Imran Bashir

Blockchain

Zaawansowane zastosowania łańcucha bloków

Wydanie 2

Helion

Packt›

Tytuł oryginału: Mastering Blockchain - Second Edition

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-283-4957-5

First published in the English language under the title 'Mastering Blockchain - Second Edition – (9781788839044)'

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)

Dodatkowe materiały do książki można znaleźć pod adresem: *ftp://ftp.helion.pl/przyklady/bloczz.zip*

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

Printed in Poland.

Spis treści

ROZDZIAŁ 2

Decentralizacja

Decentralizacja nie jest nową koncepcją. Od dawna wykorzystywano ją w strategii, zarządzaniu i rządzeniu. Podstawową ideą decentralizacji jest przeniesienie kontroli i władzy na obrzeża organizacji zamiast pozostawiania pełnej kontroli organizacji w rękach jednego centralnego ciała. Takie rozwiązanie zapewnia organizacjom różne korzyści, takie jak wzrost wydajności, przyspieszenie podejmowania decyzji, wzrost motywacji i zmniejszenie obciążenia wyższej kadry menedżerskiej.

W tym rozdziale decentralizacja jest opisana w kontekście łańcuchów bloków. Jednym z podstawowych aspektów łańcucha bloków jest brak centralnej jednostki, która go kontroluje. W tym rozdziale przedstawione zostaną przykłady różnych metod decentralizacji i dróg do jej osiągnięcia. Ponadto szczegółowo opisane zostaną decentralizacja ekosystemu łańcucha bloków, zdecentralizowane aplikacje i platformy do zapewniania decentralizacji. Poznasz też wiele ekscytujących aplikacji i idei, których źródłem są zdecentralizowane łańcuchy bloków.

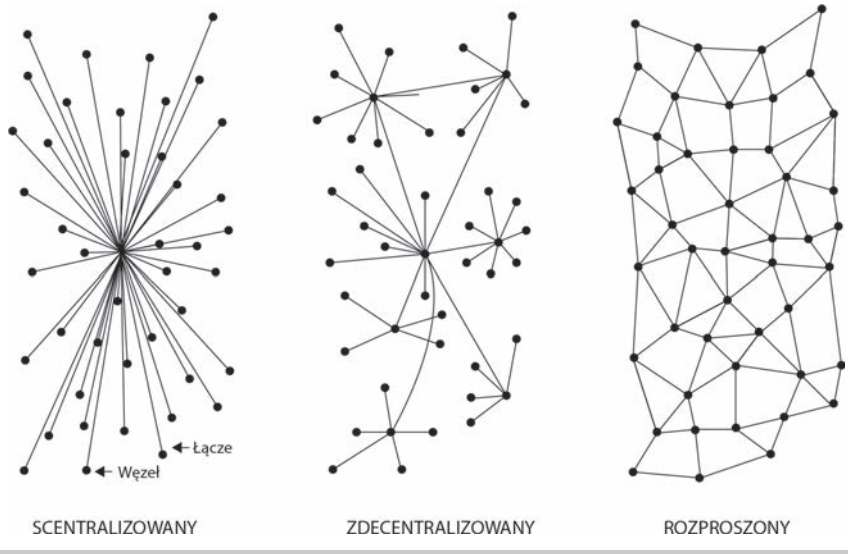
Decentralizacja z użyciem łańcucha bloków

Decentralizacja jest jedną z najważniejszych korzyści i usług zapewnianych przez technologię łańcuchów bloków. Z budowy łańcuchów bloków wynika, że są one doskonałym narzędziem do budowania platformy, która nie wymaga żadnych pośredników i może działać z wieloma różnymi liderami wybieranymi za pomocą mechanizmu osiągania konsensusu. Ten model umożliwia każdemu współzawodnictwo o pozycję jednostki podejmującej decyzje. To współzawodnictwo odbywa się na podstawie mechanizmu osiągania konsensusu, a najczęściej używaną metodą jest tu **dowód pracy**.

Decentralizacja może być stosowana na różnym poziomie: od modeli częściowo zdecentralizowanych po w pełni zdecentralizowane. Zależy to od wymogów i okoliczności. W kontekście łańcuchów bloków decentralizację można postrzegać jako mechanizm umożliwiający modyfikację istniejących aplikacji i paradygmatów oraz budowanie nowych aplikacji w celu zapewnienia pełnej kontroli użytkownikom.

Technologie teleinformatyczne tradycyjnie są oparte na scentralizowanym paradygmacie, w którym serwery bazodanowe lub serwery aplikacji są kontrolowane przez centralną jednostkę, np. administratora systemu. Wraz z pojawieniem się Bitcoina i technologii łańcuchów bloków ten model się zmienił. Obecnie istnieje technologia, która umożliwia każdemu zbudowanie zdecentralizowanego systemu, działającego bez pojedynczego punktu podatności na awarię lub jednej zaufanej jednostki zarządzającej. Taki system może działać autonomicznie lub wymagać interwencji człowieka; zależy to od typu i modelu zarządzania stosowanego w zdecentralizowanej aplikacji działającej w łańcuchu bloków.

Rysunek 2.1 ilustruje różne rodzaje istniejących obecnie systemów: scentralizowane, zdecentralizowane i rozproszone. Ten podział po raz pierwszy przedstawił Paul Baran w książce *On Distributed Communications: I. Introduction to Distributed Communications Networks* (Rand Corporation, 1964).



Rysunek 2.1. Różne typy sieci i systemów

Systemy scentralizowane to tradycyjne systemy informatyczne (klient – serwer), w których występuje pojedyncza jednostka zarządzająca — kontroluje ona dany system i samodzielnie odpowiada za wszystkie jego operacje. Wszyscy użytkownicy scentralizowanego systemu zależą od jednego źródła usług. Większość dostawców usług internetowych, w tym Google, Amazon, eBay, App Store firmy Apple itd., posługują się tym tradycyjnym modelem dostarczania usług.

W **systemie rozproszonym** dane i obliczenia są rozdzielane między wiele węzłów sieci. Czasem to pojęcie jest mylone z *przetwarzaniem równoległym*. Choć oba te rozwiązania w pewnym zakresie się pokrywają, główna różnica między nimi polega na tym, że w systemach przetwarzania równoległego obliczenia są wykonywane przez wszystkie węzły jednocześnie w celu uzyskania wyniku. Platformy przetwarzania równoległego są używane np. do badania i prognozowania pogody, do symulacji i w modelowaniu finansowym. Z kolei w systemie rozproszonym obliczenia nie muszą być wykonywane równolegle, a dane są replikowane w wielu węzłach

postrzeganych przez użytkowników jako jeden spójny system. Odmiany obu tych modeli są używane do osiągania odporności na błędy i zwiększania szybkości. W systemach równoległych nadal występuje centralna jednostka zarządzająca, która kontroluje wszystkie węzły i zarządza przetwarzaniem. To oznacza, że system jest z natury scentralizowany.

Najważniejsza różnica między systemem zdecentralizowanym a rozproszonym polega na tym, że w systemie rozproszonym występuje centralna jednostka nadrzędna zarządzająca całym systemem. W systemie zdecentralizowanym taka jednostka nie istnieje.

System zdecentralizowany to typ sieci, w której węzły nie są zależne od jednego węzła nadrzędnego. Zamiast tego kontrola jest rozproszona między wiele węzłów. Jest to zbliżone do modelu, w którym każdy dział organizacji odpowiada za własny serwer bazodanowy. W ten sposób kontrola jest odbierana centralnemu serwerowi i przekazywana do działów zarządzających własnymi bazami.

Ważną innowacją w paradygmacie zdecentralizowanym, będącą zalążkiem nowej ery decentralizacji aplikacji, jest osiąganie **konsensusu w środowisku zdecentralizowanym**. Ten mechanizm pojawił się wraz z Bitcoinem i umożliwia użytkownikom uzgadnianie rzeczy za pomocą algorytmu osiągania konsensusu, bez konieczności udziału centralnej, zaufanej trzeciej strony, pośrednika lub dostawcy usług.

Metody decentralizacji

Do zapewniania decentralizacji można stosować dwie metody: eliminowanie pośrednictwa i współzawodnictwo (decentralizacja oparta na współzawodnictwie). Zostaną one szczegółowo opisane w następnych punktach.

Eliminowanie pośrednictwa

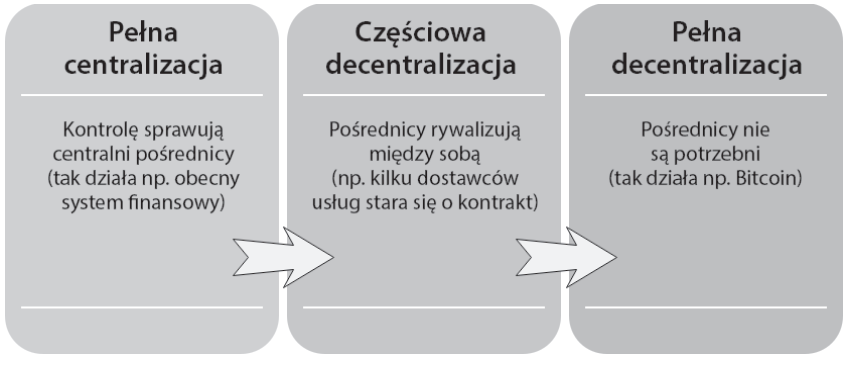
Koncepcję **eliminowania pośrednictwa** można wytłumaczyć na przykładzie. Wyobraź sobie, że chcesz przesłać pieniądze do znajomego z innego państwa. Idziesz do banku, który za opłatą prześle pieniądze do banku w docelowym kraju. W tym scenariuszu bank przechowuje centralną bazę danych, która jest aktualizowana, co potwierdza, że przesłałeś pieniądze. Łańcuch bloków umożliwia przesłanie pieniędzy bezpośrednio do znajomego bez konieczności korzystania z usług banku. Wystarczy do tego adres znajomego w łańcuchu bloków. W ten sposób pośrednik, czyli bank, przestaje być potrzebny, a decentralizacja jest uzyskiwana dzięki *wyeliminowaniu pośrednictwa*. Kwestią dyskusyjną jest to, na ile praktyczna jest decentralizacja przez eliminowanie pośrednictwa w sektorze finansowym z jego ogromnymi wymogami regulacyjnymi. Jednak ten model może być stosowany nie tylko w finansach, ale też w wielu innych branżach.

Decentralizacja oparta na współzawodnictwie

W metodzie obejmującej **współzawodnictwo** różni dostawcy usług konkurują ze sobą o to, by system wybrał ich do świadczenia usług. Ten model nie prowadzi do pełnej decentralizacji. Jednak do pewnego stopnia gwarantuje, że pośrednik lub dostawca usług nie zmonopolizuje usługi. W kontekście łańcuchów bloków można wyobrazić sobie system, w którym inteligentne kontrakty mogą wybrać zewnętrznego dostawcę danych spośród dużej ich liczby na podstawie reputacji, wcześniejszych ocen, recenzji i jakości świadczonych usług.

Ta metoda nie zapewnia całkowitej decentralizacji, ale umożliwia inteligentnym kontraktom dokonywanie swobodnych wyborów na podstawie podanych kryteriów. W ten sposób budowane jest oparte na konkurencji środowisko, w którym dostawcy usług rywalizują między sobą o to, by zostać wybranym na dostawcę danych.

Na rysunku 2.2 pokazane są różne poziomy decentralizacji. Po lewej stronie przedstawione jest tradycyjne podejście, w którym kontrolę sprawuje centralny system. W modelu widocznym po prawej stronie całkowicie wyeliminowano pośrednictwo. Pośrodku widoczni są rywalizujący ze sobą pośrednicy lub dostawcy usług. W tym rozwiązaniu pośrednicy lub dostawcy usług są wybierani na podstawie reputacji lub głosowania, co pozwala uzyskać częściową decentralizację.



Rysunek 2.2. Poziom decentralizacji

Choć decentralizacja zapewnia wiele korzyści, w tym przejrzystość, wydajność, oszczędności, rozwój zaufanych ekosystemów, a w niektórych sytuacjach także prywatność i anonimowość, to jednocześnie wymaga starannego przeanalizowania pewnych problemów, takich jak wymogi z zakresu bezpieczeństwa, błędy programowe i błędy ludzkie.

Oto przykład: jak w zdecentralizowanym systemie, takim jak Bitcoin lub Ethereum, gdzie bezpieczeństwo jest standardowo zapewniane dzięki kluczom prywatnym, zagwarantować, że cyfrowe zasoby powiązane z takimi kluczami nie staną się bezwartościowe po utracie klucza lub że błąd w kodzie inteligentnego kontraktu lub zdecentralizowanej aplikacji nie narazi użytkownika na atak? Przed rozpoczęciem decentralizowania wszystkiego za pomocą łańcucha bloków i zdecentralizowanych aplikacji trzeba zrozumieć, że nie wszystko można i trzeba decentralizować.

To podejście rodzi kilka podstawowych pytań: czy łańcuch bloków naprawdę jest potrzebny? Kiedy przydatny jest łańcuch bloków? W jakich sytuacjach jest on lepszy od tradycyjnych baz danych? Aby odpowiedzieć na te pytania, zastanów się nad prostym zestawem zaprezentowanych tu kwestii:

1. Czy potrzebna jest wysoka przepustowość obsługi danych? Jeśli odpowiedź na to pytanie brzmi „tak”, zastosuj tradycyjną bazę danych.
2. Czy aktualizacje są kontrolowane przez centralną jednostkę? Jeżeli tak jest, posłuż się tradycyjną bazą.
3. Czy użytkownicy sobie ufają? Jeśli tak, użyj tradycyjnej bazy.
4. Czy użytkownicy są anonimowi? Jeżeli tak, zastosuj publiczny łańcuch bloków. W przeciwnym razie wykorzystaj prywatny łańcuch bloków.
5. Jeśli konsensus ma być utrzymywany w ramach konsorcjum, utwórz prywatny łańcuch bloków. W przeciwnym razie zastosuj publiczny łańcuch bloków.

Udzielenie odpowiedzi na wszystkie te pytania może pozwolić zrozumieć, czy łańcuch bloków jest potrzebny. Oprócz postawionych tu pytań trzeba uwzględnić także wiele innych kwestii, takich jak opóźnienie, mechanizmy osiągania konsensusu, to, czy konsensus jest konieczny i gdzie będzie ustalany. Jeśli konsensus jest utrzymywany wewnętrznie przez konsorcjum, należy zastosować prywatny łańcuch bloków. W przeciwnym razie, gdy konsensus ma być osiągany publicznie przez wiele jednostek, należy rozważyć publiczny łańcuch bloków. W trakcie wyboru między łańcuchem bloków a tradycyjną bazą danych należy rozważyć także inne aspekty, np. niemodyfikowalność. Jeśli jest ona niezbędna, należy zastosować publiczny łańcuch bloków; w przeciwnym razie odpowiednim rozwiązaniem może być centralna baza danych.

Wraz z dojrzewaniem technologii łańcuchów bloków mogą pojawić się kolejne pytania dotyczące tego modelu. Na razie jednak podany zestaw pytań wystarcza do zdecydowania, czy rozwiązanie oparte na łańcuchu bloków jest potrzebne, czy nie.

Drogi do decentralizacji

Już przed łańcuchami bloków i Bitcoinem istniały inne systemy (np. systemy wymiany plików BitTorrent i Gnutella), które można uznać za — w pewnym stopniu — zdecentralizowane. Jednak wraz z pojawieniem się łańcuchów bloków zaczęto realizować wiele projektów wykorzystujących tę nową technologię do osiągania decentralizacji. Bitcoin jest dla wielu osób pierwszym wyborem, ponieważ okazał się najbardziej odpornym i bezpiecznym łańcuchem bloków, a w czasie, gdy powstaje ta książka, jego wartość rynkowa wynosi blisko 145 mld dolarów. Wielu programistów do budowania zdecentralizowanych aplikacji korzysta też z innych łańcuchów bloków, takich jak Ethereum. W porównaniu z Bitcoinem Ethereum stał się lepszym wyborem z powodu swobody i możliwości zaprogramowania dowolnej logiki biznesowej w łańcuchu bloków za pomocą *inteligentnych kontraktów*.

Jak przeprowadzić decentralizację?

Arvind Narayanan i in. zaproponowali w książce *Bitcoin and Cryptocurrency Technologies* (Princeton University Press) model, który można wykorzystać do oceny wymogów dotyczących decentralizacji z użyciem łańcucha bloków. W tym modelu zadawane są cztery pytania. Odpowiedzi na nie pozwalają dokładnie zrozumieć, jak zdecentralizować system:

1. Co jest decentralizowane?
2. Jaki poziom decentralizacji jest wymagany?
3. Jaki łańcuch bloków jest używany?
4. Jakie mechanizmy zabezpieczeń są stosowane?

Pierwsze pytanie wymaga określenia, jaki system jest decentralizowany. Może to być dowolny system — np. system sprawdzania tożsamości lub system tradingowy.

Drugie pytanie wymaga określenia wymaganego poziomu decentralizacji na podstawie analizy opisanej wcześniej skali. Można zastosować pełną lub częściową eliminację pośrednictwa.

Trzecie pytanie wymaga od programistów ustalenia, który łańcuch bloków jest odpowiedni w konkretnym zastosowaniu. Może to być łańcuch bloków Bitcoin lub Ethereum albo dowolny inny dostosowany do danej sytuacji.

Ostatnie pytanie, na jakie trzeba odpowiedzieć, dotyczy tego, w jaki sposób gwarantowane będzie bezpieczeństwo zdecentralizowanego systemu. Mechanizm zabezpieczeń może być oparty na atomowości (transakcja jest wtedy wykonywana albo w całości, albo nie jest wykonywana wcale). To deterministyczne podejście zapewnia integralność systemu. Można też zastosować mechanizmy oparte na reputacji, umożliwiające wprowadzenie różnych poziomów zaufania w systemie.

Przykładowy schemat analizy decentralizacji

Jako przykładową aplikację przeznaczoną do decentralizacji zbadajmy system transferu pieniędzy. Cztery podane wcześniej pytania posłużą do oceny wymogów dotyczących decentralizacji tej aplikacji. Oto odpowiedzi na te pytania:

1. System transferu pieniędzy.
2. Eliminowanie pośrednictwa.
3. Bitcoin.
4. Atomowość.

Odpowiedzi wskazują na to, że system transferu pieniędzy można zdecentralizować, eliminując pośrednika, implementując system z użyciem łańcucha bloków Bitcoin i oferując gwarancje bezpieczeństwa za pomocą atomowości. Atomowość gwarantuje, że transakcja albo zostanie wykonana w pełni poprawnie, albo w ogóle nie zostanie przeprowadzona. Wybrany został łańcuch bloków Bitcoin, ponieważ jest najstarszy i sprawdzony.

Opisany schemat można też wykorzystać dla dowolnego innego systemu, który trzeba przeanalizować w kategoriach decentralizacji. Odpowiedzi na postawione cztery proste pytania pomagają doprecyzować, jakie podejście przyjąć w celu decentralizacji systemu.

Łańcuch bloków i kompletny ekosystem związany z decentralizacją

Aby uzyskać pełną decentralizację, konieczna jest także decentralizacja środowiska związanego z łańcuchem bloków. Łańcuch bloków to rozproszony rejestr działający na bazie tradycyjnych systemów odpowiedzialnych np. za składowanie danych, komunikację i obliczenia. Występują też inne aspekty, takie jak tożsamość i bogactwo, do których tradycyjnie stosowane są modele scentralizowane. Decentralizacja musi objąć także te aspekty, aby można było uzyskać odpowiednio zdecentralizowany ekosystem.

Składowanie danych

Dane mogą być przechowywane bezpośrednio w łańcuchu bloków, co pozwala zapewnić decentralizację. Jednak poważną wadą tego podejścia jest to, że łańcuch bloków z natury nie nadaje się dobrze do składowania dużych ilości danych. Może przechowywać proste transakcje i pewną ilość dowolnych danych, jednak z pewnością nie nadaje się do składowania zdjęć lub dużych obiektów z danymi, do czego używane są tradycyjne systemy bazodanowe.

Lepszym sposobem składowania danych jest używanie **rozproszonych tablic mieszających** (ang. *Distributed Hash Table* — DHT). Tablice DHT stosowano pierwotnie w działających w modelu P2P systemach wymiany plików (np. w systemach BitTorrent, Napster, Kazaa i Gnutella). Badania nad tablicami DHT zyskały popularność dzięki projektom CAN, Chord, Pastry i Tapestry. Najbardziej skalowalną i najszybszą siecią był BitTorrent, jednak problem z tym systemem i podobnymi rozwiązaniami polega na tym, że użytkownicy nie mają interesu w przechowywaniu plików w nieskończoność. Użytkownicy zwykle nie utrzymują plików na stałe, a jeśli węzły z wciąż potrzebnymi komuś danymi opuszczą sieć, nie ma sposobu na pobranie tych danych; potrzebne węzły muszą ponownie dołączyć do sieci, aby pliki ponownie stały się dostępne.

Dwoma podstawowymi wymogami w obszarze składowania danych są wysoka dostępność systemu i stabilność łącza. Oznacza to, że dane powinny być dostępne, gdy są potrzebne, a łącza sieciowe zawsze powinny działać. System **IPFS** (ang. *InterPlanetary File System*) autorstwa Juana Beneta posiada obie te cechy. Benet marzy o tym, by dzięki zastąpieniu protokołu HTTP innym rozwiązaniem powstała zdecentralizowana sieć WWW. System IPFS składuje dane w tablicach DHT Kademlia, a wyszukiwanie obsługuje za pomocą **acyklicznych grafów skierowanych skrótów** (ang. *Merkle directed acyclic graph*). Tablice DHT i acykliczne grafy skierowane zostaną szczegółowo opisane w rozdziale 4. „Kryptografia klucza publicznego”.

Mechanizm nagradzania za składowanie danych jest oparty na protokole Filecoin. Nagrody są wypłacane właścicielom węzłów, które przechowują dane za pomocą mechanizm Bitswap. Ten mechanizm umożliwia węzłom przechowywanie prostego rejestru bajtów wysyłanych lub otrzymywanych w modelu „jeden do jednego". W systemie IPFS używany jest też oparty na narzędziu Git mechanizm wersjonowania, który zapewnia strukturę wersji danych i kontrolę nad nimi.

Istnieją też inne narzędzia do składowania danych, np. Ethereum Swarm, Storj i MaidSafe. Ethereum obejmuje własny zdecentralizowany i rozproszony ekosystem, w którym używane są narzędzie Swarm (do składowania danych) i protokół Whisper (do komunikacji). MaidSafe ma zapewnić zdecentralizowaną sieć WWW. Wszystkie te projekty są szczegółowo opisane w dalszych częściach książki.

BigchainDB to następny projekt przeznaczony do decentralizacji warstwy składowania danych, który ma zapewniać skalowalną liniowo, szybką, zdecentralizowaną bazę danych różną od tradycyjnych systemów plików. BigchainDB uzupełnia zdecentralizowane platformy przetwarzania danych i systemy plików, takie jak Ethereum i IPFS.

Komunikacja

Internet (warstwa komunikacji w łańcuchach bloków) jest uznawany za zdecentralizowany. To przekonanie jest w pewnym zakresie prawdziwe, ponieważ pierwotnie internet opracowano jako zdecentralizowany system komunikacji. Usługi takie jak e-mail i składowanie danych w internecie są obecnie oparte na modelu, w którym kontrolę sprawuje dostawca usług, a użytkownicy ufają, że taki dostawca będzie zapewniał na żądanie dostęp do danej usługi. Ten model jest oparty na bezwarunkowym zaufaniu do centralnej jednostki (dostawcy usług), ponieważ użytkownicy nie mają kontroli nad własnymi danymi. Nawet hasła użytkowników są przechowywane w systemach zaufanej trzeciej strony.

Dlatego trzeba zapewnić kontrolę poszczególnym użytkownikom w taki sposób, aby zagwarantować im dostęp do ich danych bez zależności od pojedynczej trzeciej strony. Dostęp do internetu (warstwy komunikacyjnej) jest zależny od **dostawców usług internetowych**, którzy pełnią funkcję centralnego koncentratora dla użytkowników internetu. Jeśli dostawca usług internetowych z jakiegoś powodu przestanie działać, to w opisanym modelu komunikacja będzie niemożliwa.

Inne rozwiązanie to zastosowanie **sieci w topologii siatki**. Choć w porównaniu z internetem taka sieć ma ograniczone możliwości, stanowi zdecentralizowaną alternatywę, umożliwiającą węzłom bezpośrednie komunikowanie się ze sobą bez centralnego koncentratora takiego jak dostawca usług internetowych.

> Przykładową siecią w topologii siatki jest FireChat (*http://www.opengarden.com/firechat.html*). Umożliwia ona użytkownikom iPhone'ów bezpośrednie komunikowanie się ze sobą w modelu P2P bez połączenia internetowego.

Wyobraź sobie teraz sieć, która umożliwia użytkownikom kontrolowanie komunikacji — w żadnej sytuacji nikt nie może jej wyłączyć. Mógłby to być następny krok w kierunku decentralizacji sieci komunikacyjnych w ekosystemie łańcucha bloków. Trzeba zauważyć, że ten model może być niezbędny tylko na obszarach, gdzie internet jest cenzurowany i kontrolowany przez rząd.

Wcześniej wspomniano, że pierwotnie internet miał być zdecentralizowaną siecią. Jednak wraz z upływem lat i powstaniem dużych dostawców usług, takich jak Google, Amazon i eBay, kontrola jest w coraz większym stopniu przekazywana w ręce tych ważnych graczy. Na przykład poczta elektroniczna jest w swej istocie zdecentralizowanym systemem. Oznacza to, że każdy może niewielkim nakładem pracy uruchomić serwer poczty elektronicznej i zacząć wysyłać oraz odbierać e-maile. Dostępne są jednak lepsze rozwiązania, np. Gmail i Outlook.com, które oferują dodatkowe usługi dla użytkowników końcowych. Dlatego naturalnym wyborem jest korzystanie z jednej z takich scentralizowanych usług, ponieważ są one wygodniejsze i bezpłatne. Jest to jeden z przykładów ilustrujących, że internet stał się bardziej scentralizowany.

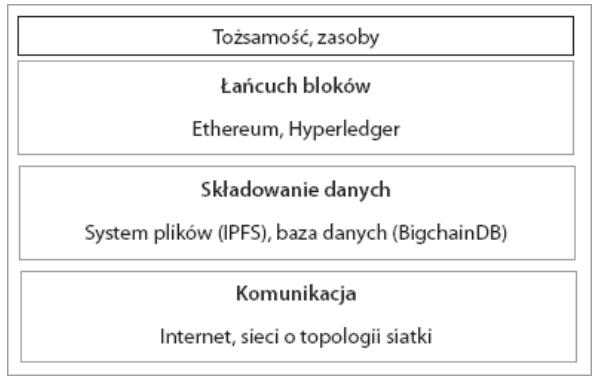
Bezpłatne usługi są jednak oferowane kosztem ujawniania cennych danych osobowych, a wielu użytkowników nie jest tego świadomych. Łańcuch bloków pozwolił znów przedstawić światu wizję decentralizacji, a obecnie aktywnie prowadzone są prace nad opanowaniem tej technologii i uzyskaniem korzyści, jakie może ona oferować.

Decentralizacja a moc obliczeniowa

Za pomocą łańcuchów bloków takich jak Ethereum, gdzie w sieci łańcucha bloków uruchamia się inteligentne kontrakty obejmujące logikę biznesową, można zdecentralizować moc obliczeniową. Inne łańcuchy bloków oferują podobne platformy z warstwą przetwarzania, pozwalające w zdecentralizowany sposób uruchamiać logikę biznesową w sieci.

Na rysunku 2.3 pokazany jest zdecentralizowany ekosystem. W dolnej warstwie internet lub sieci o topologii siatki zapewniają zdecentralizowaną sieć komunikacyjną. W następnej warstwie, składowania danych, decentralizację oferują technologie takie jak IPFS i BigchainDB. W kolejnej warstwie łańcuch bloków pełni funkcję zdecentralizowanej warstwy przetwarzania (warstwy obliczeniowej). Łańcuch bloków może, choć w ograniczonym stopniu, stanowić także warstwę składowania danych, jednak skutkuje to znacznym ograniczeniem szybkości i możliwości systemu. Dlatego do składowania dużych ilości danych w zdecentralizowany sposób lepiej nadają się inne rozwiązania, takie jak IPFS i BigchainDB. Na najwyższym poziomie znajdują się warstwy tożsamości i zasobów. Tożsamość w internecie to bardzo obszerne zagadnienie. Systemy takie jak BitAuth i OpenID zapewniają usługi uwierzytelniania i identyfikacji oraz oferują różny poziom decentralizacji i bezpieczeństwa.

Łańcuch bloków potrafi zapewnić rozwiązania różnych problemów związanych z decentralizacją. **Trójkąt Zooko** (jest to hipoteza związana z tożsamością) wymaga, by system nazw w protokole sieciowym był bezpieczny i zdecentralizowany oraz obejmował nazwy łatwe do zapamiętania i sensowne dla człowieka. Zgodnie ze wspomnianą hipotezą system może mieć tylko dwie z tych trzech cech. Jednak wraz z pojawieniem się łańcucha bloków Namecoin problem został rozwiązany. Ten łańcuch bloków zapewnia bezpieczeństwo, decentralizację i nazwy sensowne



Rysunek 2.3. Zdecentralizowany ekosystem

dla człowieka. To rozwiązanie nie jest jednak uniwersalne i pociąga za sobą wiele wyzwań; użytkownicy muszą na przykład bezpiecznie przechowywać klucze prywatne i zarządzać nimi. To rodzi ogólne pytania o to, czy decentralizacja jest odpowiednia w danej sytuacji.

Decentralizacja nie we wszystkich scenariuszach jest właściwa. Często lepiej sprawdzają się scentralizowane systemy o ustalonej reputacji. Na przykład platformy poczty elektronicznej od poważanych firm, takich jak Google lub Microsoft, zapewniają wyższy poziom usług niż model, w którym odrębne serwery poczty elektronicznej są zarządzane przez użytkowników w internecie.

Rozwijane są liczne projekty rozproszonych i opartych na łańcuchach bloków systemów o większych możliwościach. Na przykład Swarm i Whisper mają obsługiwać zdecentralizowane składowanie danych i komunikację w łańcuchu bloków Ethereum. Swarm i Ethereum zostaną opisane szczegółowo w rozdziale 11. „Jeszcze o Ethereum".

Wraz z powstaniem zdecentralizowanego modelu w mediach i pracach naukowych zaczęto stosować różne pojęcia i modne słowa. Dzięki pojawieniu się technologii łańcuchów bloków można obecnie tworzyć programowe wersje tradycyjnych fizycznych organizacji; służą do tego **zdecentralizowane organizacje** (ang. *decentralized organization* — DO) i podobne konstrukcje, szczegółowo opisane w dalszej części rozdziału.

W kontekście decentralizacji warto omówić następujące zagadnienia.

Inteligentne kontrakty

Inteligentny kontrakt to zdecentralizowany program. Inteligentne kontrakty nie wymagają do działania łańcucha bloków. Jednak z powodu zapewnianych przez łańcuchy bloków korzyści w zakresie bezpieczeństwa technologia ta stała się standardową zdecentralizowaną platformą wykonywania inteligentnych kontraktów.

Inteligentny kontrakt obejmuje zwykle logikę biznesową i ograniczoną ilość danych. Ta logika jest wykonywana, jeśli spełnione są określone kryteria. Inteligentne kontrakty są stosowane przez użytkowników łańcucha bloków lub działają autonomicznie na rzecz członków sieci.

Więcej informacji na temat inteligentnych kontraktów zawiera rozdział 9. „Inteligentne kontrakty".

Zdecentralizowane organizacje

Zdecentralizowane organizacje to programy działające w łańcuchu bloków i oparte na działaniu rzeczywistych organizacji, obejmujących ludzi i protokoły. Po dodaniu zdecentralizowanej organizacji do łańcucha bloków, do czego służy inteligentny kontrakt lub zestaw takich kontraktów, następuje decentralizacja i strony komunikują się między sobą na podstawie kodu zdefiniowanego w kodzie oprogramowania zdecentralizowanej organizacji.

Zdecentralizowane organizacje autonomiczne

Zdecentralizowana organizacja autonomiczna (ang. *decentralized autonomous organization* — DAO) jest podobnie jak organizacja zdecentralizowana programem komputerowym działającym na bazie łańcucha bloków. W takim programie umieszczone są reguły zarządzania i logiki biznesowej. Zdecentralizowane organizacje autonomiczne i organizacje zdecentralizowane są prawie identyczne. Główna różnica polega na tym, że DAO są autonomiczne. To oznacza, że są w pełni zautomatyzowane i obejmują logikę wykorzystującą sztuczną inteligencję. Z kolei DO nie posiadają tej cechy i wymagają danych wejściowych od człowieka, aby wykonywać logikę biznesową.

Pierwszym łańcuchem bloków, w którym wprowadzono DAO, był Ethereum. W DAO za jednostkę zarządzającą uważa się kod, a nie ludzi lub papierowe kontrakty. Jednak to człowiek zarządza kodem i ocenia proponowane funkcje na potrzeby społeczności. DAO mogą zatrudniać zewnętrznych pracowników kontraktowych, jeśli posiadacze tokenów (użytkownicy sieci) zapewnią wystarczającą ilość środków.

Najbardziej znanym projektem DAO jest The DAO, w którym w fazie finansowania społecznościowego zebrano 168 mln dolarów. Projekt The DAO opracowano na potrzeby tworzenia funduszu podwyższonego ryzyka mającego zapewniać obsługę zdecentralizowanego modelu biznesowego bez określonej jednostki będącej właścicielem. Niestety, projekt został złamany przez hakerów z powodu błędu w kodzie The DAO, a miliony dolarów w **walucie Ether** (**ETH**) zostały wyprowadzone z projektu do podrzędnej DAO. Niezbędny był hard fork łańcucha bloków Ethereum, aby odwrócić skutki ataku i rozpocząć odzyskiwanie środków. Ten incydent zapoczątkował debatę na temat bezpieczeństwa, jakości i potrzeby dokładnych testów kodu inteligentnych kontraktów w celu zapewnienia ich integralności i odpowiedniej kontroli. Prowadzone są też — zwłaszcza w środowisku uniwersyteckim — inne projekty, nakierowane na sformalizowanie pisania i testowania inteligentnych kontraktów.

Obecnie DAO nie mają statusu prawnego, choć mogą obejmować inteligentny kod wymuszający przestrzeganie określonych protokołów i warunków. Jednak na razie reguły te nie mają mocy w obowiązującym systemie prawnym. Możliwe, że pewnego dnia **autonomiczne agenty** (czyli działające bez interwencji człowieka fragmenty kodu zamawiane przez organy ścigania lub organy nadzoru) będą obejmować zasady i regulacje, które można będzie umieścić w DAO na potrzeby zapewniania integralności rozwiązań w kontekście prawa i zgodności z regulacjami. Ponieważ DAO są w pełni zdecentralizowane, można je uruchamiać w dowolnym miejscu. Rodzi to poważne pytania o to, jak zastosować obecny system prawny do różnych obszarów jurysdykcji i lokalizacji geograficznych.

Zdecentralizowane korporacje autonomiczne

Zdecentralizowane korporacje autonomiczne (ang. *decentralized autonomous corporations* — DAC) są podobne do DAO, choć można je uznać za podzbiór tych ostatnich. Definicje DAC i DAO mogą się pokrywać, przy czym różnica między nimi polega na tym, że DAO zwykle są uważane za rozwiązania non profit, natomiast DAC mogą być dochodowe, oferować udziały uczestnikom i wypłacać dywidendy. DAC mogą zarządzać biznesem automatycznie, bez interwencji człowieka, na podstawie zaprogramowanej logiki.

Zdecentralizowane społeczności autonomiczne

Zdecentralizowane społeczności autonomiczne (ang. *decentralized autonomous societies* — DAS) to rozwiązanie, które ma pozwolić całej społeczności funkcjonować z wykorzystaniem łańcucha bloków za pomocą wielu złożonych inteligentnych kontraktów oraz połączenia działających autonomicznie DAO i zdecentralizowanych aplikacji (ang. *decentralized applications* — DApps). Ten model niekoniecznie oznacza podejście „bezpłatne dla wszystkich". Nie jest też w pełni oparty na ideologii libertariańskiej. Jednak wiele usług świadczonych standardowo przez rządy może być zapewnianych za pomocą łańcuchów bloków. Dotyczy to np. rządowych systemów dowodów osobistych, paszportów, rejestrów aktów prawnych, małżeństw i narodzin. Inna teoria dotyczy tego, że jeśli rząd jest skorumpowany, a scentralizowane systemy nie zapewniają wystarczającego poziomu zaufania niezbędnego społeczeństwu, ludzie mogą uruchomić w łańcuchu bloków własny, wirtualny system, oparty na zdecentralizowanym konsensusie i przejrzystości. Taki scenariusz może wydawać się libertariańskim lub cyberpunkowym snem, jednak dzięki łańcuchowi bloków jest zupełnie realny.

Zdecentralizowane aplikacje (DApps)

Wszystkie wymienione do tej pory idee można przypisać do bardziej ogólnej kategorii zdecentralizowanych aplikacji. DAO, DAC i DO to zdecentralizowane aplikacje działające na bazie łańcuchów bloków w sieci P2P. Te modele reprezentują najnowsze osiągnięcia w technologiach decentralizacji. Zdecentralizowane aplikacje to programy, które mogą działać w odpowiednich łańcuchach bloków (aplikacje typu I), używać istniejących łańcuchów bloków (aplikacje typu II) lub tylko korzystać z protokołów takich łańcuchów (aplikacje typu III).

Wymogi stawiane zdecentralizowanym aplikacjom

Aby aplikacja została uznana za zdecentralizowaną, musi spełniać wymienione niżej kryteria. Ta definicja została przedstawiona w pracy Johnstona i in. *The General Theory of Decentralized Applications, Dapps*.

- Zdecentralizowana aplikacja powinna być w pełni otwartym i autonomicznym oprogramowaniem. Żadna jednostka nie powinna kontrolować większości tokenów. Wszystkie zmiany w aplikacji muszą wynikać z konsensusu osiąganego na podstawie informacji zwrotnych ze społeczności.
- Dane i rejestry operacji w aplikacji muszą być kryptograficznie zabezpieczone oraz składowane w publicznym, zdecentralizowanym łańcuchu bloków, aby uniknąć scentralizowanych punktów podatności na awarie.
- Aplikacja musi używać kryptograficznych tokenów, aby zapewnić dostęp i nagrody jednostkom, które robią coś wartościowego na rzecz aplikacji (np. górnikom w Bitcoinie).
- Tokeny muszą być generowane przez zdecentralizowane aplikacje zgodnie ze standardowym algorytmem kryptograficznym. Wygenerowane tokeny stanowią dowód wartości przekazywanej kontrybutorom (np. górnikom).

Operacje w zdecentralizowanych aplikacjach

Konsensus w zdecentralizowanej aplikacji można uzyskać za pomocą algorytmów osiągania konsensusu, takich jak dowód pracy lub dowód stawki. Do tej pory tylko dowód pracy okazał się zdumiewająco odporny na ataki z udziałem 51% zasobów, czego potwierdzeniem jest działanie Bitcoina. Zdecentralizowane aplikacje mogą rozdzielać tokeny (monety) na podstawie wydobywania, zbiórek i prac programistycznych.

Przykładowe zdecentralizowane aplikacje

W tym miejscu zaprezentowane są przykładowe zdecentralizowane aplikacje.

KYC-Chain

Ta aplikacja zapewnia mechanizmy do bezpiecznego i wygodnego zarządzania danymi typu **„poznaj swojego klienta”** (ang. *know your customer* — KYC) za pomocą inteligentnych kontraktów.

OpenBazaar

Jest to zdecentralizowana sieć P2P, która umożliwia przeprowadzanie operacji handlowych bezpośrednio między sprzedawcami i klientami, bez korzystania z centralnego operatora takiego jak eBay lub Amazon. Należy zauważyć, że ten system nie jest oparty na łańcuchu bloków. Zamiast tego w sieci P2P używane są tablice DHT, aby umożliwić bezpośrednią komunikację i wymianę danych między węzłami. W tym systemie do obsługi płatności używany jest bitcoin i inne kryptowaluty.

Lazooz

Jest to zdecentralizowany odpowiednik Ubera. Umożliwia wspólne przejazdy samochodem w modelu P2P, a użytkownicy otrzymują nagrody na podstawie dowodu przemieszczania się i mogą zarabiać monety w walucie zooz.

> Wiele innych zdecentralizowanych aplikacji zostało zbudowanych na bazie łańcucha bloków Ethereum. Są one przedstawione na stronie *http://dapps.ethercasts.com/*.

Platformy do decentralizacji

Obecnie istnieje wiele platform umożliwiających decentralizację. Podstawową cechą sieci łańcuchów bloków jest zapewnianie decentralizacji. Dlatego każda sieć łańcucha bloków, np. Bitcoin, Ethereum, Hyperledger Fabric lub Quorum, może posłużyć do udostępnienia usługi decentralizacji. Wiele organizacji z całego świata wprowadziło platformy, które mają sprawić, że budowanie rozproszonych aplikacji stanie się łatwe, przystępne i bezpieczne. Dalej opisano niektóre z tych platform.

Ethereum

Na początku listy znajduje się **Ethereum**, ponieważ jest to pierwszy łańcuch bloków, w którym wprowadzono język kompletny w sensie Turinga i maszyny wirtualne. Ten język znacznie różni się od ograniczonych języków skryptowych z bitcoina i wielu innych kryptowalut. Dzięki dostępności kompletnego w sensie Turinga języka Solidity pojawiły się nieskończone możliwości w zakresie rozwoju zdecentralizowanych aplikacji. Ethereum został po raz pierwszy zaproponowany w 2013 r. przez Vitalika Buterina i stanowi publiczny łańcuch bloków do budowania inteligentnych kontraktów i zdecentralizowanych aplikacji. Waluta używana w Ethereum to **ethery**.

MaidSafe

MaidSafe zapewnia sieć **SAFE** (ang. *secure access for everyone*, czyli bezpieczny dostęp dla każdego), która wykorzystuje nieużywane zasoby obliczeniowe użytkowników, takie jak pamięć, moc obliczeniowa i połączenia. Pliki w tej sieci są dzielone na małe porcje danych, szyfrowane i rozprowadzane losowo w sieci. Te dane mogą być pobierane tylko przez ich właścicieli. Ważną innowacją w MaidSafe jest to, że sieć automatycznie odrzuca duplikaty plików. Pomaga to ograniczyć konieczność angażowania dodatkowych zasobów obliczeniowych do zarządzania obciążeniem. Walutą używaną do nagradzania kontrybutorów jest safecoin.

Lisk

Lisk to platforma do obsługi kryptowaluty i budowania aplikacji opartych na łańcuchu bloków. Umożliwia programistom posługiwanie się JavaScriptem do tworzenia zdecentralizowanych aplikacji i umieszczania ich w łańcuchach bocznych. W Lisku do osiągania konsensusu używany jest mechanizm delegowanego dowodu stawki, w którym można wybrać 101 węzłów do zabezpieczania sieci i proponowania bloków. Na zapleczu używane są środowisko Node.js i język JavaScript, natomiast we frontonie można stosować standardowe technologie: CSS3, HTML5 i JavaScript.

W Lisku walutą w łańcuchu bloków jest **LSK**. Na podstawie Liska powstał też Rise — zdecentralizowana aplikacja i platforma dla waluty cyfrowej. W tej platformie większy nacisk położony jest na bezpieczeństwo systemu.

Bardziej praktyczne wprowadzenie do tych i innych platform znajdziesz w dalszych rozdziałach.

Podsumowanie

W tym rozdziale przedstawiono zagadnienie decentralizacji, która jest podstawową usługą oferowaną przez łańcuchy bloków. Choć koncepcja decentralizacji nie jest niczym nowym, w świecie łańcuchów bloków zyskała nowe znaczenie i spowodowała w ostatnim czasie pojawienie się różnych aplikacji opartych na zdecentralizowanej architekturze.

Rozdział rozpoczął się od wprowadzenia zagadnienia decentralizacji. Dalej omówiono decentralizację w kontekście łańcuchów bloków. Ponadto przedstawiono idee związane z różnymi warstwami decentralizacji w ekosystemie łańcucha bloków oraz kilka nowych koncepcji i pojęć powstałych wraz z pojawieniem się łańcuchów bloków i możliwej dzięki nim decentralizacji. Niektóre z tych pojęć to: DAO, DAC i DApps. W końcowej części opisano kilka przykładowych zdecentralizowanych aplikacji.

W następnym rozdziale opisane zostaną podstawowe koncepcje niezbędne do zrozumienia ekosystemu łańcuchów bloków. Przede wszystkim znajdziesz tam wprowadzenie do kryptografii, która stanowi ważną podstawę technologii łańcuchów bloków.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

Q

R

S

Ś

T

U

W

Z

Ż

Blockchain: w sieci węzłów rozproszonych nigdy nic nie zaginie!

Warto dobrze zrozumieć działanie łańcucha bloków. Ta nowatorska technologia intryguje badaczy, technologów i świat finansjery. Najlepiej jest znana z powiązań z bitcoinem i innymi kryptowalutami, jednak to rozwiązanie ma wielkie znaczenie również w finansach, administracji, multimediach i wielu innych branżach. Przejrzyste i kryptograficznie bezpieczne przechowywanie niemodyfikowalnego zapisu transakcji jest właściwością, która decyduje o wielkiej atrakcyjności łańcucha bloków. Bez wątpienia warto dobrze zaznajomić się z tą technologią i nauczyć się wykorzystywać ją w praktyce.

Ta książka jest zaktualizowanym i uzupełnionym wydaniem świetnego przewodnika po świecie blockchaina; skorzysta z niej zarówno programista, jak i prezes konstruujący strategię swojej firmy. Znalazło się tu wyczerpujące omówienie technicznych podstaw łańcuchów bloków i systemów rozproszonych. Przedstawiono mechanizmy związane z kryptowalutami i pisaniem aplikacji wykonywanych w zdecentralizowanej maszynie wirtualnej w łańcuchu bloków Ethereum. Pokazano też inne rozwiązania z tego obszaru, w tym biznesowe platformy łańcuchów bloków rozwijanych w ramach projektu Hyperledger. Okazuje się, że technologia ta znakomicie uzupełnia internet rzeczy, a zwiększanie skalowalności łańcucha bloków daje nowe, fascynujące możliwości.

W tej książce:

- podstawy przetwarzania rozproszonego, decentralizacja procesów i systemów
- wprowadzenie do kryptografii i sieci bitcoina
- techniczne zagadnienia związane z Ethereum i inteligentnymi kontraktami
- wprowadzenie do Web3 i do projektu Hyperledger
- informacje o zastosowaniu łańcucha bloków w różnych dziedzinach
- aktualne prognozy dotyczące przyszłości technologii łańcucha bloków

Imran Bashir od wielu lat rozwija oprogramowanie, tworzy architekturę rozwiązań technicznych, zarządza infrastrukturą i usługami informatycznymi. Jest członkiem prestiżowych stowarzyszeń IEEE i BCS. Od 16 lat realizuje duże projekty informatyczne dla sektora publicznego i branży usług finansowych. Obecnie pracuje dla jednego z banków inwestycyjnych w Londynie, gdzie jest wicedyrektorem działu technologii.

ISBN 978-83-283-4957-5