



Apress®

Blockchain

Podstawy technologii łańcucha
bloków w 25 krokach

—
Daniel Drescher

Helion 

Tytuł oryginału: Blockchain Basics: A Non-Technical Introduction in 25 Steps

Tłumaczenie: Leszek Sielicki

ISBN: 978-83-283-8486-6

Original edition copyright © 2017 by Daniel Drescher
All rights reserved.

Polish edition copyright © 2019, 2021 by Helion S.A.
All rights reserved.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Helion S.A.

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/blockv>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

O autorze	5
O korektorze merytorycznym	6
Wprowadzenie	7
Faza I Terminologia i założenia techniczne	11
Etap 1 Rozumowanie w kategoriach warstw i aspektów	13
Etap 2 Spojrzenie z szerokiej perspektywy	19
Etap 3 Identyfikacja potencjału	27
Faza II Dlaczego łańcuch bloków jest potrzebny	33
Etap 4 Określenie podstawowego problemu	35
Etap 5 Ujednoznacznianie terminu	39
Etap 6 Własność, co to takiego?	43
Etap 7 Wydawanie pieniędzy podwójnie	51
Faza III Jak działa łańcuch bloków	57
Etap 8 Planowanie łańcucha bloków	59
Etap 9 Dokumentowanie własności	65
Etap 10 Haszowanie danych	71
Etap 11 Wykorzystywanie skrótów w praktyce	79
Etap 12 Identyfikacja i ochrona kont użytkowników	89
Etap 13 Autoryzowanie transakcji	97
Etap 14 Przechowywanie danych transakcyjnych	103

Etap 15	Wykorzystywanie repozytorium danych	115
Etap 16	Ochrona repozytorium danych	125
Etap 17	Rozpraszanie repozytorium danych pomiędzy uczestnikami systemu	133
Etap 18	Weryfikowanie i dodawanie transakcji	139
Etap 19	Wybór historii transakcji	149
Etap 20	Cena integralności	163
Etap 21	Łączenie komponentów w całość	169
Faza IV	Ograniczenia i sposoby ich przewyżczenia	181
Etap 22	Dostrzeganie ograniczeń	183
Etap 23	Łącuch bloków na nowo	189
Faza V	Korzystanie z łańcucha bloków, podsumowanie i przegląd	197
Etap 24	Korzystanie z łańcucha bloków	199
Etap 25	Podsumowanie i perspektywy	209
Skorowidz		221

Planowanie łańcucha bloków

Podstawowe koncepcje zarządzania własnością za pomocą łańcucha bloków

Na wcześniejszych etapach ustaliliśmy istnienie związku pomiędzy zaufaniem, integralnością, całkowicie rozproszonymi systemami *peer-to-peer* i łańcuchem bloków. W efekcie tych ustaleń dobrze rozumiesz, czym jest łańcuch bloków, dlaczego jest potrzebny i jaki problem rozwiązuje. Nadal nie znasz jednak wewnętrznego sposobu funkcjonowania łańcucha bloków. Na tym etapie dowiesz się w zarysie, jak działała łańcuch bloków, zapoznając się z ogólnym scenariuszem jego stosowania, który poprowadzi Cię przez kolejne etapy. Omówimy także główne zadania związane z projektowaniem łańcucha bloków do celów zarządzania własnością oraz przyjrzymy się podstawowym koncepcjom z nim związanym. Ten etap jest punktem wyjścia do kolejnych, w których szczegółowo omówimy koncepcje i technologie składające się na łańcuch bloków.

Cel

Celem naszych aktualnych rozważań będzie zrozumienie koncepcji składających się na pojęcie łańcucha bloków. Ze względów dydaktycznych zajmiemy się działaniami związanymi z tworzeniem własnego systemu zarządzania własnością. Stanesz więc przed takimi samymi problemami, z jakimi musiał się kiedyś zmierzyć i jakie z powodzeniem rozwiązał wynalazca łańcucha bloków. Chodzi o opracowanie programu zarządzającego własnością w całkowicie rozproszonym systemie *peer-to-peer*, który będzie działał w bezwzględnie otwartym i niezaufanym środowisku.

Punkt początkowy

Oto punkt wyjścia — podstawowe fakty dotyczące rozważanego systemu możemy zestawić w następujący sposób:

- System będzie całkowicie rozproszonym systemem *peer-to-peer*, składającym się z zasobów obliczeniowych udostępnianych przez jego użytkowników.
- System *peer-to-peer* wykorzystuje Internet jako sieć łączącą poszczególne węzły.
- Ani liczba węzłów, ani ich wiarygodność i poziom zaufania nie są znane.
- Celem systemu *peer-to-peer* jest zarządzanie własnością dobra cyfrowego (np. punktów premialnych lub cyfrowej waluty).

Ścieżka postępowania

Istnieje siedem głównych zadań, którymi należy się zająć podczas opracowywania i tworzenia oprogramowania zarządzającego własnością z wykorzystaniem całkowicie rozproszonego systemu *peer-to-peer* w otwartym i niezaufanym otoczeniu. Oto one:

- opis własności,
- ochrona własności,
- przechowywanie danych transakcji,
- przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku,
- rozpraszenie rejestrów,
- dodawanie nowych transakcji do rejestrów,
- określanie, które rejestry odpowiadają prawdzie.

Zadanie 1. Opis własności

Zanim zaczniemy tworzyć łańcuch bloków, musimy zadać sobie pytanie, co zamierzamy z nim zrobić. Ponieważ będziemy chcieli zaprojektować system oprogramowania, który zarządza własnością, musimy najpierw zdecydować, jak tę własność opisać. Okazuje się, że dobrym sposobem opisu wszelkiego rodzaju przeniesień własności są transakcje, a pełna historia transakcji jest kluczem do identyfikacji aktualnych właścicieli. Na etapie 9 zajmujemy się więc transakcjami, ustalając, czym są, jak można je opisywać i wykorzystywać do ustalania własności.

Zadanie 2. Ochrona własności

Opis własności za pomocą transakcji to tylko punkt wyjścia. Niezbędny jest także sposób, aby uniemożliwić niepowołanym osobom uzyskiwanie dostępu do własności innych. W codziennym życiu łatwo jest uniemożliwić obcym skorzystanie z naszego samochodu czy wejście do naszego domu za sprawą drzwi zaopatrzonych w zamki. Okazuje się, że sposób ochrony transakcji na poziomie indywidualnym, przypominający drzwi z zamkami, które chronią samochód lub dom, zapewnia kryptografia.

Ochrona własności składa się z trzech podstawowych elementów, którymi są: identyfikacja i uwierzytelnianie właścicieli oraz umożliwianie dostępu do przedmiotu własności wyłącznie jego właścicielom. W ramach etapów 12 i 13 wyjaśnimy te pojęcia bardziej szczegółowo, posługując się koncepcją wartości skrótu. Jeżeli nigdy wcześniej nie słyszałeś o wartościach skrótu, nie ma powodów do obaw. Ich szczegółowe wyjaśnienie zawiera treść etapów 10 i 11. Interesujące informacje znajdują w nich jednak także czytelnicy dysponujący wykształceniem technicznym lub wiedzą o wartościach skrótu.

Zadanie 3. Przechowywanie danych transakcyjnych

Opisywanie własności za pomocą transakcji i posiadanie środków bezpieczeństwa, które chronią własność na poziomie poszczególnych transakcji, to istotne etapy na drodze do zaprojektowania systemu oprogramowania, który będzie zarządzał własnością. Niezbędny jest jednak także sposób przechowywania całej historii transakcji, bo historia ta służy do ustalania własności. Historia transakcji jest fundamentalnym składnikiem procesu ustalania własności, więc musi być przechowywana w bezpieczny sposób. Okazuje się, że struktura danych łańcucha bloków jest cyfrowym odpowiednikiem rejestru. W ramach etapów 14 i 15 zapoznamy się z wymaganiami, jakie musi spełniać struktura danych łańcucha bloków, aby służyć jako cyfrowy rejestr, i dowiemy się, jaki jest sposób jej implementacji.

Zadanie 4. Przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku

Dobrze jest posiadać jeden wyizolowany rejestr czy też strukturę danych łańcucha bloków, która zawiera dane transakcyjne, ale naszym celem jest zaprojektowanie rozproszonego systemu *peer-to-peer*, który będzie działał w niezaufanym środowisku. Kopie rejestru będą więc funkcjonować w niezaufanych węzłach i w niezaufanej sieci. Co więcej, kontrolę nad rejestrami przekazemy całej sieci, bez centralnego punktu kontrolnego lub koordynacyjnego. Jak w takiej sytuacji zapobiec fałszowaniu rejestrów lub manipulowaniu nimi (np. poprzez usuwanie transakcji z historii lub dodawanie do niej transakcji nielegalnych)? Okazuje się, że najlepszym sposobem zapobiegania wprowadzaniu zmian w historii transakcji jest sprawienie, aby była ona niemożliwa do zmiany. Oznacza to, że rejestrów — i tym samym historii transakcji — nie można zmieniać po ich zapisaniu. W efekcie nie będziemy musieli się obawiać, że rejestry zostaną zmanipulowane lub sfalszowane, bo po prostu nie da się ich zmienić. Jednakże posiadanie rozproszonego systemu *peer-to-peer*, do którego niemożliwe jest wprowadzanie zmian, wydaje się być czymś wyjątkowo bezpiecznym, ale za to okazuje się zupełnie bezużyteczne, bo nie da się dodawać do niego nowych transakcji. Dlatego też wyzwaniem dla struktury danych łańcucha bloków polega na tym, aby była ona z jednej strony niezmienna, a z drugiej przyjmowała nowe transakcje. Samo w sobie brzmi to jak sprzeczność, ale okazuje się, że jest możliwe dzięki sztuczce technicznej, którą wyjaśnimy na etapie 16. W efekcie jej zastosowania powstaje struktura danych łańcucha bloków z atrybutem „tylko-do-dopisywania”: możliwe jest dodawanie nowych transakcji, ale praktycznie nie da się wprowadzać zmian w danych, które zostały dodane w przeszłości.

Zadanie 5. Rozpraszanie rejestrów

Gdy rejestr ma atrybut „tylko-do-dopisywania”, można stworzyć rozproszony system rejestrów *peer-to-peer*, udostępniając jego kopie każdemu, kto o to wystąpi. Samo udostępnianie kopii rejestrów tylko do dopisywania nie spełni jednak zakładanych celów. Rozproszony system zarządzający własnością oznacza interakcje między uczestnikami czy też węzłami. Dlatego na etapie 17 wyjaśnimy, w jaki sposób węzły systemu współdziałają ze sobą i jakimi informacjami się wymieniają.

Zadanie 6. Dodawanie nowych transakcji do rejestrów

Rozproszony system *peer-to-peer* składa się z uczestników, których komputery przechowują poszczególne kopie struktury danych łańcucha bloków z atrybutem „tylko-do-dopisywania”. Ponieważ struktura danych pozwala na dodawanie nowych danych transakcyjnych, należy sprawić, aby dodawane były wyłącznie prawidłowe i autoryzowane transakcje. Okazuje się, że jest to możliwe dzięki zezwoleniu wszystkim uczestnikom systemu *peer-to-peer* na dodawanie nowych danych i dodatkowo przekształceniu wszystkich uczestników systemu *peer-to-peer* w nadzorców innych uczestników. W efekcie wszyscy uczestnicy systemu będą się wzajemnie nadzorować i wskazywać błędy popełniane przez „ich” uczestników. Na etapie 18 wyjaśnimy tę kwestię bardziej szczegółowo, a także zajmiemy się zagadnieniem zapewniania motywacji uczestników systemu, tak aby wypełniali te funkcje.

Zadanie 7. Określanie, które rejestry odpowiadają prawdzie

Gdy można już dodawać nowe transakcje do poszczególnych rejestrów w systemie *peer-to-peer*, pojawia się problem typowy dla każdego rozproszonego systemu *peer-to-peer*: do różnych użytkowników mogą docierać różne transakcje, co powoduje, że historie przechowywanych przez nich transakcji będą się różnić. W związku z tym w systemie *peer-to-peer* mogą funkcjonować różne wersje historii transakcji. Ponieważ historia transakcji jest podstawą identyfikacji uprawnionych właścicieli, dysponowanie różnymi sprzecznymi historiami transakcji stanowi poważne zagrożenie dla integralności systemu. Dlatego istotne jest, aby znaleźć sposób umożliwiający albo zapobieganie pojawianiu się różnych historii transakcji, albo decydowanie, która historia transakcji odpowiada prawdzie. Ze względu na charakter całkowicie rozproszonego systemu *peer-to-peer* zastosowanie pierwszej z metod nie jest możliwe. W efekcie musimy określić, na podstawie jakiego kryterium będziemy ustalać i wybierać jedną historię transakcji, którą uznamy za prawdziwą. I jest jeszcze jeden problem: w całkowicie rozproszonym systemie *peer-to-peer* nie ma organu centralnego, który mógłby określić, którą historię transakcji należałoby wybrać. Okazuje się, że problem ten można rozwiązać, umożliwiając każdemu z węzłów systemu *peer-to-peer* samodzielne decydowanie, która historia transakcji odpowiada prawdzie, w taki sposób, aby większość uczestników systemu niezależnie zgodziła się z tą decyzją. Okazuje się także, że rozwiązanie tego problemu zawiera sam sposób, w jaki łańcuch bloków umożliwia dodawanie nowych transakcji do struktury danych łańcucha bloków z atrybutem „tylko-do-dopisywania”. Kryteria te i sposób ich stosowania wyjaśnimy szczegółowo na etapie 19.

Streszczenie

Na tym etapie określiliśmy siedem zadań, tworzących etapy pełnej wyzwania intelektualnej podróży w świat koncepcji opisujących łańcuch bloków. Po wykonaniu tych zadań zdobędziemy szczyt: zrozumiemy łańcuch bloków. Na etapie 21 połączymy wszystkie te koncepcje i będziemy mogli cieszyć się efektami nabytej wiedzy. Etap 21 to rozdział podsumowujący, jak ten, ale wymagający wiedzy technicznej, którą zdobędziesz podczas dalszej lektury.

Podsumowanie

- Aby zaprojektować całkowicie rozproszony system rejestrów *peer-to-peer* w celu zarządzania własnością, należy odnieść się do następujących zadań, którymi są:
 - opis własności,
 - ochrona własności,
 - przechowywanie danych transakcji,
 - przygotowywanie rejestrów do rozproszenia w niezaufanym środowisku,
 - rozpraszanie rejestrów,
 - dodawanie nowych transakcji do rejestrów,
 - określanie, które rejestry odpowiadają prawdzie.
- Zadania opisane powyżej zostaną omówione na kolejnych 12 etapach.

Skorowidz

A

abstrakcja, 178
agregowanie danych transakcyjnych, 68
algorytm, 40
analiza
 systemów, 13
 zastosowań łańcucha bloków, 203
aplikacja, 14, 15, 172
architektura
 oprogramowania, 19
 rozproszona, 21
 scentralizowana, 21
 peer-to-peer, 176, 192
aspekty
 funkcjonalne, 14, 15, 20, 172
 warstwy aplikacji, 172
 warstwy implementacji, 174
 niefunkcjonalne, 14, 15, 20, 172
autoryzacja, 46, 69
 transakcji, 95, 97

B

bezpieczeństwo, 51, 173, 190
 transakcji, 175
bloki-sieroty, 156
brak
 elastyczności, 186
 prywatności, 184
budowanie zaufania, 163

C

cel łańcucha bloków, 25
cele rejestru, 47
cena integralności, 163

D

dane
 inwentaryzacyjne, 66, 214
 transakcyjne, 66, 103
definicja
 systemu peer-to-peer, 30
 łańcucha bloków, 39
dodawanie
 bloku, 153
 transakcji, 116, 139
dokumentowanie własności, 65
 historia przeniesień własności, 67
 koncepcja, 66
 opis przenoszenia własności, 67
dostępność, 173
dowód
 autorstwa, 201
 czasu, 201
 istnienia, 200
 nieistnienia, 200
 tożsamości, 201
 uporządkowania, 201
 własności, 202
drzewo, 84
 Merkle'a, 118
dystrybucja kluczy, 93
działanie łańcucha bloków, 57

E

elastyczność, 173

F

filozofia systemu, 165

funkcja

 jednokierunkowa, 73

 skrót, 72

H

haszowanie

 danych, 71

 hierarchiczne, 77

 łączone, 76

 niezależne, 75

 powtarzalne, 75

 sekwencyjne, 76

historia transakcji, 149

I

identyfikacja, 46

 kont, 94

 obiektów własności, 90

 oszustw, 100

 właścicieli, 90

implementacja, 14, 15, 172

integralność, 15, 174, 206

 historii transakcji, 68

 systemu, 164

K

klucze, 93

konsensus, 212

koszty, 163, 185

 manipulowania strukturą danych, 130

kryptografia, 90, 91

 asymetryczna, 92–94

 symetryczna, 91

kryptograficzne funkcje skrót, 72, 78

kryterium

 najcięższego łańcucha, 155

 najdłuższego łańcucha, 152

książka

 po transformacji, 109

 przed transformacją, 108

L

lista powiązana, 84

logika

 konsensusu, 177

 przechowywania, 176

 przetwarzania transakcji, 175, 176

 własności, 174

luki bezpieczeństwa, 51

Ł

łańcuch, 84

 bloków, 171, 194

 alternatywy, 210

 analiza zastosowań, 203

 aspekty, 172

 aspekty funkcjonalne warstwy aplikacji,
 172

 aspekty niefunkcjonalne, 172

 cechy, 200

 definicja, 41

 haszowanie, 88

 ograniczenia pozatechniczne, 187

 ograniczenia techniczne, 184, 190

 osiągnięcia, 214

 pakiet technologii, 178

 planowanie, 59

 przechowywanie transakcji, 111

 rola opłat, 164

 rozwiązywanie konfliktów, 191

 rozwój, 210

 sprzeczne cele, 189

 struktura danych, 109

 szczególne przypadki stosowania, 202

 techniczne koncepcje, 170

 transformacja książki, 104

 wady, 217

 warstwy, 172

 wersje, 192

 weryfikacja celu, 194

 wzorce stosowania, 200

 zastosowania, 41, 197

łączenie

 komponentów, 169

 komputerów, 35

 systemów, 24

M

manipulowanie strukturą danych, 130
 metoda prywatno-publiczna, 94
 model bezpieczeństwa, 184

N

naruszanie integralności, 53
 nawiązywanie nowych połączeń, 136
 niezmiennosc, 127

O

ochrona
 kont użytkowników, 89
 repozytorium danych, 125
 odporność
 na cenzurę, 173
 na kolizje, 73
 na manipulacje, 159
 odwoływanie się do danych, 81
 ograniczenia, 181, 183
 pozatechniczne, 188
 techniczne, 184, 187
 techniczne łańcucha bloków, 190
 skalowalność, 185
 osiągnięcie abstrakcji, 178
 ostateczna spójność, 173
 otwartość systemu, 165, 173

P

pakiet technologii, 40
 łańcucha bloków, 178
 planowanie łańcucha bloków, 59
 początek łańcucha, 84
 podpis elektroniczny, 98
 identyfikowanie oszustw, 100
 podpisywanie transakcji, 101
 weryfikowanie danych, 99
 podwójne wydatkowanie środków, 52–55
 poprawność
 formalna, 68
 semantyczna, 69
 porównywanie danych, 79
 potencjał
 łańcucha bloków, 31
 systemów peer-to-peer, 28
 poziom dostępności, 173
 prawa dostępu, 211

problem
 kopiowania dóbr cyfrowych, 53
 podwójnego wydatkowania środków, 52,
 53
 rozproszonych systemów rejestrów
 peer-to-peer, 53
 projektowanie rozproszonego systemu
 peer-to-peer, 170
 prywatność, 190, 212
 przechowywanie danych, 83
 transakcyjnych, 103, 111
 przenoszenie własności, 67
 pseudoanonimowość, 173
 pseudolosowość, 72

R

referencja
 nieważna, 82
 prawidłowa, 82
 rejestr, 47
 repozytorium danych, 115
 dodawanie nowych transakcji, 116
 niezmiennosc, 127, 131
 ochrona, 125
 rozpraszanie, 133
 wykrywanie zmian, 118
 zmiana danych, 121
 rozpowszechnianie informacji, 137
 rozpraszanie repozytorium danych, 133, 165
 rozwiązywanie konfliktów, 191

S

scentralizowanie, 185
 schemat
 głosowania, 159
 referencji zerwanej, 82
 sieci typu peer-to-peer, 23
 skalowalność, 185
 skrót
 do kryptografii, 90
 do podpisów elektronicznych, 98
 spójność, 158
 struktura danych, 39, 214
 łańcucha bloków, 109, 152, 154
 system
 peer-to-peer, 28
 architektura, 30
 definicja, 30
 integralność, 36
 zagrożenia integralności, 36

system
 zaufanie, 36
 związek z łańcuchem bloków, 31
 płatności, 20
 systemy rozproszone
 integralność, 25
 łańcuch bloków, 109, 152, 154
 peer-to-peer, 23
 rozpoznawanie, 25
 wady, 22
 zalety, 21
 szybkość, 190

Ś

świadek, 44

T

techniczne koncepcje łańcucha bloków, 170
 transakcje, 97, 101, 213
 dodawanie, 139
 weryfikowanie, 139
 wybór historii, 149
 zasady, 145
 zastępowanie, 119
 transformacja książki, 104
 transparentność, 190
 tworzenie
 bloku, 129
 kluczy, 93
 oprogramowania zarządzającego
 własnością, 60
 podpisu, 98

U

uczciwość, 163
 utrzymywanie istniejących połączeń, 136
 uwierzytelnienie, 46

W

walidacja, 129, 141
 waluty
 fiducjarne, 166
 kryptograficzne, 166
 warstwa, 15
 systemu oprogramowania, 14
 weryfikowanie
 danych, 99
 transakcji, 139

wiarygodność, 173
 wielkość krytyczna, 186
 własność, 41, 43, 48
 bezpieczeństwo, 45
 dokumentowanie, 65
 koncepcje, 45
 przenoszenie, 67
 założenia, 44
 właściwości
 instrumentu płatniczego, 165
 łańcucha bloków, 172
 rejestr, 47
 wpływ
 na filozofię systemu, 165
 na integralność systemu, 164
 na otwartość systemu, 165
 na rozproszony charakter systemu, 165
 wspólny pień, 158
 wybór
 historii transakcji, 149
 instrumentu płatniczego, 164
 jednego łańcucha, 156
 wykrywanie zmian danych, 80, 118
 wynagradzanie uczestników systemu, 165
 wzorce haszowania danych, 74

Z

zachowywanie integralności, 174
 zagadki kryptograficzne, 86, 160
 zarządzanie własnością, 41
 zasady walidacji, 129, 141
 dla danych transakcyjnych, 141
 dla nagłówków bloków, 142
 zastępowanie transakcji, 119
 zmiana
 danych w uporządkowany sposób, 121
 korzenia drzewa Merkle'a, 120
 referencji, 118
 referencji nagłówka bloku, 120
 treści danych transakcyjnych, 118
 zmiany
 niezamierzone, 122
 zamierzone, 122
 zrywanie referencji, 127

Ź

źródła konfliktów, 190

PROGRAM PARTNERSKI

— GRUPY HELION —

- 
1. ZAREJESTRUJ SIĘ
 2. PREZENTUJ KSIĄŻKI
 3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion

Łańcuch bloków. Czym jest? Do czego się przyda? W jaki sposób działa?

W pewnym uproszczeniu łańcuch bloków (blockchain) jest rozproszoną bazą danych, która utrzymuje stale rosnącą liczbę rekordów danych zabezpieczonych kryptograficznie przed manipulacją i próbą naruszenia integralności. Może posłużyć jako rozproszona księga rachunkowa. Technologia ta cieszy się dużym zainteresowaniem, a niektórzy entuzjaści nazywają ją nawet przełomową. Aby zrozumieć, do czego łańcuch bloków może się przydać, poprawnie ocenić uzasadnienie biznesowe startupów wykorzystujących łańcuch bloków czy też móc śledzić dyskusję na temat jego oczekiwanych efektów ekonomicznych, konieczne jest zrozumienie podstawowych pojęć związanych z technologią blockchain i uświadomienie sobie jej potencjalnych zastosowań.

Ta publikacja stanowi przystępne wprowadzenie do założeń technologii łańcucha bloków. Poszczególne pojęcia przedstawiono bez nadmiernej liczby szczegółów technicznych. Dzięki książce można przyswoić takie koncepcje związane z łańcuchem bloków jak transakcje, wartości haszujące, kryptografia, struktury danych, systemy peer-to-peer, systemy rozproszone, integralność systemu i konsensus w systemach rozproszonych. Książka została napisana w stylu konwersacyjnym, w sposób umożliwiający etapowe, stopniowe poznawanie problematyki. Matematyczne podstawy kryptografii i algorytmów zostały celowo pominięte, a zamiast tego zastosowano metafory i analogie. Dzięki temu zawarte tu treści będą zrozumiałe nawet dla czytelników bez przygotowania technicznego.

W książce między innymi:

- główne koncepcje inżynierii programowania i potrzebna terminologia
- zastosowanie łańcucha bloków i zalety tej technologii
- wewnętrzne zasady działania łańcucha bloków
- ograniczenia łańcucha bloków i sposoby ich przewycięzania
- omówienie kierunków prac rozwojowych nad technologią
- wykorzystywanie łańcucha bloków w warunkach rzeczywistych

Dr Daniel Drescher zawodowo zajmuje się bankowością. Od wielu lat pracuje w różnych bankach. Specjalizuje się w elektronicznym obrocie papierami wartościowymi. Jest ekspertem w dziedzinie automatyzacji, uczenia maszynowego i zagadnień big data w kontekście obrotu papierami wartościowymi.

  helion.pl	<i>Sprawdź nasze szkolenia!</i>  AKADEMIA IT & BUSINESS WWW.SZKOLENIA.HELION.PL	KOD KORZYŚCI <i>Sięgnij po więcej!</i>  ISBN 978-83-283-8486-6  9 788328 384866
INFORMATYKA W NAJLEPSZYM WYDANIU		Cena: 59,00 zł

Apress®