

Spis treści

O autorze	13
O recenzencie	14
Przedmowa	15
Rozdział 1. ABC łańcucha bloków	21
Rozwój technologii łańcucha bloków	21
Systemy rozproszone	24
Historia łańcucha bloków i Bitcoina	26
Elektroniczne pieniądze	26
Łańcuch bloków	27
Uniwersalne elementy łańcucha bloków	31
Zalety i ograniczenia łańcucha bloków	34
Warstwy łańcucha bloków	36
Cechy łańcucha bloków	37
Typy łańcuchów bloków	39
Rozproszone rejestry	40
Technologia DLT	40
Publiczne łańcuchy bloków	41
Prywatne łańcuchy bloków	41
Wspólny rejestr	42
W pełni prywatne i zastrzeżone łańcuchy bloków	42
Łańcuchy bloków z tokenami	43
Łańcuchy bloków bez tokenów	43
Konsensus	43
Mechanizmy osiągania konsensusu	43
Rodzaje mechanizmów osiągania konsensusu	44
Konsensus w łańcuchu bloków	45
Twierdzenie CAP i łańcuch bloków	47
Podsumowanie	49
Rozdział 2. Decentralizacja	51
Decentralizacja z użyciem łańcucha bloków	51
Metody decentralizacji	53
Eliminowanie pośrednictwa	53
Decentralizacja oparta na współzawodnictwie	54
Drogi do decentralizacji	55

Jak przeprowadzić decentralizację?	56
Przykładowy schemat analizy decentralizacji	56
Łańcuch bloków i kompletny ekosystem związany z decentralizacją	57
Składowanie danych	57
Komunikacja	58
Decentralizacja a moc obliczeniowa	59
Inteligentne kontrakty	60
Zdecentralizowane organizacje	61
Zdecentralizowane organizacje autonomiczne	61
Zdecentralizowane korporacje autonomiczne	62
Zdecentralizowane społeczności autonomiczne	62
Zdecentralizowane aplikacje (DApps)	62
Wymogi stawiane zdecentralizowanym aplikacjom	63
Operacje w zdecentralizowanych aplikacjach	63
Platformy do decentralizacji	64
Ethereum	64
MaidSafe	64
Lisk	65
Podsumowanie	65
Rozdział 3. Kryptografia symetryczna	67
Korzystanie z narzędzia OpenSSL w wierszu poleceń	67
Wprowadzenie	68
Matematyka	69
Kryptografia	70
Poufność	71
Integralność	71
Uwierzytelnianie	71
Niezaprzeczalność	72
Rozliczalność	73
Podstawowe mechanizmy kryptograficzne	73
Kryptografia symetryczna	74
DES	79
AES	79
Podsumowanie	83
Rozdział 4. Kryptografia klucza publicznego	85
Kryptografia asymetryczna	85
Rozkład liczb całkowitych na czynniki	87
Logarytm dyskretny	87
Krzywe eliptyczne	87
Klucze publiczny i prywatny	88
RSA	88
Problem logarytmu dyskretnego w ECC	94
Funkcje skrótu	102

Algorytm tworzenia podpisów cyfrowych za pomocą RSA	111
Algorytm ECDSA	113
Rynki i transakcje finansowe	118
Handel	119
Giełdy	119
Cykl życia transakcji	121
Osoby przewidujące zlecenia	122
Manipulowanie rynkiem	122
Podsumowanie	123
Rozdział 5. Wprowadzenie do Bitcoina	125
Bitcoin	127
Definicja Bitcoina	129
Bitcoin z lotu ptaka	130
Klucze i adresy cyfrowe	136
Klucze prywatne w Bitcoinie	136
Klucze publiczne w Bitcoinie	138
Adresy w Bitcoinie	139
Transakcje	141
Cykl życia transakcji	142
Struktura danych transakcji	143
Rodzaje transakcji	147
Sprawdzanie poprawności transakcji	150
Łańcuch bloków	151
Struktura bloku	151
Struktura nagłówka bloku	151
Blok początkowy	153
Wydobywanie	156
Zadania górników	156
Nagrody za wydobywanie bloku	157
Dowód pracy	157
Algorytm wydobywania	158
Szybkość obliczania skrótów	160
Systemy wydobywania	160
Kopalnie	163
Podsumowanie	165
Rozdział 6. Sieć Bitcoina i płatności	167
Sieć Bitcoina	167
Portfele	175
Portfele niedeterministyczne	175
Portfele deterministyczne	175
Hierarchiczne portfele deterministyczne	176
Portfele pamięciowe	176
Portfele papierowe	176

Portfele sprzętowe	176
Portfele internetowe	177
Portfele mobilne	177
Płatności w bitcoinach	178
Innowacje w Bitcoinie	180
Dokumenty BIP	181
Zaawansowane protokoły	181
Segregated Witness (SegWit)	181
Bitcoin Cash	183
Bitcoin Unlimited	183
Bitcoin Gold	183
Inwestycje w bitcoiny oraz ich kupno i sprzedaż	184
Podsumowanie	185

Rozdział 7. Klienci i interfejsy API Bitcoina **187**

Instalowanie Bitcoina	187
Typy klientów Bitcoin Core	187
Przygotowywanie węzła Bitcoina	188
Konfigurowanie kodu źródłowego	190
Konfigurowanie pliku bitcoin.conf	190
Uruchamianie węzła w sieci testnet	190
Uruchamianie węzła w sieci regtest	191
Eksperymentowanie z interfejsem bitcoin-cli	192
Programowanie w świecie Bitcoina i interfejs uruchamiany w wierszu poleceń	192
Podsumowanie	194

Rozdział 8. Inne kryptowaluty **195**

Podstawy teoretyczne	198
Co zamiast dowodu pracy?	198
Różne rodzaje stawek	201
Dostosowywanie trudności i algorytmy zmiany celu	202
Ograniczenia Bitcoina	205
Prywatność i anonimowość	205
Rozszerzone protokoły oparte na Bitcoinie	207
Rozwój alternatywnych kryptowalut	209
Namecoin	211
Handel namecoinami	213
Pozyskiwanie namecoinów	213
Generowanie rekordów w Namecoinie	215
Litecoin	217
Primecoin	220
Handel primecoinami	221
Przewodnik po wydobywaniu	221
Zcash	223

Handel zcashami	225
Przewodnik po wydobywaniu	225
Emisje ICO	230
Tokeny zgodne ze standardem ERC20	231
Podsumowanie	232
Rozdział 9. Inteligentne kontrakty	233
Historia	233
Definicja	234
Kontrakty ricardiańskie	237
Szablony inteligentnych kontraktów	239
Wyrocznie	241
Inteligentne wyrocznie	243
Umieszczanie inteligentnych kontraktów w łańcuchu bloków	243
The DAO	244
Podsumowanie	245
Rozdział 10. ABC łańcucha bloków Ethereum	247
Wprowadzenie	247
Specyfikacja techniczna	248
Łańcuch bloków Ethereum	249
Ethereum z lotu ptaka	250
Sieć Ethereum	254
Mainnet	254
Testnet	254
Sieć prywatna	254
Komponenty ekosystemu Ethereum	255
Klucze i adresy	256
Konta	256
Transakcje i komunikaty	258
Kryptowaluta i tokeny Ether (ETC i ETH)	267
Maszyna EVM	267
Inteligentne kontrakty	271
Podsumowanie	274
Rozdział 11. Jeszcze o Ethereum	275
Języki programowania	276
Wykonywany kod bajtowy	276
Bloki i łańcuchy bloków	284
Poziom opłat	290
Portfele i oprogramowanie klienckie	298
Protokoły pomocnicze	307
Skalowalność, bezpieczeństwo i inne wyzwania	309
Handel i inwestycje	309
Podsumowanie	310

Rozdział 12. Środowisko programistyczne Ethereum	311
Sieci testowe	312
Konfigurowanie sieci prywatnej	313
Identyfikator sieci	314
Plik początkowy	314
Katalog na dane	315
Uruchamianie sieci prywatnej	316
Uruchamianie przeglądarki Mist w sieci prywatnej	321
Dodawanie kontraktów za pomocą przeglądarki Mist	323
Eksplorator bloków prywatnej i lokalnej sieci Ethereum	326
Podsumowanie	329
 Rozdział 13. Narzędzia i platformy programistyczne	 331
Języki	332
Kompilatory	333
Język Solidity	344
Typy	345
Podsumowanie	356
 Rozdział 14. Wprowadzenie do Web3	 357
Web3	357
Dodawanie kontraktów	358
Żądania POST	363
Fronton napisany w HTML-u i JavaScriptcie	364
Platformy programistyczne	371
Podsumowanie	397
 Rozdział 15. Hyperledger	 399
Projekty w ramach programu Hyperledger	399
Fabric	400
Sawtooth Lake	400
Iroha	400
Burrow	401
Indy	401
Explorer	402
Cello	402
Composer	402
Quilt	402
Hyperledger jako protokół	403
Architektura wzorcowa	403
Wymogi i cele projektowe związane z platformą Hyperledger Fabric	405
Fabric	407
Hyperledger Fabric	408
Sawtooth Lake	418

Corda	424
Podsumowanie	430
Rozdział 16. Inne łańcuchy bloków	431
Łańcuchy bloków	431
Kadena	432
Ripple	436
Stellar	441
Rootstock	442
Quorum	444
Tezos	445
Storj	446
MaidSafe	447
BigchainDB	448
Multichain	448
Tendermint	448
Platformy i frameworki	449
Eris	449
Podsumowanie	451
Rozdział 17. Łańcuch bloków — poza świat walut	453
Internet rzeczy	453
Warstwa obiektów fizycznych	455
Warstwa urządzeń	455
Warstwa sieci	455
Warstwa zarządzania	456
Warstwa aplikacji	456
Eksperyment z internetem rzeczy opartym na łańcuchu bloków	459
Instytucje rządowe	474
Opieka zdrowotna	478
Finanse	478
Multimedia	481
Podsumowanie	481
Rozdział 18. Skalowalność i inne problemy	483
Skalowalność	484
Poziom sieci	484
Poziom osiągnięcia konsensusu	484
Poziom składowania danych	485
Poziom widoku	485
Zwiększenie wielkości bloku	485
Skracanie czasu wydobywania bloków	486
Tablice IBLT	486
Sharding	487
Kanały stanu	487

Prywatny łańcuch bloków	488
Dowód stawki	488
Łańcuchy boczne	488
Prywatność	491
Zaciemnianie z nieodróżnialnością danych	491
Szyfrowanie homomorficzne	492
Dowody ZKP	492
Kanały stanu	493
Bezpieczne obliczenia z udziałem wielu jednostek	493
Wykorzystanie sprzętu do zapewniania poufności	493
CoinJoin	494
Poufne transakcje	494
MimbleWimble	494
Bezpieczeństwo	495
Podsumowanie	501

Rozdział 19. Aktualna sytuacja i przyszły rozwój **503**

Pojawiające się trendy	503
Łańcuchy bloków specyficzne dla zastosowań	503
Łańcuchy bloków dla przedsiębiorstw	504
Prywatne łańcuchy bloków	504
Startupy	505
Duże zainteresowanie ze strony naukowców	505
Standaryzacja	506
Usprawnienia	507
Implementacje stosowane w praktyce	507
Konsorcja	508
Rozwiązania problemów technicznych	508
Łączenie z innymi technologiami	508
Edukacja w zakresie technologii łańcuchów bloków	509
Zatrudnienie	509
Kryptoekonomia	509
Badania w dziedzinie kryptografii	510
Nowe języki programowania	510
Badania nad sprzętem i jego rozwój	510
Badania nad metodami formalnymi i bezpieczeństwem	511
Alternatywy względem łańcuchów bloków	511
Prace nad umożliwieniem współdziałania	511
Model BaaS	512
Prace nad ograniczeniem zużycia energii	512
Inne wyzwania	512
Regulacje	512
Ciemna strona	513
Badania nad łańcuchami bloków	515
Inteligentne kontrakty	515

Problemy z centralizacją	515
Ograniczenia funkcji kryptograficznych	515
Algorytmy osiągnięcia konsensusu	515
Skalowalność	516
Zaciemnianie kodu	516
Ważne projekty	516
Zcash dla Ethereum	516
CollCo	517
Cello	517
Qtum	517
Bitcoin-NG	517
Solidus	517
Hawk	518
Town-Crier	518
SETLCoin	518
TEEChan	518
Falcon	519
Bletchley	519
Casper	519
Różne narzędzia	520
Rozszerzenie dla języka Solidity w środowisku Microsoft Visual Studio	520
MetaMask	520
Stratis	520
Embark	521
DAPPLE	521
Meteor	521
uPort	521
INFURA	522
Powiązania z innymi branżami	522
Przyszłość	523
Podsumowanie	525
Skorowidz	527