści są w dużej mierze teoretyczne, ponieważ technologia inteligentnych kontraktów jest jeszcze w powijakach, i upłynie jeszcze dużo czasu zanim zostanie wdrożona.





ROZDZIAŁ 1: Koncepcja

Cyfrowe waluty takie jak bitcoin zapoczątkowały nowy sposób śledzenia transakcji finansowych. Ich podstawa technologia – zwana blockchainem (łańcuchem bloków) – rejestruje każdą transakcję dokonaną w tej walucie w identycznych kopiach rozproszonego rejestru, który jest udostępniany między użytkownikami danej waluty.

Instytucje finansowe, organy nadzoru, banki centralne i rządy badają możliwości wykorzystania możliwości „współdzielonych rejestrów", aby usprawnić różne usługi, zarówno w administracji publicznej jak i w całej gospodarce.

Wiele z tych potencjalnych zastosowań jest możliwych w średnioterminowej perspektywie. Jednak długi cykl budowy rozwiązań w sektorze rządowym i prywatnym, i obiecujące wstępne prognozy, pokazujace potencjalnie znaczące korzyści sugerują, aby urzędy i instytucje administracji już teraz zastanowiły się się jak wykorzystać nową technologię. Poniższy rozdział nakreśla te możliwości.

CZYM JEST WSPÓŁDZIELONY REJESTR?

Współdzielony rejestr jest w zasadzie bazą danych, która zapisuje informacje kto jest właścicielem finansowych, fizycznych lub elektronicznych aktywów, na przykład diamentów, jednostek waluty, towarów w kontenerze spedycyjnym. Co istotne, każdy uczestnik rejestru może trzymać kopię łańcucha bloków, która jest uaktualniana automatycznie za każdym razem, gdy pojawia się nowa transakcja. Bezpieczeństwo i zgodność informacji jest zapewniona dzięki matematyce – szczególnie kryptografii, która gwarantuje, że wszystkie kopie rejestru są identyczne. Prawie wszystko, co może być zapisane na papierze, może istnieć w współdzielonym rejestrze (szczegółowe omówienie technologii współdzielonych rejestrów znajduje się w Rozdziale 2).

Od czasu uruchomienia w 2008 roku, bitcoin oparty jest na technologii łańcucha bloków. Wokół tej kryptowaluty i jej podstawowych zasad wyrosło wiele stereotypów i błędnych przekonań. Wszystko za sprawą Silk Road, internetowego czarnego rynku, który spowodował, że wiele osób kojarzy bitcoin z praniem brudnych pieniędzy i terroryzmem. To błędne przekonanie wciąż wpływa na sposób, w jaki myśli się o technologii łańcucha bloków. W rzeczywistości współdzielone rejestry i bazy danych, dzięki czterem ważnym właściwościom technologii blockchain, mogą być z korzyścią wykorzystane w usługach administracji publicznej i finansowej.

1. ***Uzgadnianie Poprzez Kryptografię.*** *Obecnie instytucje takie jak przedsiębiorstwa i administracja wysyłają do siebie wiadomości, by przekazać szczegóły transakcji. Po odebraniu wiadomości, każda instytucja aktualizuje swój własny rejestr. Jednak w dzisiejszych czasach nie ma łatwego sposobu, aby zapewnić, że kopie są spójne. Łańcuch bloków może to rozwiązać na kilka sposobów: na przykład poprzez współdzielenie podstawowych danych lub dostarczenie dowodów do weryfikacji bazy danych. Takie podejście może być również zastosowane w przypadku rządowych baz danych. Różni użytkownicy danego współdzielonego rejestru uzgadniają wersję stanu danych źródłowych (osiągają konsensus) za pomocą wielu różnych algorytmów konsensusu (na przykład: dowód wykonanej pracy – ang. Proof of Work, Dowód Stawki – ang. Proof of Stake)*

2. ***Powielane w Wielu Instytucjach.*** *Strony mogą mieć kopię części lub wszystkich danych, dzięki czemu jest mniej prawdopodobne, że istnieje pojedynczy błąd. Wszyscy użytkownicy danego rozproszonego rejestru pilnuj≤ą wzajemnie zgodności i prawdziwości bieżącego stanu transakcyjnego. W przypadku tradycyjnych technologii baz danych takie działanie generuje koszty i komplikacje przy realizacji projektów IT. Dodatkową zaletą tej technologii jest to, że jeśli jedna kopia zostanie zaatakowana, to pozostałe są bezpieczne. Taki rejestr jest relatywnie odporny na ataki cybernetyczne. Strony mogą również potwierdzić, że dane rekordy zostały dodane poprzez wykonanie podobnych obliczeń.*

3. Przejrzysta Kontrola Dostępu. Technologia rozproszonego rejestru używa kluczy i podpisów, aby kontrolować i przypisywać konkretnym podmiotom uprawnienie wewnątrz współdzielonego rejestru. Te klucze mogą zostać przypisane do konkretnych funkcji tylko pod pewnymi warunkami. Na przykład, organ regulacyjny może mieć klucz, który pozwala obserwować wszystkie transakcje instytucji, ale tylko wówczas, gdy klucz będący w posiadaniu sądu nadaje mu takie uprawnienia.

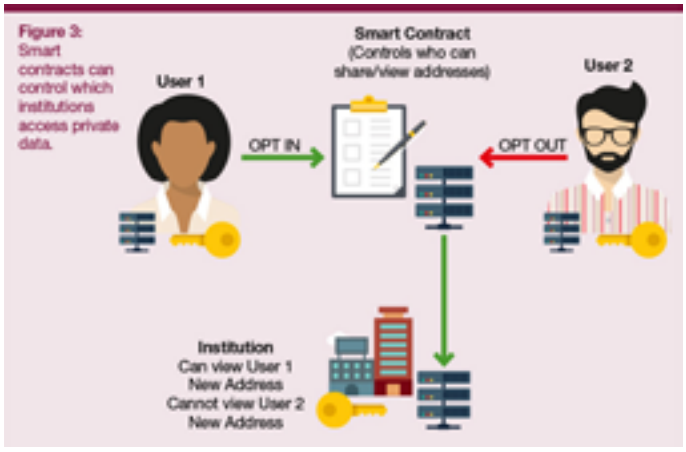
4. Przejrzyste mechanizmy Jawność i Prywatność. W związku z tym, że wiele stron ma kopię rejestru (punkt 1) i wiele stron może weryfikować każdy rekord (punkt 2), współdzielony rejestr ma wysoki stopień jawności. To pozwala organowi regulacyjnemu lub niezależnej instytucji, na przykład wymiarowi sprawiedliwości, sprawdzić czy zawartość bazy danych nie została wyedytowana lub zmieniona w nieuczciwy sposób. W odpowiednich warunkach pozwala im również odblokować rekordy, które normalnie byłyby całkowicie prywatne i niewidoczne. Mogłoby to być przydatne dla sektora biznesowego, na przykład banków, do sprawozdawczości, zapobiegania oszustwom, a także upoważnić obywateli do kontrolowania administracji rządowej (patrz Rozdział 5). Rekordy są dodawane przy pomocy unikalnego podpisu kryptograficznego, który potwierdza, że uprawniony użytkownik dodał odpowiedni rekord zgodnie z określonymi przepisami. Daje to możliwości, które wcześniej były bardzo drogie lub trudne do osiągnięcia.

CZYM SĄ INTELIGENTNE KONTRAKTY?

Jeśli łańcuch bloków jest bazą danych, wówczas inteligentne kontrakty są warstwą aplikacji, która sprawia, że wiele z obietnic związanych z technologią blockchain staje się rzeczywistością. Wiele tradycyjnych umów nie ma żadnego związku z kodem komputerowym, który egzekwuje ich realizację (patrz rozdział 3). W wielu przypadkach umowa papierowa jest archiwizowana, a oprogramowanie będzie egzekwować przybliżone warunki umowy zapisane w kodzie komputerowym.

Jest to dość skuteczne, gdy rejestrujemy się do korzystania z jednej usługi (na przykład usługi VOD), ale staje się dość trudne, w momencie, gdy dostarczamy jednemu użytkownikowi wiele skomplikowanych usług (na przykład aktualizacja adresu w wielu bazach ministerstw). Skutkowałoby to jeszcze bardziej skomplikowanym procesem ochrony danych i prywatności, który pozwoliłby zarządzać poufnością i prywatnością jednostki w gwarantowany sposób. Ponadto działania takie jak udostępnianie danych i uzgadnianie umów pozostałyby raczej na papierze niż w formie zautomatyzowanej.

Łącząc kluczowe cechy rozproszonego rejestru (uzgadnianie poprzez kryptografię, powielanie w wielu instytucjach, przejrzysta kontrola dostępu, przejrzyste zasady jawności i prywatności) z inteligentnymi kontraktami, możemy stawić czoła niektórym trudnościom, zyskując możliwość albo powielania danych albo udostępniania ich na ściśle określonych warunkach. Jeśli dwóch użytkowników podpisze inteligentny kontrakt, będzie on zawierał skrypt, który obsłuży dane we wszystkich dotyczących go współdzielonych rejestrach. Mogłoby to ułatwić automatyzację lub nawet wyeliminować procesy obsługi w instytucjach administracji publicznej i sektora publicznego, co wpłynie na efektywność i wzrost wydajności. Istnieją też inne problemy takie jak zarządzanie dotychczasowymi bazami danych i procesami, ale właśnie tam znajdą zastosowanie Inteligentne kontrakty.



W alternatywnym scenariuszu, Użytkownik 1 wybiera inteligentny kontrakt w współdzielonym rejestrze pozwalający udostępniać adres instytucji, która posiada „niebieski klucz" (może to być wiele innych instytucji z wieloma innymi kluczami). Zaś Użytkownik 2 zdecydował się tylko udostępnić adres, więc instytucja posiada tylko kopię

najnowszego adresu od Użytkownika 1. Może być to przydatne, gdy osoba zmienia adres w urzędzie gminy, ponieważ zmiana mogłaby być widoczna w bazach danych paszportów, prawa jazdy lub innych istotnych urzędowych bazach danych. Usługi takie jak Onename.io wykorzystują tę koncepcję z sieciami społecznościowymi, ale może to być rozszerzone na inne instytucje.

Rozważa się wykorzystanie inteligentnych kontraktów w szerszym kontekście, w szczególności do sprawdzania zgodności z przepisami, identyfikowalność produktu i zarządzania usługami, a także do walki z podróbkami i oszustwami w następujących sektorach:

- *Żywnościowym*
- *Usług finansowych*
- *Energetycznym*
- *Farmaceutycznym*
- *Zdrowotnym*
- *Przemysłu kosmicznego*
- *Przemysłu lotniczego*
- *Telekomunikacji*
- *Usług IT*
- *Transportowym*
- *Rolniczym*
- *Przemysłu zajmującego się wydobywaniem ropy naftowej i gazu ziemnego*

(Część z powyższych zagadnień została omówiona w rozdziale 6 i 7).

Podsumowując, inteligentna umowa jest przydatna, gdy urządzenia, firmy czy ludzie chcą stworzyć porozumienie cyfrowe, z kryptograficzną pewnością, że umowa została dotrzymana i wykonana w rejestrach, bazach danych lub rozliczeniach wszystkich stron umowy.

WIZJA PRZYSZŁOŚCI

Kluczową rolą otwartego rządu jest odpowiedni podział zasobów wśród swoich obywateli – zarówno tych indywidualnych jak i zbiorowych. To wykracza poza dystrybucję zasobów monetarnych i obejmuje społeczne wartości niematerialne, takie jak bezpieczeństwo, demokracja, warunki utrzymania praworządności oraz warunki gospodarcze tj.; promowanie wolnego rynku, utrzymywanie niskiej i stabilnej inflacji, ochronę praw własności prywatnej i umów gwarancyjnych. Ten podział z kolei opiera się na porozumieniu między obywatelami a rządem co do zasad ustanawiania przepisów. Jako że otwarty model demokracji rozwinął się, a aparat rządowy (mechanizm, dzięki któremu odbywa się zarządzanie funduszami) stał się wielki, bardziej scentralizowany i bez wątpienia oddalony od indywidualnego obywatela, pozyskiwanie zasobów (pieniężnych) poprzez różnego rodzaju podatki stało się skomplikowane i kosztowne, tak jak ich redystrybucja poprzez wsparcie socjalne, dotacje czy emerytury. Złożoność ta może częściowo wynikać z scentralizowanego charakteru tego procesu.

Sektor prywatny zaczął zdawać sobie sprawę, że scentralizowany model oferuje słabą obsługę klienta, nie jest ekonomiczny i nie uwzględnia w pełni korzyści z handlu elektronicznego oraz możliwości cyfrowych. Rządy zaczynają dostrzegać, że oczekiwania obywateli powinny być spełnione w podobny sposób, w czasie rzeczywistym, zarówno osobista jak i cyfrowa obsługa powinna być możliwa dla wszystkich usług publicznych. Zastosowanie współdzielonych rejestrów oraz inteligentnych kontraktów daje możliwość, aby rząd przewodził w tej dziedzinie, zapewniając przy tym, że z korzyści płynące z technologii czerpią również osoby które najbardziej tego potrzebują, a nie tylko te, które na to stać.

Ten trend jest również widoczny we wzroście mniej formalnej „ekonomii współdzielenia" oraz w popularnym obecnie fenomenie mediów społecznościowych, który doprowadził do zjawisk społecznych takich jak Arabska wiosna i ruch Occupy. Pokazują one zmianę sposobu w jaki społeczeństwo się komunikuje i organizuje. Do tej pory jednak nie było skutecznego sposobu, aby korzystać z decentralizacji bezpiecznie, jednocześnie kontynuując promowanie wolnych rynków i umów gwarancyjnych. Często mówi się, że powodem, dla którego nigdy nie przenieśliśmy demokracji online, jest to, że nie ma sposobu, aby zachować kontrolę nad tym procesem. Stworzenie takiego systemu bez wątpienia wymaga dużych środków finansowych i scentralizowanego systemu tożsamości.

Zakładając, że chcemy tego uniknąć – właściwości technologii blockchain (rejestr ujednolicony poprzez zapisy kryptograficzne, możliwości replikowania do wielu instytucji, kontrola dostępu, ziarnista przejrzystość i prywatność) mogłyby być stosowane z korzyścią dla obywateli.

Dodatkowo, wczesne zaangażowanie rządu w zakresie rozwoju i wdrażania technologii blockchain stwarza możliwości zminimalizowania złożoności i kosztów sprawowania władzy. To doprowadziłoby do bardziej osobistej, natychmiastowej i potencjalnie swobodniejszej podstawy zarządzania, co z kolei przyczyniłoby się do zwiększenia kosztów zgodności, efektywności kosztowej i odpowiedzialności za działania.

DZIAŁANIA MAJĄCE NA CELU WYKORZYSTANIE TECHNOLOGII BLOCKCHAIN

Technologia wspólnych rejestrów jest aktywnie promowana i rozwijana w najsilniejszych światowych gospodarkach jak Stany Zjednoczone, Chiny, Singapur i w Ameryce Łacińskiej. Wielka Brytania ma szansę konkurować w tym wyścigu poprzez zrozumienie i wspieranie rozwoju tego wschodzącego sektora.

Potencjalne zaangażowanie rządu w technologię blockchain, nazywaną także zamiennie DLT, może być rozpatrywane z trzech perspektyw

1. *Rząd: Administracja państwowa*
2. *Rząd: Ustawodawstwo*
3. *Rząd: Zarządzanie gospodarką*

Rząd: Administracja państwowa

Administracja państwowa ma szereg istotnych obowiązków, na które ta technologia mogłaby mieć istotny wpływ, koncentrując się na powiązaniu prywatności, przenoszeniu danych i możliwości sensorycznych technologii mobilnych (Zob. Rozdział 6. dla szczegółowych przykładów).

Rząd: Ustawodawstwo

Technologia blockchain/DLT jest stosunkowo młodą dziedziną i prawdopodobnie będzie można zobaczyć jeszcze kilka jej etapów rozwoju. Dlatego też działania rządu mogą być ukierunkowane na trzy oddzielne „perspektywy" w tym procesie.

Perspektywa 1:

Wspieranie rozwijających się ekosystemów

Istnieje już szereg dostawców prowadzących wymianę walut cyfrowych, wirtualnych „portfeli" oraz innego rodzaju usług, zarówno w ekosystemie bitcoina i w innych systemach współdzielonych rejestrów. Uznając, że technologia i przedsiębiorstwa będą nadal dojrzewać, Perspektywa 1. powinna obejmować następujące działania:

- *Działania wymagające procedur w celu weryfikacji tożsamości klientów (znane jako reguła Poznaj swojego klienta, ang. "Know Your Customer" KYC)*
- *Wydawanie wytycznych dla sektora bankowego, aby wykazać różnicę między typami spółek działających w tej przestrzeni: (i) dokonujących transferu wartości poprzez system blockchain (ii) dostarczających oprogramowanie dla przemysłu i użytkowników blockchaina; (iii) dostarczających oprogramowanie oparte na blockchainie pozwalające rozwiązywać typowe problemy*
- *Ustanowienie standardów bezpieczeństwa dla dostawców portfela wirtualnego*
- *Otwieranie możliwości dla środowisk akademickich i startupów aby zbadać niedoskonałości w środowisku blockchain tj.: (i) ustanowienie odpowiednich struktur technicznych; (Ii) ustalenie, w jaki sposób technologia może zwiększyć zdolności weryfikacji tożsamości klienta, przeciwdziałania praniu pieniędzy i zapobiegania przestępczości; (Iii) określenie, w jaki sposób wykorzystanie wirtualnych portfeli z wielokrotnymi podpisami cyfrowymi może zmienić komunikację na linii rząd obywatel i umożliwić obywatelom kontrolę i audyt własnych danych przechowywanych przez rząd*
- *Pozyskiwanie partnerów do utrzymania skoordynowanego dialogu pomiędzy rządem i przemysłem*

Perspektywa 2:

Próby i pilotaże

W miejscach, gdzie rząd ma możliwości, może rozpocząć wykonywanie pilotaży wykorzystania technologii. Istotne zagadnienia, które warto wziąć pod uwagę:

- *Jakie kluczowe programy mogą być beneficjentami wspólnych rejestrów / technologii współdzielonych, zdecentralizowanych baz danych?*
- *Gdzie pilotaż może wspierać politykę (reforma systemu emerytalnego, reforma opieki społecznej)?*
- *Gdzie pilotaż pozwoli uzyskać kluczową wiedzę i doświadczenie?*

Perspektywa 3:

Pozycjonowanie Wielkiej Brytanii jako lidera w globalnym wyścigu

Dotychczas znaczna część inwestycji średnio- i długoterminowych w technologię blockchain/DLT skupiała się na bitcoinie oraz Zachodnim Wybrzeżu Stanów Zjednoczonych. Jednakże obecnie pojawiają się nowe możliwości wykorzystania tej technologii w innych aplikacjach.

Wielka Brytania powinna zwrócić uwagę na tą szansę i stworzyć wytyczne w tym zakresie za pośrednictwem swoich organów regulacyjnych (więcej informacji na temat zarządzania i regulacji rozdz.3).

Wielka Brytania mogłaby stworzyć centrum doskonalenia technologii i dołączyć blockcian/DLT do globalnego FinTech/UK Trade and Investment Agenda.

Rząd: Zarządzanie gospodarką

Aby zrozumieć, w jaki sposób rząd może najlepiej wspierać i realizować korzyści technologii blockchain/DLT, pomocna będzie analiza możliwości zastosowania jej w kilku obszarach: usługach finansowych, ubezpieczeniach i innych branżach.

Usługi finansowe

Przykłady, gdzie technologia może być stosowana w sektorze finansowym:

1. Zwiększenie efektywności rynków kapitałowych

2. Zmniejszenie oszustw i zwiększenie efektywności rozliczeń w handlu

1. Zwiększenie efektywności na rynkach kapitałowych

Rynki kapitałowe nadal opierają się na papierowych księgach dokumentując handel między kontrahentami. Zdolność do potwierdzenia („akceptacji") transakcji i uzyskania pewności, że kontrahent ją zaakceptował ma szczególne znaczenie. Obecnie, wymaga to współpracy i zaufania. Wiele z opłat oraz wiele kosztów stałych bankowości wynika z koncepcji współzależności. W praktyce, jeden bank musi polegać na procesach innego banku i nie ma możliwości, aby zweryfikować zachowanie drugiego banku. Ponadto audyt danych jest kosztowny i ma miejsce dopiero po transakcji. Duże banki szukają teraz odpowiednich rozwiązań, pozwalających na wprowadzenie większej wydajności. Technologia blockchain może pomóc, pokazując łańcuch transakcji (ujednolicony kryptograficznie), a strony zaangażowane mogą pokazać to przejrzyście instytucjom kontrolnym.

2. Zapobieganie malwersacji i zwiększenie efektywności rozliczeń w handlu

Rozliczenie w handlu wygląda tak samo od tysięcy lat. Często zdarza się, że co najmniej 5 lub 6 stron jest zaangażowanych w proces kupna lub sprzedaży towaru (np. kupujący, bank kupującego, agencja transportowa, kurier, sprzedawca i bank sprzedającego). Podejmowano próby standaryzacji i stworzenia centralnego narzędzia do rozliczeń w handlu. Rozproszone rejestry posiadają w tym zakresie wiele zalet.

- *Częściowo „ograniczony" system może umożliwić bezpieczne podpisanie dokumentu w formie papierowej (np. znak rozpoznawczy stwierdzający, które, ile i jaki kolor produktów był w pojemniku, itp.). Następnie może być podpisany (w sposób dający się udowodnić i cyfrowo) przez każdą ze stron. (Kluczowe właściwości: przejrzystość umowy; kryptograficzne ujednolicenie).*
- *Zamiast przechowywania dokumentów, jak to ma miejsce obecnie, wspólny rejestr zachowywałby poświadczenie stanu dokumentów. Jeżeli system zostałby wprowadzony szerzej, dokumenty mogłyby być dystrybuowane za pośrednictwem wspólnych rejestrów, a nie jak dotychczas drukowane i podpisywane. (Kluczowe właściwości: wysoka skalowalność i powtarzalność).*

Przemysł I Instytucje

3. Kontrola aktywów i pewność pochodzenia

Wiele przedmiotów, takich jak dzieła sztuki, czy sprzęt elektroniczny posiada cyfrowe oznaczenia. Jednakże do tej pory nie ma globalnego rozwiązania do śledzenia i namierzania oznakowanych przedmiotów, które jednocześnie oferowałyby kontrolę uprawnień, określającą – kto może mieć wgląd, w jaki sposób aktywa są zarządzane i gdzie się znajdują. Większość organizacji opiera się na dokumentach papierowych w celu sprawdzenia pochodzenie produktu. Jeżeli jednak dokument jest sfałszowany, weryfikacja staje się niemożliwa. Gdyby chociaż w części tego łańcucha dostaw użyty został wspólny rejestr i podpisy cyfrowe, wszystkie strony miałyby pewność, że dokumenty nie zostały podmienione lub sfałszowane w jakikolwiek sposób.

Przykładowo Provenance.org jest startupem używającym technologii blockchain – umożliwia sprawdzenie przez sprzedawców detalicznych pochodzenie i stanu produktów. Handel detaliczny obecnie bazuje na dokumentach papierowych do potwierdzania pochodzenia przedmiotów transakcji, ale nie ma sposobu, który zapewniłby, że właściwa osoba w określonym czasie podpisała dane dokumenty. Używając technologii blockchain – konkretna osoba podpisuje cyfrowo umowę swoim prywatnym kluczem. Daje to gwarancję, że właśnie ta osoba podpisała dokument w określonym dniu i godzinie. Charakter technologii blockchain spowoduje, że będzie to widoczne dla każdego kupującego posiadającego odpowiednie uprawnienia.

4. Poufne przetwarzania danych z kontrolą użytkownika

Dokładność danych i ich poufne udostępnianie to kluczowe wyzwania dla wszystkich instytucji. Posiadając dodatkowe dane, które są zatwierdzone jako prawdziwe przez jedno lub kilka zaufanych źródeł (np. rząd, banki), firmy ubezpieczeniowe mogłyby tworzyć dokładniejsze specyfikacje produktów, cen i zniżek. Głównym problemem jest przeprowadzenie tego w bezpieczny sposób, przy jednoczesnej gwarancji, że obywatel kontroluje swoje dane.

Technologia blockchain dostarczałaby transparentną dokumentację, w jaki sposób uzyskano dostęp do każdej z danych, np. przy użyciu rozwiązań typu Guardtime. Wykorzystanie takich rozwiązań jak TEE (trusted execution enviroment) w telefonach komórkowych, czy TrustZone firmy ARM, spowodowałoby, że każda próba dostępu do przechowywanych danych rejestrowana byłaby w blockchainie. Jedyną możliwość zmiany danych miałyby osoby posiadające pozwolenie od firmy ubezpieczeniowej. Każda próba zmiany lub dostępu do danych natychmiastowo byłaby widoczna dla zarządzających.

Technologia wspólnych rejestrów w połączeniu z prostym interfejsem użytkowników telefonów komórkowych, potencjalnie pozwoliłaby ogromnie uprościć złożone procedury zarządzania bezpieczeństwem. Instytucje, które zdecydują się zrobić krok, będą musiały zdobyć zaufanie społeczeństwa, a prowadzone wcześniej prace badawcze i wdrożenia będą pomocne w osiągnięciu tego celu.

5. Urządzenia (połączony "Internet Rzeczy")

Trudnością może być zebranie dokładnych danych na temat urządzeń przemysłowych stosowanych w wielu obszarach, np. w transporcie, mediach czy rolnictwie w czasie rzeczywistym. Wraz z pojawieniem się koncepcji Internetu Rzeczy (Internet of Things, IoT), niektóre z tych trudności są rozwiązywane za pomocą niedrogiego sprzętu, ale to zastosowanie jest potencjalnie narażone na ataki. Według raportu IBM Institute for Business Value: „Wynik analizy: szybki wzrost liczby urządzeń, które nie będą droższe niż ich mniej wyspecjalizowane odpowiedniki, a dodatkowo będą w stanie funkcjonować jako część kompleksowego i zintegrowanego systemu. W sieci na skalę IoT, zaufanie może być bardzo trudne i drogie do wypracowania, jeśli nie niemożliwe do osiągnięcia. Prywatność i anonimowość dająca użytkownikom kontrolę własnej prywatności musi być integralną częścią konstrukcji cały czas rozwijającego się IoT. Obecne modele zabezpieczeń oparte na oprogramowaniu zamkniętym (określane jako "security through obscurity") są przestarzałe i muszą być zastąpione przez nowsze podejście – bezpieczeństwo dzięki przejrzystości. W naszej wizji zdecentralizowanej IoT, technologia Blockchain stanowi ramy ułatwiające przetwarzanie transakcji i koordynację pomiędzy urządzeniami. Każdy zarządza swoimi funkcjami działaniami, co prowadzi do powstania „Internetu zdecentralizowanych, autonomicznych rzeczy" Internet of Decentralized, Autonomous Things – a przez to demokratyzacji świata cyfrowego.

Jeśli każde urządzenie działa zarówno autonomicznie i zarazem jako część systemu, nie ma jednostkowego punktu awarii. W tym przypadku użycia, instytucje zastosowałyby urządzenia IoT i zyskałyby wiele korzyści związanych systemem czasu rzeczywistego i zdolnością przyłączeniową, zarysowane w sprawozdaniu Government Office for Science report on the IoT. Wspólne rejestry i technologia blockchain dostarczają nowych modeli biznesowych i technologicznych pozwalających na wprowadzenie wyższego poziomu bezpieczeństwa IoT.

Przykład 1: Ciągnik, który działa jako autonomiczna jednostka, może uprawniać wielu rolników w danym obszarze do użytkowania, umożliwiając stosowanie modelu płatności za faktyczne użycie. Ma on również zdolność do rejestrowania i opłacania danych o pogodzie oraz bezpośredniego komunikowania się z producentem w celu przeprowadzenia konserwacji i napraw.

Przykład 2: Sprzęt przemysłowy może być uprawniony do zamawiania nowych części, o ile przedstawi dowód, że jest prawdziwe i ma autoryzację. Może to również prowadzić do nowych sposobów finansowania takiego sprzętu oraz nowych rynków opartych na wydajności lub efektywności sprzętu.

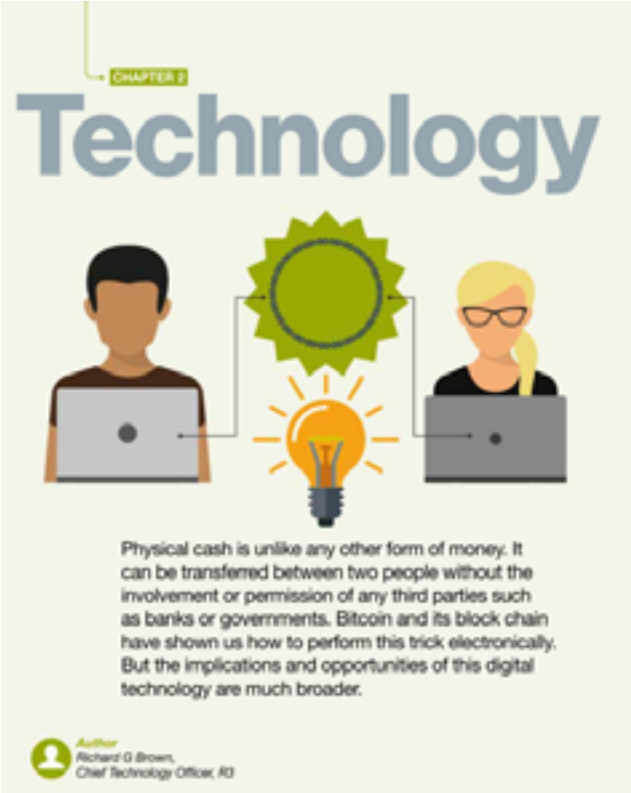
Wnioski

Możemy wyobrazić sobie przyszłość, w której technologia ta tworzy rodzaj „glass government", który jest bardziej odpowiedzialny względem obywateli. Istnieje więcej możliwości użycia tej technologii, a wraz z postępem technologicznym jest to coraz bardziej możliwe do wdrożenia. Może to przyczynić się do osiągnięcia celów polityki.

Kluczowe kwestie dla ministrów i administracji państwowej:

Technologia pomimo wczesnego stadium rozwoju jest bardzo obiecująca. Aby umożliwić jej rozwój ważne jest, aby zrozumieć jak istotne jest połączenie następujących czynników:

- *Ujednolicenia poprzez kryptografię*
- *Bezpiecznego powielania / replikacja danych w wielu miejscach na dużą skalę*
- *Udowodnienie transparentności*
- *Może być stosowane na trzech płaszczyznach*
- *Wspieranie kształtującego się ekosystemu*
- *Przeprowadzenie prób oraz pilotaży*
- *Pozycjonowanie Wielkiej Brytanii jako światowego lidera*



ROZDZIAŁ 2: Technologie

Fizyczna gotówka różni się on od wszystkich innych form pieniądza. Gotówkę mogą sobie przekazać dwie obce sobie osoby bez udziału lub zgody stron trzecich, takich jak banki i rządy. Bitcoin i blockchain pokazały, jak w taki sam sposób posługiwać się pieniądzem w postaci elektronicznej. Wpływ i możliwości tej technologii cyfrowej są znacznie szersze.

WPROWADZENIE

Bitcoin jest formą cyfrowej waluty, której emisja jest kontrolowana przez zdecentralizowaną sieć komputerów, a nie przez banki centralne. Sieć ta opiera się na kryptografii i innych technikach, wykorzystywanych do regulowania podaży bitcoinów. Może ona również kontrolować kto w danym momencie jest ich właścicielem. Banki kontrolują salda swoich klientów w rejestrach. Bitcoin również używa rejestru, utrzymywanego przez zdecentralizowaną sieć komputerów – tzw. rejestr rozproszony. Z chwilą dodania do rozproszonego rejestru nowych grup transakcji, zawierają one odniesienie do istniejących już grup, tak aby wszyscy użytkownicy mogli zweryfikować pochodzenie pozycji w rozproszonym rejestrze. Te partie nazywane są blokami, a całość łańcuchem bloków – blockchain.

Ten rozdział wyjaśni więcej na temat koncepcji, omówi jej znaczenie oraz pokaże, jak może stać się podstawą znacznie szerszego pakietu aplikacji, a także jak może ewoluować od podstawowej wersji do rozbudowanego oprogramowania użytkowego.

CZYM JEST PIENIĄDZ?

20-funtowy banknot jest czymś niezwykłym. Wręczając go komuś, od razu przekazujemy taką wartość innej osobie. Nie potrzebna jest osoba trzecia do sprawdzenia transakcji. Jeżeli dwie osoby są same, nikt inny nie wie, że tak się stało i nie może transakcji powstrzymać. Ale transfery bezpośrednie (peer-to-peer) działają tylko z bliskiej odległości. Już, aby przesłać 20 funtów do kogoś w innym mieście lub kraju, musimy zaufać innym, a także przekazać im pewien stopień kontroli np.: pracownikowi poczty, który wydaje kopertę zawierającą gotówkę lub bankowi, który dokonuje elektronicznego transferu środków. Jeśli bank uzna, że pieniądze są związane z nielegalną działalnością, może powstrzymać transakcję lub przejęć środki.

Światowy system finansowy – system płatności, robocze kontakty między bankami, systemy wymiany informacji bankowej, takie jak SWIFT (Society for Worldwide Interbank Financial Telecommunication) – są bezpośrednią konsekwencją tego, że gotówka jest fundamentalnie różna od każdej innej postaci pieniądza. Tylko materialny pieniądz jest instrumentem okaziciela i tylko w takiej postaci może być przenoszony bez czyjejś zgody – jest wówczas „odporny na cenzurę».

Tak wydawało się do 2008 roku, kiedy pojawił się bitcoin. Jego twórca twierdził, że jest to system „peer-to-peer" dla elektronicznej gotówki, który może być w pełni kontrolowany przez właściciela i wysłany do kogokolwiek bez potrzeby zgody banku lub narażania się na konfiskaty.

Użytkownicy sieci bitcoin posiadają kopię wszystkich transakcji, ułożonych w łańcuch pospinanych ze sobą «bloków", której historię mogą prześledzić od początku. Każdy blok jest kryptograficznie powiązany z poprzednim blokiem, tworząc blok łańcuchów (blockchain), zachowuje pełną historię transakcji, a tym samym działa jak rozproszony rejestr. Użytkownicy mogą sprawdzić rejestr poprzez różne aplikacje (takie jak Coinbase lub Blockchain.info – nie mylić z podstawową koncepcją techniczną), a każda kopia rejestru jest synchronizowana za pomocą algorytmów utworzonych w celu osiągnięcia konsensusu, czyli „porozumienia" na temat stanu rejestru.

Bitcoin nie pojawił się znikąd. Badania nad wirtualnymi systemami monetarnymi prowadzone były już przed dekadami, a każdy z potrzebnych elementów systemu już istniał. Przełomem dla bitcoina było połączenie istniejących technik w innowacyjny sposób. Ponadto rozwinęła się wówczas idea open source. Internet był już dojrzały, a ludzie gotowi na ideę alternatywnych systemów monetarnych. Konstrukcja systemu zakłada, że

stopniowo coraz trudniejsze (w praktyce niemożliwe) staje się korygowanie starszych bloków. W momencie, kiedy transakcja jest potwierdzona w wymagany sposób, nie może zostać cofnięta, co czyni ją odporną na cenzurę. Podsumowując, bitcoin to naprawdę cyfrowy odpowiednik gotówki.

Nic dziwnego, że rządy oraz organy nadzorujące na całym świecie przyglądają się wynalazkowi z taką uwagą. Odporne na różne formy cenzury – jako de facto wirtualne papiery wartościowe na okaziciela wydają się być idealną walutą dla siatek przestępczych, a bitcoin stał się podstawową jednostką pieniężną Silk Road (nieistniejąca już platforma aukcyjna kojarzona z handlem narkotykami).

Jednak większość regulatorów, w tym agencje w Wielkiej Brytanii, nie zdecydowały się na zakaz posługiwania się bitcoinem, a wiele legalnych firm inwestuje w tego rodzaju technologie. Dlaczego?

CZYM JEST BLOCKCHAIN?

Blok to swoisty wykaz transakcji. Blockchain jest rejestrem tych bloków, z których każdy nawiązuje do poprzedniego. Jednak, gdy ludzie mówią o blockchainie, mają tendencję do porównywania go do zbioru technologii i metod, które są podstawą systemu bitcoin, które inne projekty wykorzystały jako inspirację, ponieważ funkcja ta rozwiązuje problemy spoza zakresu finansów i innych dziedzin.

Szansa czy zagrożenie?

Po pierwsze, systemy te nie są tak niekontrolowalne, jak mogłoby się wydawać i nie każdy może stać się równoprawnym podmiotem zatwierdzającym wpisy.

Wbrew powszechnej opinii, podstawowa architektura sprawia, że stosunkowo łatwo śledzić transakcje oraz ustalić tożsamość osób działających niezgodnie z regułami. Poza tym instytucje kontrolne nauczyły się kontrolować bramy systemu (input/output), którymi pieniądze wpływają i wypływają z systemu. Platformy takie jak bitcoin mogą wydawać się niepokojące na pierwszy rzut oka, ale użytkownicy nie mają gwarancji anonimowości, a jeśli chcą wymienić bitcoiny na funty, dolary lub euro, to przy wymianie będą zastosowane przepisy dotyczące ustalania tożsamości, aby zapobiec praniu pieniędzy i finansowaniu terroryzmu. Ponadto, jak przedstawiono poniżej, wiele z najbardziej interesujących zastosowań tej technologii wprowadza ścisłe zasady kto może, a kto nie korzystać z systemu.

Stopniowo rozpowszechnia się pogląd, że technologia stanowiąca podstawę bitcoina może mieć cenne i niegroźne zastosowania i może umożliwić znaczącą innowację w przyszłości. Co prawda jest mało prawdopodobne, że duże korporacje i banki w najbliższym czasie zaczną stosować bitcoin na większą skalę. Powodem jest odporność bitcoina na cenzurę, co jest problematyczne ze względu na egzekwowanie prawa i perspektywy regulacyjne. Motorem napędzającym innowacje znów okażą się więc otwarte platformy (niekontrolowane przez firmy) i powiększająca się społeczność programistów. Mogą one nowym uczestnikom rynku dać możliwość zaoferowania produktów i usług dla zmarginalizowanej wcześniej grupy użytkowników (Zob. Rozdział 5. poświęcony rewolucyjnemu potencjałowi tej technologii).

Chociaż technologia DLT została stworzona, aby zaspokoić jeden cel (wykorzystanie wirtualnego pieniądza), firmy i inne instytucje badają obecnie, jak może być ona stosowana do rozwiązywania innych problemów. Na przykład przedsiębiorstwa często twierdzą, że rejestry posiadające jednego lub wielu właścicieli – „zamknięte" są o wiele bardziej atrakcyjne niż tzw. „otwarte" modele. Pozwala to firmom na tworzenie bezpiecznych, prywatnych sieci obejmujących ufające sobie firmy i jednostki (dokładne objaśnienie terminów permissioned (otwarty) i unpermissioned (zamknięty) w rozdziale 3).

FAQ: Czym zasadniczo różni się bitcoin od dotychczas używanych walut?

Bitcoin może być w posiadaniu każdej osoby, bez zgody banku lub rządu. Mogą one być wysyłane do kogokolwiek na świecie, kto wie, jak obsługiwać „wirtualny portfel". Jest to tzw. zasada „censorship resistance", która ukazuje zasadniczy przełom bitcoina – i wyjaśnia obawy prawodawców i regulatorów.

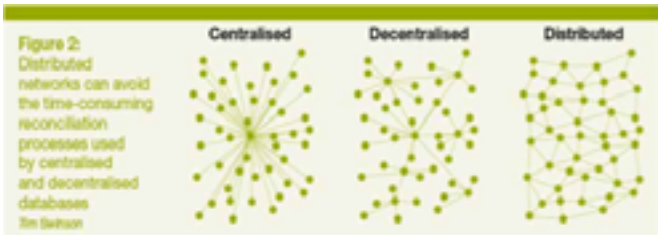
Ogólnie rzecz biorąc, technologie z tej branży można umieścić na osi w kolejności określającej poziom ich „zdecentralizowania" są (czyli w jakim stopniu nie wymagają uwierzytelnienia). Centralizacja, jednakże może być tylko jednym z wymiarów, w którym technologie te powinny być analizowane. Inne zagadnienia, które są obecnie rozważane, to np. możliwość zaprogramowania dozwolonego wykorzystania środków (np. fundusze, które mogą być wykorzystane przez dziecko tylko jeżeli rodzic zezwoli) i możliwości uwzględniania aktywów innych niż pieniądz (np. papierów wartościowych lub nawet tytułów własności nieruchomości).

Potencjalne zastosowania

Technologia blockchain/DLT może rozwiązać problemy przedsiębiorstw, które można podsumować jako: koszt, powielanie i ujednolicenie.

Przykładowo w bankowości. Każdy bank ma co najmniej jeden (zazwyczaj kilka) systemów śledzenia i zarządzania cyklem swoich transakcji finansowych. Każdy z tych systemów kosztuje – zarówno stworzenie go jak i utrzymanie. Systemy muszą zostać połączone ze sobą i zsynchronizowane, zwykle w procesie znanym jako ujednolicenie. To obejmuje całe grupy ludzi w każdym banku, którzy muszą komunikować się ze swoimi odpowiednikami w innych bankach, aby upewnić się co do zgodności i aby odpowiednio reagować, gdy tak się nie dzieje.

Dotychczasowe rozwiązanie zakładało utworzenie jednego, scentralizowanego rejestru, wspólnego dla wszystkich uczestników. Wielka Brytania ma szereg sukcesów, które opierały się na tym podejściu, szczególnie w Faster Payments Service. Jednakże centralizacja jest zazwyczaj kosztowna, tak jak przetwarzanie scentralizowanych danych, które musi być zintegrowane i synchronizowane z wszystkimi zaangażowanymi systemami. Alternatywnie, wiele zdecentralizowanych baz danych może znajdować się na krawędziach sieci, podczas gdy komunikaty przesyłane są między nimi (patrz rys. 2).



Natomiast bitcoin synchronizuje tysiące komputerów w rozproszonej sieci, używając internetu: jeśli jeden komputer myśli, że ktoś jest właścicielem danego bitcoina, to tak samo uważa każdy inny komputer w sieci. Gdyby podobna technika została zastosowana w bankowości, wszystkie systemy banków mogłyby się porozumiewać bez potrzeby większej ilości pracowników uwierzytelniających i rozwiązujących problemy. Co najważniejsze, aby to osiągnąć, niepotrzebny jest bitcoin – rozwiązanie oferuje leżąca u jego podstaw technologia blockchain/DLT.

Mogłoby to pomóc wyeliminować jeden z największych problemów w usługach finansowych: koszty papieru. W ostatnich latach pojawiło się wiele różnych inicjatyw mających na celu usunięcie papierowych dokumentów z gospodarki. Jednakże, w wielu przypadkach nowa technologia odtworzyła stare procesy lub w dalszym ciągu opiera się na używaniu papierowych dokumentów w innych stadiach procesu. Na przykład, przekazywanie środków finansowych dla eksporterów pozostaje niezwykle zbiurokratyzowanym procesem. Mianowicie bank importera wystawia list kredytowy, na podstawie którego bank eksportera otrzymuje zaliczkę. Pomimo, że proces ten jest zwykle przeprowadzany drogą elektroniczną opiera się wszędzie na ręcznie przetwarzanych dokumentach. Technologia współdzielonych rejestrów może zastąpić biurokratyczne procesy. The Engineering and Physical Sciences Research Council (EPSRC) już obecnie wspiera badania dotyczące zastosowań tych technologii w transakcjach finansowych (patrz przykład poniżej: Badania i analiza perspektyw).

Perspektywy nie ograniczają się jedynie do bankowości. Technologie są badane pod kątem zastosowania w opiece zdrowotnej (dokumentacji pacjenta), działalności rządu (rejestr gruntów i rozdział świadczeń społecznych – zob. Rozdział 6), elektroniki (w tym „Internetu rzeczy" – zob. Rozdział 1), a nawet świata sztuki i biżuterii (np. śledzenie pochodzenia diamentów – zob. Rozdział 5).

Ważne jest, aby podkreślić, że technologie te są na bardzo wczesnym etapie rozwoju i trzeba rozwiązać jeszcze wiele problemów, zanim będą mogły być wykorzystywane w pełni. Są to min. kwestie prywatności, wydajności i skalowalności. Czy technologia rzeczywiście działa wystarczająco dobrze, aby banki mogły jej zaufać? Kto zbuduje tego typu platformy, skoro przy systemach współdzielonych i wspólnych trudno jest pobierać opłatę?

Jednakże ta dziedzina rozwija się bardzo szybko, a wiele z problemów zostało już rozwiązanych. Obecnie możliwe jest rozróżnienie między tymi obszarami technologii, które ewoluują, a także tymi, które stanęły w miejscu i trudno je zmienić. Już teraz widzimy, że technologia blockchain/DLT mogłaby umożliwić firmom i rządom bardziej wydajną pracę, bez kosztownych ujednoliceń stanu danych i powielania czynności. Mogłoby to pozwolić zarówno obecnym na rynku, jak i wchodzącym na niego konkurować na równych warunkach w oferowaniu nowych produktów i usług dla konsumentów, w oparciu o otwarty dostęp do bezpiecznie współdzielonych danych.

Mogłoby to doprowadzić do światowej rewolucji, która wykracza daleko poza odporną na cenzurę cyfrową walutę.

PRZYKŁAD 1 – Badania i analiza perspektyw

John G Baird, kierujący the RCUK Digital Economy Theme, EPSRC

The Engineering and Physical Sciences Research Council (EPSRC) kieruje projektem badawczym Digital Economy (DE) w ramach Research Councils UK (RCUK). Od 2008 DE zainwestowało ponad 170 milionów funtów na stosowane badania wielodyscyplinarne kładące szczególny nacisk na wyzwania społeczne wokół cyfryzacji i ich wpływ na integrację społeczną, gospodarkę rolną, bezpieczeństwo danych osobowych, bezpieczeństwo, tożsamość, wiarygodność i prywatność. DE kieruje działaniami związanymi z walutą wirtualną i IoT, zaplanowanymi w budżecie ogłoszonym w marcu 2015 r. W dziedzinie technologii rozproszonych rejestrów do tej pory zainwestowaliśmy w następujące działania:

Skutki wdrożenia kryptowalut w Cyfrowej Transformacji (CREDIT), 18 miesięczny projekt o wartości 0,4 mln funtów, którego celem jest zbadanie zjawiska kryptowaluty i leżącej u jej podstaw technologii blockchain. Wyodrębniono cztery główne grupy tematów: transformacja cyfrowa, prywatność, społeczność i instytucje. Głównymi rezultatami badań będą:

- *przewodnik „krok po kroku", którego celem jest pomoc dla startupów i beneficjentów, pomagający zrozumieć kwestie istotne do rozważenia przed wprowadzeniem technologii blockchain do swoich produktów i usług*
- *liczne małe badania pilotażowe z firmami badającymi potencjalne skutki kryptowaluty*
- *wykształcenie grupy badaczy akademickich i specjalistów zdolnych do dalszego rozwoju tej rodzącej przestrzeni badawczej*
- *CREDIT opiera się na dwóch wcześniej przeprowadzonych analizach: „Rewolucyjna rola kryptowalut" i „ICT i przyszłość usług finansowych". Obydwie odnoszą się do aktualnego stanu wiedzy na temat kryptowalut i ukazują braki w zrozumieniu społecznych, etycznych, prawnych skutków regulacyjnych kryptowalut. W rezultacie, niedawno zainwestowaliśmy 10 milionów funtów w fundusz projektów badawczych dotyczących „Zaufania, tożsamości, prywatności i bezpieczeństwa w gospodarce cyfrowej", obejmujący „Szerokie zastosowanie technologii DLT" jako jeden z sześciu priorytetowych obszarów. Ten główny obszar ma na celu znalezienie możliwości wsparcia badań, które łączą i balansują zaawansowanie technologiczne w systemach DLT ze zrozumieniem społecznych, etycznych, prawnych i gospodarczych struktur potrzebnych do stworzenia pewności i zaufania koniecznego do przyjęcia systemu przez jednostki, społeczności, organizacje i państwa. Ostatecznie, mamy nadzieję, że te badania utorują drogę do stworzenia „inteligentnej" gospodarki, która może obsługiwać różne scenariusze wymiany wartości pieniężnej i niepieniężnej pomiędzy jednostkami oraz organizacjami, a w przyszłości z kolei pozwoli na stworzenie „inteligentnych" obiektów. Sfinansowaliśmy również projekt 3rd Party Dematerialisation and Rematerialisation of Capital (3DaRoC) wart 260,000 funtów, który zbadał, jak projektować działające cyfrowe usługi finansowe w oparciu o Case Studies. Przeprowadziliśmy go z dwoma detalicznymi organizacjami finansowymi: Zopa Limite kredytodawca bezpośredni oraz z Bristol Pound. Projekt opracował zestaw narzędzi online, aby pomóc użytkownikom i firmom zainteresowanym w kluczowych kwestiach mających wpływ na wygląd i wykorzystanie cyfrowych produktów finansowych.*

ROZDZIAŁ 3: Zarządzanie i przepisy

Zarówno obszary prawne jak i cyfrowe regulowane są przepisami, ale charakter tych przepisów jest inny. W środowisku cyfrowym działalność reguluje prawo (kodeks prawny) oraz oprogramowanie/sprzęt (kod techniczny). Ustalając przepisy dotyczące blockchain/DLT obydwa elementy składowe należy wziąć pod uwagę.

WPROWADZENIE

Niniejszy rozdział dotyczy przepisów i działań regulacyjnych związanych z systemami blockchain. Będziemy rozpatrywać kod prawny (reguły i zobowiązania prawne) oraz kod techniczny (oprogramowanie i protokoły). Będziemy także rozróżniać zarządzanie (ustalanie reguł przez właścicieli lub uczestników systemu w celu ochrony swoich prywatnych interesów) oraz prawodawstwo (ustalanie reguł przez zewnętrzną instytucję, której zadaniem jest reprezentowanie interesów społeczeństwa).

KODEKS PRAWNY VS KOD TECHNICZNY: DWA RODZAJE UREGULOWAŃ

System finansowy jest zarówno zbiorem zobowiązań prawnych między instytucjami jak i zbiorem zapisów cyfrowych tych zobowiązań. Zarówno aspekty prawne i cyfrowe rządzą się pewnymi regułami, ale charakter ich jest różny. W pracy na ten temat, Lawrence Lessig z Harvard University zwrócił uwagę w jaki sposób przepisy prawne i cyfrowe oddziałują na siebie, gdy regulują jakąś działalność. Lessig stwierdził, że w środowisku cyfrowym zarówno – przepisy (kodeks prawny) oraz oprogramowanie / sprzęt (kod komputerowy) regulują aktywność, a wpływ ich należy wziąć pod uwagę przy konstruowaniu teorii regulacji w równym stopniu. W tym rozdziale odnosimy się głównie do właściwości technicznych, a nie kodu komputerowego. Obejmuje to oprogramowanie i protokoły, gdyż funkcjonowanie rozproszonych rejestrów opiera się na tych dwóch funkcjach.

Zasadniczą różnicą pomiędzy kodeksem prawnym i kodem technicznym jest mechanizm, w jaki każdy z nich wpływa na działanie. Kodeks prawny jest czynnikiem „zewnętrznym": jego przepisy mogą być złamane, ale konsekwencje płynące z naruszenia mają zapewnić przestrzeganie ich. Kod techniczny jest „wewnętrznym" czynnikiem: jeśli jego zasady zostaną złamane, pojawia się błąd i brak możliwości aktywności, więc przestrzeganie go jest zapewnione poprzez funkcję samego kodu. Inną cechą oprogramowania jest to, że urządzenie będzie przestrzegać jego zasad, nawet jeżeli podporządkowanie się nim powoduje nieprzewidziane lub niepożądane efekty. To ukazuje uderzające różnice w funkcjonowaniu systemu rozproszonych rejestrów w stosunku do obecnego systemu finansowego.

1. Obecny system finansowy: orzekanie na podstawie kodeksu prawnego

Nowoczesny system finansowy jest już w dużej mierze cyfrowy i silnie uzależniony od kodu technicznego. Kod techniczny reguluje tworzenie i nowelizację zapisów cyfrowych zobowiązań prawnych między instytucjami. Działania instytucji nadzoru finansowej są ukierunkowane na egzekwowanie tych obowiązków prawnych np. sprawdzanie czy bank ma wystarczający kapitał lub płynność. System finansowy jest już regulowany zarówno poprzez kod techniczny jak i kodeks prawny, ale zarządzanie finansowe i przepisy podlegają temu drugiemu.

Egzekwowanie kodeksu prawnego należy do zadań wyspecjalizowanej grupy instytucji nadzoru, odpowiedzialnych za zapewnienie przestrzegania zasad systemu przez uczestników. Uczestnicy muszą dostarczyć informacji, których zgodność z zasadami systemu sprawdza instytucja kontrolna. Jeśli organizacja się nie podporządkuje, wówczas nadzór może podjąć działania, aby tak się stało. Nie oznacza to, że kod techniczny nie ma wpływu na istniejący proces wykonawczy – wszystkie informacje dostarczane instytucjom kontrolnym są cyfrowe, ale cele zarządzania i kontroli są realizowane po-

przez przepisy prawne, a nie zmianę kodu technicznego.

2. Blockchain/DLT: zarządzanie za pomocą kodu technicznego

System DLT, taki jak bitcoin wykazał możliwość funkcjonowania bez przepisów prawa. Wszystko jest regulowane za pomocą kodu technicznego. Każdy uczestnik w sieci uruchamia takie samo lub kompatybilne oprogramowanie, które określa rodzaje dopuszczalnych transakcji. Na przykład, oprogramowanie bitcoina umożliwia uczestnikom realzację transakcji cyfrowymi środkami płatniczymi, do których prawa własności potwierdzają za pomocą kodu kryptograficznego. Oprogramowanie bitcoina reguluje również możliwości i sposób ich emisji, a także określa jej limit. Nie ma przepisów lub innych dokumentów prawnych regulujących te procesy. Nikt nie może egzekwować ich przestrzegania – blockchain jest regulowany jedynie własnym kodem technicznym.

Aby zapobiec zmianom kopii kodu w celu przeprowadzenia nielegalnej transakcji, każda z nich musi zostać zweryfikowana zanim „wejdzie" do rejestru. W tzw. otwartych rejestrach DLT jak np. bitcoin, weryfikatorzy transakcji, czyli górnicy są wybierani losowo. System ten ma na celu zapewnienie integralności poprzez system zachęt ekonomicznych, w procesie rządzonym przez oprogramowanie. W zamkniętych systemach DLT, weryfikatorzy są powoływani przez właściciela systemu, a ich uczciwość gwarantowana jest przy użyciu konwencjonalnych metod, takich jak umowa prawna.

Podsumowując, DLT różni się od tradycyjnego systemu finansowego tym, że rządzi się kodem technicznym zamiast kodeksem prawnym. Jedną z zalet jest to, że koszty przestrzegania przepisów są niskie: uczestnicy muszą używać zgodnego pakietu oprogramowania, aby przeprowadzić transakcję. Mogłoby się wydawać, że koszty egzekucyjne są mniejsze, ale nie jest to regułą, ponieważ system kontroli (górnicy) używany do weryfikacji transakcji we wszystkich systemach wymaga znacznej mocyobliczeniowej. To koszt, który w przyszłości będzie ponoszony przez użytkowników systemu.

ZARZĄDZANIE VS KONTROLA: DWA SPOSOBY USTANAWIANIA REGUŁ

Ponieważ obecny system finansowy i rejestry rozproszone są regulowane przez różnego rodzaju przepisy, musimy zatem zadać pytanie: kto je ustala?

1. Obecny system finansowy: mieszanka prywatnego i publicznego ustalania reguł

Przepisy prawa dla obecnego systemu finansowego powstają w wielu różnych miejscach. Jednak z grubsza można je przypisać do dwóch kategorii: prywatne ustalanie zasad (zarządzanie) oraz publiczne ustalanie zasad (prawodawstwo). Przykładem prywatnego ustalania reguł są przepisy Visa Core Rules ogłoszone przez spółkę usług finansowych Visa Inc., regulujące działania wszystkich uczestników w systemie Visa. Takie zasady ustalane są przez właścicieli prywatnych sieci finansowych, takich jak Visa oraz przez prywatne stowarzyszenia instytucji finansowych, które chcą koordynować działania dla wzajemnego zysku. Przykładem publicznego ustalania zasad jest ustawodawczy nadzór systemu płatniczego Visa Europe przez Bank Anglii.

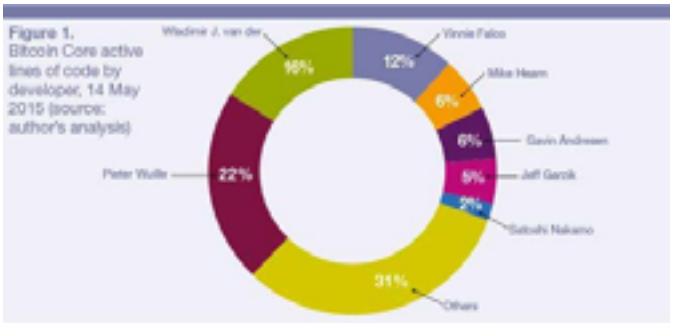
Konstrukcja publicznego kodeksu prawnego w obecnym systemie finansowym jest domeną polityków, którzy muszą wziąć pod uwagę wpływ regulacji dotyczących poszczególnych instytucji systemu finansowego (podejście „mikroostrożnościowe"), jak również wpływ na system jako całości (podejście „makroostrożnościowe"). Ponieważ system finansowy jest globalny, instytucje międzynarodowe, takie jak Bazylejski Komitet Nadzoru Bankowego zwołuje polityków z całego świata, aby dojść do porozumień, które mogą być następnie przeniesione do prawodawstwa w określonej jurysdykcji.

2. Systemy blockchain/DLT: działania podejmowane doraźnie – prywatne ustanawianie zasad

Popularne jest przekonanie, że otwarte systemy blockchain/DLT zaprojektowane są w ten sposób, aby istnieć niezależnie od ludzkiego ustanawiania reguł i opierają się jedynie na algorytmach matematycznych. Nie jest to prawdą. Podobnie jak kodeks prawny, kod techniczny musi być produkowany i utrzymywany przez ludzi określających zasady, które kod reprezentuje. Bitcoin może stanowić przykład. Początkowa wersja oprogramowania została opublikowana przez Satoshi Nakamoto (pseudonim). W 2010 Nakamoto przekazał kontrolę nad projektem Gavinowi Andresenowi, urodzonemu w Australii programiście mieszkającemu w Stanach Zjednoczonych. Jak każde inne oprogramowanie, bitcoin musi być regularnie aktualizowany, aby naprawiać pojawiające się błędy, problemy z bezpieczeństwem oraz zmiany w środowisku operacyjnym. Takie aktualizacje mogą zasadniczo zmienić każdy aspekt oprogramowania, w tym również zasady rozliczeniowe czy prawa własności. Istotne zatem jest – dla wszystkich użytkowników systemu blockchain/DLT – kto pisze oprogramowanie i jak ten proces jest zarządzany oraz komu ten proces podlega.

W przypadku bitcoina, oprogramowanie jest regulowane na bieżąco z udziałem kilku nieformalnych instytucji i władz. Bitcoin jest programem typu open source i każdy może zaproponować zmiany, ale jedynie pięciooso-

bowy zespół głównych programistów, powołany przez Andersena, może faktycznie wprowadzać te zmiany. Władza głównych programistów jest ograniczona przez nieformalną, dobrowolnie przyjętą regułę, która mówi, że znaczące zmiany wymagają szerokiego konsensusu społeczności. Każda aktualizacja oprogramowania musi być ponadto zainstalowana przez większość górników (mierzonej przez inwestowaną moc obliczeniową), aby zmiany faktycznie zaczęły działać. W ten sposób osoby, które zarządzają tzw. kombinatami wydobywczymi (mining pools) zyskują spory wpływ na to, czy aktualizacja oprogramowania zostanie zaakceptowana przez minerów czy nie.



Ten proces zarządzania działał dobrze, gdy zmiany w kodzie ograniczały się do niekontrowersyjnych napraw błędów. Jednak ostatnio zaczął się załamywać, ponieważ niektóre decyzje wiązały się z przyznawaniem priorytetu interesom niektórych udziałowców, kosztem innych. Andresen i inni stwierdzili, że proces musi stać się bardziej formalny. Główna debata toczy się o to jak taki formalny system zarządzania powinien wyglądać, jest to skomplikowane przez fakt, że bitcoin wyrósł na etosie anty-instytucjonalizmu. To interesująca zagadnienie, które wskazuje na rolę kodeksu prawnego i mówi nam, że sam kod techniczny nie da optymalnego wyniku.

W systemach „zamkniętych" rozproszonych rejestrów, zarządzanie oprogramowaniem jest prostsze przez fakt, że to nie właściciel reprezentuje wykładnię prawa i władzę nad kodem technicznym. Do właściciela należy określenie, który kod jest modyfikowany, a od użytkowników (klientów usługi) zdecydowanie, czy odpowiada im sposób zarządzania własnością nad oprogramowaniem. Ocena poziomu świadczonych usług i inne konwencjonalne środki mogą być wykorzystywane do ustalania i egzekwowania ich obowiązków. Zamknięte systemy rozproszonych rejestrów w tym względzie nie różnią się od konwencjonalnych prywatnych sieci finansowych, takich jak oprogramowanie systemów Visa lub w modelu SaaS (software-as-a-service).

JAK NALEŻY UREGULOWAĆ SYSTEMY REJESTRÓW ROZPROSZONYCH?

Ład w rozproszonym rejestrze, jak opisano powyżej dotyczy interesariuszy systemu, ale funkcje rozproszonych rejestrów mogą być związane również z szerszym zainteresowaniem społecznym. Na przykład, instytucje nadzoru mogą chcieć zbierać podatki, ścigać przestępstwa i ograniczać nielegalne wykorzystanie rejestrów. Jeżeli system rozpowszechni się do tego stopnia, że zacznie mieć potencjalny efekt domina w innych sektorach społeczeństwa, regulatorzy mogą również chcieć upewnić się, że system jest odporny wobec ryzyka systemowego oraz nieprawidłowości w funkcjonowaniu rynku. Regulacje takiego typu mogą podlegać kodeksowi prawnemu lub kodowi technicznemu.

1. Prawne regulacje rozproszonych rejestrów

Prawne regulacje działania zamkniętych systemów rejestrów rozproszonych jest kwestią nakładania zobowiązań prawnych na jego właściciela. Uregulowanie systemu otwartego takiego jak bitcoin poprzez kodeks prawny jest bardziej skomplikowane, ponieważ nie istnieje jeden podmiot prawny sprawujący nad nim kontrolę. Trudno byłoby wymagać od użytkowników instalacji na ich komputerach konkretnego oprogramowania. Dążenie do kontrolowania bitcoina poprzez przepisy prawa koncentrują się zatem na firmach, które obracają bitcoinem, takich jak kantory, giełdy i dostawcy portfeli cyfrowych. Firmy te mogą podlegać regulacjom z własnej inicjatywy (np. aby zapobiec sytuacji, gdy dostawca wirtualnego portfela znika z pieniędzmi klientów) lub w celu pośredniej kontroli nad wykorzystaniem rejestrów (np. zapewnienia zgodności z przepisami w zakresie przeciwdziałania praniu pieniędzy).

Znanym przykładem regulacji bitcoina poprzez kodeks prawny jest tzw. BitLicense, wydawana przez Departament Usług Finansowych Stanu Nowy Jork dla firm oferujących usługi związane z wirtualnymi walutami dla rezydentów Nowego Jorku. Termin pozyskania pozwolenia licencji został ustalony na 08 sierpnia 2015, a nielicencjonowani usługodawcy mogą być karani.

2. Regulacja rozproszonych rejestrów za pomocą kodu technicznego

Kody techniczne dla systemów rozproszonych rejestrów, takich jak bitcoin, tworzone są doraźnie przez prywatne podmioty. Ale kod techniczny, zawierający oprogramowanie i protokoły, może również pojawić się ze strony sektora publicznego. Na przykład, TCP/IP oraz inne podstawowe protokoły internetowe były wynikiem projektów badawczych finansowanych przez rząd i są obecnie prowadzone pod auspicjami Internet Society, międzynarodowej organizacji non-profit z otwartą strukturą członkostwa. Inne elementy infrastruktury internetu są utrzymywane poprzez międzynarodowe wielostronne

procedury, a niektóre części pozostają pod nadzorem amerykańskich państwowych regulatorów. Chociaż te rozwiązania są dalekie od ideału, pokazują, że możliwy jest udział społeczeństwa i demokratycznej reprezentacji w tworzeniu przepisów technicznych – publiczne ustanawianie reguł realizowane poprzez kod techniczny, a nie kodeks prawny.

W odniesieniu do systemów rozproszonych rejestrów może to oznaczać wszystko. Od utworzenia wielostronnych procedur dla utrzymywania kodu technicznego, po opracowanie publicznych standardów dla kodu. Jeśli pozwoliłoby to rządom lub bezpośrednio obywatelom osiągać uzasadnione cele regulacyjne poprzez wpływanie na reguły wbudowane w kod komputerowy, zapotrzebowanie na powstanie nowego podmiotu prawnego do kontrolowania tych systemów mogłoby się zmniejszyć.

Alternatywnie, sektor publiczny mógłby opracować zamknięty system, który pozwala organom władzy publicznej wywrzeć wpływ na te regulacje poprzez połączenie kodeksu prawnego i kodu technicznego, a nie wyłącznie za pośrednictwem kodeksu prawnego jak to jest chwili obecnej. Niektóre z podstawowych technologii internetowych wykazały, że możliwe jest, aby rządy skutecznie katalizowały tworzenie kodów technicznych, które stały się fundamentalne dla działalności sektora prywatnego.

Wnioski

W przeciwieństwie do konwencjonalnych prywatnych sieci finansowych, takich jak Visa, otwarte systemy rozproszonych rejestrów, jak bitcoin nie mają centralnego podmiotu prawnego biorącego formalną odpowiedzialność za system. Zamiast tego, są one regulowane przez bieżące procesy, zazwyczaj przeprowadzane przez garstkę autorów oprogramowania, którzy tworzą zasady dla oprogramowania systemu. Jeśli wartość i wpływ tych systemów będzie wzrastać, potrzebne będzie stworzenie bardziej trwałych systemów wewnętrznego zarządzania. Brak centralnego podmiotu prawnego powoduje, że większym wyzwaniem dla regulatorów publicznych jest kontrola systemu rozproszonych rejestrów za pomocą kodeksu prawnego. Rządy powinny rozważyć sposoby regulowania systemów rozproszonych rejestrów przez wpływ na kod techniczny, który sam określa swoje zasady. Szukając odpowiednich proporcji rząd powinien rozważyć mocne i słabe strony kodu technicznego oraz kodeksu prawnego, zakładając, że wzajemnie na siebie oddziałują i powinny być odpowiednio zaprojektowane.

Pojawienie się bitcoina i systemów rozproszonych rejestrów zwróciło uwagę na kwestie kodu technicznego również w kontekście obecnego systemu finansowego. Rozproszone rejestry pokazują, że systemy finansowe mogą być zarządzane i regulowane kodem technicznym, jak również kodeksem prawnym. Decydenci powinni uznać udział kodów technicznych w systemie finansowym i zastanowić się, w jaki sposób mogą się one stać częścią systemu prawnego, biorąc pod uwagę potencjalne korzyści, takie jak niższe koszty stałe.

ROZDZIAŁ 4: Bezpieczeństwo i prywatność

Istnieje wiele różnych rodzajów systemów rozproszonych rejestrów, każdy oferuje szanse, ale i zagrożenia dotyczące bezpieczeństwa i prywatności. Ważna jest analiza wymagań – w zakresie działalności i bezpieczeństwa – proponowanych implementacji każdego z typów rejestrów przed podjęciem decyzji jaki typ rejestru wykorzystać.

WPROWADZENIE

Bezpieczeństwo może być zdefiniowane jako: „Wydarzenia, które powinny się wydarzać, wydarzają się, a wydarzenia które nie powinny mieć miejsca, miejsca nie mają". Dla każdego konkretnego zastosowania rozproszonych rejestrów i technologii blockchain, ryzyko wystąpienia pożądanych i niepożądanych efektów zależy od tego jak technologia jest zaprojektowana, wdrożona i regulowana. Zainteresowane strony zmierzą się z różnymi rodzajami ryzyka.

Zagrożenia dla systemów obejmują nie tylko ataki przez podmioty zewnętrzne, ale także działania podejmowane przez interesariuszy wewnętrznych i awarie czynników składowych (takich jak oprogramowanie). Aby osiągnąć zamierzone efekty należy przed rozpoczęciem każdej realizacji, opracować szczegółowe modele zagrożeń i zidentyfikować konkretne wymogi bezpieczeństwa.

Skuteczna ochrona zapewnia konieczne, ale niewystarczające podstawy zapewnienia prywatności podmiotom indywidualnym i organizacyjnym. Musimy również wziąć pod uwagę, w jaki sposób informacje ujawnione w danej implementacji mogą być łączone z innymi dostępnymi informacjami w celu identyfikacji osoby, grupy czy wykrycia określonej działalności.

ZALETY INNOWACJI

Jedną z głównych cech bezpieczeństwa bitcoina i innych kryptowalut jest zdecentralizowana kontrola sieci. System jest zarządzany przez globalne równorzędne podmioty, działające w oparciu o konsensus (patrz definicje, str. 17), nie ma więc centralnego punktu zaufania lub awarii. Oznacza to, że każdy nielegalny atak na system jest trudny do przeprowadzenia. Dla użytkowników indywidualnych, system może osiągnąć wysoki poziom bezpieczeństwa – aby przelać bitcoiny z wirtualnego portfela, atakujący musi znać klucz prywatny związany z danym kluczem publicznym (określają one, gdzie dane bitcoiny się znajdują i do kogo aktualnie należą). Tak więc w celu kradzieży bitcoinów atakujący musi być w stanie obejść zabezpieczenia ustalonych standardów kryptograficznych (Elliptic Curve Digital Signature Algorithm ECDSA).

Bitcoin i powiązane z nimi alternatywne kryptowaluty „altcoins" wykorzystują znacznie szerszą infrastrukturę związaną z bezpieczeństwem informatycznym – rozproszone rejestry – to zapewnia wysoką integralność i spójność działań. Takie rejestry wykorzystują techniki kryptograficzne pozwalające każdemu sprawdzić czy określone dane znajdują się w rejestrze, o ile posiadają oni niewielką ilość istotnych informacji. W tym samym czasie, złożone protokoły zgodności stosuje się, aby zapewnić, że każdy użytkownik systemu otrzymuje taki sam obraz rejestru. Ma to kluczowe znaczenie dla zdolności bitcoina do zapobiegania wielokrotnym płatnościom danym bitcoinem. Może to być równie istotne przy używaniu rejestrów do innych celów, takich jak zapisywanie umów lub prawa własności. Rozproszone rejestry nadają się do wdrażania usług na wysokim poziomie takich jak usługi notarialne, rejestracja czy zintegrowana archiwizacja. Ich zastosowanie pozwoliłoby na obniżenie kosztów powyższych działań poprzez zwiększenie automatyzacji, co umożliwia łatwą zmianę usługodawców oraz transakcji.

Jednym z głównych problemów bezpiecznej komunikacji on-line, jest ustalanie, że klucz publiczny należy do usługi, do której użytkownik chce uzyskać dostęp. Przeważa mechanizm stosowany od 1990 znany jest jako Infrastruktura Klucza Publicznego (PKI) – zaufana trzecia strona, która zapewnia certyfikaty potwierdzają-

ce związek między kluczami i usługami. Ale bywa, że te instytucje certyfikujące okazują się zawodne; gdy dojdzie do włamania, mogą wydawać fałszywe certyfikaty, nawet o tym nie wiedząc.

System Certyfikat Transparency (CT) (zainicjowany przez Google, a teraz nadzorowany przez grupę roboczą) wykorzystuje technologię rejestrów rozproszonych, aby ograniczyć ten problem. Wszystkie certyfikaty są dołączane do rozproszonego rejestru, a każdy użytkownik może sprawdzić, czy certyfikat jest tym którego chce użyć. W związku z tym, podejrzane certyfikaty można wykryć szybko – to istotny czynnik zniechęcający atakujących system PKI.

Problem ustalenia autoryzacyjnych powiązań między kluczami i podmiotami istnieje także wtedy, gdy użytkownik chce chronić osobistą komunikację. Ale obecne rozwiązania (takie jak PGP Web of Trust, lub scentralizowane rozwiązania) są albo mało funkcjonalne, albo mają słabe zabezpieczenia. Jedną z obiecujących alternatyw jest CONIKS, opierający się na specjalnie spreparowanym rozproszonym rejestrze do przechowywania i pobierania kluczy publicznych użytkowników, które mogą być następnie używane do szyfrowania i podpisywania poczty elektronicznej. W przeciwieństwie do CT – która opiera się na sieci stron trzecich w celu utrzymania i audytu rozproszonego rejestru – CONIKS korzysta z usług komunikacyjnych i baz danych użytkowników do budowania rejestru o wysokiej integralności.

WYZWANIA ZWIĄZANE Z BEZPIECZEŃSTWEM

Wskazane powyżej zalety zdecentralizowanych systemów – szczególnie odporność i wytrzymałość – w całości mają tylko rejestry ogólnodostępne, opierające się na teorii powszechnego zaufania. Wymagające uwierzytelniania rejestry zamknięte lub inne scentralizowane usługi, odporność i wytrzymałość mają mniejsze, ale można w nich w większym stopniu centralnie zagwarantować wiarygodność i/lub świadczenie innych usług.

Jednakże istnieje wiele opcji pośrednich, pomiędzy całkowicie zdecentralizowanym systemem (jak bitcoin), a w pełni opartym na uwierzytelnieniu (jak prywatne, przeznaczone do konkretnego zadania sieci).

Przykładem systemu pośredniego, który oferuje zalety obu rozwiązań, są kryptowaluty emitowane przez banki centralne. Ich zastosowanie proponują George Danezis i Sarah Meiklejohn z University College London. Kryptowaluty tego typu opierałyby się na kontrolowanym centralnie serwerze i jednocześnie wykorzystywałyby sieć rozproszonych cyfrowych "mennic", które obsługiwałyby transakcje i emitowały pieniądz.

Biorąc pod uwagę wachlarz możliwości, należy przeanalizować wymogi bezpieczeństwa i opłacalność ekonomiczną każdego rodzaju rejestru przed wyborem spośród proponowanych rozwiązań.

Przykładowo dla zarządzania wypłatami z systemu zabezpieczeń społecznych w Ministerstwie Pracy i Emerytur najważniejsze jest z jednej strony zapewnienie dostępności usług a z drugiej odporność systemu na zakłócenia w działaniu sieci. Najpoważniejsze zagrożenie stanowiliby prawdopodobnie działający dla zysku przestępcy, szukający sposobności do ataku na poszczególnych użytkowników systemu.

Dlatego:

- *System powinien być zaprojektowany tak, aby od indywidualnego użytkownika wymagał jak najmniej wiedzy i wysiłku. Np. powinno być jak najmniej możliwości wyboru i konfiguracji z jasną informacją o konsekwencjach dokonywanych wyborów*
- *W przypadku korzystania z systemu przy pomocy urządzeń mobilnych, np. smartfonów, należy upewnić się, aby dostęp do haseł był zabezpieczony i aby nie były one widoczne dla innych aplikacji*
- *Sam rejestr powinien być utrzymywany w sieci licznych serwerów, co dawałoby mu odporność na utrudnienia w dostępie do sieci*

Dla szerszych zastosowań autoryzacja wypłat powinna być dokonywana centralnie na specjalnie do tego przeznaczony serwerze, dodatkowo zabezpieczonym przed atakami.

Inny przykład to dystrybucja pomocy finansowej poza granicami. System używany w tym celu przede wszystkim musi zapewniać uczciwość całego procesu, czyli zabezpieczać środki przed wykorzystywaniem w innym celu niż są przeznaczone. Jednocześnie fundusze muszą być łatwo dostępne w przypadku np. katastrof naturalnych. Zagrożenie mogą stanowić państwa trzecie, które w celu osiągnięcia korzyści geopolitycznych zakłócałyby przeprowadzanie transakcji oraz nieuczciwi partnerzy w państwach otrzymujących pomoc.

Dlatego:

- *System powinien działać w małej, zabezpieczonej, specjalnie do tego celu przeznaczonej sieci serwerów, utrzymujących rządowe kopie rejestrów wraz z zapasowymi kopiami offline*
- *Klientom należy rekomendować utworzenie własnych sieci rejestrów, zapewniając doradztwo i uaktualnianie zabezpieczeń z zasobów serwerów rządowych*

- *W przypadku podejrzenia poważnego ataku system musi mieć możliwość awaryjnego odcięcia od sieci*

Zapewne jednak najpoważniejszym zagrożeniem dla każdego systemu wspieranego przez rząd jest brak zainteresowania. Jeśli będzie zbyt skomplikowany lub nie będzie oferował funkcji, na które jest zapotrzebowanie, nie przyjmie się.

Innym zagrożeniem, które pojawiło się niedawno, jest przejęcie, czy też rozdzielenie systemu za pomocą konkurencyjnego oprogramowania.

Kryptoanalityk Nicolas Courtois z University College London, który uważnie przygląda się bitcoinowi, pisał w sierpniu 2015 r.:

"Powstaną nowe możliwości wydobywania bloków z nowym numerem wersji i nowymi zasadami. Dzięki temu bitcoin ma się stać bardziej demokratyczny: większe bloki, więcej transakcji na sekundę, niższe opłaty, a w konsekwencji większe zainteresowanie. Obecny bitcoin osiągnął w ostatnich miesiącach kres swoich możliwości (nie da się wykonać więcej niż trzy transakcje na sekundę). Społeczność bitcoina nie zdołała rozwiązać tego problemu".

To pokazuje, że projektowanie wspieranego przez rząd rozwiązania musi być poprzedzone poważnym namysłem nad możliwym postępem technologicznym i sposobami zabezpieczenia systemu przed wykorzystaniem nowych technologii do przejęcia go przez inne podmioty – wrogie lub nie.

REKOMENDACJE DOTYCZĄCE BEZPIECZEŃSTWA

Dla każdej dziedziny, w której ma być zastosowana nowa technologia, rząd powinien odrębnie przeanalizować możliwe zagrożenia. Żadne państwo nie jest co prawda zainteresowane zakłócaniem działania bitcoina, ale może być zainteresowane atakiem na państwową cyfrową walutę Wielkiej Brytanii. A jeśli dzięki tworzeniu fałszywych wpisów do rejestru można będzie osiągnąć korzyść finansową, z pewnością przestępczość zorganizowana zechce wykorzystać taką możliwość, wykorzystując użytkowników niedostatecznie dbających o bezpieczeństwo.

Biorąc pod uwagę zidentyfikowane zagrożenia, rząd powinien przyjąć odpowiedni poziom zabezpieczeń wobec każdego potencjalnego ataku. Należy też zaplanować to, jak długo dane rozwiązanie będzie w użyciu.

Jeśli można spodziewać się cyberataków na konkretny system, to od początku należy go projektować z myślą o zabezpieczeniach. Np. działanie sieci rejestrów niewymagających uwierzytelniania można zakłócić poprzez włączenie do nich własnego serwera lub przypuszczenie ataku typu DDoS na legalny serwer funkcjonujący w sieci.

Aby temu przeciwdziałać w dłuższym okresie może okazać się konieczne wprowadzenie autoryzacji odpornej na ataki ze strony algorytmów kwantowych.

Generalnie łatwiej jest zbudować nową infrastrukturę wykorzystywaną dla zapewnienia bezpieczeństwa niż przystosować istniejącą, aby pełniła nowe funkcje. Specjalnie stworzony zestaw uprawnionych serwerów będzie łatwiej skonfigurować i zabezpieczyć niż zmienić przeznaczenie istniejących serwerów internetowych. Doradztwo w zakresie budowania systemów bezpieczeństwa świadczy UK Government Communications Headquarters (GCHQ) lub działające na rynku renomowane firmy.

Systemy, które w zamierzeniu mają działać przez długi czas, od początku powinny być projektowane z myślą o łatwej modernizacji poszczególnych komponentów w kolejnych latach użytkowania (wymiana na nowe komputerów stanowiących węzły sieci, aktualizacja algorytmów szyfrowania, które przestały być bezpieczne).

Testując nowe rozwiązanie, ważne jest, aby dokonać prób podatności na penetrację – zarówno na poziomie systemu jak i użytkownika. Prawdziwe zagrożenie zapewne samo się nie ujawni na etapie prototypu, co nie oznacza, że potencjalni przestępcy nie będą zainteresowani atakiem na system uruchomiony w pełnej skali.

WYZWANIA ZWIĄZANE Z PRYWATNOŚCIĄ

Kryptowaluta bitcoin od początku była projektowana z myślą o zapewnieniu pseudoanonimowości (jej twórca Satoshi Nakamoto mówił o anonimowości, ale to niewłaściwe określenie).

Użytkownicy mogą tworzyć wiele portfeli do przechowywania bitcoinów. Nie ma ograniczeń co do liczby portfeli, ani weryfikacji tożsamości KYC (Know Your Customer) przy tworzeniu portfela. Pieniądze są przelewane z jednego portfela do drugiego. Związki między portfelami a ich właścicielami są ukryte, co zapewnia pewien poziom dyskrecji.

Decyzja, aby wykorzystywać pseudoanonimowe tożsamości i nie łączyć portfeli z żadnym zewnętrznym mechanizmem identyfikacji, była jedną z przyczyn, które zdecydowały o popularności bitcoina. Większość państw nie ma niezawodnego sposobu, pozwalającego powiązać tożsamość rzeczywistej osoby z transakcją internetową (gdyby taki mechanizm istniał, bitcoin by nie powstał, ani wtedy, ani dziś). Ponadto, biorąc pod

uwagę międzynarodowy charakter sieci bitcoin, nie bardzo wiadomo które władze miałyby zapewnić weryfikację tożsamości użytkowników, ani czy dane władze mają prawo do identyfikowania konkretnej osoby.

W końcu, gdyby operator wymagał potwierdzania tożsamości przy tworzeniu portfeli, zagrożona mogłaby być wymienialność bitcoinów jako waluty: skoro tożsamość mogłaby zostać zweryfikowana negatywnie, to operator mógłby zablokować danego użytkownika, w praktyce nie uznając wartości bitcoinów znajdujących się w jego portfelu. Inni użytkownicy nie mieliby w takich okolicznościach pewności, że wartość bitcoinów, z użyciem których dokonują transakcji, będzie uznawana.

Dzięki rezygnacji z weryfikacji tożsamości, możliwe było tak szybkie i globalne przyjęcie się bitcoina, ponieważ nie było potrzeby korzystania z niekompletnej lub nieistniejącej infrastruktury weryfikacyjnej.

Jednak ukrycie relacji między użytkownikiem a portfelem nie zapewnia pełnej anonimowości. Łańcuch transakcji, wpływów i obciążeń portfela oraz pomiędzy portfelami, jest widoczny dla każdego. Można go więc śledzić i analizować. Sarah Meiklejohn i jej koledzy z University College London wykazali, że można prześledzić kolejne transakcje w łańcuchu bloków bitcoina i np. powiązać kilka przypadków kradzieży bitcoinów ze specyficznymi próbami wymiany bitcoinów na inną walutę.

To może skutkować wprowadzeniem jakiegoś rodzaju praktyki Know Your Customer, ponieważ, gdy uda się ustalić adres konkretnego portfela i powiązać go z realną osobą, możliwe będzie zapoznanie się ze wszystkimi transakcjami tej osoby.

To właśnie połączenie jawności łańcucha transakcji bitcoinami z ułomną pseudoanonimowością jest zagrożeniem dla prywatności.

W przypadku tradycyjnych płatności online szczegóły znają tylko dwie strony transakcji i ich instytucje finansowe (banki). Płatności bitcoinami – łącznie z użytymi portfelami, przybliżonym czasem transakcji i kwotą – są zapisane w dostępnym publicznie łańcuchu bloków. Każdy może analizować blockchain i wyciągać wnioski na temat np. obrotów internetowego sklepu, profilu klienta oraz na temat transakcji pomiędzy osobami prywatnymi. Wcześniej ta wiedza była wcześniej zastrzeżona dla instytucji finansowych i organów ścigania.

REKOMENDACJE DOTYCZĄCE PRYWATNOŚCI

Wiele technik i alternatywnych kryptowalut, pojawiło się jako propozycja zminimalizowania problemu z prywatnością we w pełni jawnym blockchainie.

Pierwszym z pomysłów jest system "mieszania". W tego typu rozwiązaniach środki są pobierane od użytkowników i przekazywane odbiorcom poprzez inne adresy, niepowiązane z początkowymi użytkownikami. Wyeliminowanie bezpośredniego połączenia między płacącym a przyjmującym płatność zapewnia pewien poziom anonimowości. Jednakże są dwa poważne problemy, związane ze stworzeniem takiego systemu. Po pierwsze anonimowość, którą taki system oferuje nie jest doskonała: chociaż pieniądze mogą trafić do wielu różnych adresów, to już wśród możliwych portfeli bitcoina trudniej jest im się zagubić. Dzięki tym częściowym informacjom możliwe jest użycie narzędzi statystycznych, np. tzw. Statistical Disclosure Attacks, aby odkryć tożsamość osób dokonujących regularnych transakcji (osobną kwestią jest to na ile skuteczne są tego typu ataki). Po drugie możliwe jest oszustwo ze strony systemu, który pobiera pieniądze, ale ich nie wypłaca. Istnieją oferty, które mierzą się z tym ryzykiem (np. Mixcoin). W tym systemie część operacji "mieszania" jest jawna, co ma zapewnić uczciwość bez utraty prywatności.

Druga grupa proponowanych technik znacząco zmienia sposób dokonywania płatności bitcoinami i zapis w blockchainie, co znacząco poprawia zachowanie poufności. Przykładowo Zerocoin, Zerocash, Pinocchio Coin i niektóre protokoły Sigma wykorzystują w swoich transakcjach algorytmy grupowego podpisu. Jest to poświadczenie, że użytkownik z listy (bez wyszczególnienia który) ma środki konieczne do dokonania transakcji, jednocześnie ujawniona zostaje część informacji, aby uniknąć dwukrotnego wykorzystania tych samych środków. To pozwala użytkownikowi dokonać płatności bez możliwości bezpośredniego śledzenia jego wcześniejszych transakcji. Jednak, podobnie jak w przypadku technik mieszania, możliwe jest ukrycie tożsamości poszczególnych użytkowników, ale ich grupa jest zamknięta i nieliczna, możliwe jest więc odkrycie tożsamości poprzez analizę wielokrotnych transakcji. Jednak można je uznać za solidne, jeśli chodzi o zapewnienie uczciwości transakcji. Pozwalają też uniknąć użycia systemu mieszania, który może budzić wątpliwości, jeśli chodzi o zaufanie.

ROZDZIAŁ 5: Potencjał rewolucyjny

Technologie rejestrów rozproszonych (blockchain/DLT) stanowią znaczące wyzwanie dla dzisiejszych modeli zarządzania i prowadzenie biznesu. Innowacje techniczne, takie jak DLT mogą zapoczątkować rewolucyjne zmiany w przedsiębiorstwach, prowadząc do poważnych zmian w sposobie organizacji i zarządzania całą gospodarką i w rezultacie społeczeństwem. Takie zmiany idą dalej niż zwykłe innowacje, dotyczące produktów, usług lub sposobów działania firm.

Autor: Phil Godsiff, starszy pracownik naukowy, Surrey Centre for the Digital Economy, Surrey Business School, University of Surrey

WPROWADZENIE

Innowacje technologiczne mogą mieć omgromny wpływ na sposób działania przedsiębiorstw. Nowa technologia może umożliwić firmom oferowanie nowych produktów, zdobycie nowych źródeł przychodu, wdrożenie tańszych procedur i usprawnienie struktury organizacyjnej. Jeśli istniejące na rynku przedsiębiorstwa zbyt wolno przyjmują zmiany albo próbują je blokować, nowi gracze mogą wykorzystać innowacje do zdobycia przewagi i wyparcia dotychczasowych liderów.

Gdy innowacja jest wystarczająco radykalna, to może prowadzić do rewolucyjnych zmian nie tylko w modelach biznesowych i produkcji przemysłowej, ale w sposobie w jaki zorganizowane i rządzone jest społeczeństwo. Np. silnik parowy doprowadził do rozwoju kolei i umożliwił migrację ludności do dużych miast.

Technologie rozproszonych rejestrów (blockchain/DLT) mają potencjał rewolucyjny większy niż nowe produkty, usługi, źródła przychodu i reguły organizacyjne, możliwe do wdrożenia w ramach istniejących struktur gospodarczych. DLT mogą zakłócić funkcjonowanie całej gospodarki i społeczeństwa. Zrozumienie tego faktu pomoże nam określić jakie szanse daje nowa technologia i z jakimi się wiąże zagrożeniami, a w konsekwencji jakie zmiany wymusza w działalności rządu.

ROLA INNOWACJI

Organizacje stale wprowadzają innowacje, aby zyskać przewagę konkurencyjną. Zwykle myślimy o innowacjach jako o nowych produktach, albo procesach: produkty innowacyjne wprowadza zwykle przemysł, zaś sektor usług rozwija się poprzez innowacje w procesach. Nawet niewielkie zmiany mogą mieć wpływ na kształt rynku.

Np. wielu wytwórców napędów dysków komputerowych nie poradziło sobie, gdy pojawiła się technologia umożliwiająca produkcję mniejszych i lżejszych napędów. Innowacją może być również zmiana modelu biznesowego, prowadząca np. do powstania nowego typu relacji między firmami, nazywanej kooperacji rywalizującej, w której firmy jednocześnie kooperują i rywalizują. Dziś, dzięki rewolucji cyfrowej, mamy coraz większą świadomość tego, że innowacja może objawiać się na poziomie modelu biznesowego, a nawet na poziomie całej branży – wystarczy pomyśleć o tym jak aplikacja Uber, umożliwiająca łączenie pasażerów z kierowcami, zaburzyła działanie rynku usług taksówkarskich. Zmiana strategii przedsiębiorstwa – z myślenia o krótkoterminowym zysku na myślenie o długoterminowym budowaniu bogactwa – może prowadzić do radykalnych zmian w działalności i w wizji przyszłości i objawiać się np. użyciem oprogramowania typu open source do budowy platformy, którą inni mogą wykorzystywać i modyfikować.

NA CZYM POLEGA REWOLUCYJNY POTENCJAŁ DLT?

Technologie rozproszonych rejestrów są w stanie doprowadzić do radykalnych zakłóceń. Potencjał ten wynika z postępu w dziedzinie oprogramowania, do którego

już się przyczyniły (np. w kryptografii i inżynierii oprogramowania); z innowacji, jakie umożliwią w różnych branżach (np. usługach finansowych, nieruchomościach, opiece zdrowotnej, zarządzaniu tożsamością); z usprawnień w przetwarzaniu danych, jakie oferują (niski koszt, krótki czas, odporność na zniekształcenia). Ale potencjał rewolucyjny DLT wynika również z filozofii, na której są oparte, filozofii konsensusu, open source, przejrzystości i społeczności.

Innowacje technologiczne, takie jak aplikacje, oferują obecnie klientom bardziej aktywną rolę – sprawiają, że klienci "przyciągają" rozwiązania, a nie są biernymi odbiorcami ofert producentów. To podważa nasze dotychczasowe wyobrażenie o wytwarzaniu wartości, wprowadzając nowe koncepcje np. "prosumpcjonizm" (model stosowany np. przez usługę BlaBlaCar lub Airbnb, w którym ta sama osoba jednocześnie oferuje usługę i z niej korzysta – jest jednocześnie producentem i konsumentem), pożyczki społecznościowe lub crowdsourcing. W obliczu takich innowacji zmiany wpływają na strukturę istniejących branż i mają szansę tworzyć nowe branże, zmieniając definicje uczestników rynku, którzy "tworzą" i tych którzy "nabywają".

Rozwój systemów płatności mobilnych, oferowanych przez nowe na rynku podmioty, pozwala poszerzyć grupę klientów (np. dzięki temu, że mały sprzedawca może zmienić swój telefon w czytnik kart bankowych). Nieużywane wcześniej dane są wykorzystywane do pozyskiwania nowych źródeł dochodu. Rośnie wykorzystanie wirtualnych portfeli i wzrasta zainteresowanie płatnościami innymi niż bankowe, takich jak oferowane przez dostawców usług komórkowych (np. M-Pesa). Jednakże w wielu z tych przykładów, podstawowej transakcji dokonuje jednak tradycyjna instytucja w oparciu o państwowe regulacje prawne (np. banki albo operatorzy kart płatniczych jak Visa czy Mastercard). M-Pesa rzuciła wyzwanie założeniu, że transakcje wymiany walut i przelewy pieniężne muszą być dokonywane przez banki i przeskoczyła kilka stopni w rozwoju. Ale te innowacje nadal opierają się na istniejącej strukturze hierarchicznej, wykorzystują zastrzeżone technologie i pośredników, którzy są gwarantem zaufania. Zmiany co prawda zwiększają wygodę klientów i obniżają koszty, ale mają charakter raczej ewolucyjny niż rewolucyjny.

REWOLUCJE TECHNOLOGICZNE

Innowacje generalnie zachodzą w sposób ciągły, ale są naznaczone epizodami radykalnego postępu, opisywanymi przez ekonomistę Josepha Schumpetera jako "twórcza destrukcja", a przez Carlotę Perez jako "rewolucje technologiczne". Takie innowacje zachodzą w złożonej przestrzeni na pograniczu technologii, gospodarki i społeczeństwa. Czasami mogą fundamentalnie zmienić sposób, w jaki gospodarka lub społeczeństwo są zorganizowane.

W ciągu ostatnich kilku stuleci dokonało się kilka takich technologicznych rewolucji. Były to np.: pierwsza rewolucja przemysłowa, rozwój kolei, rewolucja przemysłu naftowego. Każda z nich doprowadziła do zmian w strukturze przemysłu, wprowadziła na rynek nowe źródło energii i miała wpływ na organizację społeczeństwa. Teraz doświadczamy rewolucji informatycznej i telekomunikacyjnej, charakteryzującej się dostatkiem informacji, usieciowieniem ludzi, specjalizacją i globalizacją.

Zwykle rewolucje opierają się na trzech filarach: znaczącym obniżeniu kosztów, nowych sposobach komunikacji i zmianach w infrastrukturze i logistyce. Obniżenie kosztów produkcji powoduje napięcia na rynku – często też doprowadza do baniek spekulacyjnych i krachów – co ostatecznie prowadzi do żądania zmian w istniejących instytucjach. Według Perez, w rewolucyjnych innowacjach występuje "zespół wzajemnie powiązanych radykalnych przełomów, składających się na konstelację wzajemnie od siebie zależnych technologii" oraz "silne połączenie zaangażowanych systemów, pod względem ich technologii i rynków oraz ich zdolność do głębokiej transformacji reszty gospodarki (i w końcu społeczeństwa)".

	Rodzaj rewolucji	Rok (około)	Nowe technologie I branże	Nowa infrastruktura	Powszechne zmiany
1	Rewolucja przemysłowa	1770	Mechanizacja przemysłu	Canały i energia wodna	Produktywność fabryk, Lokalne sieci
2	Silnik parowy i kolej	1830	Silnik parowy, maszyny żelazne	Koleje, telegraf, porty	Gospodarka aglomeracji, Standaryzacja części, urbanizacja
3	Stal, elektryczność, inżynieria	1875	Tania stal, ciężka chemia	Sieci elektryczne, transport globalny	Biznes oparty na efekcie skali, integracja pionowa, nauka jako potencjał produkcyjny, wydajność
4	Ropa naftowa, samochody, produkcja masowa	1910	Samochody, tanie paliwa, petrochemia, udogodnienia w domu	Sieć dróg, powszechna elektryfikacja	Produkcja masowa, integracja pozioma, standaryzacja produktów, dostatek energii, rozwój przedmieść
5	Informatyzacja i telekomunikacja	1970	Tanie mikroczipy, komputery, telefonia komórkowa	Globalna komunikacja elektroniczna	Dostatek informacji, zdecentralizowane sieci, wiedza jako kapitał, branże oparte na specjalizacji, globalizacja

Tabela 1: pięć rewolucji technologicznych (na podstawie prac Perez)

Każda rewolucja technologiczna przynosi powszechne zmiany w sposobie działania przedsiębiorstw i społeczeństwa, począwszy od mechanizacji w fabrykach, poprzez efekt skali i integrację pionową, masową produkcję i standaryzację, aż do specjalizacji, piramid hierarchicznych i biurokracji oraz dzisiejszego natłoku informacji i zdecentralizowanych sieci, podporządkowanych zasadom: "heterogeniczności, różnorodności, zdolności do adaptacji i kooperacji". Wszystkie te rewolucje ostatecznie prowadziły do powstania nowych techniczno-ekonomicznych paradygmatów, z nową strukturą wydatków, nowymi szansami na innowacje i z organizacjami opartymi na znacznie zmienionych założeniach. W każdym paradygmacie, organizacje przechodzą rozwój wzdłuż krzywej "S": od zakłócenia wywołanego innowacją, poprzez jej użycie (i opór wobec niej) do dojrzałości i w końcu kolejnej zmiany.

Zmiany mentalnych schematów i zastąpienie ich czymś nowym wymagają zwrotu transformacyjnego, do którego potrzeba nowych umiejętności, cech i wiedzy, a to fundamentalnie zmienia sposób w jaki działa przedsiębiorstwo.

Wcześniejsze rewolucje technologiczne miały niewielki, lub zgoła żaden wpływ na hierarchiczną strukturę przedsiębiorstw i państwa. Tymczasem nasza nowa era technologiczna, jak sugerują niektórzy, umożliwi pojawienie się zjawiska "Collaborative Commons", w którym społeczeństwo kieruje się raczej interesem współpracującej grupy niż indywidualnym zyskiem. To mogłoby oznaczać powstanie rozproszonych, działających w oparciu o konsensus, społecznych struktur, które nie byłyby zależne od zorganizowanych w sposób hierarchiczny pośredników (np. banków lub rządów). DLT może oznaczać, że przed dokładnie takim wyzwaniem staniemy.

PRZYKŁAD 1 – Diamenty

Leanne Kemp, założycielka i prezes Everledger

Branża diamentów jest bardzo podatna na wykorzystanie w celach kryminalnych. Kamienie są małe i łatwe do przetransportowania w ukryciu. Zwykle transakcje są poufne, a diamenty utrzymują swoją wartość przez wiele lat. Z tego powodu diamenty są używane do prania pieniędzy i finansowania terroryzmu na skalę globalną.

Jednym ze sposobów walki z tą nielegalną działalnością jest śledzenie pochodzenia diamentów poprzez papierową dokumentację. Ale manipulowanie dokumentami jest bardzo rozpowszechnione. Niekiedy dokumenty są wytwarzane, aby przykryć nielegalną transakcję. Wiele krajów, w których ma miejsce znaczący obrót diamentami, nadal nie ma dostatecznie dopracowanych przepisów zapobiegających przestępczej działalności.

Aby poradzić sobie z tym problemem, branża wydobycia i handlu diamentami wdraża system o nazwie Everledger, oparty na technologii łańcucha bloków. Pozwala to stworzyć "cyfrowy paszport" dla każdego diamentu. Zawiera on informacje o jego pochodzeniu, podróżach i transakcjach, których był przedmiotem z użyciem kryptograficznego "odcisku palca".

System ma trzy etapy:

- *Utworzenie e-ID (elektronicznej tożsamości) dla każdego diamentu, poprzez wprowadzenie do miarodajnego rejestru łańcucha bloków danych o jego cechach charakterystycznych i laserowo wygrawerowanego numeru seryjnego*
- *Przypisanie cyfrowego paszportu do diamentu, w celu dokumentowania jego podróży, historii transakcji i pochodzenia*
- *Monitorowanie, aby nie doszło do nielegalnych działań lub podejrzanych manipulacji*

Poprzez użycie niemodyfikowalnego blockchaina do przechowywania tych danych, rejestr umożliwia transparentny obrót wszystkimi diamentami, ujawniając ich pochodzenie, pozwalając śledzić zmiany właścicieli i ewentualną obróbkę. Ten rejestr może służyć jako źródło pewnych informacji o diamentach dla biznesu, rządów, rynku detalicznego, kontroli granicznej i organów ścigania.

System umożliwia także użycie inteligentnych kontraktów – warunki sprzedaży i transportu diamentów będą spełniane automatycznie. Dzięki użyciu łańcucha bloków do stworzenia rozproszonego rejestru, można dopuścić wgląd w inteligentne kontrakty, aby zweryfikować relacje i i współpracę przedsiębiorstw. Przejrzystość blockchaina daje możliwość egzekucji warunków kontraktu, niezależnie od tego czy dotyczy on zmiany właściciela diamentu, jego ubezpieczenia, tytułu własności itd. Potwierdzenie transakcji wraz z udokumentowanym dowodem autentyczności stanowi ważną dokumentację dowodową dla rządu i organów ścigania.

Technologie rejestrów rozproszonych

Blockchainy/DLT są częścią potencjalnie rewolucyjnych innowacji w wielu powiązanych ze sobą dziedzinach: wirtualne waluty, rozproszone otwarte i jawne prowadzenie dokumentacji, niehierarchiczne systemy sieciowe, kryptografia i inżynieria oprogramowania. DLT stanowią innowację mogącą wywołać zmianę z gatunku tych bardziej radykalnych, ze względu na swoje potencjalne oddziaływanie na wiele obszarów modelu biznesowego: od nowych produktów i usług, poprzez sposoby działalności i struktury organizacyjne firm, aż do nieznanej liczby branż, na które mogą mieć wpływ. Mogą więc stanowić część wzajemnie powiązanych, połączonych ze sobą przełomów, z których składa się rewolucja technologiczna.

Blockchainy oferują znaczącą obniżkę kosztów działalności. Są nie tylko tanie same w sobie, ale też pozwalają uniknąć dublowania zadań i nieefektywności w kontroli i koordynacji poprzez uruchomienie publicznych, otwartych rejestrów, mogących działać na poziomie całych branż (dzięki temu redukujących stałe wydatki na procesy takie jak porównywanie danych z odrębnych, prowadzonych przez różne podmioty rejestrów i baz danych). Zdolność do cyfrowego zapisania i bezpiecznego przechowywania informacji o praktycznie dowolnych zasobach, od diamentów do worków ryżu, pozwala organizacjom ustalać i śledzić, gdzie dane dobra się znajdowały i czyją były własnością (zob. Przykład 1. "Diamenty" s. 50). Nowe metody dokumentowania zobowiązań i transferu wartości z użyciem programowalnych kontraktów są rozwijane przy użyciu blockchain/DLT: np. Ethereum jest zdecentralizowaną platformą "inteligentnych kontraktów" (zob. Rodział 1). Ich potencjał do zakłócenia rynku może sięgać nawet przeobrażenia krajobrazu rynku, w którym pośrednicy (zaufani lub wymagani przez prawo), funkcjonujący w hierarchicznym monopolu zredukują swą liczbę lub zostaną zastąpieni przez bardziej otwarte, spłaszczone, oparte na społecznościach struktury, działające w oparciu o konsensus (zob. Przykład 2. "Komunikaty" s. 53).

Rozwój DLT i powiązanych z nimi technologii daje także możliwość rejestrowania w czasie rzeczywistym transakcji i połączeń, sprawiając, że transakcje są realizowane szybciej i taniej (zob. Przykład 3. "SETL" s. 56). Np. składka na ubezpieczenie komunikacyjne byłaby wyliczana w oparciu o stan samochodu i kierowcy. Ale różni ubezpieczyciele mogliby pobierać różne prowizje, w zależności od rodzaju swojej działalności, ceny ubezpieczenia i skłonności do podjęcia ryzyka. To mogłoby

doprowadzić do "gospodarki programowalnej", w której funkcjonowałyby inteligentne kontrakty – opartej na zdecentralizowanych sieciach i instrumentach wymagających mniej zaangażowania ludzi – która działałaby jak rozproszona, autonomiczna organizacja, oferująca różnorodne produkty i usługi.

? *FAQ – JAKIE ZAGROŻENIA WIĄŻĄ SIĘ Z DLT? (ZE STR. 57)*

Jak każda radykalna innowacja, DLT stwarza szanse dla podmiotów obecnych na rynku, ale też zagrożenia dla tych, którzy nie zareagują na czas. Ze względu na swoją naturę – rozproszenie i regulacje oparte na konsensusie, DLT są także zagrożeniem dla zaufanych pośredników, pełniących rolę kontrolną w strukturze hierarchicznej. Blockchainy, które dosłownie tworzą nowe waluty (jak bitcoin), rzucają wyzwanie wiodącej roli rządów, jako podmiotów zarządzających państwową i międzynarodową polityką monetarną i gospodarczą.

Najlepszym przykładem działającego blockchaina/DLT jest kryptowaluta bitcoin, a najbardziej oczywistym sektorem, w którym DLT może przynieść innowacje, jest branża usług finansowych. Blockchainy oferują obniżenie kosztów operacji przy istniejących strukturach i zarządzaniu, ale dają też szansę na uproszczenie systemu i poprawę jego wydajności. Mogą to zrobić przez eliminację dublowania kosztów utrzymywania oddzielnych systemów, będących własnością prywatnych firm i poprzez inną niż scentralizowana architekturę systemu. Np. tworzenie pieniędzy przestaje być wyłączną prerogatywą rządów państw. Zamiast tego mogą pojawić się nowe waluty, a tożsamość i połączenia pomiędzy ludźmi będą służyły do zatwierdzania i zabezpieczania transakcji w obrębie społeczności.

Dalszy rozwój, uruchomiony przez postęp technologiczny zbliża nas do możliwości dodawania do podstawowych kryptowalut informacji o konkretnych cechach (np. związanych z rzeczywistymi dobrami lub kontraktami) i tworzenia w ten sposób "kolorowych monet". To otwiera możliwość tworzenia pieniędzy niosących ze sobą nie tylko monetarną wartość. Mogą mieć atrybuty takie jak: przeznaczenie na konkretny cel, data ważności, lokalizacja dozwolonego użycia. W ten sposób można np. nałożyć na pieniądze restrykcje, dotyczące dóbr, które można za nie kupić (zob. Rozdział 6); albo można zablokować klucz elektroniczny osobie, która wynajęła mieszkanie przez Airbnb i nie zapłaciła w terminie, lub gdy czas wynajmu się skończył.

Przykład 2 – Komunikaty

Dominic Hobson, założyciel COOConnect

Firmy notowane na giełdzie są zobowiązane do publikowania w ujednoliconej formie swoich rocznych raportów. Jednak inne komunikaty, które mogą powodować reakcję ze strony udziałowców, są zwykle publikowane w formatach tekstowych lub pdf. Osoby, które chcą podjąć decyzję o dane opublikowane w komunikacie, muszą najpierw go przeczytać i zinterpretować.

Ponad 90 proc. komunikatów firm jest rozpowszechnianych przez media branżowe, a następnie przetwarzane na potrzeby inwestorów przez agenta, takich jak bank depozytariusz lub zarządający funduszem inwestycyjnym. Informacje są ręcznie wybierane z oryginalnego tekstu, interpretowane i ponownie spisywane przez poszczególnych pośredników. Poziom automatyzacji procesu jest niski, a błędy częste, co sprawia, że proces jest zdecydowanie niewydajny. Jeden z szacunków mówi o globalnych kosztach przetwarzania danych z komunikatów sięgających 10 miliardów dolarów rocznie. Depozytariusze często są zmuszeni rekompensować klientom straty wynikające ze źle wykonanych lub przeoczonych instrukcji.

Technologia blockchain może uczynić ten proces bardziej wydajnym. Komunikaty przedsiębiorstw stanowią kontraktową informację i wartość, która zasadniczo mogłaby być przekazywana bezpośrednio między stronami transakcji, bez konieczności użycia pośredników, o ile strony mają zaufanie do źródła informacji oraz niezbędną wiedzę, aby wykorzystać otrzymane dane.

Jeśli łańcuch bloków byłby powiązany z aplikacją, która pobiera i przechowuje dane z komunikatów w ustrukturyzowanym formacie, mógłby dostarczać dowodu na wiarygodność źródła i poświadczać datę wydania komunikatu. Aby wykonać, zawarte w nim, instrukcje możliwe byłoby odwrócenie kolejności działań. Rejestr rozproszony, oparty o taki blockchain, dawałby pozostałym stronom gwarancję, że informacja jest dokładna, aktualna, i niezmieniona od chwili opublikowania przez firmę. W teorii to pozwoliłoby wyeliminować wszystkich pośredników pomiędzy firmą, a inwestorem, gwarantując dokładność i punktualność przekazania informacji.

Ważną kwestią jest to, czy da się zorganizować taki system we w pełni zdecentralizowany sposób. Informacje w komunikatach firm różnią się od prostszych informacjach kontraktowych (np. takich, że pieniądze zmieniływłaściciela).

Często inwestorzy o udziałowcy muszą korzystać z pośredników, dysponujących fachową wiedzą.

Pośrednicy ci mogą chcieć zmodyfikować lub rozszerzyć dane przed przekazaniem ich dalej. Poza tym sam komunikat może ulec zmianie, jeśli firma opublikuje komunikat uzupełniający. Zmodyfikowane dane szybko tracą ciągłość kontaktu ze źródłem, ponieważ są poprzez media przekazywane dalej lub łączone w pakiety z innymi informacjami. Takim procesem nie jest łatwo zarządzać automatycznie.

Sama w sobie technologia łańcucha bloków jest na razie zbyt wolna, aby poradzić sobie z obsług≤ą transakcji w natężeniu porównywalnym do tradycyjnych sieci płatniczych, jak np. Visa. Blockchain bitcoina może obsłużyć ok. 20 tys. transakcji na godzinę, przy czym trzeba liczyć się z ok. godzinnym opóźnieniem w pełnym uwiarygodnieniu transakcji. Taki model byłby bardzo niewygodny w przetwarzaniu danych transakcyjnych np. w bankowości inwestycyjnej, ze względu na to że decyzje podejmuje się szybko i efekty są zależne od szybkości decyzji.

Firma Codel z Monmouth, zajmująca się przetwarzaniem danych z komunikatów firm, przezwyciężyła te ograniczenia, tworząc kombinację blockchaina i swojego elektronicznego systemu notarialnego. System ten generuje niemanipulowalny ciąg kontrolny zdarzeń, do którego wszystkie strony mogą się zwrócić w celu potwierdzenia ich autentyczności. To oferuje wartościową gwarancję pochodzenia danych. System współpracuje z Instant Actions, nowym centralnym wykazem informacji z komunikatów firm. Dane w wykazie są zapisane w formatach ISO 15022 i ISO 20022, które umożliwiają pozyskiwanie surowych danych finansowych z komunikatów w formatach zrozumiałych dla komputerów. To oznacza, że wykaz może być aktualizowany, gdy firma komunikat uzupełni lub zastąpi nowym. To gwarantuje rzetelność i dokładność danych, które mogą być dostępne dla wszystkich zainteresowanych stron przez zabezpieczoną sieć SWIFT. To pozwala uniknąć opóźnień związanych z weryfikacją występujących w blockchainach. Poza tym informacja – w praktyce współdzielona jako rejestr rozproszony – może być aktualizowana, przekazywana i modyfikowana w czasie rzeczywistym, dzięki czemu jest aktualna i prawidłowa.

Rząd mógłby pomóc rozwijać podobne systemy przez regulację, nakładającą na przedsiębiorstwa obowiązek publikowania komunikatów przy użyciu rejestrów rozproszonych.

UWAGI DLA RZĄDU

Rząd przeprowadza wiele różnych operacji ze względu na swoich dużą liczbę swoich interesariuszy, usług i powinności. Niektóre z tych operacji polegają na dystrybucji wartości (bardziej niż na jej tworzeniu). Inne służą nałożeniu i utrzymaniu skutecznego rygoru regulacyjnego. Wiele z tych aktywności zostanie usprawnionych dzięki innowacjom dostarczonym przez blockchain/DLT, a inne będą zagrożone. Zmiana może nastąpić na poziomie produktów i usług, ale też na poziomie organizacji i sposobów działalności. Przykładowo sposób dbania o to, aby przelewy środków, jak wypłaty świadczeń dla obywateli, trafiały do właściwych osób, może być udoskonalony na wiele sposobów (zob. Rozdział 6). Pojedynczy rejestr, zawierający informację o tożsamości i uprawnieniach potencjalnych beneficjentów, aktualizowany w czasie rzeczywistym, mógłby stanowić radykalną innowację, o wiele bardziej wydajną, poprzez redukcję kosztów zarówno działalności, jak i budowy. Do konkretnych płatności można by dodawać atrybuty, przez co kwoty, cel i terminy wydawania środków można by określić lub śledzić. To oczywiście wymagałoby przeprowadzenia intensywnych negocjacji z interesariuszami. Mogło by to też wymagać wdrożenia jakiegoś rodzaju polityki monetarnej wobec tej formy waluty, aby osiągnęła ona pożądany kurs wobec funta.

Istnieją też innowacyjne możliwości zastąpienia hierarchicznych organizacji bardziej rozproszonymi systemami. Rząd i jego agencje zwykle składają się ze szczebli władzy, zarówno jeśli chodzi o wewnętrzne struktury, jak i całość systemu. Przykładowo obywatele reprezentowani są przez wybranych urzędników w lokalnych, państwowych i międzynarodowych instytucjach. Finansami zajmują się banki, izby rozliczeniowe, banki centralne i rządy. Można sobie wyobrazić, że zamiast poprzez okresowe wybory, oparte na papierowych dokumentach, demokracja realizowałaby się dzięki blockchainom, w których wyborcy mieliby wirtualne portfele i głos w postaci "monety". Może to potencjalnie zredukować liczbę błędów i fałszerstw (ponieważ każdy wyborca będzie mógł sprawdzić czy jego głos został policzony), ale też doprowadzić do demokracji działającej w czasie rzeczywistym z głosowaniem w każdej sprawie. To oczywiście rodzi poważne pytania o odpowiedzialność społeczną oraz o chęć uczestniczenia w życiu publicznym, ale mogłoby być początkiem bardziej rozproszonej demokracji.

ZAGROŻENIA

Innowacje zapoczątkowane przez DLT mogą być atrakcyjne, ale niosą ze sobą pewne znaczące zagrożenia, w tym dotyczące natury pieniędzy oraz roli hierarchii i zaufania. DLT mogą zdezorganizować tradycyjne rynki usług finansowych, których główną działalnością są przelewy pieniężne i transfer wartości. Ale kryptowaluty, takie jak bitcoin, już teraz zakłócają funkcjonowanie pieniędzy w ich tradycyjnych formach i sposobach użycia, jako pieniądz bez wsparcia żadnego rządu. Podobnie jest z "kolorowymi monetami", które pozwalają dodawać do środków płatniczych atrybuty inne niż wartość nabywcza. Zarządzanie pieniądzem, a przez to gospodarką, jest postrzegane przez wielu jako kluczowa rola rządu, a alternatywne systemy monetarne mogą tej roli zagrozić.

DLT stanowią zagrożenie dla każdej struktury hierarchicznej, ze względu na swój sieciowy charakter oraz operowania w rozproszonych sieciach, bez pośredników (wymaganych ze względu na zaufanie lub regulacje) i ze względu na zastąpienie odgórnej kontroli konsensusem. Hierarchie mogą mieć poważne wady: dublowanie, dodatkowe koszty, potencjalne nadużycie władzy i ryzyko błędów w zarządzaniu finansami. Mogą mieć też jednak zalety, gdy np. jest potrzebny neutralny pośrednik lub w demokracji pośredniej. Demokracja pośrednia daje stabilność i ciągłość rządu, która mogłaby być zaburzona, gdyby DLT weszły do szerszego użycia. Państwa narodowe już teraz muszą stawiać czoła zagrożeniom, związanym z globalizacją i coraz bardziej płynnymi granicami, a przy tym część twórców i zwolenników bitcoina prezentuje ekstremalne antyrządowe poglądy. Wyzwaniem jest zapewnienie wykorzystania DLT i związanych z nimi innowacji, w celu tworzenia połączonego, poduktywnego społeczeństwa i przyjaznej infrastruktury.

Przykład 3 – SETL

Dominic Hobson, założyciel COOConnect

Clearing, usługi depozytariusza, rejestracja usług – wszystko to składa się na znaczny koszt emitowania, handlu i posiadania papierów wartościowych. Istnieje mrowie specjalistycznych agentów i stron trzecich, zaangażowanych w proces przepływu papierów wartościowych i gotówki pomiędzy inwestorami. Koszt stanowią nie tylko opłaty za poszczególne usługi, ale też koszty pośrednie, związane z koniecznością pogodzenia bezliku różnych systemów, które trzeba połączyć w jednym przedsięwzięciu biznesowym. Łącznie światowa branża finansowa płaci między 65 a 80 miliardów dolarów rocznie kosztów okołotransakcyjnych.

Technologia blockchain oferuje narzędzia mogące znacząco uprościć i zredukować koszt usług okołotransakcyjnych, umożliwiając stronom prowadzenie rejestru wspólnego, umiejscowionego na wielu serwerach, służących za węzły sieci. Upoważnienie do wykonywania transakcji nadaje publiczno-prywatna kryptografia dostępu.

Transakcje dodawane są do bazy danych w blokach, a każdy blok jest sprawdzany przez węzły. Dodanie bloku do bazy danych jest możliwe tylko wtedy, gdy węzły zgodzą się, że zawiera on wyłącznie prawidłowe transakcje. Poza utworzeniem i utrzymywaniem węzłów, sieć jest całkowicie autonomiczna i nie wymaga podmiotu kontrolnego.

Rozwiązanie SETL

Finansowana ze środków prywatnych inicjatywa o nazwie SETL zakłada stworzenie i wykorzystanie specjalistycznego blockchaina, który umożliwi graczom na rynku finansowym przeprowadzanie transakcji na papierach wartościowych w systemie peer-to-peer i utrzymywanie rozproszony, "złotego" rejestru rozliczeń gotówki i papierów wartościowych. W szczególności SETL dąży do tego by możliwe były transakcje w łańcuchu bloków z użyciem waluty emitowanej przez bank centralny. Projektowany blockchain będzie działał autonomicznie i zostanie zintegrowany z istniejącym rynkiem finansowym oraz infrastrukturą płatności i wymiany walut.

SETL będzie w stanie obsłużyć zarówno stronę gotówki, jak i stronę papierów wartościowych, a ponadto umożliwi jednostronny transfer pieniędzy lub papierów oraz proste płatności lub wykonanie uzgodnionych kontraktów, obsługę komunikatów firm, dywidend i obligacji.

SETL jest projektowany z myślą o obaleniu kosztownego i obarczonego ryzykiem procesu clearingu i przekazywania papierów wartościowych. Ma się on zamienić w obrót papierami w czasie rzeczywistym. Dodatkowo, poprzez utworzenie złotego rejestru własności, SETL znacząco ograniczy ogólne koszty rejestracji i obsługi papierów wartościowych.

Łańcuch bloków SETL będzie miał następujące cechy:

- *Publiczne klucze używane przez niego będą musiały być podpisane przez instytucję certyfikującą w taki sposób, aby dla wszystkich użytkowników było jasne kto posiada który certyfikowany klucz. Instytucje certyfikujące będą znały prawdziwą tożsamość użytkowników kluczy, będą też przeprowadzać kontrolę Know Your Customer i zapobiegającą praniu brudnych pieniędzy. SETL przewiduje, że instytucja ta będzie mogła udostępnić dane użytkownika na polecenie sądu.*
- *Łańcuch będzie miał moc obliczeniową wystarczającą do obsługi tysięcy transakcji na sekundę, współmierną do liczby normalnie realizowanych na rynku finansowym transakcji*
- *Będzie w stanie obsłużyć różne rodzaje zasobów, w tym gotówkę i wszystkie typy papierów wartościowych*
- *Pozwoli na dokonywanie transakcji podpisanych przez wiele stron, czyli na autoryzację przez wyszczególnioną grupę użytkowników*
- *Pozwoli na wykonywanie operacji atomowych (np. takich w których albo wszystkie transakcje są wykonywane albo żadna) sprawiając, że transakcje będą przeprowadzone tylko wtedy, gdy wszystkie etapy zostały zgłoszone i prawidłowo autoryzowane*
- *Będzie zawierał specyficzną funkcję, ułatwiającą zarządzanie płynnością finansową przez uczestników*
- *Będzie utrzymywał kompletną historyczną dokumentację transakcji i rozliczeń, aby ułatwić utrzymywanie dokumentacji organom kontrolnym oraz na potrzeby sprawozdawczości i audytu*

Dodatkowe korzyści:

Rozliczenia gotówki i innych zasobów obecnie zwykle są oparte na specjalistycznych systemach i mogą być wykorzystane wyłącznie do konkretnych celów, inaczej mówiąc są "systemowo specyficzne". Gotówka i zasoby przechowywane w blockchainie są, w przeciwieństwie do nich, możliwe do wykorzystania w dowolnym celu. To jednocześnie pomoże ograniczyć kwoty, które banki przeznaczają na rezerwy gotówkowe i uprości zarządzanie płynnością.

SETL przewiduje, że będzie działać we współpracy z istniejącym systemem obrotu papierami wartościowymi Banku Anglii – Real Time Gross Settlement (RTGS) i będzie bezpieczną oraz praktyczną alternatywą w czasie, gdy RTGS jest niedostępny. SETL będzie dostępny zawsze, co pomoże zredukować ryzyko transakcji międzybankowych, które obecnie kumuluje się w czasie przerw w pracy RTGS np. W nocy lub w weekendy.

System płatności i wymiany papierów wartościowych będzie prosty, jednolity i błyskawiczny. Jeśli to Wielka Brytania wdroży taki system jako pierwsza, będzie on promował Londyn i funta jako lokalizację i walutę preferowaną przez firmy z branży usług finansowych. W przypadku, gdy system powstanie już w Londynie, to prawdopodobnie przyjmie się szerzej, wzmacniając pozycję Londynu jako globalnego lidera w międzynarodowych operacjach finansowych.

Wnioski

Połączenie kreatywności i technologii może prowadzić do radykalnych zmian w istniejących modelach biznesowych i strukturach organizacyjnych, w których są one posadowione. DLT oferuje w tej chwili w tym samym stopniu wyzwania i niepewności dla istniejących struktur, co odpowiedzi i praktyczne możliwości.

Ale wydaje się, że ma przynajmniej kilka cech, i że pojawia się w odpowiednim kontekście, aby dokonać zmiany z gatunku tych rewolucyjnych.

DLT stanowi znaczące wyzwanie dla dominujących dziś przekonań i założeń dotyczących dobrych praktyk, nie tylko w branży dokumentowania transakcji i rejestrów. Te potencjalnie rewolucyjne struktury organizacyjne i praktyki powinny zostać przetestowane eksperymentalnie – być może w formie prototypów technicznych i nietechnicznych – w celu zbadania ich skutków praktycznych, prawnych i politycznych.

Radykalne innowacje w modelach biznesowych, zwłaszcza w strukturach i sposobie organizacji, mogą być wdrażane drogą eksperymentowania w luźnym, ale wydajnym środowisku prawnym.

Rząd powinien wziąć pod uwagę to, jak rygory regulacyjne mogą stworzyć i wykorzystać odpowiednie środowisko, w którym te oszczędne modele działalności oraz struktury organizacyjne mogą być testowane, przy swobodnym udziale potencjalnych nowych graczy.

Potrzebne są dodatkowe badania, na poziomie całego systemu, nad zyskami i kosztami stosowania technologii rozproszonych rejestrów. Korzystając z wyników, rząd mógłby określić jakie występujące dziś niepotrzebne koszty można by zredukować i gdzie jeszcze szukać oszczędności i okazji.

ROZDZIAŁ 6: Zastosowania w administracji centralnej

Autor główny:
Catherine Mulligan, Research Fellow, Imperial College London and Head of Digital Strategy and Economics, Future Cities Catapult.

Autorzy współpracujący:
Simon Taylor, VP for Blockchain R+D, Barclays; Mike Halsall, Global Grand Challenges, Singularity University, NASA Research Park, California

Technologie rejestrów rozproszonych już teraz mają głęboki wpływ na sposób zarządzania danymi w przedsiębiorstwach oraz na ich interakcje z klientami i dostawcami. Jeśli zostałyby wykorzystane w administracji państwowej, mogłyby zmniejszyć koszty, zwiększyć przejrzystość, zwiększyć dostęp obywateli do różnych usług finansowych oraz promować innowacje i wzrost gospodarczy. Poniższy rozdział podaje pięć przykładów, ilustrujących te korzyści.

WPROWADZENIE

Technologie rejestrów rozproszonych (DLT) potrafią o wiele więcej niż tylko obsługiwać transakcje prowadzone w walutach cyfrowych, jak bitcoin. Pomysły i struktury wykorzystane do stworzenia rejestrów rozproszonych (blockchainów, które wykorzystują kryptowaluty), bardzo łatwo przenieść i dostosować do innych obszarów działalności gospodarczej i społecznej. W związku z tym mają ogromny potencjał zastosowania w operacjach rządowych – w gruncie rzeczy, wpływ DLT na społeczeństwo brytyjskie może być tak samo znaczący jak wpływ przełomowych wydarzeń, takich jak uchwalenie Magna Carta.

Jeśli zostaną wykorzystane prawidłowo – przy dbałości o prywatność, bezpieczeństwo i ochronę tożsamości (zob. Rozdział 4) – technologie rejestrów rozproszonych stworzą rzeczywiste szanse dla rządu i władz lokalnych oraz regionalnych poprzez następujące usprawnienia:

- *Niższe koszty operacyjne, w tym ograniczenie oszustw i błędów w płatnościach*
- *Większa przejrzystość transakcji między agencjami rządowymi a obywatelami*
- *Zwiększenie dostępu do usług finansowych dla osób pozostających na obrzeżu systemu finansowego*
- *Niższe koszty ochrony danych obywateli przy jednoczesnej możliwości wymiany danych między różnymi podmiotami, pozwalającej na tworzenie targów informacji*
- *Ochrona kluczowej infrastruktury, takiej jak mosty tunele itp.*
- *Zmniejszony opór rynku, co ułatwi małym i średnim przedsiębiorstwom interakcję z lokalnymi i centralnymi władzami*
- *Promocja innowacji i możliwości rozwoju dla małych i średnich firm*

Ta szeroka gama potencjalnych korzyści zaistnieć może dzięki zastosowaniu DLT w trzech różnych obszarach:

- *Do obsługi walut*
- *Do zarządzania kontraktami i tworzenia nowych form kontraktów*
- *Do nowych zastosowań, zaproponowanych przez osoby trzecie i do poprawienia wydajności przeprowadzania różnego typu działań*

W tym rozdziale pokazujemy wszystkie powyższe szanse i ich praktyczne wykorzystanie w różnych technicznych obszarach, na pięciu przykładach. Są to:

- *Ochrona kluczowej infrastruktury przed cyberatakami*
- *Obniżenie kosztów i zwiększenie kontroli w systemie świadczeń społecznych, przy zwiększaniu dostępu beneficjentów do usług finansowych*
- *Przejrzystość i kontrola wydawania środków na pomoc zagraniczną*
- *Stwarzanie szans wzrostu gospodarczego, wzmacnianie małych i średnich przedsiębiorstw i wzrost zatrudnienia*
- *Ograniczenie oszustw podatkowych*

Przykład 1: Ochrona kluczowej infrastruktury

Streszczenie

DLT mogą umożliwić Wielkiej Brytanii i jej rządowi lepszą ochronę infrastruktury cywilnej przez cyberatakami

Informacje podstawowe

Technologie cyfrowe są coraz częściej osadzane w kluczowej dla kraju infrastrukturze, a wiele w tych systemów jest połączonych przez internet. To naraża je na ataki ze strony hakerów oraz ze strony innych państw. Ataki te mogą być przeprowadzone tak, że istniejące cyberzabezpieczenia nie będą w stanie ich wykryć. Możliwe jest np. przejęcie kontroli nad kluczowymi routerami w celu manipulowania nimi lub monitorowania ich aktywności.

To pozwoliłoby hakerom przechwycić dane firm i organizacji rządowych, korzystających z przejętych routerów. Ponadto, ponieważ coraz więcej technologii osadzonych jest w obiektach infrastruktury – w tym mostach, liniach kolejowych, tunelach, zaporach przeciwpowodziowych i instalacjach energetycznych – wzrasta ryzyko, że cyberatak spowoduje straty materialne lub zagrożenie dla życia ludzi.

Propozycja wykorzystania DLT

DLT może być użyte w celu zabezpieczenia systemu operacyjnego oraz oprogramowania kluczowego obiektu przed manipulacją. Rozproszony rejestr mógłby monitorować stan oprogramowania, sprawdzając, czy nie dochodzi do niedozwolonych zmian i upewniając się że nikt nie manipulował przy danych przekazywanych w technologii Internetu Rzeczy.

Efekty

- *Poprawa wydajności i skuteczności ochrony dużych obiektów infrastruktury, lepsza ochrona życia ludzi*
- *Zapewnienie wiarygodności przesyłanych danych od i do obiektu kluczowej infrastruktury*
- *Stopień rozwoju technologii*
- *Gotowa*

Przykład 2: Ministerstwo Pracy i Emerytur

Streszczenie

Nowe modele płatności umożliwią Skarbowi Jej Królewskiej Mości (HM Treasury) i Ministerstwu Pracy i Emerytur (Department for Work and Pension) wypłacanie świadczeń w sposób bardziej wydajny i poprawią wdrażanie zaplanowanej polityki z tym związanej. Dzięki zastosowaniu DLT w procesie rejestracji i wypłat rządowych świadczeń, ministerstwo pracy zyska lepsze narzędzia do:

- *Zapobiegania stratom spowodowanym oszustwami lub błędami*
- *Wspierania najbardziej potrzebujących obywateli przez oferowanie im pełnego włączenia do ekosystemu finansowego*
- *Wspierania innych celów polityki rządu, zwłaszcza walki z ubóstwem w zrównoważony sposób*
- *Dbania o zrównoważone i racjonalne wydatkowanie środków publicznych*

Informacje podstawowe

Ministerstwo Pracy i Emerytur wypłaca rocznie ok. 166 miliardów funtów, pochodzących z podatków obywateli, w postaci świadczeń socjalnych. Z tego około 3,5 miliarda jest wypłacanych niesłusznie, ponieważ dochodzi do oszustw (1,2 mld), pomyłek po stronie beneficjentów (1,5 mld) oraz pomyłek po stronie urzędów (0,7 mld). Zaledwie 930 mln z nadpłaconej sumy udaje się odzyskać. Dodając do tego oszustwa i pomyłki, do których dochodzi w systemie poboru podatków (który to obowiązek w najbliższych latach przejmie Ministerstwo Pracy i Emerytur w ramach nowych regulacji o nazwie Universal Credit – jednolita należność), łączna wysokość nadpłaty brutto wynosi przynajmniej 5 miliardów funtów.

Oprócz bezpośredniego finansowego kosztu wypłacania nienależnych pieniędzy, podatnicy ponoszą koszt interwencji w przypadku nieprawidłowości (ściąganie długu, śledztwo i ściganie, zapytania ze strony beneficjentów oraz negocjowanie porozumień).

Ponadto część środków (na razie nie ma dostępnych danych jaka), zostaje wydana niezgodnie z założonymi celami polityki społecznej, ale w mniej oczywisty sposób. Np. pomoc może pokrywać wydatki, związane z samą trudną sytuacją beneficjentów, jak np. spłata pozabankowych pożyczek lub "premia za ubóstwo".

Propozycja wykorzystania DLT

Wielu odbiorców świadczeń socjalnych nie korzysta z usług bankowych lub korzysta w ograniczonym zakresie i napotyka bariery w dostępie do tradycyjnych produktów finansowych, w budowaniu wiarygodności kredytowej i ponosi koszt transakcji w instytucjach niepodlegających kontroli. DLT daje możliwość wspierania tych beneficjentów i włączania ich w system korzystniejszych usług, przy niskich kosztach.

Cyfrowe tożsamości mogą być potwierdzane dzięki rozproszonym rejestrom, działającym na urządzeniach zabezpieczonych i zaszyfrowanych lub nawet przy użyciu oprogramowania na urządzenia mobilne, co pozwoliłoby odbiorcom otrzymywać świadczenia bezpośrednio, z pominięciem kosztów obsługi przez banki albo urzędy lokalne. To mogłoby pozwolić beneficjentom szerzej włączać się w system finansowy, przy wykorzystaniu bezpiecznych punktów odbioru środków, bardziej wiarygodnych niż konta bankowe. Takie rozwiązanie byłoby też powiązane z innymi systemami, aby ograniczyć oszustwa i pomyłki w procesie wypłacania świadczeń, jako że podrobienie tożsamości byłoby trudniejsze.

Takie działanie mogłoby pomóc w realizacji jednego z podstawowych celów Ministerstwa Pracy i Emerytur, mianowicie wydobywania obywateli z ubóstwa i uniezależniania od pomocy państwa. Dzięki innowacyjnemu zastosowaniu tych technologii, możliwe byłoby – za zgodą danego beneficjenta – ustalenie reguł wykorzystania środków. Urzędy mają więc dodatkowe narzędzie realizacji celów polityki, którego wykorzystanie mogą rozważyć.

Efekty

- *Ograniczenie strat powodowanych oszustwami i pomyłkami urzędników*
- *Umożliwienie urzędom wpływania na poprawę efektywności wydawania publicznych środków, czyli zapewnienia że będą przeznaczone na zaspokojenie rzeczywistych potrzeb*
- *Stopień rozwoju technologii*
- *Wymaga znacznej edukacji odbiorców świadczeń*
- *Wymaga integracji funta z technologią rejestrów rozproszonych*
- *Może spowodować wyodrębnienie się podkategorii w obrębie gospodarki i stygmatyzację "monet pomocowych"*

Przykład 3: Wzmocnienie systemu pomocy międzynarodowej

Streszczenie

DLT może być dla rządu narzędziem skuteczniejszej kontroli nad pomocą dla zagranicy. Za ich pomocą można lepiej czuwać nad tym by środki docierały do właściwych odbiorców. Dzięki DLT możliwa też będzie większa przejrzystość i lepsze włączenie beneficjentów skuteczne zarządzanie finansowe. Tym samym użycie DLT mogłoby pokazać wkład Wielkiej Brytanii w realizację Globalnych Celów ONZ.

Informacje podstawowe

Aby wywiązać się z międzynarodowych zobowiązań, kraje muszą realizować plan działania, związany z realizacją Globalnych Celów. Plan zakłada przejrzystość, odpowiedzialność i dbanie o uczciwość. Społeczność międzynarodowa kładzie nacisk to tworzenie systemów pomocy finansowej, które byłyby transparentne i odporne na malwersacje. Jednakże działania zapobiegające oszustwom, kradzieży i niewłaściwemu wykorzystaniu funduszy mogą być bardzo kosztowne. Postęp technologiczny, wzmacniający istniejące mechanizmy zabezpieczeń byłby więc bardzo korzystny dla systemu pomocy międzynarodowej.

Oszustwa i korupcja odbierają potrzebującym środki na walkę z ubóstwem, inwestycje czy edukację. Przy zastosowaniu DLT możliwe byłoby zapobieganie tym zjawiskom poprzez większą przejrzystość i kontrolę wydawania środków pomocowych. Wykazanie, że pieniądze są wykorzystywane we właści wy sposób, mogłoby zachęcić państwa do przeznaczania większych kwot na pomoc. Poza tym darczyńcy mogliby lepiej planować swoją pomoc, ze względu na cele, które chcą poprzez nią realizować.

Propozycja wykorzystania DLT

Propozycja wykorzystania rejestrów rozproszonych dla wsparcia systemu pomocy międzynarodowej opiera się na trzech głównych właściwościach DLT.

Po pierwsze społeczność międzynarodowa mogłaby przekazywać środki w walucie równej kursem z funtem brytyjskim z pominięciem procedur biurokratycznych i bankowych. Rejestry rozproszone umożliwiają to, ponieważ nie są ograniczone geograficznie – działają w ten sam sposób pod każdą możliwą jurysdykcją na świecie. Stwarza to możliwość redukcji kosztów wymiany walut. Ponadto pojawia się opcja tworzenia "inteligentnych kontraktów", umożliwiająca "tworzenie samogwarantujących, automatycznie wykonujących się kontraktów pomiędzy obcymi sobie stronami, oferujących obywa-

telom ramy działania dla transakcji niezależnych od narodowych władz sądowniczych i wykonawczych".

Po drugie, darczyńcy mogliby wykorzystać DLT do ograniczenia zamienności gotówki, oferując wiarygodne i nieodwracalne transfery dóbr cyfrowych – w tym przypadku środków na pomoc. Ponadto rejestry cyfrowe rozwiązują problem podwójnego wydatkowania. Podczas gdy niektóre cyfrowe waluty mogą stwarzać możliwość dwukrotnego wykorzystania tych samych środków, DLT zapobiegają temu, ponieważ każda "moneta" jest unikatowa. Dzięki temu możliwe jest przekazywanie środków bez pośredników. W przypadkach, gdy pieniądze mają bezpośrednio wesprzeć końcowego odbiorcę, możliwe jest pominięcie ograniczeń i restrykcji, nałożonych na waluty i usługi bankowe w niektórych krajach, poprzez transfery środków w systemie peer-to-peer.

Po trzecie, użycie unikatowych, powiązanych z funtem "monet" mogłoby zapobiegać wydatkowaniu środków w sposób niezgodny z intencją społeczności międzynarodowej. Np. pieniądze przekazane na budowę infrastruktury koniecznej do zwalczania ubóstwa, nie mogłyby być wydane na inny cel. Taką kontrolę umożliwia zdolność DLT do śledzenia kto i na co dokładnie wydał określoną pulę środków.

Efekty

- *Zwiększenie transparentności wydawania pomocy międzynarodowej, zwłaszcza przeznaczonej na realizację Globalnych Celów, w celu zmniejszenia korupcji i lepszej realizacji celów pomocy*
- *Stopień rozwoju technologii*
- *Niepewność co do oczekiwań darczyńców może stanowić większy problem niż oszustwa i korupcja, powinna więc być brana pod uwagę przy tworzeniu rozwiązań, jeśli mają one być efektywne*
- *W przypadku każdej pomocy międzynarodowej, darczyńcy utrzymują kontakt z miejscowym rządem. Jeśli jednak przypadki korupcji są powiązane z osobami z administracji kraju – odbiorcy pomocy lub wynikają z kształtu rządu, niezbędne będzie poparcie społeczeństwa danego kraju dla zastosowania nowego systemu pomocy*
- *Przekształcenie rejestrów rozproszonych w konkretne usługi dla powyższego zastosowania wymaga wypracowania wielu uzupełniających rozwiązań*

Przykład 4: Ograniczenie oporu rynku i wsparcie innowacji

Streszczenie

Jedną z największych potencjalnych korzyści DLT jest ich zdolność do znoszenia barier i oporu na rynku i umożliwienia powstania nowych form targów informacji. Jak pokazano w rozdziale 1., dzielenie się informacjami z użyciem rejestrów rozproszonych przez różne podmioty gospodarcze mogłoby zaowocować powstaniem nowych form innowacji. To pozwoliłoby administracji państwowej realizować cele polityki zogniskowanej na wspieraniu rozwoju małych i średnich przedsiębiorstw poprzez efektywne wykorzystanie innowacji technologicznych.

Informacje podstawowe

Zmniejszenie kosztów transakcji między małymi i średnimi przedsiębiorstwami a organami władzy państwowej pozwoliłoby tym przedsiębiorstwom swobodniej poruszać się na rynku, dzięki obniżeniu łącznych kosztów działalności. Jednocześnie, możliwość rejestrowania własności intelektualnej w rozproszonym rejestrze, zamiast poprzez tradycyjną procedurę patentową, może zredukować łączną liczbę sporów dotyczących umów. Spory dotyczące umów stanowią 57 proc. sporów sądowych w Wielkiej Brytanii, więcej niż jakakolwiek inna kategoria spraw sądowych.

Propozycja wykorzystania DLT

DLT mogłyby być wykorzystanie w wielu różnych obszarach, zwłaszcza do obsługi inteligentnych kontraktów i rejestracji zasobów. Dzięki rejestracji zasobów w rozproszonych rejestrach, każda własność mogłaby w praktyce stać się "inteligentnym zasobem", dając solidną i wiarygodną dokumentację bardzo różnorodnych usług i stanu posiadania. Dziś znacznych nakładów czasu i pieniędzy wymagają od małych i średnich przedsiębiorstw procedury związane z ochroną własności intelektualnej i patentami, testamentami, poświadczeniami notarialnymi, rejestrowaniem i pozyskiwaniem danych w systemie ochrony zdrowia NHS oraz w państwowym systemie emerytalnym i indywidualnych planach emerytalnych (Self-Invested Personal Pension – SIPP). Rejestry rozproszone dają nowe możliwości wydajnego koordynowania wszystkich tych usług.

Rejestry rozproszone dają ponadto możliwości obsługi mikropłatności, zdecentralizowanej wymiany walut, transakcji tokenami i innych transferów, w sposób, który w ramach tradycyjnych technologii sieciowych nie jest możliwy. W rezultacie DLT mają potencjał do kształtowania na nowo kosztów działania władz lokalnych i przedsiębiorstw poprzez:

- *Wydawanie licencji dla przedsiębiorstw*
- *Rejestrację*
- *Ubezpieczenia*
- *Zarządzanie opodatkowaniem oraz innymi obszarami prawnymi i komunalnymi*
- *Dane emerytalne*

Możliwe, że DLT pomogą zupełnie wyeliminować te funkcje, ponieważ przedsiębiorstwa będą w stanie rejestrować nie tylko swoje firmy, ale też należące do nich zasoby. A co ważniejsze będą to w stanie robić poszczególni obywatele, np. w odniesieniu do swoich danych zdrowotnych, które w tradycyjnych systemach przechowywane są przez instytucje rządowe. To dałoby obywatelom możliwość kontroli czy do ich danych ktoś miał dostęp i czy były one wykorzystywane w sposób właściwy i do właściwych celów.

Ponadto zastosowanie rejestrów rozproszonych pozwoliłoby różnym podmiotom dzielić się danymi (lub nawet usługami związanymi z danymi) w ramach różnego rodzaju targów informacji, co pozwoliłoby na wymianę danych emerytalnych.

Efekty

- *Obniżone koszty dla małych i średnich przedsiębiorstw i zracjonalizowane koszty dla władz centralnych i lokalnych. Dodatkowo, posiadanie wiarygodnej dokumentacji własności zasobów cyfrowych, np. własności intelektualnej ograniczy konieczność odwoływania się do rozstrzygnięć sądowych, co przyniesie korzyść dla całego brytyjskiego społeczeństwa.*
- *Stopień rozwoju technologii*
- *Wymaga przyjęcia DLT przez lokalne i centralne urzędy*

Przykład 5: Europejski VAT

Streszczenie

Gospodarka może być kategoryzowana w oparciu o różne właściwości. Możliwy jest np. podział na gospodarkę opodatkowaną, gospodarkę quasi-opodatkowaną oraz nieopodatkowaną (czarnorynkową). Niedobór wpływów z VAT występuje we wszystkich tych typach gospodarki. Wynika on z niewypłacalności przedsiębiorstw, kreatywnego wykorzystania prawa międzynarodowego w celu uniknięcia zobowiązań podatkowych; albo po prostu z modelu: "tylko gotówka, bez papierologii". Szacuje się, że wartość niezapłaconego, należnego VATu w Unii Europejskiej wynosi między 151 a 193 miliardy euro rocznie.

DLT ma możliwości rozwijania się w sposób wykładniczy, a przy tym może znacząco zwiększyć przejrzystość transakcji. Wielka Brytania mogłaby odgrywać centralną rolę w rozwoju technologii, procedur i gotowych zastosowań, wykorzystujących DLT do ograniczenia strat wynikających z niezapłaconego VAT-u w Unii Europejskiej.

Informacje podstawowe

Prawo Moore'a trafnie przewidziało wykładniczy wzrost mocy obliczeniowej komputerów w ciągu ostatnich kilku dekad. Tak naprawdę technologie informatyczne rozwijały się wykładniczo od końca XIX w. aż do dziś. I przewiduje się, że wzrost ten będzie trwał do końca obecnego stulecia. Innowacje technologiczne same napędzają własny rozwój, ponieważ ułatwiają postęp w badaniach naukowych (np. w fizyce). A to z kolei umożliwia rozwój szybszych i tańszych technologii komputerowych, co znów umożliwia odkrycia w naukach przyrodniczych, co znów owocuje postępem technologicznym.

Straty w VAT-cie pomogłoby zmniejszyć wiele technologii informatycznych, np. uczące się maszyny, superkomputery, komputery kwantowe i technologie rejestrów rozproszonych. Dla administracji rządowej najważniejsze jest to, aby stworzyć i zastosować te technologie zanim zrobią to zorganizowane grupy przestępcze.

Propozycja wykorzystania DLT

Rozwój ogólnounijnych standardów i procedur związanych z VAT-em, umożliwiłby zastosowania DLT w całej Europie, z jednolitym traktowaniem wszystkich dokumentów VAT, od faktur po bankowe potwierdzenia transakcji.

Ten system mógłby obejmować inteligentne kontrakty, zaprojektowane dla zapobiegania stratom wynikającym z działalności quasi-podatkowej, a także byłby zdolny do obsługi różnych stawek VAT, obowiązujących w różnych krajach EU.

Użycie uczących się maszyn do śledzenia transakcji VAT w UE w czasie rzeczywistym, pozwala wykryć więcej nieprawidłowych transakcji (w tym tzw. oszustw karuzelowych), niż przy użyciu innych metod kontroli.

Wzrost przejrzystości i nowe możliwości śledzenia transakcji – również jeśli chodzi o operatorów płatności, banki i inne instytucje finansowe – sprawi, że czarnorynkowe operacje będą trudniejsze do ukrycia.

Efekty

- *Zmniejszenie dla przedsiębiorstw i innych instytucji obowiązków administracyjnych związanych z pobieraniem i płaceniem podatku VAT*
- *Wzrost transparentności transakcji dokonywanych w czasie rzeczywistym w całej gospodarce*
- *Lepsze możliwości szacowania ryzyka kredytowego, pozwalające ograniczyć straty związane z niewypłacalnością*
- *Więcej danych dostępnych dla pożyczkodawców, którzy świadczą usługi dla małych i średnich przedsiębiorstw, również danych dotyczących faktoringu*
- *Umożliwienie zawierania inteligentnych kontraktów pomiędzy instytucjami publicznymi a przedsiębiorstwami*
- *Stopień rozwoju technologii*
- *Technologicznie gotowa*
- *Należy włączyć płatników do konsultacji na początkowym etapie, ponieważ oni będą dostarczać dane, potrzebne do funkcjonowania systemu*
- *Agencje rządowe muszą być w stanie posługiwać się DLT w celach podatkowych*
- *Użytkownicy i małe przedsiębiorstwa muszą potrafić używać DLT dla skutecznego zarządzania podatkami*

Wnioski

Rejestry rozproszone bez wątpienia mogą przynieść korzyść administracji państwowej, oferując nowe sposoby działania, ograniczające oszustwa, obniżkę kosztu dostarczania usług dla osób korzystających ze świadczeń społecznych. Jednocześnie, technologie te dają możliwość nowych form innowacji i oszczędności dla małych i średnich firm w Wielkiej Brytanii/ W tym rozdziale opisano jedynie część możliwych przykładów użycia DLT. Gdy rejestry rozproszone będą się upowszechniać, pojawią się nowe możliwości ich wykorzystania w administracji rządowej.

ROZDZIAŁ 7: Globalne Perspektywy

Organizacje, które robią interesy w cyberprzestrzeni muszą być w stanie zaufać i mieć zaufanie swoich partnerów. Muszą także mieć możliwość działania w dużych i rozwijających się społecznościach na całym świecie. Blockchainy mają potencjał by przyczynić się do obu.

WPROWADZENIE

Poziom globalnych zmian – zarówno dobrych i złych – przyspiesza. Napędzany jest przez globalny internet, oczekiwania społeczne i rosnącą konkurencję. W przeciwieństwie do rozwijających się krajów, kraje rozwinięte charakteryzują się wysokim poziomem konsumpcji i potrzeby prywatności, co może podkopywać tradycyjne wartości i normy społeczne dotyczące zachowania. To sprawia, że raczej władze, aniżeli społeczność, odpowiadają za pomoc osobom zagrożonym i znajdującym w trudnej sytuacji. Rządy mają kłopot z zaspokojeniem rosnących oczekiwań konsumpcyjnych i zdawałoby się nieskończonego zapotrzebowania na pomoc społeczną. Słowa amerykańskiego prezydenta Johna F. Kennedy'ego: "Nie pytaj co twój kraj może dla ciebie zrobić, lecz co ty możesz zrobić dla swojego kraju" – dziś są jeszcze ważniejsze. Wielu obywateli chciałoby pomóc swojemu państwu, ale brakuje im sposobu zaangażowania się w erze cyfryzacji. Chcą być częścią stada, a nie błąkać się na jego niebezpiecznym skraju.

Jedną z konsekwencji tego braku społecznych zachowań jest polaryzacja w postawach, pojawienie się różnych percepcji i coraz większa tendencja do nadmiernego upraszczania złożonych zmian w serie oddzielnych problemów. Globalna rzeczywistość jest złożona z elementów fizycznych, wirtualnych, prawnych, historycznych, geograficznych, społecznych, zachowawczych, ekonomicznych, informacyjnych i technologicznych. Szybkość zmian i szybkość wprowadzania nowych przełomowych technologii zwiększa tę złożoność. Skala, szybkość i złożoność muszą być rozpatrywane łącznie. To sprawia ze coraz trudniej jest przedstawicielom państw i rządom krajów zrozumieć tę mieszaninę i korzystnie zaplanować, wdrożyć i wykorzystać nowe rozwiązania, używając tradycyjnych nie-współpracujących (non-collaborative) organizacyjnych struktur. Inicjatywę przejmują ci, którzy działają sprawniej np. rynki finansowe i przestępczość zorganizowana. Coraz częściej kraje rozwijające się, takie jak Kenia lub Rwanda (wolne od słabości państw rozwiniętych) sięgają po nowe technologie. W krajach rozwiniętych niektóre mniejsze i bardziej jednorodne narody robią znaczne postępy, które przekraczają granice, co zapewnia międzynarodowych korzyści, szczególnie w Europie (zob. Przykład dotyczący europejskich rynków energetycznych s. 74 oraz Estonii s. 79).

Do cech charakterystycznych rozwojowych cyfrowych państw należą:

- *Przywództwo dojrzałe cyfrowo*
- *Wydzielone ministerstwo ds. całościowej transformacji cyfrowej, wyposażone w niezbędne uprawnienia, zorientowane na współpracę międzynarodową i współpracujące ściśle ze wszystkimi sektorami przemysłu*
- *Wspólny krajowy plan, który jest kierowany poprzez przemysł przy wsparciu inwestycyjnym rządu*
- *Technologicznie świadomi, wykwalifikowani i doświadczeni wyżsi rangą urzędnicy w każdej organizacji rządowej*
- *Wybór inżynierów i liderów rynku cyfrowego jako polityków*

Wielka Brytania ma wiele do zrobienia w każdym z tych obszarów, jeśli miałaby stać się jednym z wiodących krajów cyfrowych. Jednak coraz bardziej świat zaczyna się opierać na gospodarce cyfrowej. To wymaga od nas czegoś więcej niż stosowania technologii komputerowej do istniejących modeli ekonomicznych. Zamiast tego, musimy ponownie ocenić naszą wiedzę na temat tego, czym się staje gospodarka cyfrowa, jak również kto w niej działa i w jaki sposób.

Przypomina to przejście z rozliczeń gotówkowych do opartych na aktywach, które wymagają od każdej organizacji znacznie szerszego zrozumienia złożoności

łańcuchów dostaw, usług i rynków, oraz wymagają innego podejścia do wspólnego zarządzania ryzykiem, podejmowania decyzji, dzielenia się zyskiem i wspólnej odpowiedzialności. Aby prowadzić cyfrowy biznes w cyberprzestrzeni organizacja musi być w stanie zaufać i być wiarygodna. Również powinna być zdolna do kooperacji z dużymi i rozrastającymi się grupami innych organizacji. Zaufanie i interoperacyjność są fundamentalne dla cyberprzestrzeni o wiele bardziej niż w fizycznym świecie. Łańcuchy bloków mają potencjał, aby wspierać obie te cechy, ale magia nie tkwi w technologii – tylko w sposobie w jaki wykorzystujemy ją na państwową skalę.

ZAUFANIE I INTEROPERACYJNOŚĆ

Zaufanie jest oszacowaniem ryzyka pomiędzy dwoma lub więcej osobami, organizacjami lub państwami. W cyberprzestrzeni zaufanie opiera się na dwóch podstawowych warunkach:

1. *Udowodnij mi, że jesteś tym, kim mówisz, że jesteś (uwierzytelnianie)*

2. *Udowodnij mi, że masz uprawnienia niezbędne do tego, o co prosisz (autoryzacja)*

Jeżeli nie jestem zadowolony z odpowiedzi, którą dostaję, mogę nadal pozwolić ci kontynuować, ale ponoszę ryzyko.

Jednakże nie istnieje prawdziwa relacja, dopóki inni mi też nie zaufają. W tym sensie bycie wiarygodnym jest analogiczne do bycia wypłacalnym.

Na interoperacyjność składa się kilka czynników:

- *Interoperacyjność danych. Musimy zrozumieć siebie nawzajem, aby móc z sobą razem pracować, a więc nasze dane musze mieć takie same fundamenty składniowe i semantyczne*
- *Interoperacyjność polityki. Nasze polityki muszą zostać uzgodnione lub dostosowane w oparciu o wspólne polityki tak aby można było być pewnym, że moja informacja będzie traktowana w sposób, jakiego ja oczekuję i vice versa*
- *Skuteczna, wspólna implementacja i stosowanie międzynarodowych standardów*

Ochrona informacji jest powiązana z kontrolą dostępu, która wymaga uwierzytelniania, autoryzacji i nie tylko. Uwierzytelnianie wymaga zarządzania tożsamością wszystkich elementów biorących udział w transakcji (zwykle to dotyczy ludzi, organizacji, sprzętu i oprogramowania) na odpowiednim, ustalanym międzynarodowo poziomie wiarygodności (LoA). Uwierzytelnianie przez społeczności wielu organów władz lub organizacji wymaga federacyjnego zarządzania tożsamością (FIM).

W skali międzynarodowej, FIM obecnie istnieje tylko na poziomie "niskiej wiarygodności", odpowiadającej "LoA 1" w międzynarodowym standardzie. Jest przede wszystkim stosowane w sieciach społecznych, gdzie podległość wielu jurysdykcjom nie jest bardzo znaczącym problemem. Google, GakuNin (japońska sieć uniwersytecka), Microsoft, Ping Identity, gazeta The Nikkei, Tokyu Corporation, mixi, Yahoo! Japonia i SoftBank – we wszystkich zostały wdrożone systemy FIM; trwa też ich budowa w innych organizacjach jak Deutsche Telekom, AOL i Salesforce.com.

Średnia wiarygodność (LoA 2) wymaga dowodu tożsamości podczas rejestracji, aby sprostać wymaganiom Know Your Customer (KYC), czego instytucje finansowe wymagają od swoich klientów i przedsiębiorstw przy transakcjach finansowych. Istnieją nieliczne federacje, które osiągają poziom LoA 2, większość z nich to systemy bankowe.

Kilka branż gospodarki używa systemów bezpieczeństwa opartych na Public Key Infrastructure (PKI). Branże te opierają się na standardzie kryptograficznym zwanym X.509. Oferują one wysoki i bardzo wysoki poziom wiarygodności (LoA 3 i 4) dla uwierzytelniania pracowników w przemyśle farmaceutycznym, obronie, bankach, coraz częściej w e-zdrowiu, i szczególnie w lotnictwie. USA i Chiny mają najwięcej wdrożonych międzynarodowych federacji opartych o standardach PKI. Tuż za nimi znajduje się Korea Południowa (gdzie jest to prawnie wymagane dla wszystkich firm), Estonia, Holandia i wiele innych. Na poziomie LoA 3+ możliwe jest powiązanie tożsamości użytkownika z innymi zaufanymi funkcjami, takimi jak uznawane prawnie podpisy cyfrowe, szyfrowanie powiązane z tożsamością i fizycznej kontroli dostępu w budynkach. Federacja oparta na PKI nie jest jedynym rozwiązaniem dla łańcucha dostaw wymagającego wysokiego poziomu wiarygodności lub skalowanym udostępnianiem poufnych informacji, ale jest uważany def facto za normę.

Blockchainy oferują potencjalną alternatywę, ale połączenie federacji PKI i federacji łańcucha bloków oferuje jeszcze bardziej atrakcyjne możliwości uzyskania większej odpowiedzialności cyfrowej, wiarygodności i zaufania w procesach biznesowych, związanych z wykorzystaniem nowych technologii.

W Wielkiej Brytanii jedynie policja prowadzi federację PKI na szeroką skalę. Co prawda w formie podstawowej, ale zgodnie z międzynarodowymi standardami.

Przy współpracy różnych podmiotów można by rozszerzyć ten model do obsługi wielu brytyjskich usług publicznych, włączając w to służby ratunkowe; również

można by wykorzystać go do współpracy międzynarodowej z partnerami, którzy mają podobne federacje PKI, w dziedzinach tak szerokich jak handel, kontrola graniczna lub uchodźcy i imigranci. Strategia dla rządowej Public Services Network, aby używać federacji PKI dla uwierzytelniania pracowników nie została jeszcze wdrożona, jednakże tak samo nie ma jeszcze systemu zarządzania tożsamością pracownika lub zaufania związanego ze współpracą w obrębie instytucji rządowych, opartego na międzynarodowych standardach, który mógłby stworzyć federację partnerami przemysłowymi i sojusznikami międzynarodowymi np. USA, Francją i Holandią.

Federacja PKI połączona z łańcuchem bloków może zapewniać lepsze usługi, łącznie z przetwarzaniem danych osobowych z poszanowaniem prywatności i zwiększeniem możliwości śledzenia płatności.

NHS posiada bardzo rozbudowany system PKI, ale nie jest on zgodny z normami międzynarodowymi i z tego powodu nie może zostać (jeszcze) częścią federacji. MOD posiada zobowiązania międzynarodowe, aby utworzyć PKI wspólnie ze skoncentrowanymi na USA łańcuchami dostaw dla obronności. Podobne zobowiązania wynikają z planów działania NATO Cyber Defence, lecz nie opublikowano jeszcze żadnych planów wdrożeniowych. Przemysł był rozważany w innych potencjalnych obszarach dla federacji KPI np. zwalczania oszustw w branży spożywczej. Było to opisane w 2014 roku w Elliott Review, dotyczącym integralności i wiarygodności sieci dostaw żywności. Jest również opracowywane memorandum zaufania z Południowo Koreańskimi agencjami rządowymi, które umożliwiałoby brytyjskim firmom posiadanie poświadczenia PKI, które mogliby wykorzystać w łańcuchach dostawczych do Koreańskich firm jak np. Samsung, Kia, Hyundai i Daewoo (które obecnie jest producentem największych kontenerowców na świecie). Należąca do ONZ Międzynarodowa Organizacja Morska tworzy międzynarodowe wytyczne dotyczące morskiego bezpieczeństwa cybernetycznego. I ma potencjał, aby wykorzystać inicjatywy pokazane przez koreańską federację PKI. Istnieje więcej przykładów w innych dziedzinach. Najkorzystniej byłoby, gdyby powstało forum, gdzie wszyscy mogliby włączyć się w dyskusję.

Parlament UE zatwierdził regulację dotyczącą elektronicznej identyfikacji, uwierzytelniania oraz usług zaufanych – Electronic Identification, Authentication and Trust Services Regulation (eIDAS) we wrześniu 2014 roku, dając państwom członkowskim trzy lata na dostosowanie się. eIDAS stanowi, że jeśli jakieś państwo 'opublikuje' schemat e-ID swoich obywateli, to prawo wymaga, aby wszystkie inne państwa członkowskie honorowały owe e-ID w swojej e-administracji. Wiele jeszcze zostało do zrobienia, ale eIDAS zmusza rząd i przemysł do zastanowienia się nad wykorzystaniem swoich FIM z korzyścią dla społeczeństwa oraz gospodarki.

W Wielkiej Brytanii rząd wprowadził zintegrowane, oparte na standardach narzędzie do sprawdzania wiarygodności tożsamości: GOV.UK Verify

GOV.UKE Verify zostało zbudowany w odpowiedzi na najnowsze osiągnięcia na rynku. Użytkownicy mieli prawo wybrać, spośród konkurujących ze sobą dostawców usług związanych z tożsamością.

Rozwój Verify i połączenie go z łańcuchami bloków i federacjami PKI mogłoby zwiększyć wartość samego Verify. Łańcuchy bloków i rozwiązania PKI z wysokim poziomem wiarygodności mogłyby zostać wzbogacone o honorujące prywatność sposoby wprowadzania danych, obecne w Verify. Wspólnie, każde z tych rozwiązań na swój sposób, mogłyby mieć znaczący wkład w brytyjską gospodarkę cyfrową, kontrolę graniczną oraz zwalczanie cyberprzestępczości.

PRZYKŁAD 1 – Europejski rynek energii

Igor Nai Fovino i Jean-Pierre Nordvik, Joint Research Centre, Komisja Europejska Strategia komisji Europejskiej Energy Union Framework określa wizję "Unii Energetycznej", w której "obywatele odgrywają centralną rolę, biorąc odpowiedzialność za przepływ energii, korzystają z nowych technologii jednocześnie zmniejszając swoje rachunki, aktywnie uczestniczą na rynku, i a jednocześnie wrażliwi konsumenci podlegają ochronie." Jednakże, podczas gdy rozwój inteligentnych sieci energetycznych postępuje stopniowo, rynek energii nadal czeka modernizacja. Inicjatywa Komisji "New Energy Market Design" będzie musiała zmierzyć się z kilkoma istotnymi kwestiami:

- *Jak dostarczyć konsumentom informacje na temat kosztów i zapotrzebowania, aby mogli zidentyfikować nowe możliwości na w pełni zintegrowanym kontynentalnym rynku energii?*
- *Jak wynagradzać aktywnych użytkowników, ułatwiać zmiany umów i zarządzać reakcjami na zmiany cen?*
- *Jak zapewnić interoperacyjność na rynku dla istniejących usług energetycznych, rozszerzyć możliwości wyboru dla konsumenta i umożliwić pozyskiwanie realnych korzyści z energii wytworzonej i wykorzystanej na własne potrzeby oraz z lokalnych małych źródeł?*

W tym kontekście rozproszone rejestry mogą pełnić funkcję nowego sterownika, aby podnieść poziom integracji i rozwoju na energetycznym rynku.

Centrum badawcze The Joint Research Centre Komisji Europejskiej obecnie bada praktyczne zastosowania, takie jak w poniższych przykładach.

1. Rynek energii Micro-Generation.

Mikro-generacja to zdolność konsumentów do produkcji energii w domu lub w lokalnej społecznosci. Pojecie "rynek" oznacza możliwość obrotu energią, która została wygenerowana przez konsumentów i "prosumentów".

Jednak tradycyjnie ten rynek był obsługiwany przez predefiniowane dwustronne umowy między prosumentami a dystrybutorami energii. Do tej pory indywidualni użytkownicy wytwarzający energię nie mieli prawdziwego dostępu do rynku energetycznego, który pozostawał uprzywilejowanym polem gry dla zinstytucjonalizowanych dostawców energii. To znacznie ograniczało korzyści ekonomiczne dla mikro-generatorów i dla końcowych użytkowników.

Rozproszony rejestr w kombinacji z systemami inteligentnego pomiaru i nowej generacji bateriami (aby zbierać energię lokalnie) mają potencjał, aby otworzyć rynek energii dla indywidualnych generatorów. Inteligentne liczniki mogą być wykorzystane, aby rejestrować i rozliczać mikro-generowaną energię na rozproszonym rejestrze (stając się tym samym odpowiednikiem systemu "energy-coin").

Generowany przez samych użytkowników prąd mógłby być wykorzystany w domu, zakumulowany do baterii nowej generacji dla późniejszego wykorzystania lub w zwyczajny sposób włączony z powrotem do sieci. Alternatywnie, dzięki rozproszonej i wszechobecnej naturze rejestru, ta energia mogła by być wykorzystana również w innych miejscach na przykład do ładowania pojazdu elektrycznego za granicą lub poprzez sprzedaż klientowi oferującemu najwyższą cenę, według mechanizmu podobnego do giełdy.

2. Rejestry Kontraktów Energetycznych.

Konsument, który zamierza zmienić swojego dostawcę energii obecnie musi zamknąć swoją obecną umowę z dostawcą, a następnie otworzyć nową umowę z nowym dostawcą i jednocześnie ponownie przejrzeć warunki umów wszystkich towarzyszących usług energetycznych świadczonych przez strony trzecie. Radzenie sobie ze złożonością tych operacji administracyjnych jest prawdziwą przeszkodą dla rozwoju konkurencyjnego rynku energii i jest źródłem kosztów dla dostawców i dystrybutorów energii.

Używanie rozproszonych rejestrów do zapisywania kontraktów energetycznych w internecie znacznie uprościłoby te operacje. Pozwoliłoby konsumentom sfinalizować przejście od jednego do drugiego dostawcy za pomocą tylko kilku kliknięć na komputerze lub urządzeniu mobilnym. Także dostawcom energii i dostawcom usług energetycznych pozwoliłoby to zaoszczędzić zasoby, które byłyby poświęcone na wykonanie operacji administracyjnych. Nadal są wątpliwości dotyczące skalowalności, bezpieczeństwa oraz stabilności takich zastosowań. Jednak korzyści brzmią tak obiecująco, że na pewno zasługują one na dalsze badania.

W cyberprzestrzeni każdy podmiot i transakcja jest związana z organizacją. Osiągnięcie wiarygodności organizacji do pożądanego LoA oraz dostarczanie informacji jej dotyczących w czasie rzeczywistym lub zbliżonym do rzeczywistego jest fundamentalnym wymogiem cyfrowym. Zwiększenie użycia blockchainów znacznie zwiększy oczekiwanie, aby uniknąć skażenia jakichkolwiek zapisów w łańcuchu. Dlatego powstaje nowy międzynarodowy standard dla cyfrowej identyfikacji, organizacji – Register of Legal Organisations (ROLO).

Kilka krajów, w tym USA, już rozważają adaptację specy-

fikacji ROLO do swoich potrzeb. Dziś globalizacja i brak nowoczesnych cyfrowych rejestrów przedsiębiorstw skutkuje sytuacją, gdy większość finansowo aktywnych organizacji w kraju nie jest zarejestrowana w tym samym kraju lub nie jest zarejestrowana w ogóle, lecz nie ma możliwości ustalenia, która z tych ewentualności ma miejsce.

Instytucje rządowe i gospodarcze w Wielkiej Brytanii, w tym organy ścigania i organizacje ds. cyberbezpieczeństwa, pilnie potrzebują ROLO UK jako kotwicy cyfrowego zaufania. Przemysł zaczął rozwijać ROLO UK. Wsparcie ze strony rządu przyniosłoby temu przedsięwzięciu znaczące korzyści.

GOSPODARKI CYFROWE

Gospodarki Cyfrowe starają się sprząc szybkość, zasięg oraz efektywność. Federalne zaufanie daje większe zaufanie i zmniejszenie ryzyka. Interoperacyjność poprawia efektywność i umożliwia ponowne wykorzystanie posiadanych możliwości. W dojrzałym łańcuchu dostaw, za każdym razem, gdy firma konkuruje w nowym programie lub sektorze, ponowne wykorzystanie daje mu sprawniejsze działanie i przewagę nad konkurencja; jest to spojrzenie prezentowane przez firmy obronne i lotnicze i wyrażone publicznie przez Airbus, Boeing, BAE Systems, Lockheed Martin, Northrop Grumman, Raytheon i innych.

W lutym 2014 roku Neelie Kroes, wówczas wiceprzewodnicząca Komisji Europejskiej i komisarz ds. agendy cyfrowej stwierdziła, że „demokracja musi się komunikować z technologią". Twierdziła, że przenosimy się do świata opartego na danych, do którego zaufanie jest kluczem, i że „bez bezpieczeństwa nie ma prywatności". Zwróciła uwagę na to, że silne cyberbezpieczeństwo jest ważne dla Europejskiego Single Digital Market (wspólnego rynku cyfrowego) i że EU Cyber Security Strategy (unijna strategia cyberbezpieczeństwa) zapewnia odpowiednie klocki do budowy. Argumentowała, że bez takich inicjatyw demokracja „nie da rady zarządzać technologia".

Rozmowy na te tematy, z udziałem EU, USA i Stowarzyszenia Narodów Azji Południowo-Wschodniej (ASEAN) stopniowo skupiają się na bankowości, elektronice, farmacji, żywności, transporcie morskim, lotnictwie, cyberprzestrzeni oraz organach ścigania.

Przez ONZ i organizacje takie jak Rada Europy rośnie nacisk na rozwinięte kraje, aby pomóc krajom rozwijającym się w staniu się częścią globalnej gospodarki cyfrowej. Brak cyfrowego zarządzania jest utrudnieniem dla rozwijających się krajów, co otwiera ogromne możliwości dla cyberprzestępczości i terroryzmu, które ostatecznie biorą na cel rozwinięte kraje. Brytyjska Wspólnota Narodów mogłaby odegrać znaczącą rolę w zwalczaniu tych zagrożeń. Współpraca jest tu kluczowa.

POTENCJAŁ DLA ROZPROSZONYCH REJESTRÓW I BLOCKCHAINÓW

Gospodarki opierają się na wspólnym zarządzaniu w celu zapewnienia zaufania na rynkach finansowych, co daje gwarancję, że wszyscy przestrzegają tych samych zasad. Gospodarki cyfrowe niczym się nie różnią.

Głównym powodem, dla którego obecnie łańcuchy bloków kojarzą się z cyberprzestępczością jest brak strategicznego zarzadzania, ustanawiającego uzgodnione zasady jurysdykcji i zapewniającego podporządkowanie się im. Kiedy już takie zarządzanie zaistnieje (wraz z zasadami, procedurami i mechanizmami), wtedy mogą być zrealizowane prawdziwe społeczne korzyści łańcucha bloków. Obawy rządów związane z niestabilności i słabością kryptowalut i ich wymianą handlową sprawiły, że rządy ostrożnie podchodzą do użycia blockchainów i generalnie wolałyby, aby to sektor prywatny skierował się w stronę budowy lepszych rozwiązań.

Główne dziedziny rozwoju to dziś:

- *Otwarte blockchainy bywają używane do niekontrolowanych i nielegalnych działań, szczególnie tam, gdzie osoby starają być anonimowi i nie brać odpowiedzialności*
- *Startupy współpracują z wiodącymi bankami, aby rozwijać zaufane kryptowaluty oraz łańcuchy bloków np."zaufany bitcoin". To mogłoby oferować znaczące korzyści dla dużych internetowych firm*
- *Prywatne blockchainy są stosowane w zamkniętych społecznościach handlowych w celu wsparcia zaufanych mechanizmów cyfrowych. Nie są one interoperacyjne i nie mogą być skalowane do obsługi łańcuchów dostaw*

Dopiero niedawno rządy zaczęły współpracę z gospodarką w celu zbadania strategicznego potencjału blockchainów. Niemniej implementacja przyspieszy, napędzana przez cztery główne elementy:

- *Potrzeba zapewnienia podstawy kryptograficznego zaufania w sposób podobny do PKI. To oznacza, że łańcuchy bloków mogłyby się łączyć ze sobą a także z istniejącymi federacjami PKI. Blockchainy mogłyby wykorzystać istniejącą skale i ład PKI, natomiast PKI mogłoby wykorzystać funkcje płatnicze i rejestrowe blockchainów. Te synergie otworzą nowe możliwości, które mogłyby zostać przyspieszone przez inteligentne i wspólne zarządzanie.*
- *Zamknięte rejestry (ang. permissioned ledgers) mogą przechowywać dowolnie duże bloki danych. Informacje o transakcji mogą zawierać kontrakt,*

licencję lub prawa autorskie, zapewniając dodatkowy współczynnik zaufania. Oferują to inteligentne kontrakty (np. poprzez powiązanie kontraktu z transakcją – więcej informacji w Rozdziale 1), poprzez wydajność i niezaprzeczalność.

- *Wykorzystanie nowych protokołów, takich jak Uniform Economic Transfer Protocol łączą producenta z przewoźnikiem, klientem, produktem, płatnością i bankiem, a także z inteligentnym kontaktem. Liderem tego rozwiązania jest Holandia, wspólnie z brytyjskim przemysłem i policją. Zaangażowanie Stanów Zjednoczonych jest na razie w fazie początkowej, jednak wkrótce zwiększy się w związku z pojawieniem się przepisów dotyczących cyberzabezpieczeń we wszystkich łańcuchach dostaw. Inne kraje, takie jak Korea Południowa i Japonia, mają być wkrótce zaangażowane.*
- *Smartfony cieszą się dużym zaufaniem użytkowników. Najnowsze modele zawierają ważne nowe funkcje zabezpieczeń, w tym TPM, czyli Trusted Platform Module, który gwarantuje cyfrowe certyfikaty i klucze kryptograficzne do uwierzytelniania, szyfrowania i składania podpisów; Trusted Execution Environment, gdzie proces bezpiecznego przetwarzania danych odbywa się poza systemem operacyjnym, który może być narażony na złośliwe oprogramowanie; i Trusted User Interface, który uniemożliwia przeprowadzenie złośliwego ataku między użytkownikiem a sprzętem. Dzięki takim rozwiązaniom, smartfon może wchodzić w bezpieczną interakcję z elektronicznymi dowodami tożsamości oraz paszportami, dzięki czemu użytkownik może bezpiecznie kontaktować się online na przykład z władzami na posterunkach granicznych lub z policją. Po raz pierwszy w historii konsumenci i pracownicy mają bezpieczne, zaufane urządzenie, przy pomocy którego mogą podpisywać transakcje (np. wykorzystując blockchain) i płatności (np. używając bitcoina). Samsung, HTC i LG sprzedają dziesiątki milionów takich zaawansowanych bezpiecznych smartfonów, gotowych do zaimplementowania oprogramowania, które pojawi się w połowie 2016 roku. Apple i inne firmy wkrótce pójdą w ich ślady.*

– Aby te wszystkie funkcjonalności nie stały się polem do nadużyć i niewłaściwego stosowania, potrzebna jest silna współpraca i wszechobecny system zarządzania. Zachęci to do szerszego wykorzystania blockchainów i rozproszonych rejestrów na przykład do celów finansowych. Gdy systemy rozbudują się i uzyskają pełną funkcjonalność, te cztery czynniki pomogą rozwiązać wiele trudnych problemów społecznych i światowych.

– Przejrzyste i uczciwe struktury rządowe. Zaufanie obywateli w krajach rozwijających się jest niższe niż w krajach, gdzie stabilne i odpowiedzialne struktury prawne i regulacyjne wzbudzają lepsze zachowania społeczne i środowiskowe. Budowanie zaufania do rządu oraz oczyszczenie państwa z korupcji zajmuje dużo czasu na terenach zdewastowanych przez wojny i autokratyczne reżimy. Wbudowanie mechanizmów odpowiedzialności i wiarygodności społecznej w procesy biznesowe ma kluczowe znaczenie w zapewnieniu skutecznego wdrożenia i egzekwowania przepisów, zasad i struktur organizacyjnych.– Oszustwa podatkowe i pranie brudnych pieniędzy. Gdy krzywa rozkładu bogactwa danego kraju jest zbyt stroma, właściciele pieniędzy i aktywów szukają miejsc zagranicą, by ukryć majątek, zmniejszając płynność finansową na krajowych rynkach i tym samym zmniejszając możliwości ekonomiczne tym wszystkim, którzy znajdują się na dole krzywej rozkładu bogactwa. Ostatecznie głód kapitału może zdestabilizować gospodarkę, wywołując duże bezrobocie wśród młodych ludzi, u których pojawi się długotrwająca nieufność do rządzących.

To podważa demokrację, stwarza warunki do rozłamu społecznego, upadku państwa, terroryzmu i ludzkiej nędzy. Ponownie, takie problemy mogą rozwiązać mechanizmy odpowiedzialności i wiarygodności. – Nielegalny handel i wandalizm środowiska naturalnego. W ciągu ostatnich 30 lat około 50% gatunków zwierząt żyjących w morzach wyginęła. Podobna sytuacja dotyczy zwierząt żyjących na lądzie. Pomimo wysiłków podejmowanych w ramach Konwencji o międzynarodowym handlu dzikimi zwierzętami i roślinami gatunków zagrożonych wyginięciem (CITES), są dowody, że zmierzamy w kierunku szóstego masowego wymierania Ziemi. Jeśli chcemy mieć jakąkolwiek nadzieję na uratowanie globalnej sytuacji, musimy wdrożyć znacznie silniejsze mechanizmy wykrywania i śledzenia zasobów, z tymi samymi mechanizmami odpowiedzialności i wiarygodności.

– Oszustwa w przemyśle spożywczym i zakłócenia łańcucha dostaw. Wielka Brytania jest teraz bardziej zależna od importu żywności niż kiedykolwiek wcześniej. Łańcuch dostaw żywności może być trudny do prześledzenia – wszyscy pamiętają skandal z koniną w 2013 roku, stanowiący przykład, że istnieje wiele możliwości nadużyć. Międzynarodowy i brytyjski łańcuch dostaw żywności muszą wzorować się na najlepszych łańcuchach dostaw stosowanych w innych sektorach, w celu wdrożenia przejrzystości finansowej i precyzyjnego śledzenia produktu.

– Zagrożenia dla łańcucha dostaw. Gdy rośnie cyberprzestępczości i kradzież własności intelektualnej (szacuje się, że suma przekracza 7 bln dolarów), łańcuchy dostaw są pod rosnącą presją rynkową, społeczną i prawną. Wymaga się stosowania większych zabezpieczeń opartych na systemie wspólnego zarządzania ryzykiem, włączając wspólny system zarządzania tożsamością i przejrzystość finansowa.

Wspólnie z innymi rozwiniętymi krajami i międzynarodowymi ekspertami, Wielka Brytania mogłaby wpłynąć na Radę Europy, Bank Światowy, G20 i ONZ, aby wdrożyć technologię łańcuchów bloków z wzmocnionym uwierzytelnianiem.

PRZYKŁAD 2 – Estońskie blockchainy zmieniają system płacenia, handlu i składania podpisów Alastair Brockbank, Brytyjska Ambasada w Talinie

Eksperymentowanie z technologią blockchain było logicznym krokiem dla Estonii. Stosując na szeroką skalę rozproszone i niemanipulowalne rejestry, posiada doskonałe warunki do przechowywania i zarządzania kluczami publicznymi.

Mają one postać klucza kryptograficznego, dostarczonego przez wyznaczony organ, który może być łączony z prywatnym kluczem do skutecznego szyfrowania i uwierzytelniania podpisów cyfrowych. Estonia ma obecnie najwyższy współczynnik używania krajowej infrastruktury klucza publicznego (PKI) na świecie.

Ponadto jako rozwiązanie zdecentralizowane, blockchain jest z natury mobilny i bardziej skalowalny. Jest zdolny do przetwarzania ogromnych ilości danych w interwałach sekundowych i działa płynnie ponad granicami. Dla firm działających w państwie, gdzie żyje zaledwie 1.3 miliona ludzi, blockchainy oferują rozwiązania o zasięgu krajowym, które z łatwością mogą stać się rozwiązaniami na skalę światową. Ponadto rosnąca moc obliczeniowa przyśpiesza ich działanie, w szczególnych przypadkach technologia sprawia, że dotychczasowi pośrednicy zostają wyeliminowani.

Przedstawione poniżej case study – profilowanie banku, start-up i dostawca cyberbezpieczeństwa pokazują potencjał blockchainów dla szerokiej gamy transakcji. Wszystkie trzy przykłady zaznaczają, że blockchainy muszą być przyjazne dla użytkownika. Klient nie musi wiedzieć, że obraca kryptowalutami, ani też, że login do jego dowodu tożsamości używa funkcji skrótu kryptograficznego. Oznacza to, że blockchain działa jak cichy, bardziej wydajny koń pociągowy, który stoi za rozwiązaniem wyglądającym podobnie: aplikacja płatności mobilnych, platforma crowfundingowa i handlowa, lub portal do logowania.

Podobnie jak w Wielkiej Brytanii, potrzeba i zakres regulacji, jest kluczowym zagadnieniem dla estońskich władz. Rozumieją, że wahanie i niezdecydowanie może być równie szkodliwe dla innowacji jak stanowczość. Jest rzeczą oczywistą, że w sytuacji, gdy innowacyjne rozwiązania spotykają się z nowymi i nieścisłymi przepisami, może dojść do utraty przychodów z powodu niewykorzystania możliwości handlowych i pojawienia się działalności przestępczej.

Pionierski bank puszcza do obiegu papiery wartościowe

Na początku roku LHV Pank – największy niezależny estoński bank – jako pierwszy bank na świecie przeprowadził doświadczenie związane z programowalnymi pieniędzmi puszczając do obiegu warte 100 tysięcy euro certyfikaty depozytowe chronione kryptograficznie. W ramach realizacji tego przedsięwzięcia utworzono spółkę zależną od LHV, Cuber, zajmującą się wyłącznie cyfrowymi papierami wartościowymi opartymi na kryptowalucie bitcoin.

Papiery wartościowe CUBER (ang. Cryptographic Universal Blockchain Entered Receivable) są zwykłymi bankowymi certyfikatami depozytowymi zapisanymi w blockchainie bitcoina. Są one wyrażone w euro, mają naliczane odsetki, a także różne zastosowania: jako środek przechowywania wartości, jako środek płatniczy, usługi powiernicze i depozytowe, a nawet mogą być wykorzystane dla transakcji między urządzeniami, co może znaleźć zastosowanie w Internecie Rzeczy (IoT). LHV uważa, że papiery wartościowe CUBER będą wykorzystane w przyszłych innowacjach finansowych.

Portfel Cuber to pierwszy przykład użyteczności Cuber. Jest to element oprogramowania dla telefonów komórkowych, umożliwiające natychmiastowe transakcje P2P w euro, oraz tanie i błyskawiczne płatności dla sprzedawców i konsumentów przy użyciu papierów wartościowych Cuber.

Użytkownicy przechowują swoje klucze prywatne na smartfonie, aby zwiększyć bezpieczeństwo i mobilność. W celu ochrony przed atakami serwerów Cuber Portfel decentralizuje zaufanie serwera i sprawia, że użytkownicy są użytkownikami bitcoina. Aplikacja korzysta z SPV (Uproszczony Weryfikacja Płatności Simplified Payment Verification) –rodzaj zabezpieczenia „klienta zubożonego" – co oznacza, że użytkownik nie posiada kompletnej kopii blockchaina a jedynie jego skrót. W zamian pobiera mniejszą ilość danych, jedynie nagłówki bloków odwołujących się do miejsca transakcji w łańcuchu. To pozwala im zobaczyć, że sieć zaakceptowała transakcję, a bloki dodane później potwierdzają, że sieć ją przyjęła.

Wirtualny portfel wykorzystuje bitcoiny jako nośnik danych, który rozliczają „odznaczając", dodając do nich unikatowe znaczniki. To z kolei wyznacza roszczenia w pieniądzu fiducjarnym wobec Banku LHV: wejście do bazy danych reprezentuje roszczenie wobec tradycyjnego systemu bankowego. Używając pieniądza fiducjarnego, wirtualny portfel może być stosowany nie tylko do transferów osobistych, ale także dla płatności detalicznych – kupiec musi zatwierdzić tę metodę płatności, na takich samych zasadach jak kartę kredytową. LHV obecnie testuje rozwiązanie w kilku miejscach, ale przewidywane jest szersze zastosowanie w internecie, szczególnie jako zastosowanie dla mniejszych płatności.

Zastosowanie pieniądza fiducjarnego niewątpliwie powoduje, że usługa staje się bardziej przyjazna użytkownikom. LHV zapewnia, że podstawowa technologia jest problemem banku: nie jest i nie powinna być pro-

blemem użytkownika i handlowców – a istnieje wiele możliwości nadużyć. Międzynarodowe i brytyjskie łańcuchy dostaw żywności nie mają wyboru, powinny brać przykład z najlepszego łańcucha dostaw z innych branż, w celu zagwarantowania odpowiedzialności i precyzyjnej identyfikacji.

Zagrożenia łańcucha dostaw. Wzrost cyberprzestępczości i międzynarodowy wzrost kradzieży własności intelektualnej (szacowany na ponad 7 bln USD), łańcuchy dostaw są pod coraz większym naciskiem regulacyjnym, rynkowym i społecznym domagającym się zwiększenia wiarygodności w oparciu o wspólne zarządzanie ryzykiem, w tym odpowiedzialności i wspólnej identyfikacji.

Wkrótce inwestorzy będą mogli korzystać z platformy internetowej Funderbeam mającej na celu utworzenie konsorcjum inwestycyjnego dla jednego lub kilku startupów. Inwestycje mogą być dowolnie konfigurowane i nie ma ograniczeń co do wielkości koncernu. 100 000 funtów udziałów może posiadać jeden główny inwestor i 99 wspierających go inwestorów udziały po 1000 funtów; wiodący inwestor może mieć udziały o wartości 75 000 funtów, a pięciu wspierających po 5 000 funtów; lub jakakolwiek dowolna kombinacja. Podobnie jak w crowdfundingu zmniejsza to wartość progową inwestycji w startupy.

Co odróżnia Funderbeam od crowdfunding to emisja udziałów tzw. monet kolorowych, czyli znakowanych „coloured coins", które mogą być natychmiast kupione, sprzedane lub użyte w obrocie z innymi inwestorami. Umożliwia to płynniejsze zarządzania portfelami inwestycyjnymi oraz przyspiesza finansowania dla startupów. Blockchain bitcoina jest podstawą rynku wtórnego, pozwalając na szybki, skuteczny i przejrzysty proces śledzenia własności aktywów.

Każde konsorcjum jest połączone z mikrofunduszem. W momencie powstania syndykatu i sfinansowania startupu, rynek posprzedażowy Funderbeam wykorzystuje kolorowe monety „coloured coins", tak aby wszyscy członkowie konsorcjum otrzymali wirtualną wartość udziału również mikrofundusz, która jest natychmiastowo zbywalna. Mniejsi udziałowcy mogą zatem sprzedać cały swój udział lub jego część, gdy osiągną zysk lub chcą zminimalizować stratę.

Elastyczność dla inwestorów nie jest jedyną zaletą technologii blockchain. Kaidi Ruusalepp, CEO Funderbeam wskazuje również na korzyści, które rozproszony rejestr oferuje ograniczając biurokrację. „Nie potrzebujemy wydziału gospodarczego, centralnego depozytu lub innego formalnego uprawnienia do potwierdzenia integralności transakcji," mówi. „W blockchainie, każda inwestycja czy zmiana własności posiada bezpieczną, rozproszoną ścieżkę audytu".

Jaan Tallinn, współzałożyciel Skype i inwestor Funderbeam, chwali dodatkową warstwę zabezpieczeń i weryfikacji, którą system oferuje dla transakcji internetowych. Poprzez zdecentralizowany i niemanipulowalny blockchain, można uzyskać większą przejrzystość na rynku kapitałowym, bez naruszania prywatności.

Funderbeam – zapewnia elastyczność, szybkość, bezpieczeństwo i przejrzystość – pokazuje, jak rozproszone rejestry mogą stanowić nie tylko alternatywę, ale również całkowicie realną podstawę finansowej ekspansji w XXI wiek, zwłaszcza dla małych i średnich przedsiębiorstw (MSP).

Kolejna generacja infrastruktury klucza publicznego

Od 2013 roku, estońskie rejestry państwowe – w tym hostujące wszystkie informacje obywateli i podobne – wykorzystały Guardtime, aby uwierzytelnić dane w swoich bazach danych. Zastosowano Keyless Signature Infrastructure (KSI), który kryptograficznie łączy skrót nieodwracalny (patrz niżej) z rozproszonym rejestrem, pozwalające rządowi estońskiemu zagwarantować zapis stanu dowolnego elementu wewnątrz sieci i przechowywanie danych.

To nie lada przedsięwzięcie. Estonia ma najczęściej na świecie wykorzystywaną infrastrukturę narodowego klucza publicznego PKI. Używając swojego dowodu osobistego obywatele mogą zamówić recepty, głosować, korzystać z bankowości elektronicznej, sprawdzać w szkołach dokumentację dzieci. Ma zastosowanie również do świadczeń państwowych, można złożyć swoje zeznanie podatkowe, wnioskować o pozwolenia, sporządzić testament, zgłosić się do służby wojskowej oraz zastosować do około 3000 innych funkcji.

Przedsiębiorcy używają swoich dowodów do składania sprawozdania rocznego, wystawiania dokumentów akcjonariuszom, ubiegania się o pozwolenie, itd. Przedstawiciele rządu używają dowodu do szyfrowania dokumentów dla bezpiecznej komunikacji, rozpatrywania i zatwierdzanie pozwoleń, umów i wniosków oraz wnioskowania o udzielenie informacji do organów ścigania. Ministrowie mogą wykorzystywać swoje dowody osobiste w celu przygotowania i prowadzenia posiedzeń rządu, co pozwala na dokonanie przeglądu programów, przedstawienie swojego stanowiska czy zastrzeżenia, daje również możliwość przejrzenia protokołów.

Dlatego cyfrowe uwierzytelnianie jest krytyczne zarówno dla rządu, biznesu jak i usług publicznych, podobnie jak do tworzenia polityki i prawodawstwa, deklaracji finansowych, czy też rejestracji praw własności i prawa dziedziczenia.

Ponad 200 milionów razy w ciągu roku dowód osobisty jest używany jako cyfrowy podpis, ok. 39 razy na osobę i liczba ta wciąż rośnie. Dlatego konieczne jest, aby rząd miał pewność co do prawidłowości danych oraz

co do tego, że w dokumentacji nie zostały dokonane zmiany od wewnątrz lub poprzez cyberatak.

Jak pomaga w tym blockchain? Pomaga, ponieważ rejestruje każdą zmianę w zapisach. Dostarczając dowodu na autentyczność, tożsamość i czas wykonania operacji, KSI pozwala zachować prawdziwość danych, zabezpiecza przed antydatowaniem i daje weryfikowalną gwarancję, że nikt nie manipulował danymi.

Procedura jest przy tym przejrzysta i przynosi korzyści również użytkownikom: obywatele mogą sprawdzać kto przeglądał ich dane, dlaczego to robił i kiedy; zmiany w danych osobowych muszą zostać zatwierdzone. Ponadto, dzięki zastosowaniu funkcji skrótu (hash) (zamiast kryptografii asymetrycznej, stosowanej w większości PKI) KSI nie da się złamać algorytmami kwantowymi. Ponadto system jest tak skalowalny, że pozwala podpisywać eksabajt danych na sekundę, zużywając przy tym znikomą część ogólnej sumy mocy obliczeniowych. Użycie KSI nie wymaga obecności zaufanej instytucji kontrolnej, dane można sprawdzać niezależnie od lokalizacji i nie ma ryzyka naruszenia prywatności, ponieważ system nie pobiera danych klienta. Nie ma wątpliwości, że system ten stanowi znaczący postęp w technologiach PKI.

I wreszcie, chociaż estońskie dowody osobiste prawdopodobnie nie będą nigdy całkowicie odporne na włamanie (chociaż na razie nie było takiego przypadku), blockchain KSI daje rządowi pewność, że gdyby doszło do nieuprawnionych zmian w publicznych danych, to będą one w 100 proc. przypadków możliwe do wykrycia.