

# Spis treści |

<b>O autorze .....</b>	<b>19</b>
<b>O korektorach merytorycznych .....</b>	<b>20</b>
<b>Przedmowa .....</b>	<b>21</b>
<b>ROZDZIAŁ 1</b>	
<b>ABC łańcucha bloków .....</b>	<b>25</b>
Rozwój technologii łańcucha bloków .....	25
Droga do dojrzałości .....	26
Rosnące zainteresowanie .....	27
Systemy rozproszone .....	28
Twierdzenie CAP .....	30
Twierdzenie PACELC .....	32
Historia łańcucha bloków .....	33
Bitcoin .....	34
Elektroniczne pieniądze .....	34
Wprowadzenie do łańcucha bloków .....	36
Architektura łańcucha bloków .....	37
Uniwersalne elementy łańcucha bloków .....	40
Działanie łańcucha bloków .....	44
Zalety i funkcje łańcucha bloków .....	45
Ograniczenia technologii łańcucha bloków .....	47
Typy łańcuchów bloków .....	49
Rozproszone rejestry .....	50
Wspólny rejestr .....	50
Publiczne łańcuchy bloków .....	50
Prywatne łańcuchy bloków .....	50
Częściowo prywatne łańcuchy bloków .....	51
Rejestr oparty na uprawnieniach .....	51
W pełni prywatne i zastrzeżone łańcuchy bloków .....	51
Łańcuchy bloków z tokenami .....	52
Łańcuchy bloków bez tokenów .....	52
Łańcuchy bloków warstwy pierwszej .....	52
Łańcuchy bloków warstwy drugiej .....	53
Podsumowanie .....	54

**ROZDZIAŁ 2**

<b>Decentralizacja</b> .....	<b>55</b>
Wprowadzenie do decentralizacji .....	55
Metody decentralizacji .....	59
Eliminowanie pośrednictwa .....	60
Decentralizacja oparta na współzawodnictwie .....	60
Ilościowe ujęcie decentralizacji .....	61
Zalety decentralizacji .....	62
Ocena wymagań .....	63
Decentralizacja całego ekosystemu .....	65
Składowanie danych .....	65
Komunikacja .....	66
Moc obliczeniowa .....	67
Decentralizacja w praktyce .....	68
Inteligentne kontrakty .....	69
Autonomiczne agenty .....	69
Zdecentralizowane organizacje .....	69
Zdecentralizowane organizacje autonomiczne .....	69
Zdecentralizowane korporacje autonomiczne .....	70
Zdecentralizowane społeczności autonomiczne .....	70
Zdecentralizowane aplikacje (DApps) .....	71
Wymogi stawiane zdecentralizowanym aplikacjom .....	73
Operacje w zdecentralizowanych aplikacjach .....	74
Projekt zdecentralizowanej aplikacji .....	74
Innowacyjne trendy .....	75
Zdecentralizowany internet .....	76
Web 1 .....	76
Web 2 .....	76
Web 3 .....	77
Podsumowanie .....	77

**ROZDZIAŁ 3**

<b>Kryptografia symetryczna</b> .....	<b>78</b>
Wprowadzenie do kryptografii .....	78
Usługi zapewniane dzięki kryptografii .....	79
Podstawowe mechanizmy kryptograficzne .....	81
Podstawowe mechanizmy kryptografii bez kluczy .....	82
Podstawowe mechanizmy w kryptografii z kluczami symetrycznymi .....	94
AES .....	101
DES .....	101
Działanie algorytmu AES .....	102
Szyfrowanie i deszyfrowanie z użyciem algorytmu AES .....	103
Podsumowanie .....	105

**ROZDZIAŁ 4**

<b>Kryptografia asymetryczna .....</b>	<b>106</b>
Podstawy matematyczne .....	106
Kryptografia asymetryczna .....	107
Klucze publiczny i prywatny .....	108
Algorytmy w kryptografii asymetrycznej .....	109
System IES .....	110
Wprowadzenie do algorytmu RSA .....	111
Szyfrowanie i deszyfrowanie z użyciem algorytmu RSA .....	112
Wprowadzenie do ECC .....	114
Matematyka wykorzystywana w ECC .....	115
Problem logarytmu dyskretnego w ECC .....	120
Generowanie kluczy za pomocą algorytmu ECC .....	123
Podpisy cyfrowe .....	125
Algorytm tworzenia podpisów cyfrowych za pomocą RSA .....	126
Algorytm ECDSA .....	128
Różne typy podpisów cyfrowych .....	131
Zagadnienia kryptograficzne i technologia łańcucha bloków .....	136
Szyfrowanie homomorficzne .....	136
Dzielenie sekretu .....	137
Systemy składania zobowiązań .....	137
Dowody ZKP .....	138
Schematy kodowania .....	144
Funkcje VRF .....	145
Podsumowanie .....	145

**ROZDZIAŁ 5**

<b>Algorytmy osiągnięcia konsensusu .....</b>	<b>147</b>
Wprowadzenie do konsensusu .....	147
Odporność na błędy .....	148
FLP .....	149
Analizowanie i projektowanie .....	150
Model .....	151
Procesy .....	151
Założenia dotyczące czasu .....	151
Klasyfikacja .....	152
Algorytmy .....	153
Algorytmy CFT .....	153
Algorytmy BFT .....	158
Wybór algorytmu .....	185
Nieodwracalność .....	186
Szybkość, wydajność i skalowalność .....	186
Podsumowanie .....	187

**ROZDZIAŁ 6**

<b>Architektura Bitcoina</b> .....	<b>188</b>
Wprowadzenie do Bitcoina .....	188
Klucze kryptograficzne .....	190
Klucze prywatne w Bitcoinie .....	190
Klucze publiczne w Bitcoinie .....	191
Adresy .....	192
Typowe adresy Bitcoin .....	193
Zaawansowane adresy Bitcoin .....	195
Transakcje .....	195
Transakcje coinbase .....	196
Cykl życia transakcji .....	197
Struktura danych transakcji .....	199
Język Script .....	202
Błędy związane z transakcjami .....	207
Łańcuch bloków .....	208
Struktura .....	208
Blok początkowy .....	210
Bloki nieaktualne i osierocone .....	210
Forki .....	211
Cechy Bitcoina .....	212
Górnicy .....	213
Dowód pracy .....	214
Systemy wydobywania .....	216
Kopalnie .....	218
Sieć .....	219
Typy komunikatów .....	220
Oprogramowanie klienckie .....	225
Filtry Blooma .....	226
Portfele .....	227
Podsumowanie .....	230

**ROZDZIAŁ 7**

<b>Bitcoin w praktyce</b> .....	<b>231</b>
Bitcoin w rzeczywistym świecie .....	231
Płatności w bitcoinach .....	232
Innowacje w Bitcoinie .....	235
Dokumenty BIP .....	235
Zaawansowane protokoły .....	236
Rozszerzone protokoły oparte na Bitcoinie .....	241
Alternatywne kryptowaluty oparte na Bitcoinie .....	243

Instalowanie Bitcoina .....	244
Typy klientów i narzędzi .....	244
Przygotowywanie węzła Bitcoina .....	245
Uruchamianie węzła w sieci testnet .....	246
Uruchamianie węzła w sieci regtest .....	248
Dalsze eksperymenty z interfejsem bitcoin-cli .....	249
Obsługa Bitcoina za pomocą narzędzia działającego w wierszu poleceń .....	251
Stosowanie interfejsu JSON-RPC .....	252
Korzystanie z interfejsu HTTP REST .....	253
Programowanie w świecie Bitcoina .....	254
Podsumowanie .....	255

## ROZDZIAŁ 8

<b>Inteligentne kontrakty .....</b>	<b>256</b>
Wprowadzenie do inteligentnych kontraktów .....	256
Definicje .....	257
Cechy .....	258
Praktyczne zastosowania .....	259
Kontrakty ricardiańskie .....	261
Szablony inteligentnych kontraktów .....	264
Wyrocznie .....	266
Dowody generowane z wykorzystaniem oprogramowania i sieci .....	268
Dowody z wykorzystaniem sprzętu .....	269
Typy wyroczni dla łańcuchów bloków .....	272
Usługi wyroczni dla łańcuchów bloków .....	276
Umieszczanie inteligentnych kontraktów w łańcuchu bloków .....	276
The DAO .....	278
Postępy w technologii inteligentnych kontraktów .....	279
Solana Sealevel .....	279
Digital Asset Modeling Language .....	280
Podsumowanie .....	282

## ROZDZIAŁ 9

<b>Architektura Ethereum .....</b>	<b>283</b>
Wprowadzenie do Ethereum .....	283
Kryptowaluta .....	285
Klucze i adresy .....	286
Konta .....	290
Transakcje i komunikaty .....	292
Drzewa MPT .....	292

Komponenty transakcji .....	294
Format RLP .....	298
Paliwo .....	299
Typy transakcji .....	301
Komunikaty .....	303
Sprawdzanie poprawności i wykonywanie transakcji .....	304
Stan i składowanie w łańcuchu bloków Ethereum .....	305
Maszyna EVM w Ethereum .....	308
Środowisko uruchomieniowe .....	311
Stan maszyny .....	312
Bloki i łańcuchy bloków .....	312
Blok początkowy .....	314
Sprawdzanie poprawności, finalizowanie i przetwarzanie bloków .....	315
Mechanizm zmiany trudności wydobywania bloku .....	316
Węzły i górnicy .....	317
Mechanizm osiągnięcia konsensusu .....	318
Forki w łańcuchu bloków .....	319
Sieć Ethereum .....	320
Mainnet .....	320
Sieci testowe .....	320
Sieci prywatne .....	321
Prekompilowane inteligentne kontrakty .....	325
Języki programowania .....	327
Portfele i oprogramowanie klienckie .....	328
Portfele .....	328
Geth .....	328
Uprozczone klienty .....	329
Protokoły pomocnicze .....	329
Whisper .....	329
Swarm .....	330
Podsumowanie .....	331

## ROZDZIAŁ 10

<b>Ethereum w praktyce .....</b>	<b>332</b>
Płatności w Ethereum .....	332
Innowacje w Ethereum .....	334
Bomba trudności .....	334
EIP 1559 .....	335
The Merge i nadchodzące aktualizacje .....	337
Programowanie z użyciem klienta Geth .....	338
Instalowanie i konfigurowanie klienta Geth .....	338

Tworzenie nowego konta za pomocą klienta Geth .....	339
Kierowanie zapytań do łańcucha bloków za pomocą klienta Geth .....	340
Konfigurowanie środowiska programistycznego .....	343
Łączenie się z sieciami testowymi .....	344
Tworzenie sieci prywatnej .....	345
Wprowadzenie do środowiska IDE Remix .....	356
Komunikowanie się z łańcuchem bloków Ethereum za pomocą narzędzia MetaMask .....	359
Instalowanie narzędzia MetaMask .....	359
Tworzenie i zasilanie konta za pomocą narzędzia MetaMask .....	360
Stosowanie narzędzia MetaMask i środowiska IDE Remix do umieszczania inteligentnego kontraktu w łańcuchu .....	362
Podsumowanie .....	376
 <b>ROZDZIAŁ 11</b>	
<b>Narzędzia, języki i platformy dla programistów Ethereum .....</b>	<b>377</b>
Języki .....	378
Kompilator języka Solidity .....	378
Instalowanie kompilatora solc .....	378
Eksperymentowanie z kompilatorem solc .....	379
Narzędzia, biblioteki i platformy .....	381
Node.js .....	381
Ganache .....	381
Truffle .....	384
Drizzle .....	385
Inne narzędzia .....	385
Pisanie i dodawanie kontraktów .....	386
Pisanie inteligentnych kontraktów .....	386
Testowanie inteligentnych kontraktów .....	387
Dodawanie inteligentnych kontraktów .....	387
Język Solidity .....	387
Funkcje .....	389
Zmienne .....	393
Typy danych .....	394
Struktury sterujące .....	398
Zdarzenia .....	399
Dziedziczenie .....	400
Biblioteki .....	401
Obsługa błędów .....	401
Podsumowanie .....	402

**ROZDZIAŁ 12**

<b>Programowanie w Ethereum z użyciem biblioteki Web3 .....</b>	<b>403</b>
Interakcja z kontraktami za pomocą interfejsu Web3 i klienta Geth .....	403
Dodawanie kontraktów .....	404
Stosowanie kompilatora solc do generowania interfejsu ABI i kodu .....	408
Kierowanie zapytań do kontraktów za pomocą klienta Geth .....	409
Interakcje z klientem Geth za pomocą żądań POST .....	412
Interakcja z kontraktami za pomocą frontendów .....	413
Instalowanie javascriptowej biblioteki web3.js .....	413
Tworzenie obiektu web3 .....	414
Tworzenie javascriptowego pliku app.js .....	415
Tworzenie strony internetowej używanej jako frontend .....	418
Wywoływanie funkcji kontraktu .....	419
Tworzenie strony internetowej używanej jako frontend .....	419
Dodawanie kontraktów i komunikowanie się z nimi za pomocą platformy Truffle .....	422
Instalowanie i inicjalizowanie platformy Truffle .....	422
Kompilowanie, testowanie i przenoszenie kontraktów za pomocą platformy Truffle .....	423
Interakcja z kontraktem .....	427
Używanie platformy Truffle do testowania i dodawania inteligentnych kontraktów .....	429
Umieszczanie danych w zdecentralizowanym magazynie w systemie IPFS .....	433
Podsumowanie .....	435

**ROZDZIAŁ 13**

<b>The Merge i późniejsze aktualizacje .....</b>	<b>436</b>
Wprowadzenie .....	436
Ethereum po aktualizacji The Merge .....	437
Beacon Chain .....	439
Interfejs P2P (sieci) .....	452
The Merge .....	452
Sharding .....	463
Plan przyszłych prac nad Ethereum .....	472
Podsumowanie .....	473

**ROZDZIAŁ 14**

<b>Hyperledger .....</b>	<b>474</b>
Projekty w ramach programu Hyperledger .....	475
Rejestry rozproszone .....	475
Biblioteki .....	477

Narzędzia .....	479
Projekty specyficzne dla dziedziny .....	479
Architektura wzorcowa w programie Hyperledger .....	480
Cele projektowe związane z platformą Hyperledger .....	482
Hyperledger Fabric .....	484
Najważniejsze zagadnienia .....	484
Komponenty .....	489
Aplikacje .....	492
Mechanizm osiągania konsensusu .....	494
Cykl życia transakcji .....	495
Fabric 2.0 .....	497
Nowy sposób zarządzania cyklem życia kontraktów chaincode .....	497
Nowe wzorce stosowania kontraktów chaincode .....	499
Podsumowanie .....	500

## ROZDZIAŁ 15

<b>Tokenizacja .....</b>	<b>501</b>
Tokenizacja w łańcuchu bloków .....	502
Zalety tokenizacji .....	502
Wady tokenizacji .....	504
Rodzaje tokenów .....	505
Tokeny wymienne .....	505
Tokeny niewymienne .....	506
Stabilne tokeny .....	507
Tokeny inwestycyjne .....	508
Proces tokenizacji .....	508
Oferty tokenów .....	509
Pierwsza oferta tokenów .....	509
Oferty STO .....	510
Oferty IEO .....	510
Oferty ETO .....	510
Oferty DAICO .....	511
Inne oferty tokenów .....	511
Standardy związane z tokenami .....	512
ERC-20 .....	513
ERC-223 .....	513
ERC-777 .....	513
ERC-721 .....	514
ERC-884 .....	514
ERC-1400 .....	514
ERC-1404 .....	514

ERC-1155 .....	515
ERC-4626 .....	515
Tworzenie tokenów ERC-20 .....	516
Tworzenie kontraktu w języku Solidity .....	517
Dodawanie kontraktu za pomocą maszyny wirtualnej JavaScriptu w środowisku Remix .....	521
Dodawanie tokenów w narzędziu MetaMask .....	525
Nowe koncepcje .....	527
Tokenomia (ekonomia tokenów) .....	527
Inżynieria tokenów .....	528
Taksonomia tokenów .....	528
Podsumowanie .....	528

## ROZDZIAŁ 16

<b>Korporacyjne łańcuchy bloków .....</b>	<b>529</b>
Rozwiązania korporacyjne a łańcuch bloków .....	530
Czynniki wpływające na powodzenie .....	531
Czynniki ograniczające .....	532
Wymagania .....	534
Prywatność .....	534
Wydajność .....	535
Zarządzanie dostępem .....	536
Dodatkowe wymagania .....	536
Łańcuchy korporacyjne a łańcuchy publiczne.....	539
Architektura korporacyjnego łańcucha bloków .....	540
Projektowanie rozwiązań opartych na korporacyjnym łańcuchu bloków ...	544
TOGAF .....	544
Metoda rozwoju architektury .....	545
Łańcuch bloków w chmurze .....	548
Obecnie dostępne korporacyjne łańcuchy bloków .....	549
Wyzwania związane z korporacyjnymi łańcuchami bloków .....	552
Interoperacyjność .....	552
Brak standaryzacji .....	552
Zgodność z przepisami .....	553
Wyzwania biznesowe .....	553
Łańcuch VMBC .....	554
Komponenty .....	554
Protokół osiągnięcia konsensusu .....	555
Architektura .....	555
VMBC for Ethereum .....	557

Quorum .....	558
Architektura .....	558
Kryptografia .....	560
Prywatność .....	561
Kontrola dostępu oparta na uprawnieniach .....	564
Wydajność .....	566
Wymienne algorytmy osiągnięcia konsensusu .....	567
Konfigurowanie sieci Quorum z algorytmem IBFT .....	567
Instalowanie i uruchamianie narzędzia Quorum Wizard .....	568
Przeprowadzanie transakcji prywatnej .....	570
Dołączanie klienta Geth do węzłów .....	571
Wyświetlanie transakcji w narzędziu Cakeshop .....	573
Dalsze sprawdzanie w kliencie Geth .....	574
Inne projekty na platformie Quorum .....	577
Wtyczka dla środowiska Remix .....	577
Architektura oparta na wtyczkach .....	577
Podsumowanie .....	578
<b>ROZDZIAŁ 17</b>	
<b>Skalowalność .....</b>	<b>579</b>
Czym jest skalowalność? .....	579
Trylemat łańcuchów bloków .....	580
Metody zwiększania skalowalności .....	583
Rollupy .....	595
Podsumowanie .....	619
<b>ROZDZIAŁ 18</b>	
<b>Prywatność .....</b>	<b>620</b>
Prywatność .....	620
Anonimowość .....	621
Poufność .....	621
Techniki osiągnięcia prywatności .....	622
Warstwa 0. .....	623
Prywatność oparta na dowodach ZK .....	633
Przykład .....	650
Podsumowanie .....	657
<b>ROZDZIAŁ 19</b>	
<b>Bezpieczeństwo w łańcuchach bloków .....</b>	<b>658</b>
Bezpieczeństwo .....	658
Warstwy i ataki w łańcuchach bloków .....	660
Warstwa sprzętu .....	661

Warstwa sieci .....	663
Warstwa łańcucha bloków .....	664
Warstwa aplikacji łańcucha bloków .....	668
Warstwa interfejsu .....	673
Ataki na łańcuchy bloków warstwy 2. ....	676
Warstwa kryptografii .....	677
Narzędzia i mechanizmy do analizy zabezpieczeń .....	681
Formalna weryfikacja .....	683
Bezpieczeństwo inteligentnych kontraktów .....	688
Solgraph .....	690
Modelowanie zagrożeń .....	691
Regulacje i zgodność z przepisami .....	693
Podsumowanie .....	694

## ROZDZIAŁ 20

<b>Zdecentralizowana tożsamość .....</b>	<b>695</b>
Tożsamość .....	695
Tożsamość cyfrowa .....	696
Tożsamość w Ethereum .....	719
Tożsamość w świecie Web3, DeFi i metawersum .....	720
Projekty łańcuchów bloków specyficznych dla tożsamości suwerennej .....	723
Hyperledger Indy, Aries, Ursa i AnonCreds .....	723
Inne projekty .....	724
Inne inicjatywy .....	724
Wyzwania .....	725
Podsumowanie .....	725

## ROZDZIAŁ 21

<b>Zdecentralizowane finanse .....</b>	<b>726</b>
Wprowadzenie .....	726
Rynki finansowe .....	728
Handel .....	728
Giełdy .....	729
Zastosowania łańcucha bloków w finansach .....	732
Ubezpieczenia .....	733
Rozliczenia potransakcyjne .....	733
Zapobieganie przestępstwom finansowym .....	734
Płatności .....	736
Zdecentralizowane finanse .....	737
Cechy rozwiązań z obszaru DeFi .....	739
Warstwy w DeFi .....	740

Podstawowe elementy ekosystemu DeFi .....	741
Usługi DeFi .....	743
Zalety DeFi .....	756
Uniswap .....	758
Wymiana tokenów .....	758
Pula płynności na giełdzie Uniswap .....	759
Podsumowanie .....	762

## ROZDZIAŁ 22

### Zastosowania i przyszłość łańcuchów bloków .....

Zastosowania .....	763
Internet rzeczy .....	764
Architektura internetu rzeczy .....	765
Warstwa obiektów fizycznych .....	766
Warstwa urządzeń .....	766
Warstwa sieci .....	766
Warstwa zarządzania .....	766
Warstwa aplikacji .....	767
Korzyści z łączenia internetu rzeczy z łańcuchem bloków .....	767
Implementowanie internetu rzeczy opartego na łańcuchach bloków w praktyce .....	770
Konfigurowanie Raspberry Pi .....	772
Konfigurowanie pierwszego węzła .....	774
Konfigurowanie węzła w Raspberry Pi .....	775
Instalowanie Node.js .....	776
Budowanie obwodu elektronicznego .....	777
Tworzenie i uruchamianie kontraktu w języku Solidity .....	778
Administracja publiczna .....	783
Kontrola graniczna .....	783
Wybory .....	785
Identyfikacja obywateli .....	786
Opieka zdrowotna .....	787
Media .....	788
Łańcuchy bloków a sztuczna inteligencja .....	789
Wybrane nowe trendy .....	791
Wybrane wyzwania .....	793
Podsumowanie .....	796

## ROZDZIAŁ 23

<b>Inne rozwiązania z obszaru łańcuchów bloków .....</b>	<b>798</b>
Wprowadzenie .....	798
Kadena .....	798
Pact .....	801
EOS .....	803
Zasoby .....	804
Komponenty .....	804
Programowanie w łańcuchu bloków EOS .....	806
Tezos .....	806
Architektura .....	808
Sieć .....	808
Klient .....	808
Węzeł .....	808
Jednostka zatwierdzająca .....	809
„Piekarz” .....	809
Oskarżyciel .....	810
Konta .....	810
Tworzenie kontraktów .....	812
Portfele .....	813
Ripple .....	813
Transakcje .....	815
Interledger .....	817
Stellar .....	819
Protokół osiągnięcia konsensusu w systemie Stellar .....	819
Rootstock .....	820
Solana .....	822
Dowód historii .....	823
Projekty łańcuchów bloków dla warstwy przechowywania .....	827
Storj .....	827
MaidSafe .....	828
Inne platformy .....	829
MultiChain .....	829
Tendermint .....	829
Podsumowanie .....	830