

[opis]

Inflacja, sterowane kryzysy gospodarcze, pękające bańki, afery związane z udzielaniem kredytów i zadłużaniem się - to tylko kilka problemów, których doświadczamy w efekcie scentralizowanej bankowości powiązanej z polityką. Z drugiej strony bitcoin i łańcuch bloków kojarzą się z mrocznym półświatkiem i łatwymi pieniędzmi, przez co rozbudzają ludzkie lęki i chciwość. Jeśli jednak odsunie się na bok wątki sensacyjne, łatwo zauważyć, że zdecentralizowana cyfrowa waluta ma potencjał wyrwania wielu ważnych aspektów naszego życia spod kontroli polityków i bankowców. Aby jednak trafnie ocenić przydatność bitcoina w niepowtarzalnej, osobistej sytuacji, trzeba dobrze pojąć tę koncepcję i zasady, na których się opiera.

Dzięki tej książce zrozumiesz mechanizmy rządzące technologią bitcoina oraz łańcucha bloków. Poznasz też wiele koncepcji leżących u podstaw bitcoina, takich jak podpisy cyfrowe, dowód pracy oraz sieci peer-to-peer. Dowiesz się, jak zainstalować i korzystać z portfela bitcoina, jak przechowywać klucze prywatne oraz jak uruchomić pełny węzeł bitcoina, a także ? jak rozpoznawać fałszywe deklaracje oszustów liczących na łatwy zysk. Aby w pełni skorzystać z zawartych tu informacji, nie musisz dysponować umiejętnością programowania ani zaawansowaną wiedzą techniczną i matematyczną. Dzięki przystępnemu językowi i łatwym do przyswojenia schematom zrozumiesz, czym w rzeczywistości jest bitcoin i czym może się stać w niedalekiej przyszłości.

Najważniejsze zagadnienia:

- solidne podstawy bitcoina
- anatomia transakcji bitcoinowych
- adresy odbiorców i portfele w sieci bitcoina
- łańcuch bloków i kopanie bitcoina
- nowości w zaktualizowanym protokole bitcoina

Bitcoin: zrozum, czym jest ta przełomowa technologia!

[spis]

- Przedmowa (xiii)
- Wprowadzenie (xv)
- Podziękowania (xvii)
- O tej książce (xix)
- Informacje o autorze (xxiii)

1. Wprowadzenie do bitcoina (1)

- Czym jest bitcoin? (2)
- Jak to działa? (3)
- Dzisiejsze problemy z pieniędzmi (10)
- Podejście Bitcoina (13)

- Do czego wykorzystuje się bitcoiny? (16)
- Inne kryptowaluty (23)
- Najważniejsze kwestie w skrócie (25)

2. Kryptograficzne funkcje skrótu i podpisy cyfrowe (27)

- Tabelka tokenów ciasteczkowych (28)
- Skróty kryptograficzne (32)
- Ćwiczenia (40)
- Podpisy cyfrowe (42)
- Podsumowanie (55)
- Ćwiczenia (58)
- Najważniejsze kwestie w skrócie (59)

3. Adresy (61)

- Ujawnienie ciasteczkożerców (62)
- Zastąpienie imion kluczami publicznymi (63)
- Skracanie klucza publicznego (66)
- Unikanie kosztownych literówek (70)
- Jeszcze raz prywatność (78)
- Podsumowanie (79)
- Ćwiczenia (81)
- Najważniejsze kwestie w skrócie (83)

4. Portfele (85)

- Pierwsza wersja portfela (86)
- Kopie zapasowe kluczy prywatnych (89)
- Hierarchiczne portfele deterministyczne (93)
- Jeszcze raz kopia zapasowa (100)
- Rozszerzone klucze publiczne (104)
- Generowanie wzmocnionych kluczy prywatnych (108)
- Matematyka klucza publicznego (110)
- Mnożenie klucza publicznego (111)
- Podsumowanie (117)
- Ćwiczenia (119)
- Najważniejsze kwestie w skrócie (121)

5. Transakcje (123)

- Problemy ze starym systemem (124)
- Obsługa płatności z użyciem transakcji (125)
- Język Script (134)
- Nietypowe płatności (140)
- Więcej rzeczy w transakcjach (151)
- Wynagrodzenie i bicie monet (151)
- Zaufanie do Eli (153)
- Podsumowanie (155)
- Ćwiczenia (158)

- Najważniejsze kwestie w skrócie (159)

6. Łańcuch bloków (161)

- Ela może usuwać transakcje (162)
- Tworzenie łańcucha bloków (162)
- Lekkie portfele (173)
- Drzewa skrótów (182)
- Bezpieczeństwo lekkich portfeli (190)
- Podsumowanie (192)
- Ćwiczenia (196)
- Najważniejsze kwestie w skrócie (199)

7. Dowód pracy (201)

- Sklonujmy Ełę! (202)
- Wymuszanie uczciwości podczas losowania (211)
- Górnicy muszą się wynieść (219)
- Dopasowanie trudności (222)
- Jakie szkody mogą wyrządzić górnicy? (226)
- Opłaty transakcyjne (235)
- Podsumowanie (241)
- Ćwiczenia (244)
- Najważniejsze kwestie w skrócie (245)

8. Sieć peer-to-peer (247)

- Katalog sieciowy (249)
- Budujemy sieć peer-to-peer (250)
- Jak komunikują się ze sobą węzły? (252)
- Protokół sieciowy (253)
- Żegnamy się z systemem tokenów ciasteczkowych (264)
- Przygotowywanie sieci (267)
- Własny pełny węzeł (278)
- Podsumowanie (288)
- Ćwiczenia (292)
- Najważniejsze kwestie w skrócie (294)

9. Więcej o transakcjach (295)

- Transakcje z blokadą czasową (296)
- Wyjścia z blokadą czasową (301)
- Przechowywanie informacji w łańcuchu bloków Bitcoin (308)
- Zastępowanie transakcji oczekujących na zatwierdzenie (314)
- Różne typy podpisów (318)
- Podsumowanie (320)
- Ćwiczenia (322)
- Najważniejsze kwestie w skrócie (323)

10. Segwit (325)

- Problemy rozwiązywane przez segwit (326)
- Rozwiązania (335)
- Kompatybilność portfela (350)
- Podsumowanie rodzajów płatności (352)
- Limity bloków (353)
- Podsumowanie (357)
- Ćwiczenia (360)
- Najważniejsze kwestie w skrócie (362)

11. Aktualizacje protokołu Bitcoin (363)

- Forki protokołu Bitcoin (364)
- Powtórzenie transakcji (375)
- Mechanizmy aktualizacji (378)
- Podsumowanie (391)
- Ćwiczenia (394)
- Najważniejsze kwestie w skrócie (395)

Dodatek A. Praca z Bitcoinem w wierszu poleceń (397)

- Komunikacja z demonem bitcoind (397)
- Graficzny interfejs użytkownika (398)
- Poznajemy bitcoin-cli (399)
- Rozpoczynanie pracy (400)

Dodatek B. Rozwiązania ćwiczeń (413)

- Rozdział 2. (413)
- Rozdział 3. (414)
- Rozdział 4. (415)
- Rozdział 5. (416)
- Rozdział 6. (418)
- Rozdział 7. (420)
- Rozdział 8. (421)
- Rozdział 9. (423)
- Rozdział 10. (424)
- Rozdział 11. (425)

Dodatek C. Zasoby internetowe (429)