

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.

Niniejsza publikacja stanowi przystępne wprowadzenie do założeń technologii łańcucha bloków. Poszczególne pojęcia przedstawiono bez nadmiernej liczby szczegółów technicznych. Dzięki książce można przyswoić sobie 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 Czytelnika 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

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 PRZEZWYCIĘŻANIA 181

Etap 22. Dostrzeganie ograniczeń 183

Etap 23. Łańcuch 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