**Índice**

**Prefácio** xxvii

**Capítulo 1: Blockchain 101** 1  
O crescimento da tecnologia blockchain ........................................................................................ 1  
Progresso rumo à maturidade • 2  
Interesse crescente • 3

Sistemas distribuídos .................................................................................................................. 4  
Teorema CAP • 6  
Teorema PACELC • 8

A história do blockchain ............................................................................................................. 8  
Bitcoin • 9  
Dinheiro eletrônico • 9

Introdução ao blockchain .......................................................................................................... 11  
Arquitetura do blockchain • 12

Blockchain por camadas • 12  
Blockchain nos negócios • 14

Elementos genéricos de um blockchain • 14  
Funcionalidade do blockchain • 18  
Benefícios e características do blockchain • 20  
Limitações da tecnologia blockchain • 21

Tipos de blockchain .................................................................................................................. 23  
Registros distribuídos • 23  
Livro-razão compartilhado • 24  
Blockchains públicos • 24  
Blockchains privados • 24  
Blockchains semi-privados • 24  
Livro-razão com permissão • 25  
Blockchains totalmente privados e proprietários • 25  
Blockchains tokenizados • 25  
Blockchains sem tokens • 25  
Blockchains de Camada 1 • 26  
Blockchains monolíticos e polilíticos • 26  
Blockchains de Camada 2 • 26  
Sidechains • 26

Resumo ....................................................................................................................................... 27

**Capítulo 2: Descentralização** 29  
Introdução à descentralização ................................................................................................... 29  
Métodos de descentralização • 33  
Desintermediação • 33  
Descentralização orientada por competição • 34  
Quantificando a descentralização • 34  
Benefícios da descentralização • 36  
Avaliando os requisitos • 37

Descentralização do ecossistema completo ............................................................................. 38  
Armazenamento • 38  
Comunicação • 39  
Poder computacional • 40

Descentralização na prática ...................................................................................................... 42  
Contratos inteligentes • 42  
Agentes autônomos • 42  
Organizações descentralizadas • 43  
Organizações autônomas descentralizadas • 43  
Corporações autônomas descentralizadas • 43  
Sociedades autônomas descentralizadas • 44  
Aplicações descentralizadas • 44  
Critérios para uma DApp • 46  
Operações de uma DApp • 46  
Design de uma DApp • 46

Tendências inovadoras ............................................................................................................. 48  
Web descentralizada • 48  
Web 1 • 49  
Web 2 • 49  
Web 3 • 49

Resumo ....................................................................................................................................... 49

**Capítulo 3: Criptografia Simétrica** 51  
Introdução à criptografia .......................................................................................................... 52  
Serviços fornecidos pela criptografia • 52

Primitivas criptográficas .......................................................................................................... 54  
Primitivas sem chave • 55

Números aleatórios • 55  
Funções de hash • 56

Primitivas de chave simétrica • 67  
Códigos de autenticação de mensagens • 68  
Cifras de chave secreta • 69

Padrão de Criptografia Avançado ............................................................................................ 74  
Padrão de Criptografia de Dados • 74  
Como o AES funciona • 74  
Criptografando e descriptografando com AES • 76

Resumo ..................................................................................................................................... 77

**Capítulo 4: Criptografia Assimétrica** 79  
Matemática fundamental .......................................................................................................... 79  
Criptografia assimétrica ........................................................................................................... 80

Chaves públicas e privadas • 80  
Algoritmos de criptografia assimétrica • 82

Fatoração de inteiros • 82  
Logaritmo discreto • 82  
Curvas elípticas • 83

Esquema de criptografia integrada • 83  
Introdução ao RSA .................................................................................................................. 83

Criptografando e descriptografando com RSA • 85  
Introdução ao ECC .................................................................................................................. 87

Matemática por trás do ECC • 87  
Adição de pontos • 88  
Dobramento de pontos • 91  
Multiplicação de pontos • 92

O problema do logaritmo discreto • 93  
Gerando chaves com ECC • 95

Assinaturas digitais .................................................................................................................. 98  
Algoritmos de assinatura digital RSA • 98  
Gerando assinaturas digitais RSA • 100  
O algoritmo de assinatura digital de curva elíptica • 100  
Gerando assinaturas digitais ECDSA • 102  
Diferentes tipos de assinaturas digitais • 104

Assinaturas cegas • 104  
Multassinaturas • 105  
Assinaturas limiares • 106  
Assinaturas agregadas • 108  
Assinaturas em anel • 108

Construções criptográficas e tecnologia blockchain ............................................................... 109  
Criptografia homomórfica • 109  
Compartilhamento secreto • 109  
Esquemas de compromisso • 110  
Provas de conhecimento zero • 111

zk-SNARKs • 113  
zk-STARKs • 115  
Provas de intervalo de conhecimento zero • 116

Esquemas de codificação • 116  
Base64 • 117  
base58 • 117

Funções aleatórias verificáveis • 117

Resumo ................................................................................................................................... 118

**Capítulo 5: Algoritmos de Consenso** 119  
Introdução ao consenso ........................................................................................................... 119  
Tolerância a falhas • 120  
Impossibilidade de FLP • 121

Análise e projeto ...................................................................................................................... 122  
Modelo • 122  
Processos • 122  
Suposições de tempo • 123

Classificação ........................................................................................................................... 123  
Algoritmos .............................................................................................................................. 124

Algoritmos CFT • 124  
Paxos • 124  
Raft • 127

Algoritmos BFT • 129  
Tolerância Prática a Falhas Bizantinas • 129  
Tolerância Bizantina de Istambul • 134  
Tendermint • 137  
Consenso de Nakamoto • 144  
Variantes de PoW • 146  
HotStuff • 151

Escolhendo um algoritmo ........................................................................................................ 155  
Finalidade • 155  
Velocidade, desempenho e escalabilidade • 156

Resumo .................................................................................................................................... 156

**Capítulo 6: Arquitetura do Bitcoin** 157  
Introdução ao Bitcoin ............................................................................................................... 157  
Chaves criptográficas .............................................................................................................. 159

Chaves privadas no Bitcoin • 159  
Chaves públicas no Bitcoin • 160

Endereços ................................................................................................................................. 161  
Endereços típicos de Bitcoin • 161  
Endereços avançados de Bitcoin • 163

Transações ................................................................................................................................ 163  
Transações coinbase • 164  
O ciclo de vida da transação • 165

Validação de transação • 166  
Taxas de transação • 166

A estrutura de dados da transação • 167  
Metadados • 169  
Entradas • 169  
Saídas • 170  
Verificação • 170

A linguagem Script • 170  
Códigos de operação • 171  
Scripts de transação padrão • 171  
Contratos • 174

Erros em transações • 175  
Blockchain ............................................................................................................................... 176

Estrutura • 176  
O bloco gênese • 178  
Blocos obsoletos e órfãos • 179  
Bifurcações • 179  
Propriedades • 180

Mineradores ............................................................................................................................. 181  
Prova de trabalho (PoW) • 182  
Sistemas de mineração • 184

CPU • 184  
GPU • 184  
FPGAs • 185  
ASICs • 185

Pools de mineração • 186  
Rede ......................................................................................................................................... 186

Tipos de mensagens • 187  
Software cliente • 192  
Filtros Bloom • 192

Carteiras .................................................................................................................................. 194  
Resumo .................................................................................................................................... 196

**Capítulo 7: Bitcoin na Prática** 197  
Bitcoin no mundo real .............................................................................................................. 197  
Pagamentos em Bitcoin ........................................................................................................... 198  
Inovação no Bitcoin .................................................................................................................. 200

Propostas de melhoria do Bitcoin • 201  
Protocolos avançados • 202

Segregated Witness • 202  
Bitcoin Cash • 204  
Bitcoin Unlimited • 205  
Bitcoin Gold • 205  
Taproot • 205

Protocolos estendidos sobre o Bitcoin • 206  
Moedas coloridas • 206  
Counterparty • 207

Altcoins a partir do Bitcoin • 208  
Instalação do cliente Bitcoin ..................................................................................................... 209

Tipos de clientes e ferramentas • 209  
Configurando um nó Bitcoin • 210

Configurando o código-fonte • 210  
Configurando o bitcoin.conf • 211  
Iniciando um nó na testnet • 211  
Iniciando um nó no regtest • 212

Experimentando mais com o bitcoin-cli .................................................................................... 214  
Usando a ferramenta de linha de comando do Bitcoin • 216  
Usando a interface JSON-RPC • 217  
Usando a interface HTTP REST • 218

Programação com Bitcoin ........................................................................................................ 219  
Resumo ..................................................................................................................................... 219

**Capítulo 8: Contratos Inteligentes** 221  
Introdução aos contratos inteligentes ....................................................................................... 221  
Definições • 222  
Propriedades • 222  
Aplicação no mundo real • 224

Contratos Ricardianos .............................................................................................................. 225  
Modelos de contratos inteligentes ............................................................................................ 229  
Oráculos ................................................................................................................................... 231

Provas assistidas por software e rede • 233  
TLSNotary • 233  
Mecanismo baseado em TLS-N • 233

Provas assistidas por dispositivos de hardware • 234  
Prova no Android • 234  
Prova da Ledger • 234  
Provas assistidas por hardware confiável • 235

Tipos de oráculos blockchain • 236  
Oráculos de entrada • 236  
Oráculos de saída • 238  
Oráculos criptoeconômicos • 239

Serviços de oráculos blockchain • 239  
Implantando contratos inteligentes ......................................................................................... 240  
O DAO ...................................................................................................................................... 241  
Avanços na tecnologia de contratos inteligentes ....................................................................... 242

Solana Sealevel • 242  
Linguagem de Modelagem de Ativos Digitais • 243

Resumo ..................................................................................................................................... 245

**Capítulo 9: Arquitetura do Ethereum** 247  
Introdução ao Ethereum ............................................................................................................ 247  
Criptomoeda ............................................................................................................................. 250  
Chaves e endereços .................................................................................................................. 250  
Contas ....................................................................................................................................... 254  
Transações e mensagens .......................................................................................................... 255

MPTs • 256  
Componentes da transação • 257  
Prefixo de Comprimento Recursivo (RLP) • 261  
Gas • 262  
Tipos de transações • 264

Transações simples • 264  
Transações de criação de contrato • 264  
Transações de chamada de mensagem • 265

Mensagens • 265  
Validação e execução da transação • 266  
Estado e armazenamento no blockchain do Ethereum • 267

O estado global • 268  
O estado da conta • 268  
Recibos de transações • 269

Máquina virtual do Ethereum (EVM) ....................................................................................... 270  
Ambiente de execução • 273  
O estado da máquina • 273

Blocos e blockchain .................................................................................................................. 274  
O bloco gênese • 276  
Validação, finalização e processamento de blocos • 276  
Mecanismo de dificuldade de bloco • 278

Nós e mineradores ................................................................................................................... 279  
O mecanismo de consenso • 279  
Bifurcações no blockchain • 281

A rede Ethereum ...................................................................................................................... 281  
Rede principal • 282  
Redes de teste • 282  
Redes privadas • 282

Contratos inteligentes pré-compilados ..................................................................................... 286  
Linguagens de programação • 287

Solidity • 287  
Bytecode de tempo de execução • 288  
Códigos de operação (opcodes) • 288

Carteiras e software cliente ..................................................................................................... 289  
Carteiras • 289  
Geth • 289  
Clientes leves • 289

Protocolos de suporte .............................................................................................................. 290  
Whisper • 290  
Swarm • 290

Resumo ..................................................................................................................................... 292

**Capítulo 10: Ethereum na Prática** 293  
Pagamentos com Ethereum ...................................................................................................... 294  
Inovações no Ethereum ............................................................................................................ 295

Bomba de dificuldade • 295  
EIP-1559 • 296  
A fusão (The Merge) e atualizações futuras • 298

Programando com Geth ............................................................................................................ 298  
Instalando e configurando o cliente Geth • 299  
Criando uma nova conta no Geth • 299  
Consultando o blockchain usando o Geth • 301

Console Geth • 301  
Geth attach • 301  
API JSON-RPC do Geth • 302

Configurando um ambiente de desenvolvimento .................................................................... 304  
Conectando-se a redes de teste • 305  
Criando uma rede privada • 305

Iniciando a rede privada • 307  
Experimentando com o console JavaScript do Geth • 310  
Minerando e enviando transações • 312

Introdução ao Remix IDE .......................................................................................................... 318  
Interagindo com o blockchain Ethereum com MetaMask ........................................................ 321

Instalando o MetaMask • 321  
Criando e financiando uma conta com MetaMask • 322  
Usando MetaMask e Remix IDE para implantar um contrato inteligente • 324  
Adicionando uma rede personalizada ao MetaMask e conectando-a com o Remix IDE • 325  
Importando contas no MetaMask usando arquivos keystore • 328  
Implantando um contrato com MetaMask • 331  
Interagindo com um contrato por meio do MetaMask usando o Remix IDE • 336

Resumo ..................................................................................................................................... 342

**Capítulo 11: Ferramentas, Linguagens e Frameworks para Desenvolvedores Ethereum** 343  
Linguagens ................................................................................................................................ 344  
O compilador Solidity ............................................................................................................... 344

Instalando o solc • 344  
Experimentando com o solc • 345

Ferramentas, bibliotecas e frameworks ..................................................................................... 347  
Node.js • 347  
Ganache • 348

ganache-cli • 348  
Ganache UI • 349

Truffle • 351  
Drizzle • 352  
Outras ferramentas • 352

Desenvolvimento e implantação de contratos .......................................................................... 353  
Escrevendo contratos inteligentes • 353  
Testando contratos inteligentes • 353  
Implantando contratos inteligentes • 354

A linguagem Solidity ................................................................................................................ 354  
Funções • 355  
Variáveis • 359

Variáveis locais • 359  
Variáveis globais • 359  
Variáveis de estado • 360

Tipos de dados • 361  
Tipos por valor • 361  
Tipos por referência • 363

Estruturas de controle • 365  
Eventos • 366  
Herança • 367  
Bibliotecas • 367  
Tratamento de erros • 368

Resumo ..................................................................................................................................... 369

**Capítulo 12: Desenvolvimento Web3 Usando Ethereum** 371  
Interagindo com contratos usando Web3 e Geth ....................................................................... 371  
Implantando contratos • 372  
Usando solc para gerar ABI e código • 376  
Consultando contratos com Geth • 377  
Interagindo com Geth usando requisições POST • 380

Interagindo com contratos por meio de frontends .................................................................... 381  
Instalando a biblioteca JavaScript web3.js • 382  
Criando um objeto web3 • 383  
Criando um arquivo JavaScript app.js • 384  
Criando uma página web frontend • 387  
Chamando funções de contrato • 388  
Criando uma página web frontend • 389

Implantando e interagindo com contratos usando Truffle ....................................................... 391  
Instalando e inicializando o Truffle • 392  
Compilando, testando e migrando com o Truffle • 393  
Interagindo com o contrato • 398  
Usando o Truffle para testar e implantar contratos inteligentes • 399  
Implantação em armazenamento descentralizado usando IPFS • 404

Resumo ..................................................................................................................................... 406

**Capítulo 13: The Merge e Além** 407  
Introdução ................................................................................................................................ 407  
Ethereum após The Merge ....................................................................................................... 408

A Beacon Chain • 409  
Nós Beacon • 410  
Cliente de consenso • 411  
Cliente de execução • 411  
Cliente validador • 411  
Prova de participação (Proof-of-stake) • 415

Interface P2P (rede) • 421  
The Merge ................................................................................................................................. 422  
Sharding .................................................................................................................................... 432  
O roteiro futuro do Ethereum ................................................................................................... 440  
Resumo ..................................................................................................................................... 441

**Capítulo 14: Hyperledger** 443  
Projetos sob o Hyperledger ....................................................................................................... 444  
Registros distribuídos • 444

Fabric • 444  
Sawtooth • 445  
Iroha • 445  
Indy • 446  
Besu • 446

Bibliotecas • 446  
Aries • 446  
Transact • 447  
Ursa • 447  
AnonCreds • 447

Ferramentas • 447  
Cello • 448  
Caliper • 448

Domínio específico • 448  
Grid • 448

Arquitetura de referência do Hyperledger ................................................................................ 449  
Princípios de design do Hyperledger • 451

Hyperledger Fabric .................................................................................................................. 452  
Conceitos-chave • 452

Serviço de membros • 453  
Serviços de blockchain • 454  
Serviços de contratos inteligentes • 456  
APIs e CLIs • 456

Componentes • 456  
Peers/nós • 457  
Clientes • 457  
Canais • 457  
Banco de dados de estado mundial • 457  
Coleções de dados privados • 458  
Transações • 458  
Provedor de Serviço de Membros • 458  
Contratos inteligentes • 459  
Provedor de serviços criptográficos • 459

Aplicações • 459  
Implementação de chaincode • 460  
O modelo de aplicação • 462

Mecanismo de consenso • 462  
Ciclo de vida da transação • 463

Fabric 2.0 .................................................................................................................................. 465  
Novo gerenciamento do ciclo de vida do chaincode • 465  
Novos padrões de aplicação de chaincode • 466

Resumo ..................................................................................................................................... 468

**Capítulo 15: Tokenização** 469  
Tokenização em um blockchain ............................................................................................... 470  
Vantagens da tokenização • 470  
Desvantagens da tokenização • 472

Tipos de tokens ......................................................................................................................... 473  
Tokens fungíveis • 473  
Tokens não fungíveis • 473  
Tokens estáveis • 474  
Tokens de segurança • 475

Processo de tokenização ........................................................................................................... 475  
Ofertas de tokens ..................................................................................................................... 476

Ofertas iniciais de moedas (ICO) • 476  
Ofertas de tokens de segurança (STO) • 477  
Ofertas iniciais em exchanges (IEO) • 477  
Ofertas de tokens de ações (ETO) • 477  
Oferta inicial de moedas autônoma descentralizada • 478  
Outras ofertas de tokens • 478

Padrões de tokens .................................................................................................................... 479  
ERC-20 • 479  
ERC-223 • 480  
ERC-777 • 480  
ERC-721 • 480  
ERC-884 • 480  
ERC-1400 • 481  
ERC-1404 • 481  
ERC-1155 • 482  
ERC-4626 • 482

Construindo um token ERC-20 ................................................................................................. 483  
Construindo o contrato Solidity • 483  
Implantando o contrato na máquina virtual JavaScript do Remix • 488  
Adicionando tokens no MetaMask • 493

Conceitos emergentes ............................................................................................................... 495  
Tokenomics/economia dos tokens • 495  
Engenharia de tokens • 495  
Taxonomia de tokens • 496

Resumo ..................................................................................................................................... 496

**Capítulo 16: Blockchain Empresarial** 497  
Soluções empresariais e blockchain ......................................................................................... 498  
Fatores de sucesso • 499  
Fatores limitantes • 500

Requisitos .................................................................................................................................. 501  
Privacidade • 502  
Desempenho • 502  
Governança de acesso • 503  
Requisitos adicionais • 503

Conformidade • 503  
Interoperabilidade • 504  
Integração • 505  
Facilidade de uso • 505  
Monitoramento • 505  
Cálculo seguro fora da cadeia • 505  
Melhores ferramentas • 506

Blockchain empresarial versus blockchain público ................................................................... 506  
Arquitetura de blockchain empresarial .................................................................................... 507  
Projetando soluções de blockchain empresarial ....................................................................... 509

TOGAF • 510  
Método de desenvolvimento de arquitetura (ADM) • 511  
Blockchain na nuvem • 513

Blockchains empresariais atualmente disponíveis .................................................................... 515  
Desafios do blockchain empresarial ......................................................................................... 517

Interoperabilidade • 517  
Falta de padronização • 517  
Conformidade • 518  
Desafios de negócios • 518

VMware Blockchain .................................................................................................................. 518  
Componentes • 519  
Protocolo de consenso • 519  
Arquitetura • 520  
VMware Blockchain para Ethereum • 522

Quorum ..................................................................................................................................... 522  
Arquitetura • 522

Nós • 523  
Gerenciador de privacidade • 524

Criptografia • 525  
Privacidade • 525

Criptografia em enclave • 527  
Propagação de transações para gerentes de transação • 527  
Descriptografia em enclave • 528

Controle de acesso com permissão • 529  
Desempenho • 531  
Consenso plugável • 531

Configurando uma rede Quorum com IBFT ............................................................................. 532  
Instalando e executando o Quorum Wizard • 532  
Executando uma transação privada • 535  
Conectando o Geth aos nós • 535  
Visualizando a transação no Cakeshop • 538  
Investigação adicional com o Geth • 539

Outros projetos Quorum ............................................................................................................ 542  
Plugin do Remix • 542  
Arquitetura plugável • 542

Resumo ..................................................................................................................................... 543

**Capítulo 17: Escalabilidade** 545  
O que é escalabilidade? ............................................................................................................ 545  
O trilema do blockchain • 546  
Métodos para melhorar a escalabilidade • 548

Camada 0 – soluções multichain • 549  
Polkadot • 549  
Camada 1 – soluções de escalabilidade on-chain • 551  
Camada 2 – soluções off-chain • 555

Camada 2 • 555  
Rollups • 559

Validade dos dados • 560  
Disponibilidade dos dados • 560  
Como os rollups funcionam • 561  
Tipos de rollups • 563  
Rollups otimistas • 563  
ZK-rollups • 564  
Tecnologias usadas na construção de ZK-rollups • 566  
ZK-ZK-rollups • 573  
Rollups otimistas vs ZK-rollups • 573  
Classificação de rollups baseada em provas de fraude e validade • 575  
Exemplo • 577  
Camada 3 e além • 579

Resumo ..................................................................................................................................... 580

**Capítulo 18: Privacidade em Blockchain** 583  
Privacidade ................................................................................................................................ 583  
Anonimato • 584  
Confidencialidade • 584

Técnicas para alcançar privacidade ......................................................................................... 585  
Camada 0 • 586

Tor • 586  
I2P • 586  
Ofuscação por indistinguibilidade • 586  
Criptografia homomórfica • 587  
Computação multipartidária segura • 587  
Confidencialidade assistida por hardware confiável • 587  
Protocolos de mistura (mixing) • 588  
CoinSwap • 589  
TumbleBit • 590  
Dandelion • 590  
Transações confidenciais • 592  
MimbleWimble • 592  
Zkledger • 593  
Criptografia baseada em atributos • 593  
Assinaturas anônimas • 593

Zether • 594  
Privacidade usando protocolos de Camada 2 • 594  
Gerenciadores de privacidade • 594

Privacidade usando conhecimento zero • 594  
Compromissos criptográficos • 595  
Provas de conhecimento zero • 597  
Construindo zk-SNARKs • 601

Exemplo • 610

Resumo ..................................................................................................................................... 616

**Capítulo 19: Segurança em Blockchain** 619  
Segurança .................................................................................................................................. 619  
Camadas do blockchain e ataques ........................................................................................... 621

Camada de hardware • 622  
Camada de rede • 623  
Camada do blockchain • 624

Ataques às transações • 624  
Ataques de repetição de transações • 625  
Ataques aos protocolos de consenso • 626  
Gasto duplo • 627  
Mineração egoísta • 627  
Reorganização da cadeia e bifurcação • 627

Camada de aplicação do blockchain • 628  
Vulnerabilidades em contratos inteligentes • 628  
Ataques em DeFi • 631

Camada de interface • 631  
Ataques/manipulações de oráculos • 632  
Ataques a carteiras • 632

Ataques a blockchains de Camada 2 ........................................................................................ 634  
Camada de criptografia • 635

Ataques à criptografia de chave pública • 635  
Ataques a funções de hash • 636  
Vulnerabilidades e ataques relacionados à gestão de chaves • 636  
Ataques relacionados a provas de conhecimento zero • 637

Ferramentas e mecanismos de análise de segurança ............................................................... 638  
Verificação formal • 639

Verificação formal de contratos inteligentes • 640  
Verificação de modelos • 641

Segurança de contratos inteligentes • 644  
Oyente • 645  
Solgraph • 646

Modelagem de ameaças ........................................................................................................... 646  
Regulamentação e conformidade ............................................................................................ 649  
Resumo ..................................................................................................................................... 649

**Capítulo 20: Identidade Descentralizada** 651  
Identidade .................................................................................................................................. 651  
Identidade digital ...................................................................................................................... 652

Modelo de identidade centralizada • 652  
Modelo de identidade federada • 653  
Modelo de identidade descentralizada • 657  
Identidade autossoberana (SSI) • 658  
Componentes do SSI • 659

Identidade no Ethereum ........................................................................................................... 672  
Identidade no mundo do Web3, DeFi e Metaverso .................................................................. 672  
Projetos específicos de blockchain para SSI ............................................................................ 675

Hyperledger Indy, Aries, Ursa e AnonCreds • 675  
Outros projetos • 676  
Outras iniciativas • 676

Desafios ..................................................................................................................................... 676  
Resumo ..................................................................................................................................... 677

**Capítulo 21: Finanças Descentralizadas (DeFi)** 679  
Introdução .................................................................................................................................. 679  
Mercados financeiros ................................................................................................................ 681

Negociação • 681  
Exchanges • 682

Ordens e propriedades de ordens • 682  
Sistemas de gerenciamento e roteamento de ordens • 683  
Componentes de uma negociação • 683  
Ciclo de vida de uma negociação • 684

Aplicações de blockchain nas finanças ..................................................................................... 685  
Seguros • 685  
Liquidação pós-negociação • 685  
Prevenção de crimes financeiros • 686  
Pagamentos • 688

Finanças descentralizadas ....................................................................................................... 690  
Propriedades do DeFi • 691  
Camadas do DeFi • 692  
Primitivas do DeFi • 693  
Serviços DeFi • 694

Tokenização de ativos • 694  
Exchanges descentralizadas • 695  
Empréstimos instantâneos (flash loans) • 701  
Derivativos • 702  
Transmissão de dinheiro (money streaming) • 703  
Farming de rendimento (yield farming) • 703  
Seguros • 704  
Empréstimos descentralizados – empréstimos e financiamentos • 704

Benefícios do DeFi • 707  
Uniswap • 708  
Trocando o token • 708  
Pool de liquidez da Uniswap • 710

Resumo ..................................................................................................................................... 714

**Capítulo 22: Aplicações de Blockchain e O Que Vem a Seguir** 715  
Casos de uso ............................................................................................................................ 715  
IoT ............................................................................................................................................ 716

Arquitetura do IoT .................................................................................................................... 716  
A camada de objetos físicos • 718  
A camada de dispositivos • 718  
A camada de rede • 718  
A camada de gerenciamento • 718  
A camada de aplicação • 718  
Benefícios da convergência entre IoT e blockchain • 719

Implementando IoT baseado em blockchain na prática ........................................................... 722  
Configurando o Raspberry Pi • 723  
Configurando o primeiro nó • 725  
Configurando o nó do Raspberry Pi • 726  
Instalando o Node.js • 727  
Montando o circuito eletrônico • 728  
Desenvolvendo e executando um contrato Solidity • 729

Governo ..................................................................................................................................... 735  
Controle de fronteiras • 735  
Eleições • 737  
Identificação do cidadão • 737

Saúde ........................................................................................................................................ 738  
Mídia ......................................................................................................................................... 739  
Blockchain e IA ......................................................................................................................... 740  
Algumas tendências emergentes ............................................................................................. 741  
Alguns desafios ........................................................................................................................ 743

Resumo ..................................................................................................................................... 745

**Prefácio**

O objetivo deste livro é ensinar a teoria e a prática da tecnologia de contabilidade distribuída a qualquer pessoa interessada em aprender esse fascinante novo assunto. Qualquer um pode se beneficiar deste livro, seja um tecnólogo experiente, estudante, executivo de negócios ou entusiasta. Para isso, procuro oferecer uma referência abrangente e aprofundada sobre tecnologia de contabilidade distribuída que atenda ao especialista e também seja acessível aos iniciantes. Foco principalmente em descrever as características centrais do blockchain para que os leitores possam construir uma base sólida sobre a qual desenvolver ainda mais conhecimento e especialização. Os principais tópicos incluem os princípios centrais do blockchain, criptografia, algoritmos de consenso, teoria de sistemas distribuídos e contratos inteligentes. Além disso, tópicos práticos, como programação de contratos inteligentes em Solidity, construção de redes blockchain, uso de frameworks de desenvolvimento blockchain como o Truffle e escrita de aplicações descentralizadas e descrições, constituem uma parte significativa deste livro.  
Além disso, muitos tipos de blockchains, casos de uso relacionados e aplicações intersetoriais da tecnologia blockchain são discutidos em detalhes.

Este livro é uma combinação única de princípios teóricos e aplicação prática. Os leitores não apenas poderão entender os fundamentos técnicos dessa tecnologia, mas também serão capazes de escrever código para contratos inteligentes e construir redes blockchain. Profissionais podem usar este livro como referência, e ele também pode servir como livro-texto para estudantes que desejam aprender essa tecnologia. De fato, algumas instituições adotaram edições anteriores deste livro como livro-texto principal para seus cursos sobre tecnologia blockchain.

Este livro contém seis novos capítulos sobre os tópicos mais recentes em blockchain, incluindo escalabilidade, segurança, privacidade, o Ethereum Merge, identidade descentralizada e finanças descentralizadas.

Espero que este trabalho sirva bem a tecnólogos, professores, estudantes, cientistas, desenvolvedores, executivos de negócios e qualquer pessoa que deseje aprender essa tecnologia fascinante por muitos anos.

**Para quem este livro é**

Este livro é para qualquer pessoa que queira entender a tecnologia blockchain em profundidade. Ele também pode ser usado como um recurso de referência por desenvolvedores que estão criando aplicações para blockchain. Pode também ser usado como livro-texto para cursos relacionados à tecnologia blockchain e criptomoedas, além de ser um recurso de aprendizado para diversos exames e certificações relacionados a criptomoedas e tecnologia blockchain.

**O que este livro cobre**

* **Capítulo 1**, *Blockchain 101*, introduz os conceitos básicos de computação distribuída, sobre os quais a tecnologia blockchain se baseia. Ele também aborda a história, definições, características, tipos e benefícios dos blockchains, juntamente com vários mecanismos de consenso que estão no núcleo da tecnologia blockchain.
* **Capítulo 2**, *Descentralização*, cobre o conceito de descentralização e sua relação com a tecnologia blockchain. Vários métodos e plataformas que podem ser usados para descentralizar um processo ou sistema também serão apresentados.
* **Capítulo 3**, *Criptografia Simétrica*, introduz os fundamentos teóricos da criptografia simétrica, que são necessários para entender como diversos serviços de segurança como confidencialidade e integridade são fornecidos.
* **Capítulo 4**, *Criptografia Assimétrica*, introduz conceitos como chaves públicas e privadas, assinaturas digitais e funções hash com exemplos práticos.
* **Capítulo 5**, *Algoritmos de Consenso*, cobre os fundamentos dos algoritmos de consenso e descreve o design e funcionamento interno de vários algoritmos de consenso. Abrange tanto protocolos tradicionais quanto protocolos de consenso de blockchain.
* **Capítulo 6**, *Arquitetura do Bitcoin*, cobre o Bitcoin, o primeiro e maior blockchain. Introduz conceitos técnicos relacionados à criptomoeda Bitcoin em detalhes.
* **Capítulo 7**, *Bitcoin na Prática*, cobre a rede Bitcoin, protocolos relevantes e várias carteiras Bitcoin. Além disso, protocolos avançados, negociação e pagamentos em Bitcoin também são introduzidos. Clientes Bitcoin e APIs de programação para construção de aplicações Bitcoin também são cobertos.
* **Capítulo 8**, *Contratos Inteligentes*, fornece uma discussão aprofundada sobre contratos inteligentes. Tópicos como a história, definição de contratos inteligentes, contratos Ricardianos, oráculos e os aspectos teóricos dos contratos inteligentes são apresentados.
* **Capítulo 9**, *Arquitetura do Ethereum*, introduz o design e a arquitetura do blockchain Ethereum em detalhe. Cobre vários conceitos técnicos relacionados ao Ethereum e explica os princípios subjacentes, características e componentes desta plataforma em profundidade. Outros tópicos abordados são a Máquina Virtual Ethereum, mineração e protocolos de suporte ao Ethereum.
* **Capítulo 10**, *Ethereum na Prática*, cobre tópicos relacionados à configuração de redes privadas para desenvolvimento e programação de contratos inteligentes no Ethereum.
* **Capítulo 11**, *Ferramentas, Linguagens e Frameworks para Desenvolvedores Ethereum*, oferece uma introdução prática detalhada à linguagem de programação Solidity e diferentes ferramentas e frameworks relevantes usados no desenvolvimento Ethereum.
* **Capítulo 12**, *Desenvolvimento Web3 Usando Ethereum*, cobre o desenvolvimento de aplicações descentralizadas e contratos inteligentes usando a blockchain Ethereum. Uma introdução detalhada à API Web3 é fornecida junto com vários exemplos práticos e um projeto final.
* **Capítulo 13**, *The Merge e Além*, introduz os desenvolvimentos mais recentes no Ethereum, como a Beacon Chain, sharding e futuras atualizações.
* **Capítulo 14**, *Hyperledger*, apresenta uma discussão sobre o projeto Hyperledger da Linux Foundation, que inclui diferentes projetos de blockchain introduzidos por seus membros.
* **Capítulo 15**, *Tokenização*, introduz o tema da tokenização, stablecoins e outras ideias relevantes como ofertas iniciais de moedas e padrões de desenvolvimento de tokens.
* **Capítulo 16**, *Blockchain Empresarial*, cobre o uso e aplicação da tecnologia blockchain em ambientes empresariais e plataformas de DLT como o Quorum.
* **Capítulo 17**, *Escalabilidade*, é dedicado à discussão de um dos principais desafios enfrentados pela tecnologia blockchain e como abordá-lo. Focamos nas soluções de camada 2, embora outras soluções também sejam discutidas.
* **Capítulo 18**, *Privacidade em Blockchain*, introduz o problema da falta de privacidade em blockchains e explica várias técnicas para superar essa limitação. Cobrimos soluções para alcançar confidencialidade e anonimato usando técnicas como zk-SNARKs, mixers e vários outros métodos.
* **Capítulo 19**, *Segurança em Blockchain*, introduz os diversos desafios de segurança nas blockchains e como resolvê-los. Isso inclui segurança de contratos inteligentes, verificação formal, preocupações de segurança e boas práticas em cada camada do sistema blockchain.
* **Capítulo 20**, *Identidade Descentralizada*, cobre um dos tópicos mais quentes do mundo blockchain. A identidade descentralizada é a base do ecossistema Web3. Neste capítulo, exploramos os métodos, técnicas e ecossistemas que sustentam o Web3 e o cenário de identidade descentralizada.
* **Capítulo 21**, *Finanças Descentralizadas (DeFi)*, cobre o uso e aplicação das finanças descentralizadas, seus diversos aspectos, casos de uso de blockchain em finanças e diferentes protocolos DeFi.
* **Capítulo 22**, *Aplicações de Blockchain e O Que Vem a Seguir*, fornece uma introdução prática e detalhada às aplicações da tecnologia blockchain em áreas além das criptomoedas, incluindo Internet das Coisas, governo, mídia e finanças. O objetivo é fornecer informações sobre o panorama atual, projetos e esforços de pesquisa relacionados à tecnologia blockchain.
* **Capítulo 23**, *Blockchains Alternativos*, introduz soluções e plataformas alternativas de blockchain como conteúdo bônus disponível online. Ele cobre detalhes técnicos e características de blockchains e plataformas alternativas. Este é um capítulo online e você pode lê-lo no seguinte link: <https://packt.link/OceZK>.

**Para aproveitar ao máximo este livro**

Para tirar o melhor proveito deste livro, é desejável alguma familiaridade com ciência da computação e conhecimento básico de uma linguagem de programação.

**Baixar os arquivos de exemplo de código**

O pacote de código do livro está hospedado no GitHub:  
📎 <https://github.com/PacktPublishing/Mastering-Blockchain-Fourth-Edition>

**Baixar as imagens coloridas**

Fornecemos um arquivo PDF com imagens coloridas das capturas de tela/diagramas usados neste livro:  
📎 <https://packt.link/5y4vk>

**Convenções utilizadas**

* CodeInText: indica trechos de código no texto, nomes de tabelas, nomes de pastas, arquivos, extensões, caminhos, URLs fictícias, entradas do usuário e handles do Twitter.

**Entre em contato**

* Feedback geral: envie e-mail para feedback@packtpub.com com o título do livro no assunto.
* Perguntas sobre o conteúdo: questions@packtpub.com
* Relatar erros: <http://www.packtpub.com/submit-errata>
* Pirataria: envie o link para copyright@packtpub.com
* Quer escrever para a Packt? Visite: <http://authors.packtpub.com>

**Compartilhe sua opinião**

Depois de ler *Mastering Blockchain – Fourth Edition*, adoraríamos ouvir seu feedback. Por favor, clique aqui para acessar diretamente a página de avaliação na Amazon.