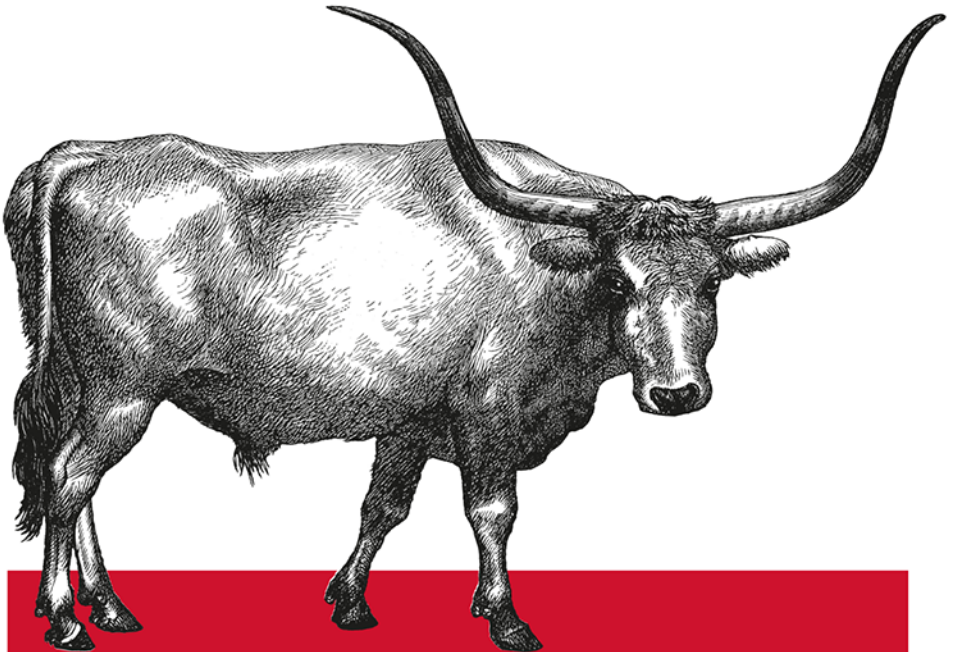
O'REILLY®



Blockchain

FUNDAMENT NOWEJ GOSPODARKI

Helion

Melanie Swan

Tytuł oryginału: Blockchain: Blueprint for a New Economy

Tłumaczenie: Michał Lipa

ISBN: 978-83-283-5921-5

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/blofun
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Przedmowa

Powinniśmy traktować łańcuch bloków tak samo jak traktujemy internet: jak kolejną klasę technologii, wszechstronne rozwiązanie informatyczne o wielu poziomach technicznych i licznych zastosowaniach w sferze rejestrowania, katalogowania i wymiany aktywów, zaczynając od wszystkich dziedzin finansów, ekonomii i gospodarki pieniężnej, zarządzania aktywami trwałymi (zasobami materialnymi, nieruchomościami, samochodami) oraz wartościami niematerialnymi (głosami wyborców, pomysłami, reputacją, intencjami, danymi dotyczącymi zdrowia, informacjami itd.). Koncepcja łańcucha bloków jest jednak czymś więcej — to nowy model odkrywania, wyceny i przesyłania kwantów (czyli dyskretnych jednostek) czegokolwiek, mogący również posłużyć do koordynowania wszelkiej ludzkiej działalności w skali znacznie większej, niż było to możliwe w przeszłości.

Być może stoimy u progu nowej rewolucji. Zaczęła się ona od narodzin gospodarki alternatywnej w internecie, od pojawienia się nieoficjalnej waluty cyfrowej zwanej bitcoinem, która nie jest emitowana i gwarantowana przez władzę centralną, lecz funkcjonuje na bazie zautomatyzowanego mechanizmu konsensusu pomiędzy użytkownikami sieci. Źródłem jej wyjątkowości jest brak potrzeby istnienia zaufania pomiędzy ludźmi. Każda próba oszukania systemu zostanie powstrzymana przez algorytmy samoregulacji. Według bardzo precyzyjnej i technicznej definicji, bitcoin jest cyfrowym pieniądzem służącym do zawierania transakcji przez internet za pośrednictwem zdecentralizowanego, niewymagającego zaufania systemu opartego na rejestrze publicznym mającym postać łańcucha bloków (ang. *blockchain*). Jest to nowa forma pieniądza, łącząca opartą na protokole BitTorrent technologię wymiany plików

w sieci *peer-to-peer*[1] z technologią kryptografii klucza publicznego[2]. Od momentu stworzenia bitcoina w 2009 roku pojawiło się wiele jego imitacji — alternatywnych kryptowalut opartych na takim samym podejściu ogólnym, ale inaczej zoptymalizowanych i pod pewnymi względami ulepszonych. Co ważniejsze, technologia łańcucha bloków może idealnie wpasować się w strukturę globalnej sieci, stając się jej ekonomicznym pierwiastkiem, którego dotąd nie miała. Może służyć jako technologiczna podstawa płatności, zdecentralizowanej wymiany dóbr, zarabiania i wydawania tokenów, powoływania się na cyfrowe zasoby i przekazywania ich, a także wystawiania i wykonywania inteligentnych kontraktów. Bitcoin i technologia łańcucha bloków jako środek decentralizacji mogą się okazać następnym czynnikiem twórczej destrukcji i nowym ogólnoświatowym paradygmatem w informatyce (po komputerach typu mainframe, pecetach, internecie oraz sieciach społecznościowych i telefonach komórkowych), obdarzonym potencjałem rekonfiguracji ludzkiej aktywności równym temu, który miała sieć WWW.

Waluta, kontrakty i aplikacje poza rynkami finansowymi

Potencjalne korzyści oferowane przez łańcuch bloków nie mają wyłącznie ekonomicznego charakteru, gdyż będą odczuwane także w sferze politycznej, humanitarnej, społecznej i naukowej, a niektóre grupy już teraz wykorzystują możliwości techniczne łańcucha bloków do rozwiązywania realnych problemów. Technologii tej można użyć w celu przeciwstawiania się represyjnym reżimom politycznym, przenosząc do zdecentralizowanej chmury funkcje, które wcześniej były realizowane przez organy o ograniczonej jurysdykcji. Oczywiście będzie to przydatne dla takich organizacji jak WikiLeaks (która po wybuchu afery Edwarda Snowdena została odcięta od datków, gdyż rządy państw zabraniały firmom przetwarzającym płatności kartami przekazywania jej pieniędzy) oraz wszelkich podmiotów o ponadnarodowym charakterze i neutralnych politycznie, takich jak wyznaczająca standardy w internecie grupa ICANN oraz

[1] R. Kayne, *What Is BitTorrent?*, wiseGEEK, 25 grudnia 2014, *http://www.wisegeek.com/what-is-bittorrent.htm#didyouknowout* [dostęp: 31 sierpnia 2019].

[2] Vangie Beal, *Public-key encryption*, Webopedia, *http://www.webopedia.com/TERM/P/public_key_cryptography.html* [dostęp: 31 sierpnia 2019].

system DNS. Poza tego typu sytuacjami, w których interes społeczny musi stać ponad strukturami władzy państwowej, pojawia się także możliwość uwolnienia niektórych branż i gałęzi gospodarki od wypaczonych rozwiązań regulacyjnych i licencyjnych podlegających hierarchicznej władzy oraz wpływom wywieranym na rządy przez mocno ugruntowane grupy interesu, co umożliwi powstawanie nowych modeli biznesowych wykluczających pośrednictwo struktur centralnych. Choć regulacje wymuszone przez lobby instytucjonalne skutecznie zablokowały rozwój sektora usług konsumenckich związanych z sekwencjonowaniem genomu ludzkiego[3], nowe modele działalności oparte na idei współdzielenia zasobów, stosowane przez takie firmy jak Airbnb i Uber, dotychczas skutecznie opierały się atakom zasiedziałych przedstawicieli branży[4].

Korzyści ekonomiczne i polityczne to nie wszystko: koordynacja transakcji, ich rejestrowanie oraz gwarantowanie ich nieodwołalności za pomocą technologii blockchain mogą się okazać tak ważne dla dalszego rozwoju społeczeństwa jak Magna Carta czy kamień z Rosetty. Łańcuch bloków może służyć całym społeczeństwom jako ogólnodostępne archiwum zawierające rejestry wszystkich dokumentów, zdarzeń, tożsamości i aktywów. W takim systemie każdy składnik majątku nabiera cech *inteligentnej własności*: można go zaszyfrować w łańcuchu bloków, nadając mu niepowtarzalny identyfikator, za pomocą którego będzie można go śledzić, kontrolować i wymieniać (kupować i sprzedawać) w ramach łańcucha. Inaczej mówiąc, wszelkiego rodzaju aktywa fizyczne (domy, samochody) i cyfrowe będzie można rejestrować w łańcuchu bloków i wprowadzać do obrotu za jego pośrednictwem.

Rozważmy następujący przykład (pierwszy z wielu, które znajdują się w tej książce): możliwość zmieniania świata przez łańcuch bloków wykorzystywany do rejestrowania i ochrony własności intelektualnej. Rodząca się branża sztuki cyfrowej oferuje usługi prywatnego rejestrowania dokładnej zawartości dowolnego zasobu cyfrowego (pliku, obrazu, kartoteki medycznej, oprogramowania itd.)

---

[3] Robert Hof, *Seven Months After FDA Slapdown, 23andMe Returns with New Health Report Submission*, „Forbes", 20 czerwca 2014, *https://www.forbes.com/sites/roberthof/2014/06/20/seven-months-after-fda-slapdown-23andme-returns-with-new-health-report-submission/* [dostęp: 31 sierpnia 2019].

[4] Heather Knight, Benny Evangelista, *S.F., L.A. Threaten Uber, Lyft, Sidecar with Legal Action*, SFGATE, 25 września 2014, *http://m.sfgate.com/bayarea/article/S-F-L-Athreaten-Uber--Lyf-Sidecar-with-5781328.php* [dostęp: 31 sierpnia 2019].

Łańcuch bloków mógłby zastąpić albo uzupełnić wszystkie istniejące systemy zarządzania własnością intelektualną. Sposób jego działania polega na zastosowaniu standardowego algorytmu w odniesieniu do dowolnego pliku w celu skompresowania go do postaci krótkiego, niepowtarzalnego kodu składającego się z 64 znaków (*skrótu*, zwanego też *haszem*), przypisanego do tego dokumentu[5]. Każdy plik, bez względu na jego wielkość (może to być np. 9-gigabajtowy plik zawierający sekwencję genomu ludzkiego), zyskuje postać bezpiecznego skrótu składającego się z 64 znaków, którego nie da się rozszyfrować za pomocą obliczeń wstecznych. Jest on następnie przypisywany do transakcji w łańcuchu bloków i otrzymuje znacznik czasu, który potwierdza, że w danym momencie istnieje jako zasób cyfrowy. Skrótu nie da się ponownie obliczyć na podstawie pliku będącego jego podstawą (przechowywanego bezpiecznie na komputerze właściciela, nie w łańcuchu bloków), co daje gwarancję, że oryginalna zawartość pliku nie ulegnie zmianie. Zestandaryzowane mechanizmy, takie jak prawo dotyczące umów, były rewolucyjnymi krokami do przodu dla społeczeństwa, a rejestracja własności intelektualnej (sztuki cyfrowej) w łańcuchu bloków mogłaby być jednym z takich punktów zwrotnych w dziedzinie usprawniania koordynacji dużych społeczeństw, ponieważ coraz większa część aktywności gospodarczej opiera się na generowaniu nowych idei.

Blockchain 1.0, 2.0 i 3.0

Korzyści o charakterze ekonomicznym, politycznym, humanitarnym i prawnym, wynikające z używania bitcoina i technologii łańcucha bloków coraz bardziej świadczą o tym, że wynalazek ten ma ogromny potencjał wywoływania twórczej destrukcji i może doprowadzić do rekonfiguracji wszystkich aspektów funkcjonowania społeczeństwa. Różne rodzaje istniejących i możliwych w przyszłości zastosowań łańcucha bloków podzielono dla porządku i wygody na trzy kategorie: blockchain 1.0, 2.0 i 3.0. Blockchain 1.0 to *waluta*, czyli wszelkie zastosowania kryptowalut związane z obrotem pieniężnym, takie jak przelewy walutowe, przekazy środków pieniężnych i cyfrowe systemy płatności. Blockchain 2.0 to *kontrakty*, a więc cały szereg zastosowań ekonomicznych, rynkowych

[5] Choć nie jest całkiem wykluczone, żeby dwa pliki miały taki sam hasz, całkowita liczba możliwych 64-znakowych skrótów jest nieporównanie większa niż liczba plików, które ludzkość zdoła utworzyć w przewidywalnej przyszłości. Przypomina to standard kryptograficzny, zgodnie z którym nawet w przypadku istnienia możliwości złamania szyfru potrzebne do tego obliczenia trwałyby dłużej niż okres istnienia wszechświata.

i finansowych opartych na łańcuchu bloków, wychodzących poza proste transakcje pieniężne, takie jak akcje, obligacje, kontrakty terminowe, kredyty hipoteczne, tytuły własności, inteligentna własność i inteligentne kontrakty. Blockchain 3.0 oznacza inne *zastosowania* łańcucha bloków niż walutowe, finansowe i rynkowe, zwłaszcza w administracji państwowej, ochronie zdrowia, nauce, literaturze, kulturze i sztuce.

Czym jest bitcoin?

Bitcoin to cyfrowy pieniądz. Jest cyfrową walutą i elementem systemu płatności internetowych, w którym generowanie jednostek pieniężnych i weryfikowanie transferu środków odbywa się za pomocą technik szyfrowania, niezależnie od banku centralnego. Terminologia może być myląca, ponieważ słowa *bitcoin* i *blockchain* są używane na określenie dowolnego z trzech elementów całej koncepcji: podstawowej *technologii* łańcucha bloków, *protokołu* i *klienta*, za pomocą których realizowane są transakcje, oraz samej *kryptowaluty* (pieniądza cyfrowego). Odnoszą się też bardziej ogólnie do całej koncepcji kryptowalut. To tak, jakby PayPal użyczył internetowi swojej nazwy i za pomocą protokołu PayPal wykonywał w nim transfery waluty określanej tym samym mianem. Środowisko skupione wokół technologii blockchain czasem używa wymienionych terminów zamiennie, ponieważ nadal jeszcze trwa proces krystalizowania się łańcucha bloków jako potencjalnie permanentnej warstwy technologii internetowej.

Bitcoin został stworzony w 2009 roku (wyemitowano go 9 stycznia[6]) przez nieznaną osobę lub organizację występującą pod pseudonimem Satoshi Nakamoto. Koncepcję i szczegóły działania opisano w zwięzłym i przystępnie napisanym dokumencie zatytułowanym *Bitcoin: A Peer-to-Peer Electronic Cash System*[7]. Płatności dokonywane w zdecentralizowanej, wirtualnej walucie są zapisywane w rejestrze rozproszonym, przechowywanym na wielu — w miarę możliwości na wszystkich — komputerach użytkowników bitcoina i bez przerwy dostępne do wglądu w internecie. Bitcoin jest pierwszą i największą spośród zdecentralizowanych kryptowalut. Istnieją też setki „altcoinów" („monet alternatywnych"),

[6] Satoshi Nakamoto, *Bitcoin v0.1 Released*, The Mail Archive, 9 stycznia 2009, *http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html* [dostęp: 31 sierpnia 2019].

[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (dane publikacji niedostępne), *https://bitcoin.org/bitcoin.pdf* [dostęp: 31 sierpnia 2019].

takich jak litecoin i dogecoin, ale bitcoin stanowi 90% kapitalizacji rynkowej wszystkich kryptowalut i obecnie wyznacza faktyczny standard branży. Bitcoin jest pseudonimowy (nie jest anonimowy) w tym sensie, że adresy klucza publicznego (ciągi od 27 do 32 znaków alfanumerycznych pełniące podobną funkcję jak adresy poczty elektronicznej) są wykorzystywane do wysyłania i przyjmowania bitcoinów oraz rejestrowania transakcji bez przekazywania danych osobowych umożliwiających identyfikację użytkownika.

Bitcoiny powstają jako zapłata za wykonaną pracę obliczeniową, określaną mianem *kopania*, w ramach której użytkownicy użyczają mocy obliczeniowej swoich komputerów do weryfikowania i rejestrowania płatności w rejestrze publicznym. Osoby prywatne oraz firmy zajmują się kopaniem wirtualnych pieniędzy w zamian za opłaty transakcyjne i nowo wygenerowane bitcoiny. „Bitmonety" można również nabyć za pieniądze albo otrzymać jako zapłatę za produkty i usługi. Użytkownicy mogą wysyłać i otrzymywać bitcoiny w postaci elektronicznej, uiszczając opłatę transakcyjną w optymalnej wysokości, przy użyciu *oprogramowania portfela* na komputerze osobistym, urządzeniu mobilnym albo w aplikacji internetowej.

Czym jest łańcuch bloków?

Łańcuch bloków to publiczny rejestr wszystkich transakcji bitcoinowych, jakie kiedykolwiek przeprowadzono. Rozrasta się on przez cały czas, w miarę jak górnicy dodają do łańcucha nowe bloki (co 10 minut), rejestrując najnowsze transakcje. Bloki dodaje się do łańcucha liniowo, w porządku chronologicznym. Każdy pełny węzeł (tj. każdy komputer podłączony do systemu Bitcoin, używający programu klienckiego do weryfikowania i przekazywania transakcji) posiada kopię łańcucha bloków, pobieraną automatycznie w momencie przyłączenia się górnika do sieci Bitcoin. Łańcuch zawiera kompletny zbiór informacji na temat adresów i sald od bloku genezy (obejmującego pierwsze wykonane transakcje) do ostatniego ukończonego bloku. Łańcuch bloków jako rejestr rozproszony umożliwia łatwe sprawdzenie w dowolnym eksploratorze bloków (np. *https://blockchain.info/*), jakie transakcje są powiązane z danym adresem bitcoinowym — przykładowo można wyszukać adres własnego portfela i sprawdzić, wskutek jakiej transakcji otrzymano swojego pierwszego bitcoina.

Łańcuch bloków jest uważany za najważniejszy wynalazek techniczny związany z bitcoinem, ponieważ ustanawia niewymagający zaufania mechanizm potwierdzania wszystkich transakcji w sieci. Użytkownicy wierzą w rzetelność rejestru

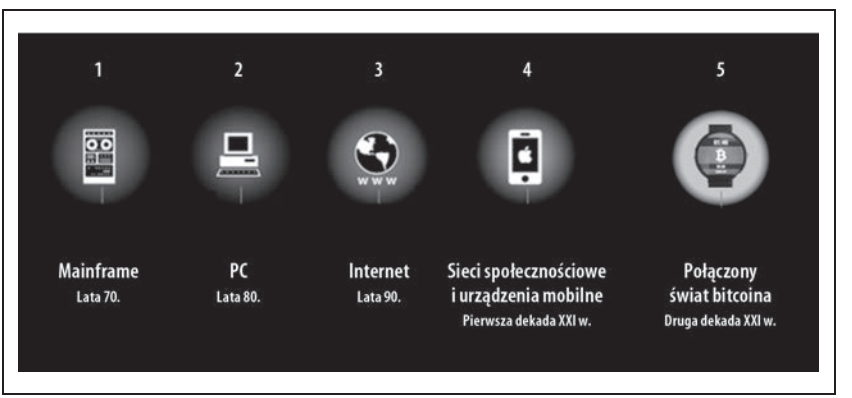
rozproszonego przechowywanego w wielu różnych węzłach zdecentralizowanej, ogólnoświatowej sieci, utrzymywanych przez „górników księgowych", zamiast nawiązywać i podtrzymywać oparte na zaufaniu relacje z drugą stroną transakcji (inną osobą) lub pośredniczącą stroną trzecią (taką jak bank). Łańcuch bloków jako wzorzec architektury nowego systemu zdecentralizowanych, niewymagających zaufania transakcji należy do tzw. kluczowych innowacji. Umożliwia decentralizację wszelkich transakcji zawieranych przez strony na całym świecie i wykluczenie z nich pośredników.

Łańcuch bloków przypomina kolejną warstwę aplikacji działających na istniejącej podbudowie protokołów internetowych — wzbogaca globalną sieć o nowy wymiar technologiczny umożliwiający zawieranie transakcji gospodarczych zarówno przy użyciu natychmiastowych płatności walutą cyfrową (w powszechnie używanej kryptowalucie), jak i bardziej długookresowych i skomplikowanych kontraktów finansowych. W systemie opartym na tej technologii przedmiotem transakcji może być każda waluta, kontrakt finansowy albo rzeczowy lub niematerialny składnik aktywów. Łańcuch bloków nie musi służyć wyłącznie do zawierania transakcji, gdyż może być używany w charakterze rejestru i inwentarza do zapisywania, śledzenia, monitorowania i uskuteczniania przepływów wszystkich składników majątku. Blockchain to w gruncie rzeczy wielki arkusz kalkulacyjny do rejestrowania aktywów oraz księgowania transakcji w skali globalnej, który może obejmować aktywa wszelkiego rodzaju należące do podmiotów z całego świata. Może pełnić funkcję rejestru, inwentarza i narzędzia wymiany we wszystkich dziedzinach finansów, ekonomii i rynku pieniężnego, aktywów rzeczowych (fizycznych) oraz wartości niematerialnych (głosów, pomysłów, reputacji, intencji, danych medycznych itd.)

Połączony świat a łańcuch bloków: piąty paradygmat przełomowych technologii obliczeniowych

Jeden z modeli pojmowania współczesnego świata oparty jest na pojawiających się mniej więcej co dekadę paradygmatach obliczeniowych (zob. rysunek P.1). Na początku były komputery typu mainframe, potem pojawiły się pecety, a następnie powstał internet, który zrewolucjonizował wszystko. Ostatnim etapem dotychczasowego postępu były urządzenia mobilne i sieci społecznościowe. Może się okazać, że owocem tej dekady będzie rodzący się właśnie paradygmat *połączonego świata obliczeniowego* opartego na kryptografii łańcucha bloków.

Świat, w którym wszystko jest połączone, może z łatwością zasymilować tę technologię jako ekonomiczną warstwę coraz rozleglejszej, ściśle zintegrowanej sieci urządzeń o różnym charakterze, wśród których znajdą się ubieralne urządzenia obliczeniowe, sensory działające w internecie rzeczy (ang. *internet of things*, IoT), smartfony, tablety, laptopy, urządzenia monitorujące aktywność użytkownika (takie jak Fitbit) oraz akcesoria będące wyposażeniem inteligentnych domów, samochodów i miast. Gospodarka, której zaistnienie jest możliwe dzięki łańcuchowi bloków, nie opierałaby się jednak wyłącznie na przepływie pieniędzy. Jej podstawą byłyby przepływy informacji oraz efektywna alokacja zasobów gospodarczych wśród ludzi i korporacji, możliwa dzięki swobodnym transferom pieniędzy.



Rysunek P.1. Przełomowe technologie obliczeniowe: komputery mainframe, pecety, internet, media społecznościowe i urządzenia mobilne, łańcuch bloków[8]

Przy tak rewolucyjnym potencjale, nie mniejszym od tego, który wykreowało pojawienie się internetu, technologia łańcucha bloków może zostać wdrożona i upowszechniona znacznie szybciej niż globalna sieć ze względu na efekty sieciowe ogólnoświatowej dostępności internetu i telefonii komórkowej.

Tak jak mobilne zastosowania społecznościowe wyznaczające czwarty paradygmat stały się wszechobecne i powszechnie pożądane, przybierając postać różnorodnych aplikacji mobilnych i społecznościowych elementów stron internetowych (polubień, komentarzy, narzędzi do zawierania znajomości i uczestniczenia

[8] Rozwinięcie rysunku zawartego w: Mark Sigal, *You Say You Want a Revolution? It's Called Post-PC Computing*, Radar (O'Reilly), 24 października 2011, *http://radar.oreilly.com/2011/10/post-pc-revolution.html* [dostęp: 31 sierpnia 2019].

w dyskusjach internetowych), tak łańcuch bloków jako piąty paradygmat może zrodzić nowe oczekiwania dotyczące wymiany wartości. Funkcjonalność piątego paradygmatu mogłaby się opierać na nieprzerwanej łączności, płynności połączeń i fizycznej realności warstwy obliczeniowej, składającej się z różnorodnych urządzeń z nadbudową w postaci łańcucha bloków odpowiedzialnego za płatności — nie tylko podstawowe transfery pieniężne, ale też mikropłatności, zdecentralizowaną wymianę, zarabianie i wydawanie tokenów, powoływanie się na aktywa cyfrowe i wymienianie ich, a także wystawianie i realizację sprytnych kontraktów — jako ekonomicznej warstwy, której sieć Web była dotychczas pozbawiona. Świat jest już gotowy na szersze rozpowszechnienie się pieniądza internetowego: usługa Apple Pay (mobilna aplikacja portfela elektronicznego oparta na tokenach cyfrowych emitowanych przez firmę Apple) oraz jej coraz liczniejsi konkurenci mogą być bardzo ważnym krokiem pośrednim na drodze do w pełni rozwiniętego świata kryptowalut, w którym łańcuch bloków przerodzi się w ekonomiczny pierwiastek internetu.

Sieć płatności bitcoinowych M2M w internecie rzeczy jako początek gospodarki maszynowej

Łańcuch bloków to rewolucyjny paradygmat dla świata ludzi („internetu osób"), ale też może być czynnikiem umożliwiającym upowszechnienie waluty gospodarki maszynowej. Gartner szacuje, że do 2020 roku internet rzeczy rozrośnie się do 26 mld urządzeń i będzie generował obroty w wysokości 1,9 bln dolarów[9]. Odpowiadająca mu kryptowaluta „internetu pieniądza" jest potrzebna do obsługi transakcji zawieranych między tymi urządzeniami[10], a wynikające z nich mikropłatności mogą wyewoluować w nowy wymiar gospodarki[11]. Cisco szacuje, że połączenia między maszynami (ang. *machine to machine*, M2M) rozwijają się szybciej niż inne kategorie połączeń (stanowią już 84%), a globalny ruch IP nie tylko wzrośnie trzykrotnie w latach 2012 – 2018, ale zwiększy się też udział

[9] Gartner, *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*, Gartner Press Release, 12 grudnia 2013, *http://www.gartner.com/newsroom/id/2636073*.

[10] Steve Omohundro, *Cryptocurrencies, Smart Contracts, and Artificial Intelligence*, „AI Matters" vol. 1, no. 2, grudzień 2014, *https://dl.acm.org/citation.cfm?id=2685334* [dostęp: 31 sierpnia 2019].

[11] Ross Dawson, *The New Layer of the Economy Enabled by M2M Payments in the Internet of Things*, „Trends in the Living Networks", 16 września 2014, *https://rossdawson.com/blog/new-layer-economy-enabled-m2m-payments-internet-things/* [dostęp: 31 sierpnia 2019].

w nim urządzeń mobilnych, sieci bezprzewodowych i komunikacji między maszynami[12]. Tak jak gospodarka pieniężna umożliwia lepszą, szybszą i bardziej efektywną alokację zasobów w świecie ludzi, tak gospodarka maszynowa może stworzyć prężny, zdecentralizowany system realizujący to samo zadanie w świecie urządzeń.

Przykładem dokonywania mikropłatności między urządzeniami może być sytuacja, w której podłączone do internetu samochody kierowców, którym się spieszy, automatycznie negocjują wyższe prędkości jazdy z pojazdami kierowców mających więcej czasu, wypłacając im mikrorekompensaty za ustąpienie drogi. Innym przykładem może być koordynacja doręczania przesyłek dronami z uwzględnieniem indywidualnych priorytetów odbiorców, także oparta na mikropłatnościach między urządzeniami. Z kolei czujniki stosowane w rolnictwie mogłyby być połączone w system stosujący zasady ekonomiczne do odsiewania nieistotnych danych i nadawania priorytetu informacjom o przekroczeniu konkretnych wartości odczytów (np. dotyczących wilgotności) zebranych przez wystarczająco dużą liczbę sensorów w rozproszonym roju.

Zdecentralizowany model niewymagającej zaufania sieci transakcji typu *peer-to-peer*, opartej na technologii łańcucha bloków, oznacza w gruncie rzeczy możliwość zawierania transakcji bez pośredników. Potencjalne przejście do zdecentralizowanych transakcji bezpośrednich w skali globalnej, obejmującej wszelkie możliwe interakcje i operacje gospodarcze (między ludźmi, między ludźmi a maszynami oraz między maszynami), mogłoby doprowadzić do powstania zupełnie nowej struktury społeczeństwa oraz całkiem nowego modelu jego funkcjonowania. Nie da się przewidzieć, jak miałyby one wyglądać, ale łatwo można sobie wyobrazić, że w wyniku ich powstania obecne, ustalone hierarchie i relacje władzy przestałyby być użyteczne.

Wejście do głównego nurtu: zaufanie, użyteczność, łatwość zastosowania

Ponieważ za bitcoinem i technologią łańcucha bloków kryje się wiele bardzo nowatorskich i złożonych pomysłów oraz koncepcji, często pojawia się zarzut,

[12] K. Petschow, *Cisco Visual Networking Index Predicts Annual Internet Traffic to Grow More Than 20 Percent (Reaching 1.6 Zettabytes) by 2018*, informacja prasowa firmy Cisco, 2014, *http://newsroom.cisco.com/release/1426270* [dostęp: 31 sierpnia 2019].

że kryptowaluty są zbyt skomplikowane, by mogły się upowszechnić w głównym nurcie gospodarki. Podobnie było w przypadku internetu, a przecież na początku każdej nowej epoki w technice ludzie zadają pytania o to, czym jest nowe narzędzie i jak działa. To nie jest poważna przeszkoda, gdyż nie trzeba rozumieć, jak działa protokół TCP/IP, żeby wysłać e-mail, a każda nowa technologia trafia w końcu do powszechnego użytku i większość korzystających z niej ludzi nie wnika w szczegóły techniczne, o ile ma do dyspozycji odpowiednie, użyteczne, godne zaufania aplikacje. Przykładowo nie każdy musi widzieć 32-znakowe, alfanumeryczne adresy publiczne portfeli kryptowalutowych (a na pewno nie musi ich ręcznie przepisywać). Działające już firmy oferujące portfele cyfrowe, takie jak Circle Internet Financial i Xapo, tworzą aplikacje przeznaczone dla użytkowników końcowych, mające ułatwić korzystanie z bitcoina w życiu codziennym (celem biznesowym tych podmiotów jest zostanie odpowiednikiem Gmaila w świecie kryptowalut pod względem użyteczności i udziału w rynku). Skoro bitcoin i e-portfele są związane z pieniędzmi, aplikacje przeznaczone dla użytkowników są oczywiście bardziej narażone na niebezpieczeństwa, a świadczone za ich pośrednictwem usługi muszą się cieszyć większym zaufaniem klientów niż inne programy. Zanim uda się wychować wystarczająco liczną grupę osób obeznanych w tym temacie i używających portfeli klienckich, trzeba rozwiązać wiele problemów z bezpieczeństwem kryptowalut, w tym kwestię tworzenia kopii zapasowej portfela, ewentualnej utraty klucza prywatnego oraz postępowania w przypadku otrzymania w wyniku transakcji monety objętej proskrypcją (wcześniej skradzionej) i niemożności pozbycia się jej w legalny sposób. Branża związana z rozwojem technologii łańcucha bloków przez cały czas szuka jednak rozwiązań tych problemów, a waluty alternatywne mogą się okazać kolejnym kamieniem milowym na drodze rozwoju technologii finansowej (określanej mianem „fintech"), tak jak wcześniej bankomaty i bankowość internetowa, a ostatnio usługa Apple Pay.

Kryptowaluty mogą się dość łatwo upowszechnić, o ile pojawią się godne zaufania, użyteczne narzędzia dla użytkowników, ale skuteczne wprowadzanie aplikacji łańcucha bloków do głównego nurtu zastosowań poza dziedziną kryptowalut może się okazać bardziej subtelnym zadaniem. Przykładowo wirtualne usługi notarialne wydają się oczywistym rozwiązaniem umożliwiającym łatwą, tanią, bezpieczną, trwałą i zapewniającą szybkie wyszukiwanie informacji rejestrację własności intelektualnej, umów, testamentów i podobnych dokumentów. Bez wątpienia jednak ludzie z przyczyn społecznych będą woleli w niektórych sprawach nadal korzystać z usług prawników (być może ze względu na możliwość uzyskania porady sformułowanej z punktu widzenia drugiego człowieka, z uwzględnieniem

czynników psychologicznych albo ze względu na możliwość zweryfikowania sytuacji przez osobę zorientowaną w przepisach), przez co wdrażanie technologii wyłącznie w oparciu o argument efektywności może napotykać problemy. Jednak ogólnie rzecz biorąc, jeżeli bitcoin i technologia łańcucha bloków mają dojrzewać, będzie to następowało etapami, tak jak w przypadku internetu, którego propozycja wartości przemawiała kolejno do różnych grup użytkowników, stopniowo przenoszących się do globalnej sieci z nowymi technologiami. Początkowo internet usuwał przeszkody we współpracy badawczej między członkami bardzo konkretnych grup użytkowników, czyli naukowcami i wojskowymi. Potem do sieci weszli gracze oraz hobbyści korzystający z niej w celach rekreacyjnych, aż w końcu z internetu zaczęli korzystać dosłownie wszyscy. W przypadku bitcoina pierwszymi użytkownikami są subkultury ludzi interesujących się pieniędzmi i pewną ideologią leżącą u podstaw stworzenia pierwszej kryptowaluty, natomiast kolejne etapy upowszechniania się technologii łańcucha bloków będą skutkiem rozwiązywania przez nią praktycznych problemów dużych grup potencjalnych użytkowników. Do najważniejszych grup, których istotne problemy może rozwiązać technologia łańcucha bloków, można zaliczyć np. osoby dotknięte cenzurą internetu w opresyjnych systemach politycznych. W takiej sytuacji zdecentralizowany system nazw domen oparty na łańcuchu bloków mógłby być bardzo przydatny. Technologię tę można by również wykorzystać na rynku własności intelektualnej do rejestrowania łańcucha wynalazków w patentach oraz zrewolucjonizować za jego pomocą spory sądowe dotyczące własności intelektualnej, związane z nadzorem nad dobrami cyfrowymi, dostępem do nich i przypisywaniem ich konkretnym użytkownikom.

Kultura bitcoina: festiwal Bitfilm

Jednym ze wskaźników przenikania nowej technologii do głównego nurtu jest jej obecność w kulturze popularnej. Sygnałem przedostawania się kryptowalut do globalnej świadomości społecznej jest festiwal Bitfilm (*https://www.bitfilm.com/bitfilm-festival/*), prezentujący filmy o treści związanej z bitcoinem. Do programu dobierane są produkcje przedstawiające uniwersalne, a jednak kulturowo wyróżniające się interpretacje i oddziaływania bitcoina. Festiwal poświęcony kryptowalutom jest organizowany od 2014 roku w Hamburgu (gdzie mieści się siedziba firmy Bitfilm) oraz gościnnie w innych miastach na całym świecie. Zgodnie z wizją organizatorów widzowie filmów mogą głosować na wybrane pozycje za pomocą bitcoinów. Firma Bitfilm nie tylko organizuje festiwal, zajmuje się także produkcją filmów promocyjnych dla branży kryptowalut (zob. rysunek P.2).

Rysunek P.2. Filmy promocyjne wyprodukowane przez Bitfilm

Założenia, metodologia i struktura tej książki

Branża związana z technologią łańcucha bloków jest jeszcze w powijakach i obecnie (pod koniec 2014 roku) znajduje się w fazie niezwykle dynamicznego tworzenia innowacji. Pojęcia, terminologia, standardy, główni gracze, normy oraz podejście całego sektora do określonych przedsięwzięć zmieniają się w szybkim tempie. Może się okazać, że za rok spojrzymy wstecz i dojdziemy do wniosku, że bitcoin i technologia łańcucha bloków, które dzisiaj znamy, stały się niefunkcjonalne i zostały zastąpione nowymi rozwiązaniami albo w inny sposób odeszły do lamusa. Przykładem dziedziny, w której zachodzą bardzo istotne i szybkie zmiany, jest bezpieczeństwo konsumenckich portfeli elektronicznych — kwestia bardzo poważna, biorąc pod uwagę ataki hakerskie, które mogą stać się plagą branży kryptowalut. W powszechnym przekonaniu najlepszym obecnie standardem bezpieczeństwa portfeli jest *multisig* (zatwierdzanie transakcji za pomocą kilku podpisów), ale większość użytkowników (zaliczających się wciąż do grona prekursorów, a nie mainstreamowych użytkowników) nie zaktualizowała nawet swoich portfeli, by osiągnąć ten poziom bezpieczeństwa.

Celem tej książki ma być analiza ogólnych koncepcji, cech i funkcjonalności bitcoina oraz technologii łańcucha bloków i związanych z nimi przyszłych możliwości, a także implikacji. Nie zawiera ona ani nie uwiarygodnia żadnych rad czy przewidywań dotyczących zdolności branży do utrzymania się na rynku. Co więcej, tekst ten został pomyślany jako prezentacja i omówienie zaawansowanych koncepcji, ponieważ istnieje już wiele źródeł podstawowej wiedzy na temat technologii łańcucha bloków. Związana z nią branża dopiero się rodzi i jest bardzo niedojrzała, a jej dynamiczny rozwój niesie ze sobą różne rodzaje ryzyka. Ze względu na tę dynamikę i pomimo starań autorki tekst może zawierać

nieścisłości, gdyż zawarte w nim informacje mogą się szybko zdezaktualizować; celem książki jest jednak przedstawienie ogólnego obrazu i stanu branży związanej z technologią łańcucha bloków oraz jej możliwości. To najlepszy moment, by dowiedzieć się czegoś o tej technologii, jej możliwych zastosowaniach oraz związanych z nią zagrożeniach i ryzyku, a także — co być może ważniejsze — o związanych z nią koncepcjach i możliwościach ich rozwijania. Chodzi zatem o wyczerpujący przegląd natury, zakresu i rodzaju działalności odbywającej się w branży kryptowalut i roztoczenie wizji jej szerokiego upowszechnienia. Tekst z konieczności może być niekompletny, zawierać błędy techniczne (aczkolwiek został przejrzany i poprawiony przez specjalistów) oraz szybko stracić aktualność, ponieważ różne opisane w nim przedsięwzięcia mogą zakończyć się sukcesem lub porażką. Równie dobrze cała branża kryptowalut i technologia łańcucha bloków w kształcie, jaki znamy obecnie, może szybko odejść do lamusa albo zostać zastąpiona innymi modelami.

Podczas pisania książki korzystano z różnych źródeł informacji związanych z bitcoinem i jego rozwojem. Wśród najważniejszych należy wymienić fora programistów, podgrupy w serwisie Reddit, opracowania publikowane w serwisie GitHub, podcasty, serwisy informacyjne, YouTube, blogi i Twittera. Szczególnie przydatne były zasoby internetowe, w tym zamieszczane na serwisach YouTube i Slideshare relacje z konferencji branżowych dotyczących bitcoina, podcasty (Let's Talk Bitcoin, Consider This!, Epicenter Bitcoin), serwisy informacyjne poświęcone bitcoinowi (*CoinDesk*, *Bitcoin Magazine*, *Cryptocoins News*, *Coin Telegraph*) oraz fora internetowe (Bitcoin StackExchange, Quora). Ponadto cennym źródłem informacji była korespondencja e-mailowa z osobami z branży, bezpośrednie rozmowy z nimi oraz obecność autorki na konferencjach, warsztatach, sesjach tradingowych oraz spotkaniach programistów.

Struktura książki jest podporządkowana omówieniu trzech różnych warstw technologii bitcoina i łańcucha bloków, zgodnie z wyłaniającym się coraz wyraźniej podziałem na blockchainy 1.0, 2.0 i 3.0. Na początku omówione zostaną definicje i koncepcje związane z bitcoinem i technologią łańcucha bloków oraz płatnościami kryptowalutowymi jako głównymi zastosowaniami blockchaina 1.0. Następnie poruszony zostanie temat blockchaina 2.0 — wykraczających poza kryptowaluty rynkowych i finansowych zastosowań tej technologii, takich jak kontrakty. Kolejny rozdział będzie zawierał wizję blockchaina 3.0, czyli zastosowań łańcucha bloków wychodzących poza waluty, finanse i operacje rynkowe. Do tej szerokiej kategorii należy zaliczyć zastosowania w obszarze sprawiedliwości, takie jak sprawowanie nadzoru za pomocą łańcucha bloków,

przenoszenie organizacji (takich jak WikiLeaks, ICANN czy usługi DNS) do zdecentralizowanej chmury, poza zasięg opresyjnych reżimów, ochrona własności intelektualnej oraz weryfikacja i autoryzacja tożsamości cyfrowej. Opisana zostanie również inna klasa zastosowań technologii blockchain 3.0, poza dziedziną kryptowalut, finansów i działań rynkowych. Chodzi o naukę, genomikę, ochronę zdrowia, nauczanie, publikowanie prac naukowych, szeroko pojmowany rozwój oraz działalność pomocową i kulturalną. W tych wszystkich dziedzinach technologia łańcucha bloków może doprowadzić do zwiększenia skali działalności, jej efektywności, poprawy organizacji i koordynacji. Wreszcie pojawią się bardziej zaawansowane koncepcje, takie jak waluty komplementarne obciążone demurażem, omówione w szerszym kontekście powszechnego wdrożenia technologii łańcucha bloków.

Podziękowania

Chciałabym podziękować Andreasowi M. Antonopoulosowi, Trentowi McConaghy'emu, Steve'owi Omohundro, Piotrowi Piaseckiemu, Justinowi Sherowi, Chrisowi Tse oraz Stephanowi Tualowi.


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

O'REILLY®

Łańcuch bloków: już dziś warto wiedzieć, jak jutro wpłynie na gospodarkę!

Bitcoin i inne kryptowaluty na dobre zagościły w powszechnej świadomości. Technologią, która dała im twarde podstawy, jest łańcuch bloków. Prawdopodobnie zostanie piątym nowatorskim paradygmatem obliczeniowym po komputerach typu mainframe, pecetach, internecie i mobilnych sieciach społecznościowych. Okazuje się to jasne, jeśli uświadomimy sobie, czym w istocie jest łańcuch bloków: publicznym rejestrem, który może się stać ogólnoświatową, zdecentralizowaną księgą służącą do rejestrowania, inwentaryzowania i organizowania transferów wszelkiego rodzaju aktywów.

Ta książka zawiera interesujące rozważania na temat teoretycznych, filozoficznych oraz społecznych implikacji kryptowalut i łańcucha bloków. Analizuje ogólne koncepcje, cechy i funkcjonalności bitcoina oraz technologii łańcucha bloków, a także związane z nimi możliwości dla światowej gospodarki. W wyczerpujący sposób omówiono tu naturę, rodzaje i zakresy działalności związanej z łańcuchem bloków. Poza dziedziną kryptowalut, finansów i działań rynkowych sporo miejsca poświęcono takim zagadnieniom jak genomika, ochrona zdrowia, nauczanie, działalność pomocowa i kulturalna.

W tej książce między innymi:

- najważniejsze koncepcje dotyczące bitcoina i łańcucha bloków
- modele organizacyjne odporne na cenzurę
- tworzenie zdecentralizowanego repozytorium cyfrowego do weryfikowania tożsamości
- zastosowanie łańcucha bloków do poprawy wykorzystania sieci do eksploracji danych
- osobiste kartoteki medyczne a łańcuch bloków

Melanie Swan – wykładowca akademicki, filozof, autorka książek i założycielka start-upów. W swojej działalności koncentruje się na kanałach płatności, zagadnieniach ryzyka w biznesie i wpływie łańcucha bloków na gospodarkę. Wykłada na Singularity University oraz w Institute for Ethics and Emerging Technologies. Opracowała zasady wyceny i księgowania wirtualnych aktywów cyfrowych dla firmy Deloitte.

ISBN 978-83-283-5921-5

Cena: 39,90 zł