BLOCKCHAIN W BIZNESIE

Możliwości i zastosowania łańcucha bloków

WILLIAM MOUGAYAR

Helion
onepress

Tytuł oryginału: The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology

Tłumaczenie: Leszek Sielicki

ISBN: 978-83-283-4932-2

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/blokbi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

SPIS TREŚCI

CZYM JEST ŁAŃCUCH BLOKÓW?

Jeżeli nie rozumiesz bez tłumaczenia, to znaczy,
że nie zrozumiesz, choćbym ci nie wiem ile tłumaczył.

— HARUKI MURAKAMI

UWAGA, UWAGA! Ten rozdział jest prawdopodobnie najważniejszy w całej książce, bo jego celem jest próba przedstawienia fundamentalnych założeń łańcucha bloków. To pierwszy etap na drodze do zrealizowania zawartej w niej obietnicy zaprezentowania holistycznego spojrzenia na potencjał łańcucha bloków.

Łańcuchy bloków niełatwo pojąć. Zanim będziemy mogli docenić ich potencjał, musimy zrozumieć przesłanie, jakie ze sobą niosą. Oprócz możliwości technologicznych łańcuchy bloków zawierają fundamenty filozoficzne, kulturowe i ideologiczne, które także należy zrozumieć.

Dla wszystkich poza programistami łańcuchy bloków nie są produktem, który można po prostu włączyć i zacząć stosować. Łańcuchy bloków uaktywniają inne produkty, z których korzystamy — a my często nawet nie wiemy, że funkcjonują one za sprawą łańcucha bloków, podobnie jak nie orientujemy się w złożoności procesów kryjących się za tym, do czego w danej chwili uzyskujemy dostęp w sieci.

Kiedy zaczniesz samodzielnie wyobrażać sobie możliwości łańcuchów bloków, bez podejmowania ciągłych prób jednoczesnego ich zrozumienia,

osiągniesz etap, który z punktu widzenia wykorzystywania ich można określić jako „dojrzałość".

Wierzę, że transfer wiedzy wiążący się ze zrozumieniem łańcucha bloków jest łatwiejszy niż nabycie wiedzy o tym, gdzie można go umieścić. To jak nauka jazdy samochodem. Mogę Cię nauczyć nim jeździć, ale nie potrafię przewidzieć, dokąd pojedziesz. Ty sam najlepiej znasz obszar działalności, którą się zajmujesz, czy też własną sytuację ekonomiczną i tylko Ty sam będziesz w stanie ustalić, w jaki sposób mógłbyś posłużyć się łańcuchami bloków, gdy już się dowiesz, do czego mogą one służyć. Najpierw jednak, aby zapewnić Ci materiał do przemyśleń, przeprowadzimy oczywiście szereg testów drogowych i prób na torach wyścigowych.

PRZEGLĄD ARTYKUŁU SATOSHIEGO

Po stworzeniu w 1990 roku pierwszej strony w sieci WWW Tim Berners-Lee napisał: „Kiedy łączymy informacje w sieci WWW, umożliwiamy sobie odkrywanie faktów, tworzenie koncepcji, kupowanie i sprzedawanie oraz nawiązywanie nowych relacji w tempie i w skali niewyobrażalnych w erze analogowej".

Za sprawą tego krótkiego stwierdzenia Berners-Lee przewidział wyszukiwanie, publikowanie, handel elektroniczny, pocztę e-mail i media społecznościowe — wszystko naraz, za jednym zamachem. Odpowiednik tego rodzaju przewidywań w sferze bitcoina, autorstwa kogoś, kto właśnie stworzył coś spektakularnego, można znaleźć w artykule Satoshiego Nakamoto z 2008 roku, zatytułowanym *Bitcoin: A Peer-to-Peer Electronic Cash System*[1], stanowiącym bez wątpienia fundament innowacyjności nowoczesnej kryptowaluty opartej na łańcuchu bloków.

Treść artykułu przedstawia założenia dotyczące bitcoina i wyjaśnia jego podstawowe zasady:

- Elektroniczny pieniądz w wersji całkowicie *peer-to-peer* umożliwia przesyłanie płatności online *bezpośrednio między stronami transakcji, z pominięciem instytucji finansowej*.

- *Zaufana strona trzecia nie jest niezbędna, aby zapobiegać podwójnemu wydatkowaniu środków*.
- Proponowane jest *rozwiązanie* problemu podwójnego wydatkowania środków *z wykorzystaniem sieci peer-to-peer*.
- *Sieć opisuje transakcje za pomocą znaczników czasu*, szyfrując je do postaci ciągłego łańcucha opartych na wartościach skrótu dowodów pracy i tworząc *rejestr, który nie może zostać zmieniony bez zmiany dowodów pracy*.
- Najdłuższy łańcuch służy nie tylko jako dowód sekwencji obserwowanych zdarzeń, ale jest także dowodem na to, że pochodzi ona z największej puli mocy obliczeniowej. Dopóki *większość mocy obliczeniowej pozostaje pod kontrolą węzłów niepodejmujących współpracy w celu zaatakowania sieci*, to tworzą one także najdłuższy łańcuch i wyprzedzają atakujących.
- Sieć jako taka wymaga minimum struktury. Komunikaty są przesyłane z wykorzystaniem zasady najwyższej staranności, a *węzły mogą opuszczać sieć i do niej dołączać w dowolnym momencie, przyjmując najdłuższy łańcuch dowodów pracy za potwierdzenie tego, co wydarzyło się podczas ich nieobecności.*

Jeśli nie masz inklinacji technicznych, skoncentruj się na zapisach kursywą. Czytaj zamieszczone powyżej informacje tak długo, aż przyswoisz sobie sekwencyjną logikę Nakamoto! Mówię poważnie. Musisz uwierzyć i przyjąć do wiadomości, że walidację transakcji *peer-to-peer* można przeprowadzić, pozwalając po prostu sieci na funkcjonowanie w roli dysponenta zaufania, bez jakiejkolwiek centralnej ingerencji lub prowadzenia za rękę.

Można zatem stwierdzić, że clou artykułu Nakamoto stanowią następujące koncepcje:

- Transakcje i interakcje elektroniczne *peer-to-peer*.
- Brak instytucji finansowych.
- Dowód kryptograficzny zamiast centralnego zaufania.
- Zaufanie do sieci, a nie instytucji centralnej.

Okazuje się, że „łańcuch bloków" to wynalazek technologiczny, dzięki któremu możliwe jest istnienie bitcoina. Pamiętając o treści artykułu Satoshiego, zastanówmy się nad trzema różnymi, ale wzajemnie się uzupełniającymi definicjami łańcucha bloków: techniczną, biznesową i prawną.

Z perspektywy technicznej łańcuch bloków jest bazą danych, przechowującą rozproszony rejestr, który jest dostępny dla wszystkich.

W znaczeniu biznesowym łańcuch bloków to sieć wymiany danych do zawierania transakcji i przenoszenia wartości oraz zasobów pomiędzy równorzędnymi podmiotami bez udziału pośredników.

Z prawnego punktu widzenia łańcuch bloków przeprowadza walidację transakcji, zastępując zaufane podmioty, które zajmowały się tym do tej pory.

DEFINICJA TECHNICZNA	Baza danych, która w jawny sposób przechowuje rozproszony rejestr.
DEFINICJA BIZNESOWA	Sieć wymiany danych służąca do przenoszenia wartości między równorzędnymi podmiotami.
DEFINICJA PRAWNA	Mechanizm walidacji transakcji niewymagający udziału pośrednika.

Możliwości łańcucha bloków = techniczne + biznesowe + prawne.

SIEĆ WWW — JESZCZE RAZ

Przeszłość nie jest dokładnym prognostykiem przyszłości, ale zdanie sobie sprawy z tego, skąd przychodzimy, pomaga nam uzyskać jasną perspektywę i określenie w bardziej jednoznacznym kontekście tego, dokąd zmierzamy. Łańcuch bloków jest po prostu elementem biegu historii technologii internetowej w postaci sieci WWW. To historia, która wpływa na nasz świat — na biznes, społeczeństwa i władze — a wiele jej cykli i faz często możemy zaobserwować, wyłącznie spoglądając wstecz.

Internet powstał w 1983 roku, ale to właśnie sieć WWW zapewniła nam przełom ewolucyjny, bo dzięki niej informacje i bazujące na informacjach usługi stały się w otwarty i natychmiastowy sposób dostępne dla każdego, kto miał dostęp do sieci.

W ten sam sposób, w jaki miliardy ludzi na całym świecie obecnie łączą się z siecią, miliony, a potem miliardy ludzi będą się łączyć z łańcuchami bloków. Nie powinniśmy być zaskoczeni, jeżeli okaże się, że skala wzrostu liczby użytkowników łańcuchów bloków przewyższy wartość danych historycznych dotyczących wzrostu liczby użytkowników sieci WWW.

Według danych z połowy 2016 roku dostęp do internetu miało 47% z 7,4 miliarda mieszkańców Ziemi. W 1995 roku było to mniej niż 1%, a w roku 2005 liczba użytkowników internetu wynosiła już miliard. Popularność telefonów komórkowych rosła z kolei jeszcze szybciej — ich liczba przekroczyła liczbę linii naziemnych w 2002 roku, a liczbę ludności świata w roku 2013. Jeśli chodzi o strony internetowe, ich łączna liczba w 2016 roku wynosiła około miliarda. Całkiem możliwe, że łańcuchy bloków rozwiną się wielotorowo i staną się równie łatwo konfigurowalne jak strony internetowe, które można tworzyć w Wordpressie lub Squarespace.

Liczba użytkowników łańcuchów bloków rośnie szybciej, niż w przeszłości rosła liczba użytkowników sieci WWW, bo już od punktu wyjścia odbywa się to za pośrednictwem czterech segmentów: użytkowników sieci, użytkowników telefonów komórkowych, właścicieli witryn i wszelkich innych „ustrojstw" posiadających atut w postaci połączenia z siecią, dzięki czemu stają się „inteligentne". Oznacza to, że rozwój łańcucha bloków możemy rozpatrywać w tych czterech kategoriach, a nie tylko bazować na poszukiwaniu nowych użytkowników.

JEDEN CZY WIELE ŁAŃCUCHÓW BLOKÓW?

Łańcucha bloków nie dotyczą dotychczasowe paradygmaty. Nie jest on nową wersją protokołu sieciowego TCP/IP. Nie jest także jakimś innym „całym" internetem. W 2015 roku niektórzy zwolennicy pojedynczego łańcucha bloków bitcoina narzekali na to, że istnieje wiele łańcuchów bloków. Łańcuch bloków był postrzegany jednowymiarowo (maksymalizm bitcoina[2]), z perspektywy podobnej do tej, z jakiej postrzegano internet. Tak, to dobrze, że jest tylko jeden internet, bo w innym przypadku nigdy nie byłby w stanie tak gwałtownie się rozprzestrzeniać. Łańcuch bloków jest jednak inną konstrukcją. To raczej nowy protokół, będący nakładką na internet, podobnie

jak nakładką na internet jest za sprawą własnych standardów technologicznych sieć WWW.

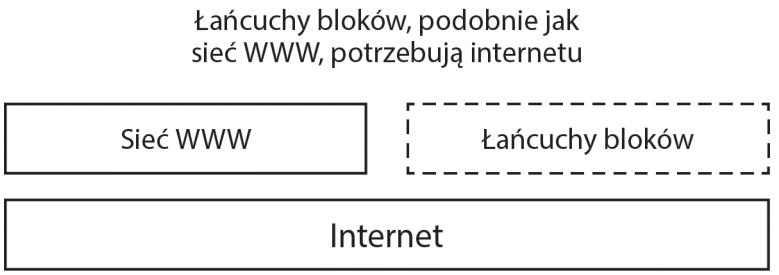
Łańcuch bloków to po części baza danych, a po części platforma programistyczna i moduł obsługowy, niezbędne jest więc istnienie wielu jego wystąpień i odmian. Jako nakładka na internet łańcuchy bloków mogą być wykorzystywane na wiele różnych sposobów. Łańcuch bloków można postrzegać jako warstwę zaufania, środek wymiany, bezpieczny kanał komunikacji, zestaw zdecentralizowanych opcji i o wiele więcej.

Faktem jest jednak, że istnieje wiele analogii pomiędzy wczesnymi latami sieci WWW i dzisiejszą ewolucją łańcucha bloków, zwłaszcza biorąc pod uwagę sposób, w jaki ta technologia będzie wdrażana.

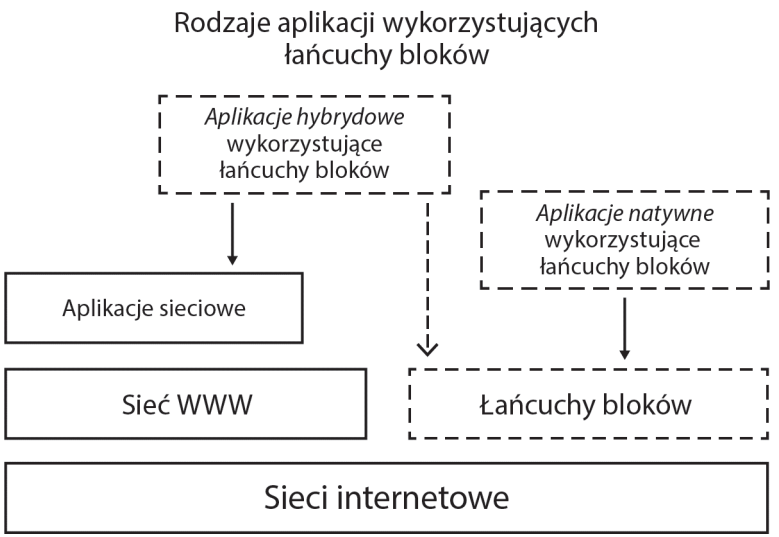
Nie zapominajmy, że sieć WWW pojawiła się siedem lat po zaistnieniu internetu, a po jej wstępnej komercjalizacji pełne zrozumienie tkwiącego w niej potencjału zajęło większości firm około trzech lat (działo się to mniej więcej w okresie od roku 1994 do 1997). Nie ma wątpliwości, że łańcuch bloków pozostaje w okresie od roku 2015 do 2018 zjawiskiem nieco tajemniczym i stosunkowo skomplikowanym, podobnie jak bitcoin, który w latach 2009 – 2012 rozwijał się „w izolacji", zanim trafił do powszechnej świadomości.

WPROWADZENIE DO APLIKACJI WYKORZYSTUJĄCYCH ŁAŃCUCHY BLOKÓW

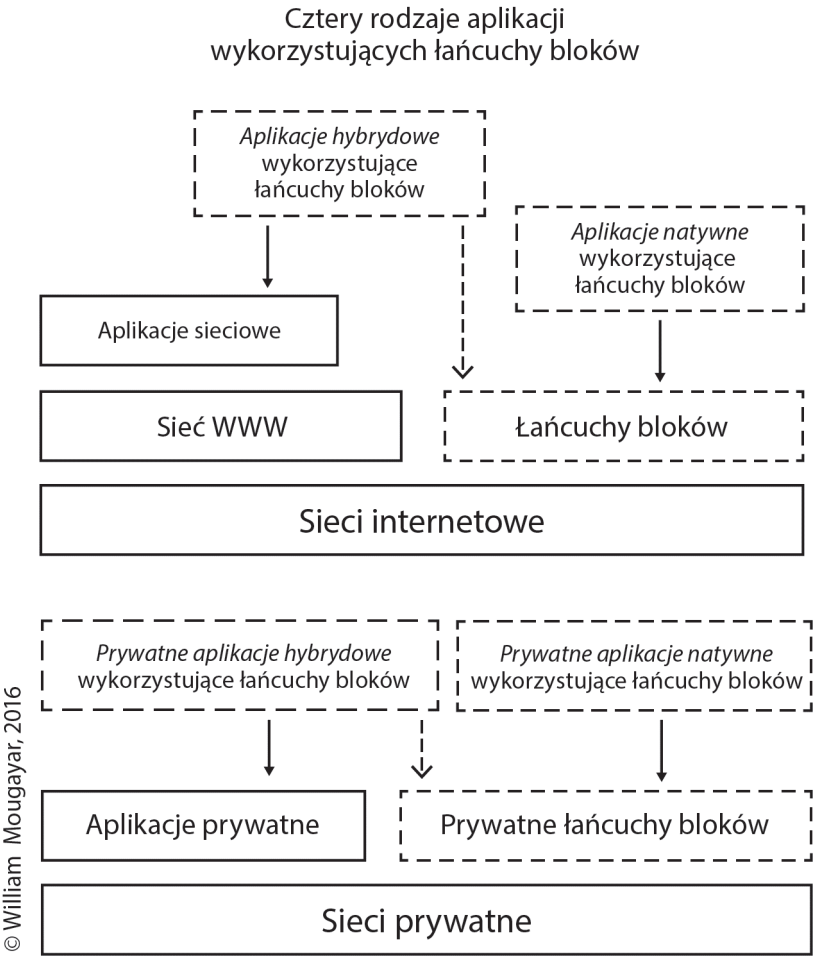
Sieć WWW nie mogłaby istnieć bez internetu. To samo dotyczy łańcuchów bloków. Sieć WWW sprawiła, że internet stał się bardziej użyteczny, bo użytkowników bardziej interesowało wykorzystywanie informacji niż zastanawianie się, jak łączyć ze sobą komputery. Aplikacje bazujące na łańcuchach bloków wymagają istnienia internetu, ale są w stanie pominąć sieć WWW i dać nam inną wersję sieci, która będzie bardziej zdecentralizowana i być może bardziej sprawiedliwa. To jedna z najistotniejszych deklaracji technologii łańcucha bloków.



Istnieje wiele sposobów tworzenia aplikacji bazujących na łańcuchach bloków. Można nabudowywać je natywnie na łańcuchach bloków albo łączyć z istniejącymi aplikacjami internetowymi, tworząc coś, co moglibyśmy nazwać „aplikacjami hybrydowymi wykorzystującymi łańcuchy bloków".



Internet składa się z wersji publicznej i kilku odmian prywatnych, więc łańcuchy bloków także będą rozwijać się w ten sposób. Powstaną łańcuchy bloków o charakterze publicznym i o charakterze prywatnym. Niektóre z nich będą natywnymi elementami technologii łańcucha bloków, a inne być może implementacjami hybrydowymi, stanowiącymi składnik istniejącej sieci WWW czy też określonych aplikacji prywatnych.



SIŁA NARRACJI ŁAŃCUCHA BLOKÓW

Przejawem potencjału technologii lub trendu jest to, czy posiadają one silną narrację. Jaka jest różnica pomiędzy opowieścią a narracją? Opowieść jest zazwyczaj czymś spójnym i znanym, narracja natomiast tworzy zindywidualizowane opowieści dla konkretnych podmiotów, które wchodzą w interakcje z danym trendem.

Różnicę tę dobrze wychwycił John Hagel, który stwierdził[3]:

Opowieści są samodzielne — mają wstęp, rozwinięcie i zakończenie. Narracje natomiast są otwarte — ich wynik nie jest określony, pozostaje do ustalenia. Poza tym opowieści odnoszą się do mnie, opowiadającego, lub innych ludzi; nie są o Tobie. Wynik narracji zależy z kolei od dokonanego wyboru i działań, które podejmujesz Ty — i to Ty sam określasz jej rezultat.

Internet miał silną narrację. Pytając różne osoby o to, w jaki sposób korzystają z internetu albo co on dla nich oznacza, z pewnością usłyszysz różne odpowiedzi, bo każdy oswaja internet i korzysta z niego po swojemu, w zależności od tego, które z zastosowań uznaje za najistotniejsze.

Łańcuch bloków posiada silną narrację, bo pobudza naszą wyobraźnię. Według Hagela narracje niosą ze sobą określone korzyści. Oto one:

DYFERENCJACJA — pomaga wyróżnić się z tłumu.

DŹWIGNIA — mobilizuje osoby spoza firmy.

DYSTRYBUOWANIE INNOWACYJNOŚCI — pobudza innowacyjność i kieruje ją na nieoczekiwane tory.

PRZYCIĄGANIE — przyciąga ludzi dzięki okazji i wyzwaniu, które stawiasz.

RELACJE — rodzi trwałe relacje z osobami, które przekonała Twoja narracja.

John Hagel stwierdza także, że „chodzi o nawiązywanie kontaktów z innymi i mobilizowanie ich tak, aby przekraczali granice wyznaczone przez…". Wstawiając zamiast kropek wyrażenie „łańcuch bloków", zyskamy mocny fundament silnej i długotrwałej narracji łańcucha bloków.

METATECHNOLOGIA

Łańcuch bloków jest metatechnologią, bo wpływa na inne technologie i sam składa się z wielu technologii. Jest nakładką na komputery i sieci bazujące na internecie. Eksplorując warstwy architektoniczne łańcucha bloków, można

zauważyć, że składa się on z kilku elementów: bazy danych, aplikacji, szeregu połączonych ze sobą komputerów, klientów umożliwiających dostęp do tych komputerów, środowiska programistycznego umożliwiającego prowadzenie prac, narzędzi do jego monitorowania i innych elementów (które omówię w rozdziale 6.).

Łańcuch bloków to nie jakaś tam nowa technologia. To technologia, która rzuca wyzwanie innym już istniejącym technologiom komputerowym, bo ma potencjał, aby zastąpić lub uzupełnić obecnie stosowane rozwiązania. W gruncie rzeczy to technologia, która zmienia technologię.

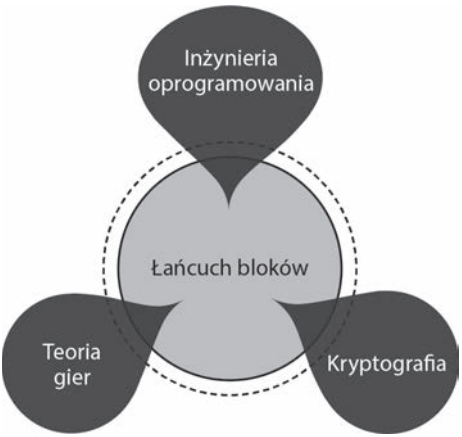
Ostatnio świadkami pojawienia się takiej katalitycznej technologii byliśmy wtedy, gdy pojawiła się sieć WWW. Zmieniła ona sposób pisania aplikacji i przyniosła ze sobą nową technologię oprogramowania, która rzuciła wyzwanie wcześniejszym technologiom i je zastąpiła. W 1993 roku HTML — język znaczników — zmienił sferę publikowania treści. W roku 1995 Java — język programowania — zmieniła sferę programowania. Kilka lat wcześniej TCP/IP — protokół sieciowy — zaczął zmieniać sieć, sprawiając, że stała się ona w globalnym ujęciu interoperacyjna.

Z punktu widzenia tworzenia oprogramowania jedną z największych zmian paradygmatów za sprawą łańcucha bloków wydaje się zakwestionowanie funkcji i monopolu tradycyjnej bazy danych, takiej, jaką znamy obecnie. Musimy więc dogłębnie zrozumieć, w jaki sposób łańcuch bloków zmusza nas do ponownego przemyślenia istniejących konstrukcji baz danych.

Łańcuch bloków zmienia sposób tworzenia aplikacji za sprawą nowego rodzaju języków skryptów, dzięki którym możliwe jest programowanie logiki biznesowej w postaci inteligentnych kontraktów funkcjonujących w ramach łańcuchów bloków.

OPROGRAMOWANIE, TEORIA GIER I KRYPTOGRAFIA

Innym sposobem na zrozumienie łańcucha bloków jest postrzeganie go jako triady znanych dziedzin: 1) teorii gier, 2) kryptografii i 3) inżynierii oprogramowania. Oddzielnie istnieją one już od dawna, ale po raz pierwszy zostały harmonijnie skonsolidowane i przekształciły się w technologię łańcucha bloków.



Teoria gier to „nauka o matematycznych modelach konfliktów i współpracy między inteligentnymi, racjonalnymi decydentami”[4]. Wiąże się ona z łańcuchem bloków, bo zadaniem łańcucha bloków bitcoina, który stworzył Satoshi Nakamoto, miało być rozwiązanie tak zwanego problemu bizantyjskich generałów — zagadnienia znanego właśnie z teorii gier[5]. Rozwiązanie tego problemu polega na udaremnieniu knowań generałów, którzy mogą być zdrajcami, i takim skoordynowaniu ataku, aby zagwarantować bizantyjskim armiom zwycięstwo. Odbywa się to poprzez uruchomienie procesu weryfikacji pracy włożonej w tworzenie komunikatów oraz ograniczenie w czasie dostępu do niezmienionych komunikatów, co umożliwia ich walidację. Istotne jest tutaj zaimplementowanie „tolerancji błędów bizantyjskich”, bo zaczynamy od założenia, że nie wolno ufać nikomu, a mimo to możemy mieć pewność, że transakcja przebiegła bezpiecznie, znalazła się tam, gdzie powinna być, i przetrwała potencjalne ataki, bo mamy zaufanie do sieci.

Ta nowa metoda zapewniania bezpieczeństwa w sferze finalizowania transakcji rodzi niezwykle istotne implikacje, bo kwestionuje potrzebę istnienia i podejmowania określonych działań przez obecnie zaufanych pośredników, będących do tej pory tradycyjnymi autorytetami w dziedzinie walidacji transakcji. Musimy wobec tego zadać sobie pytanie egzystencjalne: dlaczego potrzebujemy centralnego organu mającego być dysponentem centralnego zaufania, jeżeli taki sam poziom wiarygodności możemy osiągnąć,

przeprowadzając transakcję pomiędzy dwoma równorzędnymi podmiotami w sieci, która sama jest gwarantem zaufania?

Kryptografia wykorzystywana jest na szeroką skalę, aby zapewnić bezpieczeństwo sieci łańcuchów bloków, i opiera się na trzech podstawowych koncepcjach, którymi są haszowanie, klucze i podpisy cyfrowe. „Hasz" to niepowtarzalny odcisk palca, który pomaga zweryfikować, czy określona informacja nie została zmieniona, bez konieczności jej faktycznego odczytywania. Klucze są wykorzystywane parami — jeden z nich jest publiczny, a drugi prywatny. Jako analogię można byłoby wyobrazić sobie drzwi, do których otwarcia niezbędne są dwa klucze. Za pomocą klucza publicznego nadawca szyfruje informacje, które mogą zostać odszyfrowane wyłącznie przez posiadacza klucza prywatnego. Klucza prywatnego nie wolno ujawniać. Podpis cyfrowy to wyliczenie matematyczne, które służy do potwierdzania autentyczności (cyfrowego) komunikatu lub dokumentu.

Kryptografia bazuje na relacji „publiczne – prywatne", która jest dla łańcucha bloków niczym yin i yang — łańcuch jest publicznie widoczny, ale dostępny wyłącznie prywatnie. To coś w rodzaju adresu zamieszkania. Można go podać do publicznej wiadomości, ale nie wiąże się to z żadnymi informacjami na temat tego, jak nasz dom wygląda wewnątrz. Aby wejść do domu, musimy użyć swojego klucza prywatnego, a ponieważ określony adres podaliśmy jako swój, nikt inny nie może go zawłaszczyć.

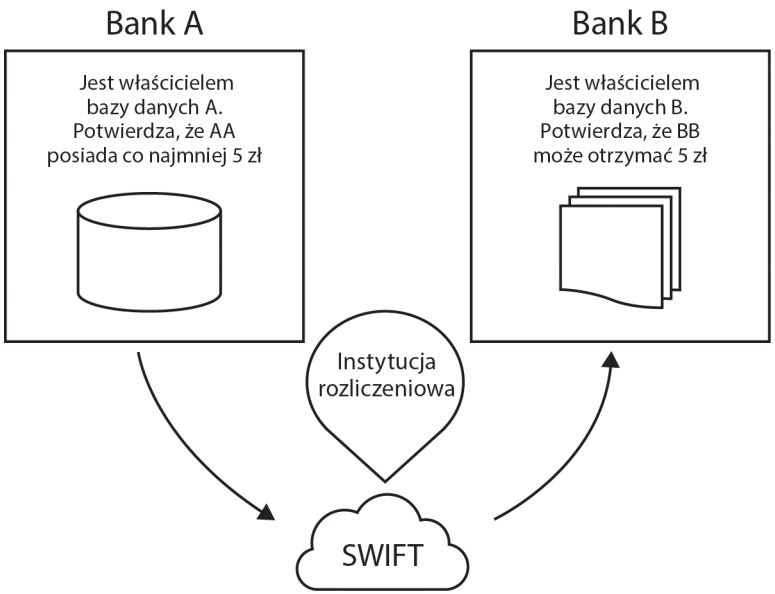
Chociaż koncepcje kryptograficzne istnieją już od jakiegoś czasu, inżynierowie oprogramowania stale pracują nad możliwościami łączenia ich z innowacyjnością teorii gier, tworząc takie konstrukcje łańcuchów bloków, w ramach których pozorną niepewność zastępuje całkowita pewność w ujęciu matematycznym.

BAZA DANYCH A REJESTR

Możemy już weryfikować transakcje bez udziału osób trzecich. Teraz zadajesz sobie pewnie pytanie: „A co z bazami danych?". Zawsze uważaliśmy, że bazy danych są zaufanymi repozytoriami do przechowywania aktywów.

W przypadku łańcucha bloków takim niepodważalnym repozytorium, które przechowuje rejestr transakcji zatwierdzonych przez sieć łańcucha bloków, jest rejestr.

Zilustrujmy implikacje tej sytuacji: baza danych w porównaniu z rejestrem (łańcucha bloków).

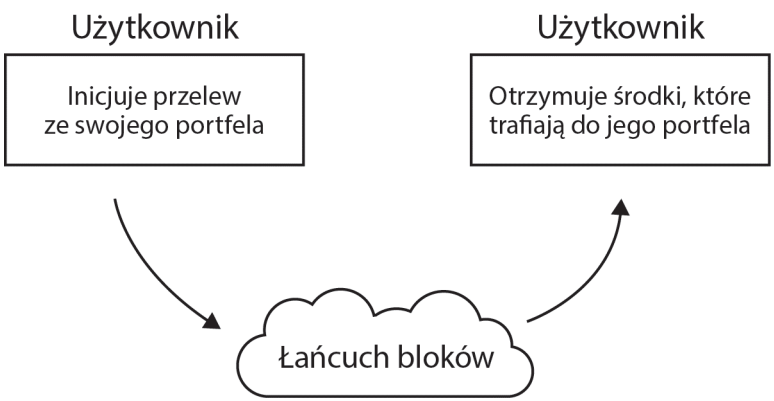


Kiedy otwierasz rachunek w banku, tak naprawdę przenosisz na bank uprawnienia do zarządzania nim. W zamian otrzymujesz natomiast iluzję dostępu do rachunku i możliwości śledzenia wykonywanych na nim operacji. Zawsze, gdy chcesz przelać pieniądze, zdeponować je lub komuś zapłacić, bank zapewnia Ci do nich jasno określony dostęp, bo Ty obdarzyłeś go dorozumianym zaufaniem w kwestii prowadzenia Twoich rozliczeń. Ten „dostęp" jest jednak także iluzją. To tak naprawdę dostęp do zapisu w bazie danych, według którego dysponujesz taką, a nie inną kwotą. Bank oszukuje Cię za pomocą złudzenia, że „posiadasz" te pieniądze. On natomiast ma władzę, bo jest właścicielem bazy danych, w której znajduje się wpis mówiący o tym, że masz pieniądze, a Ty jedynie zakładasz, że faktycznie je masz.

Bankowość jest skomplikowana, ale starałem się uprościć powyższy przykład, aby podkreślić fakt, że to bank posiada władzę i kontrolę nad przyznawaniem lub odmawianiem dostępu do pieniędzy, którymi zarządza. Ta sama koncepcja odnosi się do wszelkich aktywów cyfrowych (akcji, obligacji, papierów wartościowych), które instytucja finansowa może przechowywać w naszym imieniu.

I tu pojawia się łańcuch bloków.

W najprostszej postaci identyczny scenariusz może zaistnieć bez przedstawionych powyżej zawiłości. Użytkownik może wysyłać pieniądze innemu użytkownikowi za pośrednictwem specjalnego portfela, a sieć łańcucha bloków uwierzytelnienia i zatwierdza transakcję oraz wykonuje przelew — co trwa zazwyczaj około 10 minut — przeprowadzając jednocześnie w międzyczasie wymianę kryptowalut lub jej nie przeprowadzając.



Oto magia łańcucha bloków w najczystszej postaci. Proponowałbym każdemu, kto zastanawia się nad możliwościami zastosowania łańcucha bloków, aby przeprowadził tego rodzaju transakcję, posługując się własnym portfelem, po pobraniu jednej z wielu dostępnych wersji łańcucha bloków lub zarejestrowaniu się na lokalnej giełdzie kryptowalut, niezależnie od tego, gdzie mieszka. Gdy tak zrobi, zrozumie rzeczywiste znaczenie określenia „bez pośredników" i zacznie zadawać sobie pytanie, dlaczego wciąż potrzebujemy pośredników, którzy funkcjonują obecnie.

SPOJRZENIE WSTECZ, ABY MÓC POPATRZEĆ W PRZYSZŁOŚĆ

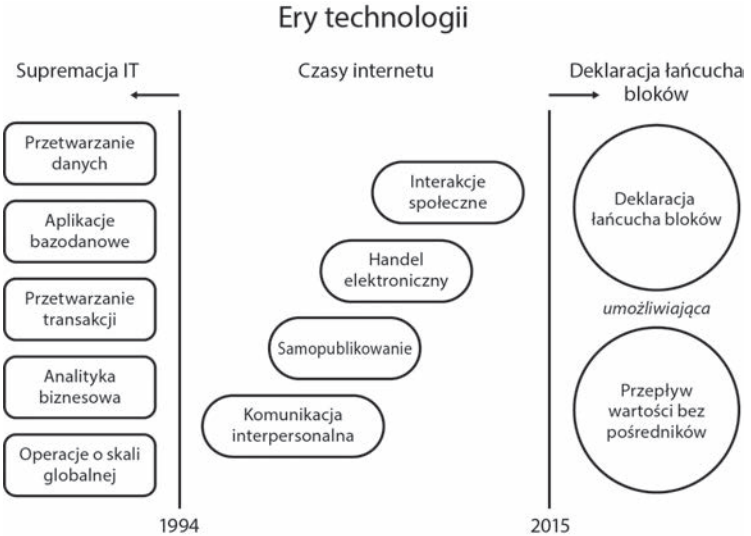
Gdzie zatem powinniśmy umieścić łańcuch bloków w ogólnym kontekście różnych epok ewolucji technologicznej?

W 2003 roku Nicholas G. Carr opublikował w „Harvard Business Review" nowatorski artykuł pod tytułem *IT Does Not Matter*[6], który wywołał niemałe zamieszanie w korporacyjnych kręgach branży technologii informatycznych i zakwestionował ich strategiczne znaczenie. Według niego:

> *Tym, co czyni zasób naprawdę strategicznym — co zapewnia mu możliwość stania się podstawą trwałej przewagi konkurencyjnej — jest nie wszechobecność, lecz deficytowość. Przewagę nad rywalami zdobywa się, wyłącznie robiąc coś, czego oni nie mogą zrobić, lub dysponując czymś, czego oni nie mają. Obecnie podstawowe funkcje IT — przechowywanie danych, przetwarzanie danych i przenoszenie danych — stały się dostępne, także pod względem finansowym, dla wszystkich.*

Po ukazaniu się artykułu przez dwa lata żarliwie polemizowano z Carrem, ale treść jego pracy trafiła już do dyskursu publicznego, co zbiegło się z początkami sieci WWW — potężnej nowej platformy obliczeniowej. Sieć WWW zaskoczyła decydentów z zakresu IT w firmach i większość z nich przez co najmniej trzy lata nie mogła się pozbierać, zwłaszcza że prawie wszyscy koncentrowali się wtedy raczej na problemie roku 2000. Tak naprawdę pojawienie się sieci WWW stało się początkiem upadku IT, bo zapewniała ona przewagę konkurencyjną tym, którzy odpowiednio wcześnie nauczyli się nią posługiwać.

Na wykresie zamieszczonym poniżej widać, że po okresie supremacji IT pojawiły się czasy internetu, po których z kolei powinniśmy przygotować się na to, co niesie ze sobą łańcuch bloków.



Innym sposobem postrzegania ciągłości w ramach ewolucji technologicznej jest określenie faz ewolucji sieci WWW i zrozumienie, że łańcuch bloków to kolejna nowa faza, skoncentrowana na opartych na zaufaniu transakcjach zasobami typu *peer-to-peer*. Przypomnijmy sobie kluczowe minirewolucje, które od 1994 roku przyniósł nam internet w sferach: komunikacji interpersonalnej, samopublikowania, e-handlu i sieci społecznościowych. Z perspektywy czasu każdą z tych czterech faz moglibyśmy zdefiniować w kontekście funkcji, które zakłóciła, a więc działania poczty, mediów papierowych, łańcuchów dostaw i fizycznie istniejących detalistów oraz świata rzeczywistego (tabela na kolejnej stronie).

Cała ta sytuacja podszyta jest pewną ironią, bo wszelkie aplikacje internetowe mogą zastąpić aplikacje oparte na łańcuchach bloków. Chociaż wydaje nam się, że to sieć WWW zapewniła nam nowy paradygmat publikowania informacji, komunikacji i handlu, to jednak właśnie tym funkcjom zagrożą ich nowe wersje, oparte na protokołach *peer-to-peer* wykorzystywanych przez technologie łańcuchów bloków.

FAZA	CEL	ZAKŁÓCENIE	SKUTEK
Komunikacja	Dostęp do wszystkich na świecie	Poczta	Komunikacja interpersonalna
Działalność wydawnicza	Propagowanie idei	Media papierowe	Samopublikowanie
Handel	Wymiana dóbr	Łańcuchy dostaw i fizycznie istniejący detaliści	Handel elektroniczny
Interakcje społeczne	Więź z przyjaciółmi	Świat rzeczywisty	Sieć społecznościowa
Transakcje aktywami	Zarządzanie własnością	Istniejący dysponenci	Usługi oparte na zaufaniu

ROZPAKOWYWANIE ŁAŃCUCHA BLOKÓW

Kontynuujmy eksplorację warstw łańcucha bloków! O ile istnieje jakaś konkretna kwestia, którą zamierzam stale podkreślać, to jest nią fakt, że łańcuch bloków nie jest jednym elementem, przedmiotem, trendem czy jedną cechą. To zbiór wielu elementów, z których jedne funkcjonują łącznie, a inne niezależnie od siebie.

Kiedy około 1995 roku rozpoczęła się komercjalizacja internetu, często opisywaliśmy ją jako zjawisko wieloaspektowe. W mojej wcześniejszej książce, *Opening Digital Markets*, wydanej w 1997 roku, napisałem, że internet posiada „pięć różnych tożsamości", i dodałem, że „wykorzystywanie każdej z nich wymaga opracowania innej strategii". Sieć WWW była więc jednocześnie siecią jako taką, platformą programistyczną, platformą transakcyjną, medium i rynkiem (nie dostrzegaliśmy wówczas jej aspektu społecznościowego, bo pojawił się on później).

Łańcuch bloków nadal wykorzystuje tę mnogość funkcji i posiada symultanicznie dziesięć właściwości. Oto one:

1. Kryptowaluta.
2. Infrastruktura obliczeniowa.
3. Platforma transakcyjna.

4. Zdecentralizowana baza danych.
5. Rozproszony rejestr księgowy.
6. Platforma programistyczna.
7. Oprogramowanie *open source*.
8. Rynek usług finansowych.
9. Sieć *peer-to-peer*.
10. Warstwa usług opartych na zaufaniu.

Omówię po kolei te właściwości, aby wyjaśnić podstawy łańcucha bloków.

1. CYFROWA KRYPTOWALUTA

Funkcja cyfrowej waluty jest zapewne najbardziej „widocznym" elementem łańcucha bloków, zwłaszcza jeśli jest on publiczny, jak na przykład bitcoin (BTC) lub ethereum (ETH). Kryptowaluta jest zasadniczo ekonomicznym wyznacznikiem opłacalności określonych operacji i poziomu bezpieczeństwa łańcucha bloków. Jednostkami wartości kryptowaluty bywają czasem tak zwane tokeny (żetony), które odzwierciedlają jej aspekt finansowy.

Jednym z bardziej skomplikowanych problemów związanych z kryptowalutami jest zmienność ich cen, która sprawia, że większość potencjalnych użytkowników trzyma się od nich z daleka. W artykule z 2014 roku, opisującym metodę stabilizacji kryptowaluty, Robert Sams zacytował Nicka Szabo: „Podstawą zmienności cenowej bitcoina jest zróżnicowanie spekulacyjne, będące z kolei wynikiem rzeczywistej niepewności odnośnie do jego przyszłości. Tej faktycznej niepewności nie są w stanie ograniczyć nawet bardziej wydajne mechanizmy zwiększające płynność". Obecnie poziom społecznej aprobaty dla kryptowalut i poziom ich zrozumienia stają się jednak coraz wyższe, więc przyszłość kryptowalut jawi się jako mniej niepewna, a potencjalny wygląd krzywej ich akceptacji możemy sobie wyobrazić jako coraz bardziej stabilny i regularny.

Kryptowaluta może pełnić funkcję „produkcyjną", a więc służyć jako wynagrodzenie dla kopiących, którzy zdobywają nagrody po pomyślnej weryfikacji transakcji. Może także pełnić funkcję „konsumpcyjną", a więc być nośnikiem niewielkich opłat za doprowadzanie do inteligentnych kontraktów

(na przykład ETH w przypadku ethereum) lub ekwiwalentem opłaty transakcyjnej (na przykład XRP w przypadku ripple lub BTC w przypadku bitcoina). Zadaniem tego rodzaju motywacji ekonomicznych i kosztów jest zapobieganie nadużyciom w ramach łańcuchów bloków. Bardziej złożonym przypadkiem użycia kryptowaluty może być wykorzystywanie tokenów jako nośników wartości wewnętrznej, na przykład w autonomicznych organizacjach rozproszonych (DOA), które omówię w rozdziałach 5. i 7.

Poza tym, że kryptowaluta funkcjonuje w kontekście łańcuchów bloków, przypomina ona każdą inną walutę. Może być przedmiotem obrotu giełdowego, można ją też wykorzystywać do kupowania lub sprzedawania towarów i usług. Kryptowaluta jest bardzo efektywna w sieciach łańcuchów bloków, ale wkraczając do świata walut rzeczywistych (zwanych także walutami fiducjarnymi), zawsze spotyka się z pewnym oporem.

2. ZDECENTRALIZOWANA INFRASTRUKTURA OBLICZENIOWA

Łańcuch bloków może być również postrzegany jako metoda projektowania oprogramowania, w ramach której wiele komputerów łączy się ze sobą i wprowadza się proces „konsensusu", zarządzający obiegiem informacji, a wszelkie interakcje między tymi komputerami są weryfikowane kryptograficznie.

Z fizycznego punktu widzenia faktycznym napędem dla łańcuchów bloków są połączone w sieć serwery komputerowe. Programiści nie muszą jednak tych serwerów konfigurować — w tym właśnie między innymi przejawia się magia łańcuchów bloków. Inaczej niż w przypadku sieci WWW, gdzie żądania do serwera wysyłane są za pośrednictwem protokołu HTTP (Hypertext Transfer Protocol), aplikacje wykorzystujące łańcuchy bloków obsługują żądania wysyłane przez sieć właśnie do łańcuchów bloków.

3. PLATFORMA TRANSAKCYJNA

Sieć łańcuchów bloków może weryfikować różnorodne transakcje związane z przenoszeniem wartości i odnoszące się do cyfrowych środków pieniężnych lub zasobów, które zostały zdigitalizowane. Za każdym razem, gdy osiągnięty zostaje konsensus, transakcja jest rejestrowana w „bloku", będą-

cym repozytorium danych. Łańcuch bloków rejestruje transakcje, które później można zweryfikować jako przeprowadzone. Łańcuch bloków jest zatem gigantyczną platformą przetwarzania transakcji, zdolną do obsługi zarówno mikropłatności, jak i transakcji o znacznej wartości.

Gdybyśmy mieli porównać łańcuch bloków z innymi sieciami przetwarzania transakcji, moglibyśmy posłużyć się pojęciem przepustowości, którą mierzy się liczbą transakcji na sekundę (TPS). Za punkt odniesienia moglibyśmy uznać Visę, która w 2015 roku notowała w swojej sieci VisaNet średnio 2000 TPS, a maksymalnie 4000 TPS, osiągając maksymalną przepustowość wynoszącą 56 000 TPS. W 2015 roku PayPal zrealizował łącznie 4,9 miliarda płatności[7], co odpowiada 155 TPS. Według danych za rok 2016 łańcuch bloków bitcoina był daleki od takich wartości, zawierając się w granicach 5 – 7 TPS, ale z perspektywami znacznego wzrostu w tym zakresie dzięki postępom technologii łańcuchów bocznych i oczekiwanym przyrostom wielkości bloków bitcoina. Niektóre inne łańcuchy bloków są szybsze niż bitcoin. Ethereum zaczęło na przykład od 10 TPS w 2015 roku, zbliżając się do 50 – 100 TPS w roku 2017, a docelowo mierząc w 50 000 – 100 000 TPS do roku 2019[8]. Prywatne łańcuchy bloków są jeszcze szybsze, bo mają mniej ograniczeń odnośnie do wymogów bezpieczeństwa, i już w roku 2016 osiągały 1000 – 10 000 TPS, w roku 2017 zanotowały wzrost do 2000 – 15 000 TPS, a po roku 2019 pułap ten może być już potencjalnie nieograniczony. Przepustowość w zakresie tempa realizacji transakcji może także zwiększyć połączenie efektywności łańcuchów bloków z technologią klastrów baz danych, co zapewne stanie się przyczynkiem do dalszego rozwoju tej technologii.

4. ZDECENTRALIZOWANA BAZA DANYCH

Łańcuch bloków narusza paradygmat baz danych i przetwarzania transakcji. W 2014 roku zdecydowanie stwierdziłem, że łańcuch bloków to nowa baza danych i ostrzegłem programistów, że powinni przygotować się na konieczność przepisania wszystkiego, co wcześniej stworzyli.

Łańcuch bloków jest rodzajem miejsca, w którym przechowujemy dane w sposób częściowo publiczny, w jednym kawałku (bloku). Każdy może zweryfikować, że to my umieściliśmy określone informacje w zasobniku, bo

zawiera on nasz podpis, ale tylko my (lub program) możemy zobaczyć, co znajduje się w zasobniku, bo tylko my dysponujemy przechowywanymi w bezpiecznym miejscu prywatnymi kluczami do tych danych.

Łańcuch bloków zachowuje się więc prawie jak baza danych, z wyjątkiem tego, że część przechowywanych w nim informacji, ich „nagłówki", jest dostępna publicznie. Łańcuchy bloków nie są być może wyjątkowo efektywnymi bazami danych, ale to nie problem — ich zadanie nie polega na zastępowaniu dużych baz danych. To raczej zadaniem programistów jest ustalenie, w jaki sposób mogliby przepisać swoje aplikacje, aby wykorzystać możliwości łańcuchów bloków w zakresie przejść między stanami.

5. WSPÓŁDZIELONY, ROZPROSZONY REJESTR KSIĘGOWY

Łańcuch bloków jest także rozproszonym, publicznym, opatrzonym znacznikami czasu rejestrem księgowym, przechowującym zapisy wszystkich transakcji, jakie zostały kiedykolwiek przeprowadzone w ramach jego sieci, i umożliwiającym komputerom użytkowników weryfikację poprawności każdej transakcji w taki sposób, aby niemożliwe było podwójne wydatkowanie środków. Rejestr ten może współdzielić wiele podmiotów i może on być prywatny, publiczny lub częściowo prywatny.

Chociaż opis łańcucha bloków jako rozproszonego rejestru transakcji jest popularny i niektórzy uważają tę jego właściwość za najistotniejszą, to faktycznie stanowi ona tylko jedną z jego cech.

6. PLATFORMA PROGRAMISTYCZNA

Dla programistów łańcuch bloków to przede wszystkim zestaw technologii związanych z tworzeniem oprogramowania. Owszem, zawierających fundamentalne implikacje polityczne i społeczne (w postaci decentralizacji), ale dla nich będących przede wszystkim źródłem nowinek technologicznych. Taki nowy zestaw narzędzi programistycznych to dla twórców oprogramowania niebywała gratka. Łańcuch bloków zawiera technologie umożliwiające tworzenie nowego rodzaju aplikacji, które są zdecentralizowane i zabezpieczone kryptograficznie. Łańcuchy bloków można więc uznać za nowy sposób tworzenia aplikacji.

Łańcuchy bloków mogą także dysponować wieloma interfejsami programowania aplikacji (API), w tym językiem skryptowym transakcji, interfejsem API do komunikacji między węzłami P2P oraz klientem API do sprawdzania transakcji w sieci. Aspekt programistyczny łańcucha bloków omówię bardziej szczegółowo w rozdziale 6.

7. OPROGRAMOWANIE OPEN SOURCE

Większość prawidłowo funkcjonujących łańcuchów bloków ma otwarty kod źródłowy, co oznacza nie tylko to, że źródło oprogramowania ma charakter publiczny, ale także to, że innowacyjne rozwiązania mogą być wprowadzane do oprogramowania bazowego przez różne podmioty — na zasadach współpracy.

Otwarty jest na przykład podstawowy protokół bitcoina. Od momentu jego stworzenia przez Satoshiego Nakamoto prace prowadzi nad nim grupa „kluczowych programistów", którzy stopniowo go doskonalą. Dodatkowo niezawodność protokołu bitcoina wykorzystują jednak tysiące niezależnych programistów, którzy także wprowadzają innowacyjne rozwiązania w zakresie produktów, usług i aplikacji.

To, że oprogramowanie łańcuchów bloków ma charakter *open source*, jest bardzo istotne, bo im bardziej otwarty jest sam rdzeń łańcucha bloków, tym silniejszy stanie się zbudowany wokół niego ekosystem.

8. RYNEK USŁUG FINANSOWYCH

Pieniądze są centralnym punktem łańcuchów bloków opartych na kryptowalutach. Gdy traktujemy kryptowaluty jak wszelkie inne waluty, to mogą się one stawać elementami instrumentów finansowych, co prowadzi do powstawania różnego rodzaju nowych produktów finansowych.

Łańcuchy bloków tworzą niezwykle innowacyjne środowisko dla usług finansowych nowej generacji, które zdobędą popularność, gdy zniknie niepewność związana z kryptowalutami. Instrumenty pochodne, opcje, transakcje swap, instrumenty syntetyczne, inwestycje, kredyty i inne tradycyjne instrumenty finansowe zyskają wersje kryptowalutowe, dzięki czemu stworzą nowy rynek obrotu usługami finansowymi.

9. SIEĆ PEER-TO-PEER

W łańcuchach bloków nie ma elementów „centralnych". Z punktu widzenia architektury podstawową warstwą łańcucha bloków jest sieć *peer-to-peer*. Łańcuchy bloków promują decentralizację, zlecając przetwarzanie danych równorzędnym podmiotom w lokalizacjach zwanych węzłami. Sieć to tak naprawdę komputer. Wszystkie transakcje weryfikowane są na poziomie *peer-to-peer*. Łancuch bloków można zasadniczo uznać za stosunkowo płaską chmurę obliczeniową, która jest faktycznie zdecentralizowana.

Każdy użytkownik może w każdej chwili nawiązać kontakt z innym użytkownikiem i zawrzeć z nim transakcję, bez względu na to, gdzie się znajduje, i niezależnie od pory dnia. Filtrowanie, blokowanie czy opóźnianie transakcji między dowolnymi dwoma lub wieloma użytkownikami, czyli między węzłami prowadzącymi transakcję, przeprowadzane jest bez jakichkolwiek pośredników. Każdy węzeł sieci ma możliwość prowadzenia działań na podstawie własnej wiedzy o transakcjach zawieranych w całej sieci.

Oprócz technicznych sieci P2P łańcuchy bloków tworzą także rynek użytkowników. Sieci łańcuchów bloków i działające na ich bazie aplikacje tworzą własne (rozproszone) systemy ekonomiczne, charakteryzujące się różną wielkością i różnymi poziomami dynamiki. Łańcuchy bloków niosą więc ze sobą model ekonomiczny — to ich kluczowa cecha, którą omówię szerzej w dalszej części książki.

10. WARSTWA USŁUG OPARTYCH NA ZAUFANIU

Wszystkie łańcuchy bloków funkcjonują na bazie zaufania, wbudowanego w ich strukturę na poziomie „atomowym". To zasadniczo zarówno funkcja, jak i zapewniana usługa. Zaufanie odnosi się jednak nie tylko do transakcji. Obejmuje także dane, usługi, procesy, tożsamość, logikę biznesową, warunki umów, a nawet obiekty fizyczne. Ma zastosowanie do niemal wszystkiego, co da się zdigitalizować jako (inteligentny) zasób o przypisanej wartości.

A teraz wyobraź sobie połączenie innowacji, które pojawią się za sprawą tych 10 właściwości i cech. Łącząc je ze sobą, zaczniesz dostrzegać nieprawdopodobne możliwości łańcuchów bloków w zakresie uaktywniania zmian.

PRZEJŚCIA MIĘDZY STANAMI I MASZYNY STANOWE — CO TO TAKIEGO?

Łańcuch bloków nie nadaje się do wszystkiego. I nie wszystko spełnia paradygmat łańcucha bloków. Łańcuch bloków to „maszyna stanowa", czyli kolejna koncepcja, nad którą należy się zastanowić.

Pod względem technicznym stan oznacza po prostu „przechowywane informacje" w określonym momencie. Maszyna stanowa to komputer lub urządzenie, które zapamiętuje stan czegoś w danej chwili. Stan ten może ulec zmianie na podstawie rozmaitych danych wejściowych, a maszyna na podstawie wprowadzonych zmian tworzy dane wyjściowe. Śledzenie przejść między stanami jest istotne, a właśnie łańcuch bloków doskonale sobie z tym radzi i funkcjonuje w sposób zapewniający niezmienność. Zapis w bazie danych jest natomiast zmienny, bo może być wielokrotnie nadpisywany. Nie wszystkie bazy danych posiadają ścieżki audytu, a nawet jeśli tak jest, mogą one zostać zniszczone lub utracone, bo nie są zabezpieczone przed manipulacjami. W przypadku łańcuchów bloków historia przejść między stanami jest trwałym elementem informacji o tych stanach. W łańcuchu bloków ethereum przechowywane są odrębne „drzewo stanów", określające bieżące saldo każdego adresu, oraz „lista transakcji", będąca zapisem transakcji między bieżącym blokiem a blokami, które go poprzedzają.

Maszyny stanowe dobrze nadają się do stosowania w systemach rozproszonych, które muszą być odporne na awarie.

ALGORYTMY KONSENSUSU

Podstawowe znaczenie dla zrozumienia tego, w jak ogromnym stopniu łańcuch bloków zmienia dotychczasowy paradygmat, ma zapoznanie się z koncepcją „zdecentralizowanego konsensusu", kluczowego założenia rewolucji obliczeniowej opartej na kryptografii.

Zdecentralizowany konsensus łamie dawny paradygmat konsensusu scentralizowanego, wywodzącego się z czasów, gdy do weryfikowania poprawności transakcji służyła jedna centralna baza danych. Schemat zdecentralizowany (na którym bazują protokoły łańcuchów bloków) przekazuje uprawnienia i zaufanie zdecentralizowanej sieci wirtualnej i umożliwia jej węzłom

nieprzerwane i sekwencyjne rejestrowanie transakcji w publicznym „bloku", tworząc niepowtarzalny „łańcuch" — łańcuch bloków. Każdy kolejny blok zawiera „hasz" (niepowtarzalny cyfrowy odcisk palca) wcześniejszego kodu, a do uwierzytelniania źródeł transakcji służy kryptografia (za sprawą kodów skrótu), która jednocześnie eliminuje potrzebę istnienia centralnego pośrednika. Dzięki połączeniu kryptografii i technologii łańcucha bloków nie ma możliwości zduplikowania zapisu tej samej transakcji. Istotną kwestią w kontekście naszych rozważań jest to, że przy tak znacznym stopniu rozdzielenia logika konsensusu zostaje oddzielona od aplikacji jako takiej, więc aplikacje mogą być tworzone w sposób zapewniający im organiczne zdecentralizowanie — i to właśnie powinno inspirować zmieniające system innowacje w zakresie architektury oprogramowania aplikacji, niezależnie od tego, czy miałyby one obsługiwać sferę finansów, czy nie.

Konsensus moglibyśmy uznać za pierwszą warstwę architektury zdecentralizowanej. Stanowi on podstawę protokołu, który określa zasady działania łańcucha bloków.

Algorytm konsensusu jest jądrem łańcucha bloków, metodą czy też protokołem, który zatwierdza transakcję. To istotna sprawa, bo my musimy mieć do tych transakcji zaufanie. Jako użytkownicy biznesowi nie musimy dogłębnie rozumieć sposobów działania określonych algorytmów, o ile jesteśmy przekonani, że są bezpieczne i niezawodne.

Bitcoin zainicjował metodę konsensusu zwaną dowodem pracy (ang. *Proof-of-Work* — POW), którą można uznać za praprzodka tych algorytmów. POW opiera się na rozwiązaniu zagadnienia bizantyjskich generałów (ang. *Practical Byzantine Fault Tolerant*)[9], umożliwiając bezpieczne przeprowadzanie transakcji zgodnie z danym stanem. Alternatywą POW w sferze osiągania konsensusu jest dowód stawki (ang. *Proof-of-Stake* — POS[10]). Istnieją także inne protokoły konsensusu, takie jak RAFT, DPOS i Paxos, ale nie będę się tutaj zajmować ich porównywaniem, bo z czasem staną się rozwiązaniami standardowymi. Istotniejsze będą dla nas niezawodność narzędzi i technologii oprogramowania pośredniego, tworzonych na bazie tych algorytmów, a także ekosystem otaczających ich podmiotów tworzących wartość dodaną.

Jedna z wad algorytmu dowodu pracy polega na tym, że nie jest on przyjazny dla środowiska, bo wymaga dużej mocy obliczeniowej pozyskiwanej

z wyspecjalizowanych urządzeń generujących ogromne ilości energii. Silnym rywalem dla POW będzie algorytm dowodu stawki (POS), który opiera się na koncepcji wirtualnego kopania i głosowania opartego na tokenach, a ten proces nie wymaga tak intensywnego przetwarzania danych jak POW i wygląda na to, że umożliwi zapewnianie bezpieczeństwa systemom w mniej kosztowny sposób.

Na koniec, skoro zajmujemy się algorytmem konsensusu, powinniśmy zastanowić się nad metodą „ograniczania dostępu", która określa, kto kontroluje proces konsensusu i bierze w nim udział. W tym zakresie istnieją trzy popularne opcje:

1. Publiczna (na przykład POW, POS, delegowanie POS).
2. Prywatna (z wykorzystaniem tajnych kluczy do kontrolowania zamkniętych łańcuchów bloków).
3. Częściowo prywatna (na przykład o charakterze konsorcjalnym, wykorzystująca tradycyjny algorytm tolerancji wady bizantyjskiej w sposób zbiorowy).

KLUCZOWE KONCEPCJE Z ROZDZIAŁU 1.

1. Łańcuch bloków jest warstwą technologii o charakterze nakładki na internet, podobnie jak sieć WWW.
2. Łańcuch bloków posiada definicje: techniczną, biznesową i prawną.
3. Dowód kryptograficzny to wykorzystywana przez łańcuch bloków zaufana metoda potwierdzania prawidłowości i finalizacji transakcji zawieranych między określonymi stronami.
4. Łańcuch bloków zmieni definicję zasad funkcjonowania istniejących pośredników (o ile zgodzą się oni na tę zmianę) i stworzy jednocześnie nowych pośredników, a tym samym zakłóci tradycyjnie określone granice wartości.
5. Łańcuch bloków posiada dziesięć charakterystycznych cech, które należy pojmować całościowo.

SKOROWIDZ

Z


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Łańcuch bloków: otwórz się na całkowicie nowe koncepcje i modele biznesowe!

Technologia blockchain (łańcuch bloków) permanentnie rejestruje transakcje w taki sposób, że nie da się ich usunąć, lecz tylko można je sekwencyjnie aktualizować, tworząc w istocie niekończący się zapis historii. Ta pozornie prosta funkcjonalność ma znaczące implikacje, bo wymusza ewolucję sposobów zawierania transakcji, przechowywania danych i przenoszenia zasobów. Łańcuchy bloków są katalizatorami ogromnych zmian, oddziałujących na sferę sprawowania władzy, zarządzanie własnością, styl życia, tradycyjne modele korporacyjne, społeczeństwo i instytucje globalne.

Ta książka jest przewodnikiem, który jak żadna inna publikacja skłania do przemyśleń i oddania się pracy koncepcyjnej. Dzięki tej książce zrozumiesz podstawy technologii blockchain, dowiesz się więcej o jej zastosowaniach i przekonasz się, że już dziś należy postawić sobie kilka strategicznych pytań, aby za chwilę być gotowym na jeszcze ambitniejsze wyzwania. Z całą pewnością łańcuch bloków jest technologią bardziej skomplikowaną niż sieć WWW. Dzięki tej książce zrozumiesz jej znaczenie dla rozwoju cywilizacji.

W tej książce między innymi:

- Wyjaśnienie koncepcji blockchain
- Łańcuch bloków jako nowa warstwa zaufania
- Możliwości łańcucha bloków i przeszkody w jego wdrażaniu
- Techniczne aspekty implementacji łańcucha bloków
- Decentralizacja sieci, przenikanie technologii i nowy kształt gospodarki

WILLIAM MOUGAYAR

bada biznesowe zastosowania łańcucha bloków i ma wpływ na rozwój tej technologii. Jest też komplementariuszem Virtual Capital Ventures, funduszu *venture capital* inwestującego w młode startupy technologiczne. Zasiada w radzie nadzorczej konsorcjum OB1, pracującego nad pionierskim projektem: protokołem *open source* o nazwie OpenBazaar, który ma decentralizować obrót handlowy na zasadach *peer-to-peer*.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-4932-2

INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 49,00 zł
onepress