O'REILLY®

Blockchain

Przewodnik po technologii łańcucha bloków

Kryptowaluty, inteligentne kontrakty i aplikacje rozproszone

Lorne Lantz
Daniel Cawrey

Helion

Tytuł oryginału: Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications

Tłumaczenie: Marcin Machnik

ISBN: 978-83-283-9361-5

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

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

Printed in Poland.

Spis treści

ROZDZIAŁ 1.

Początki technologii blockchain

Termin *blockchain* niewtajemniczonym może się wydawać tajemniczy lub wręcz przerażający. Jego dosłowne tłumaczenie — *łańcuch bloków informacji* — to jednocześnie chyba najprostszy sposób na wyjaśnienie jego znaczenia. Ale do czego służy? Po co ktoś miałby potrzebować czegoś zwanego „łańcuchem bloków"?

Aby odpowiedzieć na to pytanie, musimy cofnąć się w czasy bliżej początków sieci. Istotą internetu jest przechowywanie i dystrybucja informacji dla dużej liczby ludzi. Blockchain ma podobny cel i wyrasta na wcześniejszych eksperymentach z ulepszaniem sposobów tej dystrybucji.

Systemy elektroniczne i zaufanie

Żeby w ogóle mogły powstać blockchain, kryptowaluta i systemy wykorzystujące tę technologię, potrzebny był wiarygodny i rozproszony internet, z którego korzysta mnóstwo ludzi. Tymczasem w latach sześćdziesiątych ubiegłego wieku była to względnie mała i prosta sieć, używana głównie przez badaczy uniwersyteckich i rząd USA do cyfrowego przesyłania informacji.

Z czasem pionierzy internetu uczynili go bardziej użytecznym. Największe znaczenie miało opracowanie *protokołów* TCP/IP (który stał się standardem komunikacji), HTTP (umożliwiającego przeglądanie sieci) oraz SMTP (pozwalającego na przesyłanie poczty elektronicznej). Za sprawą tych protokołów internet stał się dostępny nie tylko dla badaczy i ich sprzętów, lecz dla wszystkich ludzi oraz dla coraz większej liczby urządzeń, w tym komputerów, a później tabletów i smartfonów.

Rozwój internetu zmienił życie na zawsze — mamy dziś na wyciągnięcie ręki niewiarygodne ilości informacji, w większości za darmo. Ale korzystanie z większości produktów lub usług online wymaga osoby lub jednostki zwanej trzecią stroną, która funkcjonuje jako zaufany portier. Te systemy wymagają dwóch typów zaufanych jednostek. Są to:

- *zaufany pośrednik* — trzecia strona stanowiąca bazę racjonalnych i sprawiedliwych decyzji,
- *zaufany emitent* — trzecia strona stanowiąca bazę bezpieczeństwa dla wszelkich zasobów.

Transakcje finansowe to jeden z przykładów wykorzystania tych dwóch rodzajów zaufania, jako że większość transakcji odbywa się cyfrowo. Z różnych powodów następuje stopniowe odchodzenie od *papierowych pieniędzy fiducjarnych*, czyli emitowanej przez rządy fizycznej gotówki — współcześni ludzie chętniej niż kiedykolwiek wcześniej korzystają z elektronicznych narzędzi płatniczych

w rodzaju kart kredytowych i debetowych. W niektórych państwach, takich jak Szwecja, systemy płatności są niemal w całości elektroniczne i większość klientów używa w punktach sprzedaży smartfonów i kart[1]. O ile jednak dla konsumentów przejście z płatności gotówkowych na cyfrowe jest względnie młodym trendem, o tyle umożliwiające to systemy są od dawna elektroniczne. Chociaż gotówka jest nadal dostępna dla większości osób, pieniądze w dużej mierze z papierków i monet zmieniły się w cyferki w systemie komputerowym, zasadniczo niezauważalnie.

Aby przetransferować zasoby z przedmiotów fizycznych do bazy danych, musi istnieć element zaufania między wieloma zaangażowanymi w to stronami. Powstałe na całym świecie wielkie korporacje płatnicze opierają się na założeniu, że mogą im zaufać ludzie chcący przechować jakieś zasoby cyfrowo. Ale w finansach zaufanie nie zawsze jest uzasadnione. Kryzys finansowy z 2008 roku dał ludziom do myślenia i wielu zaczęło się zastanawiać, czy nie doprowadziły do niego właśnie ślepe zaufanie i wiara pokładane w instytucjach finansowych.

Blockchain to próba odbudowania utraconego zaufania. Wykorzystuje technologię — a kon-kretnie kryptografię — w celu automatycznego egzekwowania zaufania trzeciej strony.

Bitcoin jest pierwszym działającym systemem wykorzystującym blockchain. Ale zanim się pojawił, próbowano zastosować te koncepcje — bezskutecznie — u kilku jego poprzedników. Upadły one między innymi dlatego, że nie udało się stworzyć w internecie prawdziwie *rozproszonego* systemu.

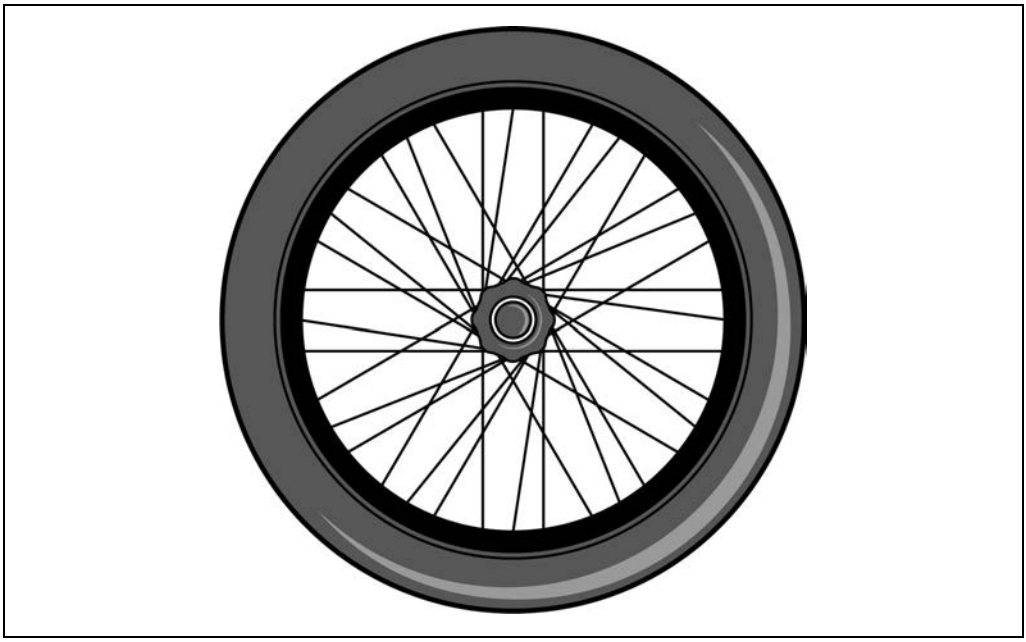
Rozproszony kontra scentralizowany kontra zdecentralizowany

Współczesny internet to mieszanina zastosowań scentralizowanych i rozproszonych, chociaż zaprojektowano go jako technologię rozproszoną. Pionierzy internetu chcieli stworzyć odporniejszy system niż scentralizowana infrastruktura z jednym wrażliwym punktem. Idea rozproszonego internetu wynikała z założenia (podsuniętego przez wojsko), że zaatakowanie jednej części systemu nie powinno uniemożliwiać funkcjonowania reszcie sieci.

Na kole rowerowym (zobacz rysunek 1.1) liczne szprychy są przytwierdzone do jednej piasty (osi). Ten układ realizuje ideę rozproszenia — gdy jedna ze szprych pęknie, koło nadal będzie funkcjonalne[2]. *Rozproszenie* oznacza, że żaden pojedynczy słaby punkt nie położy całego systemu, takiego jak sieć komputerów składających się na wczesną wersję internetu.

[1] *https://www.npr.org/2019/02/11/691334123/swedens-cashless-experiment-is-it-too-much-too-fast?t=1648828391426*

[2] *http://caravan.hobby.ru/materiel/Bicycle_Wheel_-_Jobst_Brandt.pdf*



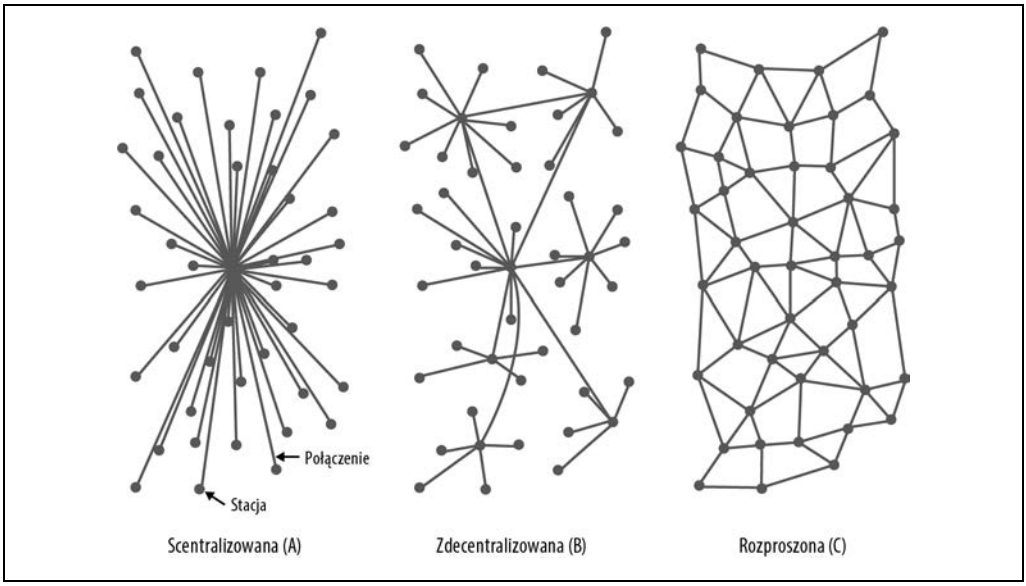
Rysunek 1.1. Koło rowerowe opiera się na idei rozproszenia

Dekady temu internet pomyślano jako rozproszony, żeby chronić sieć przed jakimkolwiek rodzajem przerwań, i taki system sprawdził się aż do dziś. W ostatnich czasach został jednak zdominowany[3] przez scentralizowane korporacje w rodzaju Google, Facebooka, Apple i Amazona. Niektórzy ludzie liczą na to, że rozproszona natura technologii blockchain pomoże zmniejszyć dominację w sieci tych nielicznych potężnych korporacji, dając większą kontrolę pojedynczym użytkownikom — w co zagłębimy się nieco dalej w tej książce.

W dziedzinie przetwarzania danych system rozproszony to taki, w którym przetwarzanie nie odbywa się na pojedynczym komputerze. Zamiast tego jest podzielone na kilka systemów obliczeniowych. Takie systemy komunikują się ze sobą za pomocą jakiegoś rodzaju komunikatora. Rysunek 1.2 przedstawia kilka różnych architektur sieci[4]. System rozproszony cechuje decentralizacja w tym sensie, że awaria pojedynczej jednostki (*węzła*) nie oznacza awarii całej sieci. Wspólnym celem jest wykorzystywanie mocy obliczeniowej do zbiorowej realizacji zadań przez rozdzielenie obowiązków na wiele komputerów. Ale decentralizacja zmienia koncepcję wspólnych celów i komunikacji. W systemie w pełni zdecentralizowanym dany węzeł niekoniecznie współpracuje w realizacji swojego zadania z każdym innym węzłem, a podejmowanie decyzji opiera się na jakiegoś rodzaju konsensusie, a nie na odpowiedzialności pojedynczej jednostki.

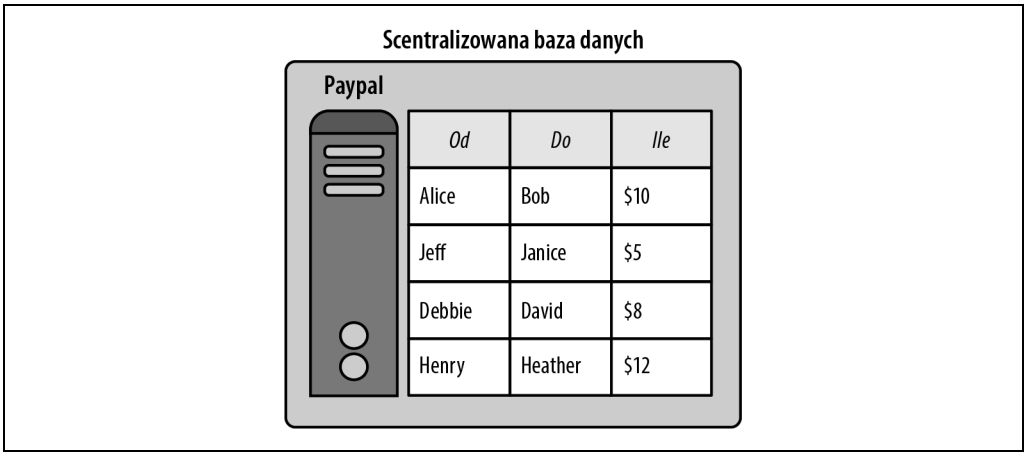
[3] *https://hackernoon.com/the-evolution-of-the-internet-from-decentralized-to-centralized-3e2fa65898f5*

[4] *https://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf*

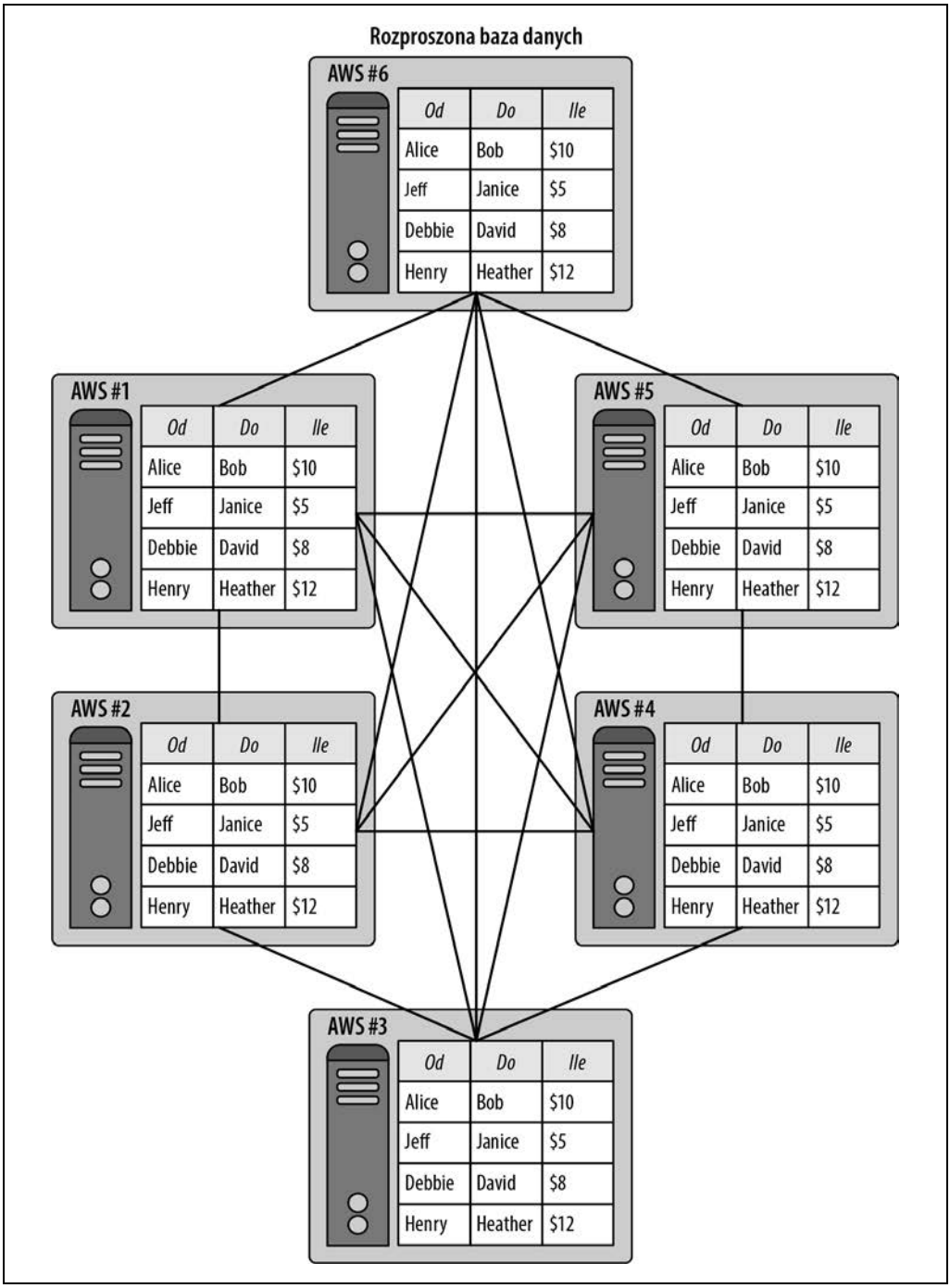


Rysunek 1.2. Sieć scentralizowana, zdecentralizowana i rozproszona

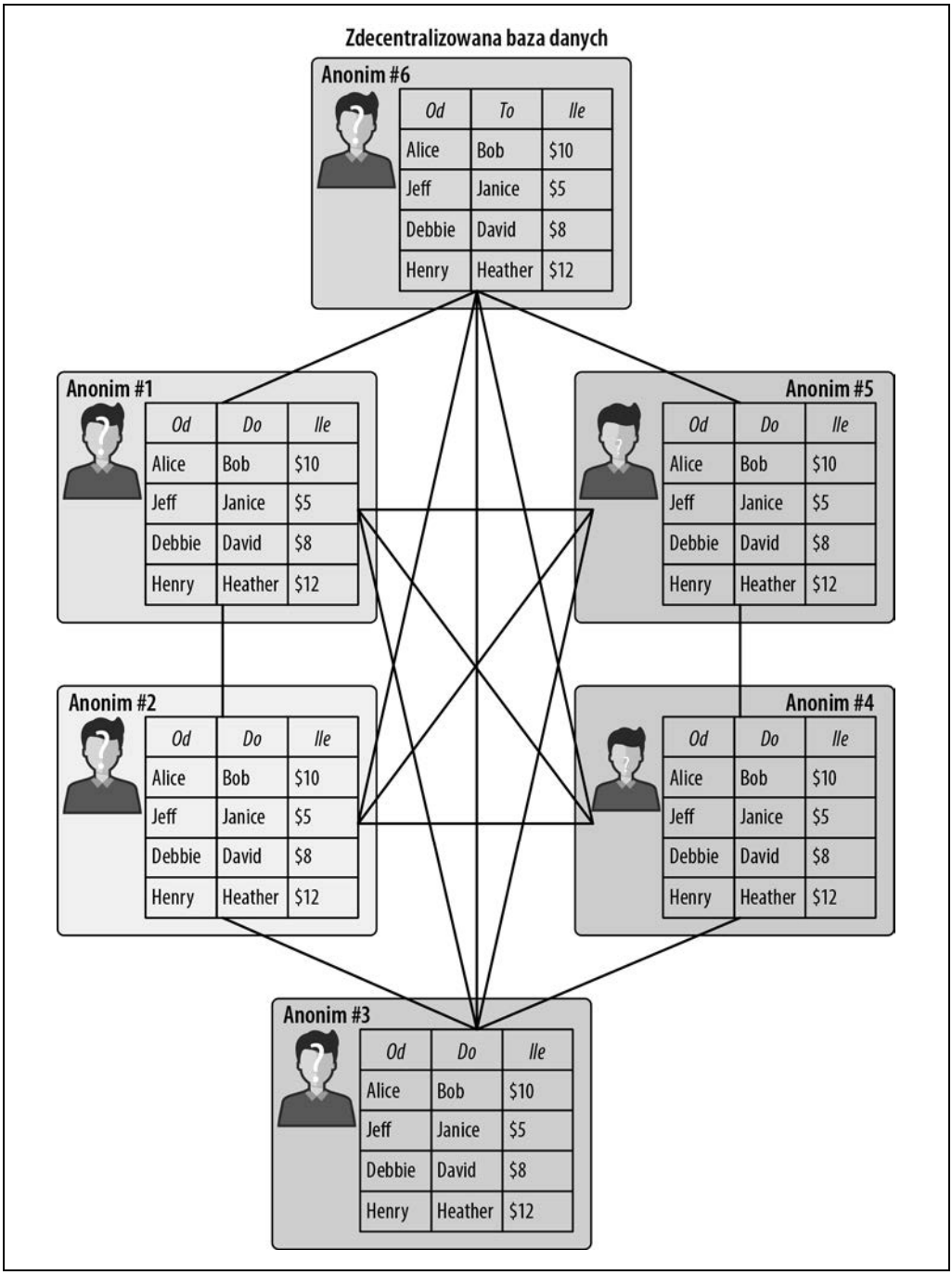
Rysunki od 1.3 do 1.5 przedstawiają różnice między systemami scentralizowanymi, rozproszonymi i zdecentralizowanymi na przykładzie baz danych przechowujących informacje.



Rysunek 1.3. W scentralizowanej bazie danych takiej jak PayPal wszystkie węzły są połączone z pojedynczym centralnym węzłem, kontrolowanym przez jedną jednostkę



Rysunek 1.4. W rozproszonej bazie danych, takiej jak liczne bazy hostowane w Amazon Web Services (AWS), każdy węzeł może przechowywać powieloną kopię tych samych danych i zna tożsamość innych węzłów, a wszystkie węzły są kontrolowane przez jedną jednostkę



Rysunek 1.5. W zdecentralizowanej bazie danych, takiej jak łańcuch bloków sieci Bitcoin, każdy węzeł może przechowywać powieloną kopię tych samych danych, ale niekoniecznie zna tożsamość pozostałych węzłów, a wszystkie węzły są kontrolowane przez wiele jednostek, które mogą być anonimowe

Poprzednicy sieci Bitcoin

Wszechobecność internetu wprowadziła zamęt i zmieniła wiele branż. Żeby podać chociaż kilka spośród wielu przykładów — w ciągu ostatnich paru dekad Wikipedia w znacznym stopniu zastąpiła encyklopedie, portale ogłoszeniowe przejęły od gazet ogłoszenia drobne, a za sprawą Google Maps drukowane atlasy odeszły do lamusa.

Mimo to branży finansowej przez długi czas udawało się oprzeć tym gwałtownym przemianom. Przed 2009 rokiem, w którym pojawił się Bitcoin, kontrola nad pieniędzmi nie zmieniła się zbyt wiele poza przejściem użytkowników z domeny analogowej (fizycznej gotówki i czeków) na cyfrową (bankowość elektroniczną). To przejście oswoiło ludzi z ideą cyfrowych pieniędzy, ale kontrola nad nimi jest nadal scentralizowana.

Liczne przedbitcoinowe koncepcje z różnych powodów upadły, łączył je jednak ostateczny cel: zwiększenie suwerenności finansowej lub zwiększenie kontroli użytkowników nad swoimi pieniędzmi. Przegląd niektórych nieudanych wczesnych projektów może rzucić światło na przyczyny rosnącej popularności sieci Bitcoin.

DigiCash

Założone przez Davida Chauma w 1989 roku DigiCash było firmą umożliwiającą anonimowe płatności w internecie. Chaum jest wynalazcą technologii ślepego podpisu[5], w której kryptografia zabezpiecza prywatność płatności internetowych. Kryptografia polega na wykorzystaniu obliczeń szyfrujących w celu ukrycia wrażliwych informacji i była od dawna wykorzystywana przez władze na całym świecie jako narzędzie komunikacyjne. W rozdziale 2. przyjrzymy się nieco bardziej szczegółowo kwestii kryptografii i szyfrowania.

Platforma DigiCash posługiwała się własną walutą zwaną *cyberbucks* („cyberdolcami”)[6]. Użytkownicy, którzy zarejestrowali się w serwisie, otrzymywali 100 takich cyberdolców, zwanych też *tokenami* lub *coinami*. Firma zapoczątkowała stosowanie kart z mikroczipami, takich jak większość współczesnych kart kredytowych. Była także pionierem w kwestii idei cyfrowego portfela do przechowywania zasobów[7] — w tym przypadku cyberdolców.

Systemy DigiCash były testowane przez kilka banków, w tym Deutsche Bank. Garść sprzedawców także się zarejestrowała, by przyjmować cyberdolce, w tym wydawca encyklopedii Britannica. W latach dziewięćdziesiątych ubiegłego wieku handel internetowy był nowością, a z obawy przed przekrętami ludzie bali się korzystać w sieci nawet z kart kredytowych, nie mówiąc już o akceptacji zupełnie nowego systemu płatności. Mimo to sporo zainteresowanych prywatnością osób zaczęło korzystać z cyberdolców, powstał nawet rynek wysyłkowy, który jakiś czas funkcjonował. Nie udało się jednak spowodować efektu lawiny z powodu braku chętnych sprzedawców i ostatecznie firma DigiCash w 1998 roku ogłosiła upadłość[8].

---

[5] *http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF*

[6] *https://www.theguardian.com/technology/2003/feb/25/comment.comment*

[7] *https://www.wired.com/1994/12/emoney/*

[8] *https://www.forbes.com/forbes/1999/1101/6411390a.html#72c58610715f*

E-gold

Za założoną w 1996 roku cyfrową przechowalnią zasobów o nazwie E-gold (czyli „e-złoto") stały prawdziwe jednostki tego cennego kruszcu. Zarządzane przez firmę Gold & Silver Reserve E-gold umożliwiało swoim użytkownikom dokonywanie natychmiastowych transferów przez internet. Wszystko było denominowane w jednostkach złota lub innych metali szlachetnych. W 2006 roku platforma miała 3,5 miliona kont. W tamtym czasie firma przetwarzała dziennie transakcje o wolumenie 5,9 miliona dolarów[9].

Z nominałami tak małymi jak jedna stutysięczna grama złota platforma jako pierwsza wprowadziła koncepcję *mikropłatności*, czyli przelewania przez internet niewielkich kwot. Innowacją na owe czasy było także zaoferowanie deweloperom interfejsu programistycznego, umożliwiającego nadbudowywanie na platformie dodatkowych usług[10]. Sprzedawcy internetowi przyjmowali E-gold jako formę płatności obok kart kredytowych. W 1999 roku wprowadzono obsługę płatności mobilnych (*https://oreil.ly/X7DeN*).

E-gold było technologicznym majstersztykiem w kontekście funkcjonalności oferowanych w latach dziewięćdziesiątych ubiegłego wieku i na początku lat dwutysięcznych. Od samego początku jednak borykało się z problemami, które ostatecznie doprowadziły do jego upadku. Jako scentralizowany system pozbawiony mechanizmu powiązania konta z tożsamością użytkownika, było wykorzystywane do niecnych celów, gdyż ułatwiało pranie pieniędzy, oszustwa internetowe i inne nielegalne działania. Rząd USA zamknął E-gold w 2008 roku[11], przejmując jego zasoby i ustanawiając system rekompensat dla właścicieli kont.

Hashcash

Wymyślony przez Adama Backa w 1997 roku Hashcash wprowadził ideę dowodu pracy (*proof-of-work*) jako sposobu weryfikacji ważności cyfrowych zasobów oraz koncepcję pieniędzy istniejących wyłącznie w internecie. *Dowód pracy* oznacza, że komputery muszą wykonać jakiegoś rodzaju weryfikowalną i intensywną obliczeniowo pracę, aby elektroniczne pieniądze miały jakąkolwiek wartość (bardziej szczegółowo wyjaśniamy to w rozdziale 2.). W przypadku Hashcash dowód pracy był realizowany za pomocą kryptografii, a Back zaproponował w tym celu użycie algorytmu SHA1[12].

W swojej wstępnej propozycji Adam Back nawiązał do DigiCash i zasugerował, że wprowadzenie dla maili opłaty (lub czegoś w rodzaju znaczka pocztowego) w cyfrowej walucie pomogłoby w walce ze spamem. Zastosowanie funkcji *skrótu* (*hash*), czyli funkcji wymagającej przetwarzania komputerowego, miało stanowić w Hashcash koszt ekonomiczny, który ograniczałby ilość spamu w systemach pocztowych. W przypadku waluty cyfrowej pomysł wykorzystania funkcji skrótu rozwiązywało problem *podwójnego wydatkowania* (*double spending*), czyli możliwości skopiowania jednostki cyfrowej tak jak pliku i zapłacenia nią więcej niż jeden raz. W końcu duplikowanie

[9] *https://web.archive.org/web/20061109161419/http:/www.e-gold.com/stats.html*

[10] *https://web.archive.org/web/20010123225700/http:/e-gold.com/unsecure/sci_home.html*

[11] *https://legalupdate.e-gold.com/2008/07/consent-order-of-forfeiture-20080721.html*

[12] *https://cypherpunks.venona.com/date/1997/03/msg00774.html*

plików na komputerze nie stanowi żadnego kłopotu i każdy może powielić jakiś obraz i uzyskiwać kolejne jego kopie. Zastosowanie funkcji skrótu miało na celu ograniczenie tej możliwości w odniesieniu do cyfrowego pieniądza przez narzucenie kosztu w postaci dowodu pracy, czyli mocy obliczeniowej.

Chociaż Hashcash testowano w systemach pocztowych Microsoftu i Apache, dostawcy otwartoźródłowego oprogramowania, nie odniósł sukcesu[13]. Koncepcyjnie był to świetny pomysł na wprowadzenie niezbędnego w internetowej walucie efektu cyfrowej rzadkości, ale od strony technologii nie była to dobra forma waluty cyfrowej.

B-money

Zaproponowana przez Wei Dai w 1998 roku sieć B-money wprowadzała koncepcję wykorzystania informatyki do tworzenia wartości monetarnych poza systemami rządowymi (*http://www.weidai.com/bmoney.txt*). Tak samo jak w Hashcash, w B-money pieniądze cyfrowe miały być wytwarzane za pomocą obliczeń, czyli dowodu pracy. Wei podobnie jak Adam Back sugerował, że kosztem wytworzenia pieniądza cyfrowego będzie moc obliczeniowa użyta do jego stworzenia. Taka cyfrowa waluta byłaby wyceniana na podstawie koszyka realnych zasobów, takich jak złoto i inne dobra, oraz miałaby ograniczoną podaż, żeby zabezpieczyć ją przed inflacją, czyli utratą wartości wraz z upływem czasu.

B-money rozwijało ideę publikowania transakcji w sieci. Na przykład, gdy jedna strona chciała drugiej zapłacić, do sieci trafiała wiadomość o treści: „Osoba 1 wysyła X dolarów osobie 2". System miał być weryfikowalny za pomocą sieci cyfrowych kontraktów. Te kontrakty w teorii służyły do rozwiązywania wszelkich sporów na podobnej zasadzie, na jakiej operatorzy kart kredytowych radzą sobie z takimi problemami jak oszustwa. Zarówno płatności, jak i sporne kwestie miały być regulowane nie przez scentralizowany system, lecz przez kryptografię, dzięki czemu użytkownicy sieci mogli zachować anonimowość — nikt nie musiał weryfikować swojej tożsamości.

Koncepcja sieci B-money zebrała w całość kilka komponentów cyfrowego pieniądza. Wykorzystywała między innymi ideę kontraktów, które zapewniały porządek w anonimowym i rozproszonym systemie, oraz ideę dowodu pracy do tworzenia pieniędzy. Była jednak głównie teoretycznym ćwiczeniem Weia. Eksplorował on koncepcję pozarządowej waluty odpornej na inflację za sprawą kontrolowanej podaży jednostek monetarnych.

Bit gold

Zaproponowane w 2005 roku przez informatyka Nicka Szabo „bitowe złoto" (*https://nakamotoinstitute.org/bit-gold*) miało w zamierzeniu twórcy odzwierciedlać rzadkość tego cennego kruszcu w rzeczywistości cyfrowej. Szabo zauważył, że dobra w rodzaju złota poza tym, że mają określoną wartość, są też „niepodrabialne" — bardzo trudno je sfałszować ze względu na ich rzadkość i pewne określone koszty wydobycia i transportu. Chciał stworzyć takie dobro w domenie cyfrowej.

[13] *https://www.nasdaq.com/articles/the-genesis-files%3A-hashcash-or-how-adam-back-designed-bitcoins-motor-block-2018-06-04*

Pomysł wyrastał z koncepcji sieci E-gold, w której wartość cyfrowa miała swój odpowiednik w złocie. Nick Szabo zastosował dowód pracy typu „zagadka dla klienta". Zaproponował korzystanie z generowanego na komputerze użytkownika „zagadkowego ciągu", który następnie miał być bezpiecznie oznakowany czasowo „w rozproszony sposób". To z kolei miało trafić do „rozproszonego rejestru tytułów własności" i stanowić cyfrowy dowód własności.

Jak większość pomysłów Szabo bit gold było w głównej mierze ćwiczeniem intelektualnym. Tworząc bitowe złoto, Szabo próbował uzyskać niewymagającą zaufania wersję E-gold.

Eksperyment Bitcoin

W 2008 roku świat był już uzależniony od internetu jako rozproszonej jednostki będącej bazą dla dużej liczby usług. Elektroniczne mapy i aplikacje GPS pomagały ludziom trafić z punktu A do B. E-maile, wiadomości tekstowe, Skype, WhatsApp i inne aplikacje komunikacyjne umożliwiały niemal natychmiastowy kontakt z przyjaciółmi i członkami rodziny, na małe i duże odległości.

Dodatkowo ludzie zaczęli kupować coraz więcej rzeczy przez internet zamiast w tradycyjnych sklepach. Karty kredytowe i debetowe stały się popularnymi narzędziami płatniczymi wraz z PayPalem i podobnymi serwisami. Jak jednak wspomnieliśmy w poprzednim podrozdziale, wiele osób pragnęło odpornego na manipulacje i rozproszonego sposobu na przekazanie zasobów przez internet — a wtedy taki sposób wciąż jeszcze nie został opracowany i wprowadzony.

Kryzys finansowy 2008 roku

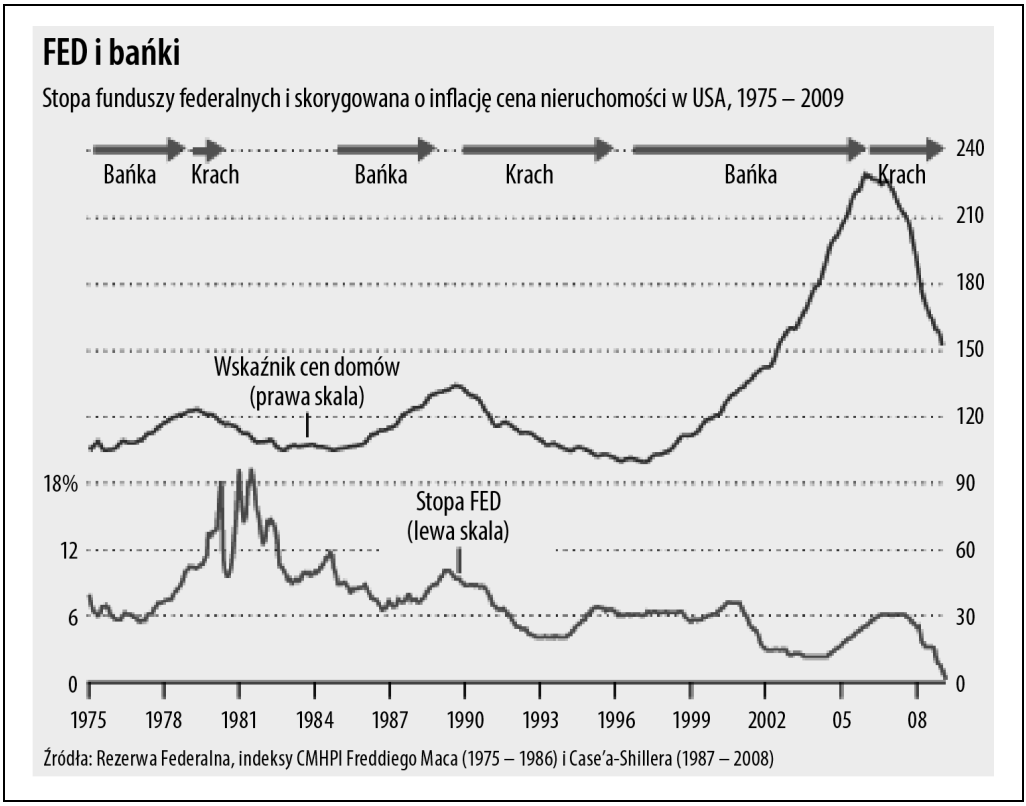
Na początku 2006 roku światowa ekonomia kwitła. Był to czas ekonomicznego wzrostu, ale właśnie w tym roku pojawiły się pierwsze rysy. Rynek nieruchomości w USA po raz pierwszy zanotował spadek po takim rozluźnieniu zasad udzielania kredytów, że wielu kredytobiorców nie było w stanie spłacić swoich zobowiązań.

Doprowadziło to do zamieszania w bankach, ponieważ te na podstawie hipotek i innych rodzajów niepewnych pożyczek utworzyły papiery wartościowe, którymi instytucje finansowe handlowały tak jak obligacjami i akcjami. Gdy sporo takich papierów okazało się nie mieć żadnej wartości, doszło do zapaści systemu finansowego i rządy na całym świecie musiały wstrzykiwać gotówkę w system, żeby ocalić globalną gospodarkę.

W USA współczesne bańki nieruchomości kontrolowała Rezerwa Federalna przez podnoszenie stóp procentowych[14], co ilustruje rysunek 1.6. Ale kryzysu w 2008 roku nie dało się opanować, prawdopodobnie z powodu nieprzejrzystości systemu finansowego.

Dlaczego ten fragment historii finansów ma znaczenie w dyskusji o Bitcoinie? Dlatego, że chociaż w 2008 roku istniało już wiele koncepcji stojących u podstaw tej sieci, nikt nie poskładał wszystkich elementów wcześniejszych e-pieniędzy w całość i nie stworzył systemu, który oferowałby cyfrowe zaufanie i przejrzystość.

[14] *https://www.wsj.com/articles/SB123897612802791281*



Rysunek 1.6. Podnoszenie stóp procentowych przez Rezerwę Federalną w celu opanowania baniek na rynku nieruchomości

Whitepaper

18 sierpnia 2008 roku zarejestrowano domenę *bitcoin.org*. Następnie 31 sierpnia 2008 roku opublikowano *whitepaper* (czyli dokument informacyjny) napisany przez osobę lub grupę posługującą się pseudonimem Satoshi Nakamoto i udostępniono go na wielu listach mailingowych programistów. Dokument pod tytułem „Bitcoin: A Peer-to-Peer Electronic Cash System" („Bitcoin: system elektronicznych pieniędzy typu peer-to-peer") zawierał szczegółowy opis systemu finansowego, który miał istnieć tylko w internecie. Celem było stworzenie cyfrowej waluty funkcjonującej bez jakiegokolwiek powiązania z bankiem lub rządem i zbudowanie bardziej przejrzystego systemu finansowego, który zapobiegałby ponownym katastrofalnym krachom finansowym w przyszłości.

Dokument uwzględniał szereg pomysłów znanych z poprzedzających sieć Bitcoin systemów, w tym:

- bezpieczne cyfrowe transakcje jak w kontraktach Nicka Szabo,
- wykorzystanie kryptografii w celu zabezpieczenia transakcji jak w DigiCash,
- teoretyczną możliwość przesyłania drobnych zabezpieczonych sum jak w E-gold,
- stworzenie pieniędzy poza systemami rządowymi jak w B-money,
- wykorzystanie dowodu pracy w celu zweryfikowania ważności cyfrowych środków jak w Hashcash.

Dokument opisywał też kilka kwestii, które dla wielu osób były nowością, w tym:

- *podwójne wydatkowanie* — ryzyko, że jednostka płatnicza zostanie użyta więcej niż raz za sprawą nieuprawnionego skopiowania,
- *dowód pracy* — matematyczny problem, do którego rozwiązania potrzebna jest moc obliczeniowa komputera,
- *hash (funkcja skrótu)* — tworzy się stałej długości dane wyjściowe, żeby ułatwić porządkowanie danych o różnych rozmiarach,
- *nounce (identyfikator jednorazowy)* — losowa liczba służąca do zapewnienia, że określona komunikacja zostanie użyta tylko raz.

Ulepszenie modelu waluty opartego na mennicy

Rządowe waluty wykorzystują model oparty na mennicy, w którym centralny autorytet (mennica) pilnuje, by nie dochodziło do podwójnego wydatkowania. Waluta jest zwracana do mennicy i okresowo się ją niszczy, żeby stworzyć nową.

W dokumencie informacyjnym Bitcoina zaproponowano wyeliminowanie tego centralnego autorytetu opartego na mennicy i zamiast tego publikowanie każdej transakcji wyłącznie w cyfrowej sieci:

> „Aby było to możliwe bez zaufanej trzeciej strony, transakcje muszą być ogłaszane publicznie, a z punktu widzenia użytkowników system musi honorować jedną historię kolejności ich otrzymywania. Odbiorca potrzebuje dowodu, że w czasie danej transakcji większość węzłów zgodziła się, że otrzymała ją jako pierwszą".

Wprowadzenie serwera z sygnaturą czasową

Poza zabezpieczeniem sieci Bitcoin dowodem pracy Satoshi zaproponował weryfikację transakcji za pomocą systemu sygnatur czasowych, podobnie jak w systemach plików i bazach danych. Wykorzystanie informacji wygenerowanych podczas transakcji i przepuszczenie ich przez algorytm haszujący generuje stały ciąg liczb i liter zwany haszem (skrótem). Dla Bitcoina Satoshi zaproponował popularny w kryptografii algorytm SHA-256.

Oto przykład:

```
keccak256("hello") =
1c8aff950685c2ed4bc3174f3472287b56d9517b9c948127319a09a7a36deac8
```

A teraz to samo z jedną małą zmianą:

```
keccak256("hello1") =
57c65f1718e8297f4048beff2419e134656b7a856872b27ad77846e395f13ffe
```

Używanie skrótów do przechowywania informacji jest także kluczowe przy zabezpieczaniu dużych ilości informacji. Jak widać na powyższym przykładzie, różne dane wejściowe dają unikalny, stałej długości skrót[15]. Ułatwia to odwoływanie się do przechowywanych danych, które da się zidentyfikować po skrócie.

[15] *https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb*

Przechowywanie danych w łańcuchach bloków

W modelu mennicowym rząd lub władza centralna rejestruje transakcje za pomocą standardowych praktyk księgowych. Dokument informacyjny o Bitcoinie wprowadził koncepcję śledzenia transakcji za pomocą *łańcucha* sygnatur, czyli skrótów. Są one zebrane w bloki czasowe w porządku chronologicznym.

Ten schemat zasadniczo tworzy jednostkę księgującą, która nie wymaga żadnego pojedynczego autorytetu pilnującego transakcji. Zamiast tego transakcje są śledzone cyfrowo w łańcuchach bloków z wykorzystaniem kryptograficznego matematycznego zaufania. Sieć nie wymaga skomplikowanej struktury, gdyż weryfikacja i publikowanie owych łańcuchów są oparte na systemie peer-to-peer. Potrzebna jest jedynie rozproszona struktura danych do *przechowywania* i *protokół* systemu komunikacyjnego, które tworzą *publiczną sieć* w internecie. Jak wyjaśnimy bliżej w rozdziale 2., łańcuch bloków składa się z wielu bloków transakcji, które są ze sobą połączone za pomocą haszy. Wiele łańcuchów jest swobodnie dostępnych w internecie, ale niektóre są niepubliczne — zwłaszcza te użyte w pewnych biznesowych scenariuszach, o czym więcej piszemy w rozdziale 9.

Oto wyzwanie, z jakim Bitcoin musiał się uporać: jak zapewnić współpracę licznych stron, które nie znają się nawzajem i sobie nie ufają. Rozwiązaniem tego problemu jest prowadzenie księgi głównej z transakcjami uznanymi przez wszystkich za zasadne i warte przetworzenia. Blockchain Bitcoina to właśnie globalna księga główna, którą wszystkie strony w sieci Bitcoin uznają za zasadną i bezbłędną. Niezgoda może oznaczać rozwidlenie w łańcuchu i stworzenie nowego, co opisujemy w rozdziale 3.

W sieci płatniczej *księga główna* to nieustannie modyfikowany dokument. Za każdym razem, gdy ktoś chce wysłać transakcję, do księgi jest dopisywany nowy rząd danych. W przypadku sieci Bitcoin do rejestru, który można określić jego księgą główną, nowy blok transakcji jest dodawany co mniej więcej 10 minut.

Poniżej wyłuszczamy istotne atrybuty każdego bloku sieci Bitcoin.

Skrót (hasz) bloku
: Unikalny identyfikator bloku. Skrót jest generowany z danych wejściowych, które stanowią 256-bitową migawkę obecnego stanu łańcucha. Ta migawka jest jak techniczna wersja bilansu całego bloku. Blok sieci Bitcoin nie zawiera własnego skrótu, zawiera jednak skrót poprzedniego bloku, na którym został zbudowany — to w ten sposób bloki są połączone w *łańcuch*. Skrót bloku można ustalić przez haszowanie jego nagłówka.

Transakcja bazowa
: Pierwsza transakcja każdego nowego bloku wykopanego w sieci. Powiększa zasób sieci o nowe bitcoiny, będące nagrodą dla górnika, który dodał go do łańcucha. Więcej o górnikach znajdziesz w rozdziale 2.

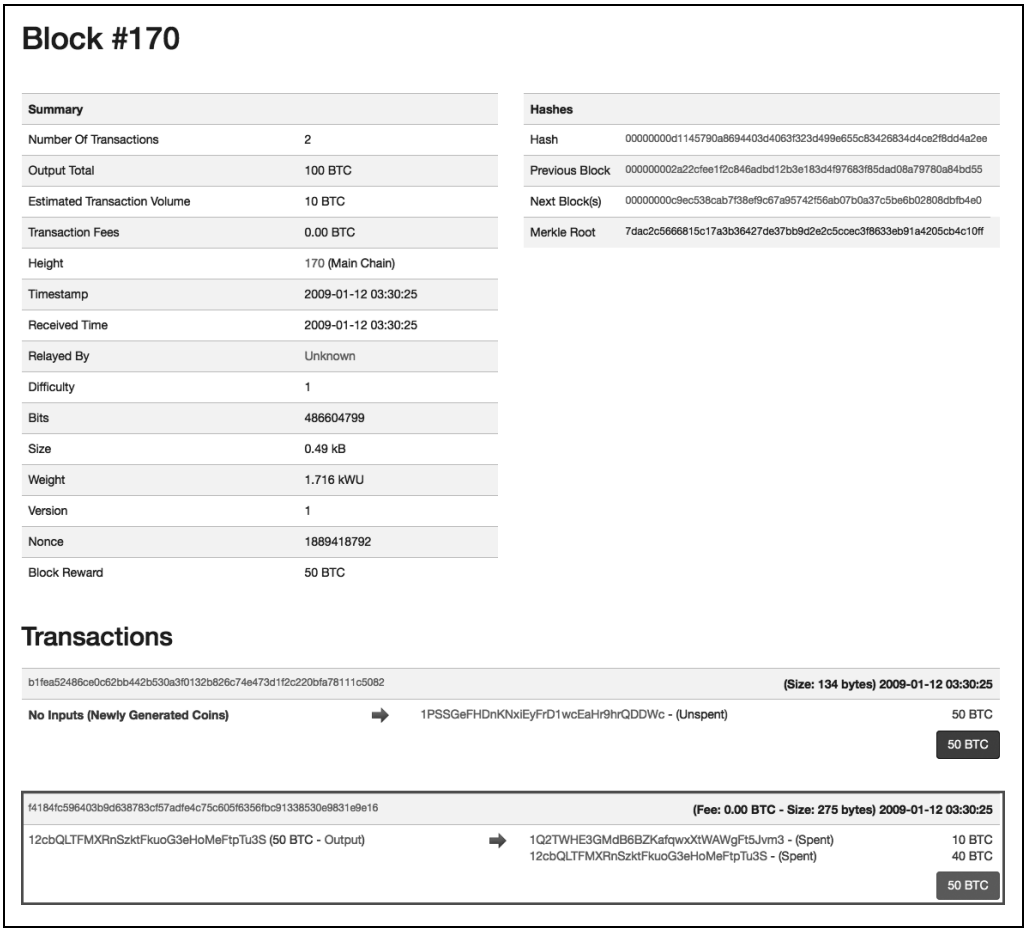
Wysokość bloku
: Liczba bloków między najnowszym a pierwszym blokiem w łańcuchu (zwanym także *blokiem Genesis*).

Korzeń Merkle'a

Hasz umożliwiający udowodnienie zasadności łańcucha bloków (więcej o korzeniach Merkle'a w rozdziale 2.).

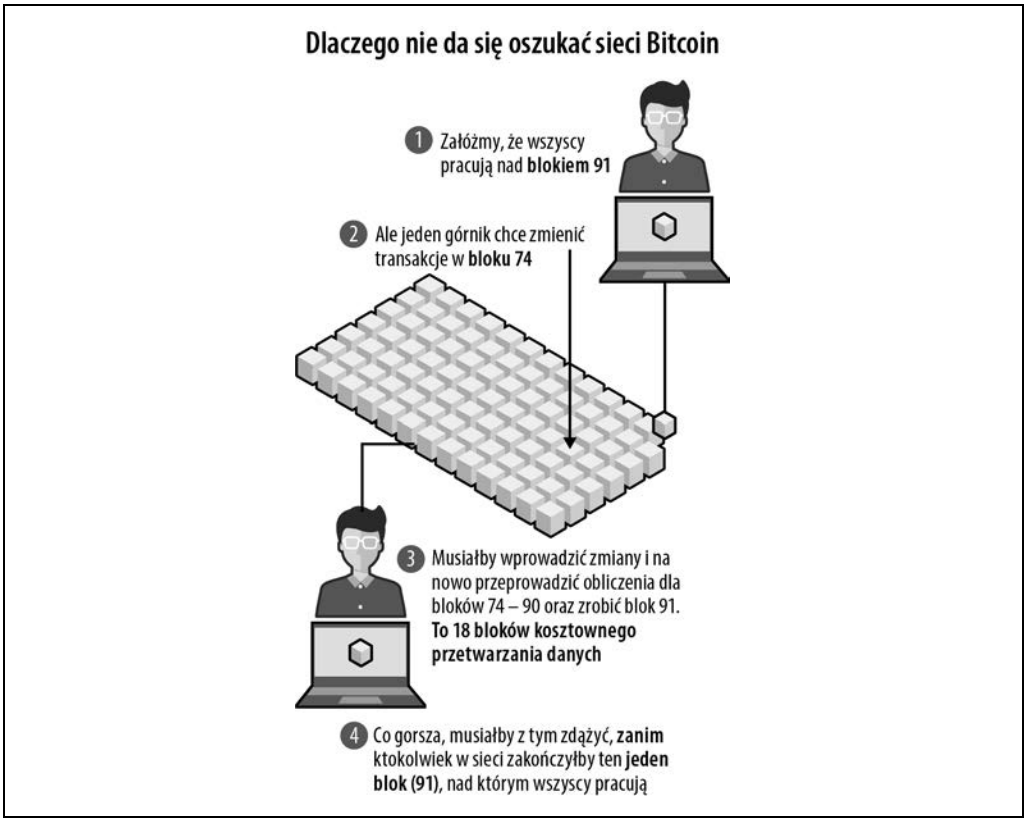
Nazwa łańcucha bloków jest najczęściej używana jako nazwa własna, natomiast jednostka jako zwykły rzeczownik. Dlatego nazwę *sieci kryptowalutowej* piszemy od wielkiej litery („Alicja uwielbia zdecentralizowany aspekt Bitcoina), ale nazwę *jednostki walutowej* piszemy z małej litery („Alicja wysłała dwa bitcoiny Bobowi").

Rysunek 1.7 przedstawia blok łańcucha Bitcoin.



Rysunek 1.7. Blok Bitcoin #170, rejestrujący przesłanie 10 BTC od Satoshiego Nakamoto do dewelopera i pioniera łańcuchów bloków Hala Finneya

Rysunek 1.8 ilustruje, dlaczego trudno jest zmienić przeszłe transakcje.



Rysunek 1.8. Dlaczego trudno wycofać bitcoinowe transakcje

Zniknięcie Satoshiego Nakamoto

Wiele osób interesuje tożsamość Satoshiego Nakamoto. Po opublikowaniu dokumentu informacyjnego sieci Bitcoin Satoshi aż do 2012 roku działał w społeczności, pomagając uczynić z tej sieci funkcjonalny system.

Dziennikarze od dawna próbują odkryć tożsamość Satoshiego Nakamoto[16]. Możliwe jednak, że wcale nie jest to jeden człowiek, lecz konglomerat współpracujących ze sobą osób, które dostrzegły w kryzysie finansowym roku 2008 okazję do zaproponowania technologii łańcucha bloków jako remedium na przyczyny krachu. Społeczność kryptowalutowa mniej się przejmuje prawdziwą tożsamością Satoshiego i skupia się na ideach, które przyczyniły się do powstania łańcucha bloków i sieci Bitcoin.

[16] *https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html*

Jako najwcześniejszy mistrz sieci Bitcoin, Satoshi Nakamoto wywarł olbrzymi wpływ na raczkującą otwartoźródłową społeczność deweloperów tej sieci. Był on aktywny mniej więcej przez pierwsze dwa lata istnienia sieci Bitcoin, komunikując się z takimi osobami jak Nick Szabo, Wei Dai i informatyk Hal Finney za pośrednictwem tablic ogłoszeń, list deweloperów i adresu podanego na początku dokumentu informacyjnego (*satoshin@gmx.com*). W okresie swojej aktywności Satoshi wykopał około miliona bitcoinów[17].

W grudniu 2010 roku część członków społeczności Bitcoin zaczęła zabiegać o to, by wykorzystać kryptowalutę jako mechanizm wspierania publikującej przecieki organizacji non profit WikiLeaks, która miała problemy z przetwarzaniem tradycyjnych płatności. Idea była taka, że Bitcoin mógłby pomóc wypełnić ten niedobór. Satoshi nie zgodził się z tym na popularnym forum w poście, w którym argumentował, że WikiLeaks okazało się zbyt kontrowersyjne i że jego (ich) zdaniem istotniejsze jest skupienie się na postępie technicznym. W ciągu tygodnia od podrzucenia pomysłu z WikiLeaks, a dokładnie 13 grudnia 2010 roku, Satoshi opublikował ostatni komunikat[18], w którym ogłosił pomniejszą nową wersję softwarowego klienta Bitcoin. Jeden bitcoin był wtedy wart 20 centów.

Urzeczywistnienie sieci Bitcoin

Koncepcja sieci Bitcoin zaprezentowana w dokumencie informacyjnym z 2008 roku łączyła technologie kryptograficznego, prywatnego i rozproszonego przetwarzania danych, proponując inne podejście do platform finansowych. Trzeba jednak było włożyć jeszcze sporo pracy, by te idee mogły zaowocować. Na szczęście w potencjał sieci Bitcoin uwierzyło wielu programistów oddanych otwartoźródłowemu oprogramowaniu. Urzeczywistnienie tej sieci było kolejnym zadaniem wymagającym nakładu pracy jej pionierów.

Przekonujące komponenty

To, że oprogramowanie jest *otwartoźródłowe*, oznacza, że nie jest prawnie zastrzeżone — każdy deweloper może przejrzeć kod źródłowy i go zmodyfikować. Poza otwartością źródła sieci kryptowalutowe w rodzaju Bitcoina mają jeszcze trzy inne cechy, za sprawą których są tak atrakcyjne[19].

Wartość
: Jednostka obiegowa zwana bitcoinem (często oznaczana skrótem BTC) jest używana do rejestrowania transakcji w księdze zwanej łańcuchem bloków Bitcoina.

Rozproszenie
: Jak podkreślono w dokumencie informacyjnym Bitcoina, sieć Bitcoin rejestruje transakcje za pomocą zdecentralizowanych węzłów.

Konsensus
: Górnicy w sieci Bitcoin korzystają wspólnie z dowodu pracy, by zapewnić bezpieczeństwo i stabilność tej rozproszonej księdze transakcji.

[17] *https://qz.com/1159188/bitcoin-price-approaches-20000-making-satoshi-nakamoto-worth-19-4-billion/*

[18] *https://sourceforge.net/p/bitcoin/mailman/message/26744510/*

[19] *https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html*

To za sprawą tych czterech komponentów sieć Bitcoin była tak atrakcyjna dla wąskiej grupy zdeterminowanych deweloperów, gotowych współpracować ze sobą nad stworzeniem odpornego i bezpiecznego modelu przechowywania zasobów w internecie. Chociaż niewolna od wad, sieć Bitcoin znacznie wykroczyła poza wcześniejsze próby zrealizowania w pełni cyfrowego i rozproszonego przechowywania zasobów.

Dojście do konsensusu

3 stycznia 2009 roku Satoshi Nakamoto „wykopał" pierwsze 50 bitcoinów, zainwestowawszy moc obliczeniową do stworzenia pierwszego bloku Bitcoina. Zwany *blokiem Genesis*, zawiera odniesienie do kryzysu finansowego jako przyczyny powstania tej sieci. W *coinbase*, czyli transakcyjnej treści wejściowej bloku Genesis, znajduje się następująca informacja[20]:

```
The Times 03/Jan/2009 Chancellor on brink of second bailout for banks[21]
```

Bitcoin to sieć rozproszona, co oznacza, że potrzebni są w niej ludzie pracujący jako górnicy. Satoshi stworzył pierwszego klienta Bitcoin. Prowadzenie klienta pozwoliło użytkownikom na uruchomienie węzłów i kopanie bloków. „Jeśli możesz utrzymać działający węzeł, który przyjmuje połączenia przychodzące, naprawdę bardzo pomożesz sieci", napisał Satoshi w poście dotyczącym publikowanego programu[22] zatytułowanym: „Bitcoin v0.1 released — P2P e-cash".

Blockchain to żywy, nieustannie uaktualniany dokument. Wraz z upływem czasu pojawia się w nim coraz więcej transakcji. Użytkownicy scentralizowanych sieci płatności w rodzaju PayPala ufają, że centralny autorytet będzie na bieżąco dopisywał w księdze głównej nowe transakcje. W zdecentralizowanej sieci płatności takiej jak Bitcoin zamiast centralnego autorytetu są tysiące anonimowych górników utrzymujących działanie sieci.

Komu więc użytkownicy powinni zaufać w kwestii uaktualnienia łańcucha bloków o nowy blok transakcji? Zdobycie tego zaufania nazywa się *dojściem do konsensusu*. Wszyscy górnicy utrzymujący sieć korzystają z tego procesu, aby realizować dwa cele:

- *odkrywanie bloków* — zgoda na to, który górnik zdobywa prawo do dodania bloku transakcji,
- *potwierdzanie transakcji* — zgoda na to, że transakcje zawarte w tym nowym bloku są zasadne i poprawne.

W większości łańcuchów bloków wykorzystywanych do kryptowalut konsensus jest osiągany na dwa sposoby (bardziej szczegółowo opisujemy to w rozdziale 2.):

- za pomocą dowodu pracy,
- za pomocą dowodu stawki (*proof-of-stake*).

W firmowych łańcuchach bloków stosuje się inne sposoby osiągania konsensusu, które omawiamy w rozdziale 9.

---

[20] *https://www.blockchain.com/btc/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b*

[21] The Times… banks — „Times", 3 stycznia 2009, minister finansów planuje drugą transzę dopłat ratunkowych dla banków — *przyp. tłum.*

[22] *https://sourceforge.net/p/bitcoin/news/2009/01/bitcoin-v01-released---p2p-e-cash/*

Kryptografia z kluczem publicznym i prywatnym

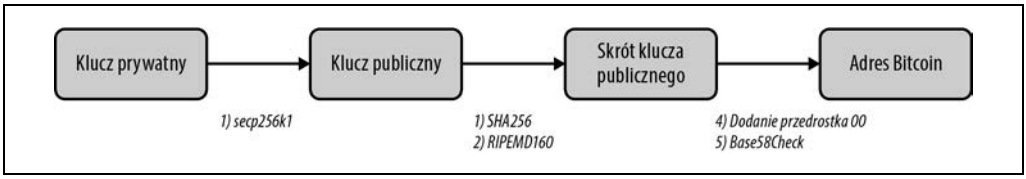
Sieć Bitcoin wykorzystuje kryptografię z kluczem publicznym i prywatnym do udowodnienia prawdziwości transakcji. *Klucze prywatne* w tej sieci służą do cyfrowego podpisywania transakcji na bitcoinach. W ten sposób właściciel adresu Bitcoin udowadnia w sieci, że jest jego prawowitym właścicielem. Prywatne klucze autoryzują transakcje. Są utrzymywane w tajemnicy, jak hasła.

Klucze publiczne służą w Bitcoinie wyłącznie do generowania adresów. Adres to zasadniczo skompresowana wersja klucza publicznego, poniekąd ułatwiająca jego odczytanie. Adres Bitcoin to wartość, którą można podać publicznie dowolnej osobie, zazwyczaj prosząc o przesłanie bitcoinów. W ten sposób działa on podobnie jak adres mailowy.

Generowanie kluczy

Klucz prywatny to losowa 256-bitowa liczba, niemal zawsze przedstawiana w formacie szesnastkowym. Jest generowana przez komputer — większość języków programowania ma funkcję generowania losowych liczb.

Klucz prywatny paruje się z kluczem publicznym, żeby przeprowadzić transakcję w sieci Bitcoin. Dokonanie tego bez klucza prywatnego jest z zasady niemal niemożliwe (więcej o tym w rozdziale 2.). W kryptografii klucz publiczny możemy wygenerować, gdy przepuścimy klucz prywatny przez funkcję secp256k1 algorytmu o nazwie Elliptic Curve Digital Signature Algorithm (ECDSA). Następnie klucz publiczny zostaje przepuszczony przez funkcje kryptograficzne SHA256 i RIPEMD160 w celu wygenerowania jego skrótu. Adres Bitcoin powstaje przez dodanie „00” do skrótu klucza publicznego i przepuszczenie tej wartości przez funkcję Base58Check. Cały proces został zilustrowany na rysunku 1.9.



Rysunek 1.9. Proces generowania adresu Bitcoin z klucza prywatnego

Część osób korzysta z klientów Bitcoin, które mają opcję generowania nowych adresów zgodnie z określonymi regułami (*https://en.bitcoin.it/wiki/Address*):

- zaczyna się od 1, 3 lub bc1,
- pozostały ciąg znaków ma długość od 25 do 34 znaków,
- dopuszczalne znaki to 0 – 9, A – Z i a – z,
- większość adresów nie zawiera l (małego L), I (wielkiego i), O (wielkiego o) ani 0 (zera), co ma zapobiegać wizualnym wieloznacznościom.

Można też skorzystać z witryny *https://www.bitaddress.org*. Serwis generuje losowość w adresie na podstawie ruchu myszy użytkownika, jednak użytkownicy muszą zaufać serwisowi, że ten nie zarejestruje ich kluczy prywatnych. Większość ludzi do generowania nowych adresów Bitcoin wykorzystuje giełdy w rodzaju Coinbase, które robią to za nich za pomocą wewnętrznego oprogramowania.

Generowanie transakcji

Transakcje Bitcoin wykorzystują unikalny sposób księgowania zwany UTXO (od *unspent transaction output*, czyli niewydatkowane wyjście transakcji). Transakcja to zasadniczo lista wejść i wyjść. Każde wejście to adres, który stanowi źródło funduszy z niewydatkowanych transakcji odebranych przez ten adres w przeszłości. Wejście zawiera także podpis cyfrowy, dowodzący, że właściciel adresu autoryzował daną transakcję. Każde wyjście wskazuje adres Bitcoin otrzymujący fundusze oraz ilość, jaką ten adres ma otrzymać.

Strukturę transakcji bitcoinowych omówimy w następnym rozdziale, tam też bardziej szczegółowo opiszemy te wszystkie koncepcje.

Wczesna podatność

Jako nowy protokół Bitcoin nie był wolny od problemów. Nie był łatwy w użyciu, więc niewiele osób pobrało klienta Bitcoin. Część najwcześniejszych propagatorów tej sieci stanowili ludzie, którzy wcześniej zaproponowali wykorzystane w niej rozwiązania. Byli wśród nich Wei Dai (autor B-money) i Nick Szabo, którego koncepcja bitowego złota w znacznym stopniu rozwinęła temat bezpieczeństwa transakcji. Wczesnym orędownikiem sieci Bitcoin był także Hal Finney, odbiorca pierwszej transakcji bitcoinowej od Satoshiego Nakamoto.

W niespełna dwa lata od uruchomienia sieci Bitcoin odkryto poważną lukę bezpieczeństwa. 6 sierpnia 2010 roku członek społeczności zauważył nienaturalnie duży wynik transakcji i opisał go na popularnej internetowej tablicy ogłoszeń[23]. „Wartość wyjściowa w bloku #74638 jest dość dziwna" — napisał Jeff Garzik, gdy ktoś próbował wyczarować z powietrza 91 979 000 000. Przykład 1.1 przedstawia tę transakcję.

Przykład 1.1. Nienaturalnie duża transakcja bitcoinowa

```
CBlock(hash=0000000000790ab3, ver=1, hashPrevBlock=0000000000606865, hashMerkleR
oot=618eba, nTime=1281891957, nBits=1c00800e, nNonce=28192719, vtx=2)
    CTransaction(hash=012cd8, ver=1, vin.size=1, vout.size=1, nLockTime=0)
         CTxIn(COutPoint(000000, -1), coinbase 040e80001c028f00)
         CTxOut(nValue=50.51000000, scriptPubKey=0x4F4BA55D1580F8C3A8A2C7)
    CTransaction(hash=1d5e51, ver=1, vin.size=1, vout.size=2, nLockTime=0)
         CTxIn(COutPoint(237fe8, 0), scriptSig=0xA87C02384E1F184B79C6AC)
         CTxOut(nValue=92233720368.54275808, scriptPubKey=OP_DUP OP_HASH160 0xB7A7)
         CTxOut(nValue=92233720368.54275808, scriptPubKey=OP_DUP OP_HASH160 0x1512)
    vMerkleTree: 012cd8 1d5e51 618eba
```

Lukę załatano, a łańcuch bloków „rozwidlono", żeby ominąć ten blok (więcej o rozwidleniach, czyli forkach, znajdziesz w rozdziale 3.). Rozwidlenie było konieczne, żeby łańcuch bloków nie odzwierciedlał tej nieprawidłowej transakcji. Po dziś dzień ta odkryta w 2010 roku podatność pozostaje największą luką bezpieczeństwa w historii Bitcoina i jest świadectwem rosnącej siły społeczności kryptowalutowej.

[23] *https://bitcointalk.org/index.php?topic=822.0*

Adopcja

Dość popularny jest pogląd, że zniknięcie Satoshiego pomogło sieci Bitcoin stać się w pełni zdecentralizowaną jednostką. Wynika to z tego, że twórca nie jest już częścią systemu, w przeciwieństwie do Ethereum i innych łańcuchów bloków, które mają tendencję do podążania za wskazówkami swoich twórców i de facto liderów.

Zapewne nieprzypadkowo mniej więcej w okolicach zniknięcia Satoshiego Bitcoin zaczął zdobywać popularność. Społeczność systematycznie się powiększała. Informatyk Gavin Andersen, którzy ostatecznie przejął czołową rolę po odejściu Satoshiego, stworzył „kran Bitcoina", który przydzielał małe ilości bitcoinów w nadziei na zwiększenie zainteresowania. Andersen wygłosił prezentację przed CIA na temat tej sieci i został głównym badaczem w obecnie nieistniejącej już Bitcoin Foundation, organizacji non profit poświęconej kryptowalutom.

22 maja 2010 roku programista Laszlo Hanyecz dokonał pierwszej transakcji wymiany bitcoinów na dobro lub usługę. Zapłacił 10 000 BTC (wtedy równowartość około 25 dolarów) za dostarczenie dwóch pizz. Ten dzień jest świętowany w społeczności jako Bitcoin Pizza Day.

W lipcu 2010 roku Mt. Gox, platforma pierwotnie założona przez dewelopera Jeda McCaleba w celu wymiany kart do gry *Magic: The Gathering*, zaczęła oferować wymianę bitcoinów[24]. Koncepcja wymiany bitcoinów na tradycyjne waluty zaczęła coraz bardziej się upowszechniać, napędzając spekulacje i wynikające z nich podbicie kursu.

Podsumowanie

Sieć Bitcoin miała fundamentalne znaczenie w genezie technologii łańcucha bloków. Jej koncepcje technologiczne nie wzięły się jednak znikąd, a sieć nie rozwinęła się z dnia na dzień. Większość wielkich idei nie powstaje w próżni. Bitcoin z całą pewnością w niej nie powstał, podobnie jak blockchain.

Obecny poziom dojrzałości sieci opiera się na licznych technologiach, które wymagały dekad pracy rozwojowej oddanych deweloperów. Dzięki ich wspólnemu wysiłkowi technologia łańcucha bloków jest dziś w takim punkcie, w jakim jest. Otwartoźródłowa natura sieci Bitcoin i zgromadzona wokół niej społeczność także przyczyniły się do szerszego przyjęcia na samym początku. Fundamentalne cechy kryptowalut pochodzą od tej właśnie sieci i przyjrzymy się im w następnym rozdziale.

[24] *https://thenextweb.com/news/a-brief-history-of-mt-gox-the-3b-bitcoin-tragedy-that-just-wont-end*

Łańcuch bloków: zostań mistrzem technologii jutra!

Blockchain, czyli łańcuch bloków, niefortunnie kojarzy się z kryptowalutami i przestępczością. Tymczasem potencjał tej technologii jest ogromny i zapewne wciąż nie znamy wszystkich możliwych jej zastosowań. Łańcuch bloków jest w istocie publicznym rejestrem, który może się stać ogólnoświatową, zdecentralizowaną księgą służącą do rejestrowania, inwentaryzacji i organizowania transferów wszelkiego rodzaju aktywów. Najwyższy więc czas, aby emocje i sensacyjno-kryminalne wyobrażenia dotyczące blockchaina zastąpić zrozumieniem tej technologii i aktualną wiedzą.

Ta książka jest przeznaczona dla osób chcących zrozumieć działanie łańcucha bloków i rozważających praktyczne zastosowanie tej technologii. Skorzystają z niej i menedżerowie, i specjaliści IT. Omówiono tu ewolucję blockchaina i najróżniejsze sposoby jego użycia — przy czym to wyjaśnienie wychodzi daleko poza tematykę kryptowalut. Zaprezentowano też tematykę tworzenia inteligentnych kontraktów i zdecentralizowanych aplikacji z uwzględnieniem problemów wiążących się z tymi zastosowaniami łańcucha bloków. Nie zabrakło sprawdzonych informacji dotyczących naruszania prawa z wykorzystaniem łańcucha bloków, na przykład prania brudnych pieniędzy, hakowania giełd czy kradzieży. Dzięki temu przewodnikowi można łatwo zrozumieć, czym blockchain jest, a czym nie jest, do czego się nadaje i jakie modele biznesowe szczególnie mogą skorzystać na tej technologii.

W książce między innymi:

- najważniejsze koncepcje dotyczące bitcoina i łańcucha bloków
- możliwości technologii blockchain
- skalowalność i rozwidlenia łańcucha bloków
- Ethereum i inne łańcuchy bloków
- możliwe sposoby zastosowania łańcucha bloków
- perspektywy technologii blockchain

Lorne Lantz jest inżynierem i przedsiębiorcą. Napisał Breadcrumbs, narzędzie do analizowania łańcuchów bloków. Zajmował się też usługami przekazów bitcoinowych, portfela kryptowalutowego, bitcoinowego systemu sprzedaży i kryptoplatformy traderskiej.

Daniel Cawrey od niemal dekady rozwija projekty oparte na technologii łańcucha bloków. Przez kilka lat prowadził kryptowalutowy fundusz hedgingowy i zajmował się doradztwem w tym zakresie.

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 978-83-283-9361-5
9 788328 393615
Cena: 69,00 zł