

Imran Bashir 著

精通区块链

第2版（影印版）

Mastering Blockchain, 2nd Edition



东南大学出版社
SOUTHEAST UNIVERSITY PRESS

Packt>

精通区块链 第2版(影印版)

Mastering Blockchain, 2nd Edition

Imran Bashir 著



南京 东南大学出版社

图书在版编目(CIP)数据

精通区块链:第2版:英文/(英)伊姆兰·巴希尔
(Imran Bashir)著. —影印本. —南京:东南大学出版社,
2019.5

书名原文:Mastering Blockchain, 2nd Edition

ISBN 978-7-5641-8319-6

I. ①精… II. ①伊… III. ①电子商务—支付方式—
英文 IV. ①F713.361.3

中国版本图书馆 CIP 数据核字(2019)第 046198 号

图字:10-2018-498 号

© 2018 by PACKT Publishing Ltd.

Reprint of the English Edition, jointly published by PACKT Publishing Ltd and Southeast University Press, 2019.

Authorized reprint of the original English edition, 2018 PACKT Publishing Ltd, the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 PACKT Publishing Ltd 出版 2018。

英文影印版由东南大学出版社出版 2019。此影印版的出版和销售得到出版权和销售权的所有者——PACKT Publishing Ltd 的许可。

版权所有,未得书面许可,本书的任何部分和全部不得以任何形式重制。

精通区块链 第2版(影印版)

出版发行:东南大学出版社

地 址:南京四牌楼2号 邮编:210096

出 版 人:江建中

网 址: <http://www.seupress.com>

电子邮件: press@seupress.com

印 刷:常州市武进第三印刷有限公司

开 本:787毫米×980毫米 16开本

印 张:41

字 数:803千字

版 次:2019年5月第1版

印 次:2019年5月第1次印刷

书 号:ISBN 978-7-5641-8319-6

定 价:118.00元

本社图书若有印装质量问题,请直接与营销部联系。电话(传真):025-83791830



mapt.io

Mapt is an online digital library that gives you full access to over 5,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Mapt is fully searchable
- Copy and paste, print, and bookmark content

PacktPub.com

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the author

Imran Bashir has an M.Sc. in Information Security from Royal Holloway, University of London, and has a background in software development, solution architecture, infrastructure management, and IT service management. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE) and the British Computer Society (BCS).

Imran has sixteen years' of experience in the public and financial sectors. He worked on large scale IT projects in the public sector before moving to the financial services industry. Since then, he has worked in various technical roles for different financial companies in Europe's financial capital, London. He is currently working for an investment bank in London as Vice President in the Technology department.

I would like to thank the talented team at Packt, including Ben Renow-Clarke, Suzanne Coutinho, Alex Sorrentino, Gary Schwartz, and Bhagyashree Rai, who provided prompt guidance and valuable feedback throughout this project. I am also extremely thankful to the reviewer, Pranav Burnwal, who provided constructive and very useful feedback that helped me tremendously to improve the material in this book.

I thank my wife and children for putting up with my all-night and weekend-long writing sessions.

Above all, I would like to thank my parents, whose blessings have made everything possible for me.

About the reviewer

Pranav Burnwal has a background in Research and Development, and he has been working with cutting-edge technologies for the past few years. The technologies he works on range from blockchain, big data, analytics (log and data), cloud, to message queues, NoSQL, web servers, and so on. He has worked across various domains ranging from BFSI, HLS, FMCG, and automobiles to name a few.

Pranav is an active community member in multiple communities. He is the Regional Head for Blockchain Education Network (BEN), a registered NGO and a worldwide network of people of blockchain. He has also organized multiple meetups and a start-up weekend in India.

Pranav has also been an active trainer in the blockchain space for an exciting period of three years now, for an audience ranging from junior developers to senior VPs. This has also given him insights into how people understand a new and complex technology, which helped him frame this book in the best interest of the readers.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit authors.packtpub.com and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface	1
Chapter 1: Blockchain 101	9
The growth of blockchain technology	9
Distributed systems	13
The history of blockchain and Bitcoin	15
Electronic cash	15
Blockchain	17
Blockchain defined	17
Peer-to-peer	17
Distributed ledger	18
Cryptographically-secure	18
Append-only	18
Updateable via consensus	18
Generic elements of a blockchain	21
How blockchain works	24
How blockchain accumulates blocks	24
Benefits and limitations of blockchain	25
Tiers of blockchain technology	27
Features of a blockchain	28
Types of blockchain	31
Distributed ledgers	32
Distributed Ledger Technology	32
Public blockchains	33
Private blockchains	33
Semiprivate blockchains	33
Sidechains	34
Permissioned ledger	34
Shared ledger	34
Fully private and proprietary blockchains	35
Tokenized blockchains	35
Tokenless blockchains	35
Consensus	36
Consensus mechanism	36
Types of consensus mechanisms	37
Consensus in blockchain	37
CAP theorem and blockchain	40
Summary	42
Chapter 2: Decentralization	43
Decentralization using blockchain	43

Methods of decentralization	45
Disintermediation	46
Contest-driven decentralization	46
Routes to decentralization	48
How to decentralize	49
The decentralization framework example	50
Blockchain and full ecosystem decentralization	50
Storage	51
Communication	52
Computing power and decentralization	53
Smart contracts	54
Decentralized Organizations	55
Decentralized Autonomous Organizations	55
Decentralized Autonomous Corporations	56
Decentralized Autonomous Societies	56
Decentralized Applications (DApps)	57
Requirements of a Decentralized Application	57
Operations of a DApp	57
DApp examples	58
KYC-Chain	58
OpenBazaar	58
Lazooz	58
Platforms for decentralization	58
Ethereum	59
MaidSafe	59
Lisk	59
Summary	60
Chapter 3: Symmetric Cryptography	61
Working with the OpenSSL command line	61
Introduction	62
Mathematics	63
Set	63
Group	63
Field	63
A finite field	64
Order	64
An abelian group	64
Prime fields	64
Ring	64
A cyclic group	64
Modular arithmetic	65
Cryptography	65
Confidentiality	66
Integrity	66
Authentication	66

Entity authentication	67
Data origin authentication	67
Non-repudiation	68
Accountability	68
Cryptographic primitives	69
Symmetric cryptography	70
Stream ciphers	70
Block ciphers	71
Block encryption mode	72
Electronic Code Book	73
Cipher Block Chaining	73
Counter mode	74
Keystream generation mode	74
Message authentication mode	74
Cryptographic hash mode	75
Data Encryption Standard	75
Advanced Encryption Standard	75
How AES works	76
Summary	80
Chapter 4: Public Key Cryptography	81
Asymmetric cryptography	81
Integer factorization	84
Discrete logarithm	84
Elliptic curves	84
Public and private keys	85
RSA	85
Encryption and decryption using RSA	87
Elliptic Curve Cryptography	87
Mathematics behind ECC	87
Point addition	88
Point doubling	91
Discrete logarithm problem in ECC	94
RSA using OpenSSL	96
RSA public and private key pair	96
Private key	96
Public key	97
Exploring the public key	99
Encryption and decryption	99
Encryption	99
Decryption	100
ECC using OpenSSL	100
ECC private and public key pair	100
Private key	101
Private key generation	101
Hash functions	104
Compression of arbitrary messages into fixed-length digest	104
Easy to compute	104
Preimage resistance	104
Second preimage resistance	105

Collision resistance	105
Message Digest	106
Secure Hash Algorithms	106
Design of Secure Hash Algorithms	107
Design of SHA-256	107
Design of SHA-3 (Keccak)	109
OpenSSL example of hash functions	110
Message Authentication Codes	110
MACs using block ciphers	110
Hash-based MACs	111
Merkle trees	112
Patricia trees	112
Distributed Hash Tables	113
Digital signatures	114
RSA digital signature algorithm	114
Sign then encrypt	115
Encrypt then sign	116
Elliptic Curve Digital Signature Algorithm	116
How to generate a digital signature using OpenSSL	118
ECDSA using OpenSSL	119
Homomorphic encryption	121
Signcryption	122
Zero-Knowledge Proofs	122
Blind signatures	123
Encoding schemes	123
Financial markets and trading	124
Trading	124
Exchanges	125
Orders and order properties	125
Order management and routing systems	125
Components of a trade	126
The underlying instrument	126
General attributes	126
Economics	126
Sales	127
Counterparty	127
Trade life cycle	127
Order anticipators	128
Market manipulation	128
Summary	129
Chapter 5: Introducing Bitcoin	131
Bitcoin	134
Bitcoin definition	136
Bitcoin – a bird's-eye view	137
Sending a payment to someone	138
Digital keys and addresses	145
Private keys in Bitcoin	146
Public keys in Bitcoin	147

Addresses in Bitcoin	148
Base58Check encoding	150
Vanity addresses	150
Multisignature addresses	151
Transactions	152
The transaction life cycle	152
Transaction fee	153
Transaction pools	154
The transaction data structure	154
Metadata	155
Inputs	156
Outputs	156
Verification	157
The script language	157
Commonly used opcodes	157
Types of transactions	158
Coinbase transactions	161
Contracts	161
Transaction verification	162
Transaction malleability	163
Blockchain	163
The structure of a block	163
The structure of a block header	164
The genesis block	166
Mining	169
Tasks of the miners	170
Mining rewards	170
Proof of Work (PoW)	171
The mining algorithm	171
The hash rate	174
Mining systems	174
CPU	175
GPU	175
FPGA	175
ASICs	176
Mining pools	177
Summary	180
Chapter 6: Bitcoin Network and Payments	181
The Bitcoin network	181
Wallets	191
Non-deterministic wallets	192
Deterministic wallets	192
Hierarchical Deterministic wallets	192
Brain wallets	193
Paper wallets	193
Hardware wallets	193

Online wallets	194
Mobile wallets	194
Bitcoin payments	195
Innovation in Bitcoin	197
Bitcoin Improvement Proposals (BIPs)	198
Advanced protocols	198
Segregated Witness (SegWit)	199
Bitcoin Cash	200
Bitcoin Unlimited	200
Bitcoin Gold	201
Bitcoin investment and buying and selling bitcoins	202
Summary	204
Chapter 7: Bitcoin Clients and APIs	205
Bitcoin installation	205
Types of Bitcoin Core clients	206
Bitcoin	206
Bitcoin-cli	207
Bitcoin-qt	207
Setting up a Bitcoin node	208
Setting up the source code	209
Setting up bitcoin.conf	209
Starting up a node in testnet	210
Starting up a node in regtest	210
Experimenting with Bitcoin-cli	211
Bitcoin programming and the command-line interface	213
Summary	214
Chapter 8: Alternative Coins	215
Theoretical foundations	218
Alternatives to Proof of Work	219
Proof of Storage	222
Proof of Stake (PoS)	222
Various stake types	222
Proof of coinage	222
Proof of Deposit (PoD)	223
Proof of Burn	223
Proof of Activity (PoA)	223
Nonoutsourcable puzzles	223
Difficulty adjustment and retargeting algorithms	224
Kimoto Gravity Well	225
Dark Gravity Wave	226
DigiShield	226
MIDAS	227
Bitcoin limitations	227
Privacy and anonymity	227
Mixing protocols	228

Third-party mixing protocols	229
Inherent anonymity	230
Extended protocols on top of Bitcoin	230
Colored coins	230
Counterparty	231
Development of altcoins	232
Consensus algorithms	233
Hashing algorithms	233
Difficulty adjustment algorithms	233
Inter-block time	233
Block rewards	234
Reward halving rate	234
Block size and transaction size	234
Interest rate	234
Coinage	234
Total supply of coins	234
Namecoin	235
Trading Namecoins	237
Obtaining Namecoins	237
Generating Namecoin records	240
Litecoin	242
Primecoin	246
Trading Primecoin	247
Mining guide	248
Zcash	250
Trading Zcash	252
Mining guide	252
Address generation	256
GPU mining	257
Downloading and compiling nheqminer	257
Initial Coin Offerings (ICOs)	259
ERC20 tokens	261
Summary	261
Chapter 9: Smart Contracts	263
History	263
Definition	264
Ricardian contracts	267
Smart contract templates	271
Oracles	272
Smart Oracles	275
Deploying smart contracts on a blockchain	275
The DAO	276
Summary	277
Chapter 10: Ethereum 101	279
Introduction	279

The yellow paper	280
Useful mathematical symbols	281
Ethereum blockchain	282
Ethereum – bird's eye view	283
The Ethereum network	287
Mainnet	287
Testnet	288
Private net	288
Components of the Ethereum ecosystem	289
Keys and addresses	290
Accounts	290
Types of accounts	291
Transactions and messages	292
Contract creation transaction	295
Message call transaction	296
Messages	297
Calls	298
Transaction validation and execution	299
The transaction substate	299
State storage in the Ethereum blockchain	299
The world state	300
The account state	300
Transaction receipts	301
Ether cryptocurrency / tokens (ETC and ETH)	303
The Ethereum Virtual Machine (EVM)	304
Execution environment	306
Machine state	307
The iterator function	308
Smart contracts	309
Native contracts	310
Summary	312
Chapter 11: Further Ethereum	313
 Programming languages	314
Runtime bytecode	315
Opcodes and their meaning	315
Arithmetic operations	315
Logical operations	316
Cryptographic operations	317
Environmental information	317
Block information	318
Stack, memory, storage, and flow operations	319
Push operations	319
Duplication operations	320
Exchange operations	320
Logging operations	321
System operations	321
Blocks and blockchain	322

The genesis block	324
The block validation mechanism	325
Block finalization	326
Block difficulty	326
Gas	328
Fee schedule	329
Forks in the blockchain	330
Nodes and miners	330
The consensus mechanism	331
Ethash	333
CPU mining	334
GPU mining	335
Benchmarking	336
Mining rigs	337
Mining pools	338
Wallets and client software	339
Geth	339
Eth	339
Pyethapp	339
Parity	339
Light clients	339
Installation	340
Eth installation	340
Mist browser	340
Geth	343
The geth console	344
Funding the account with bitcoin	345
Parity installation	346
Creating accounts using the parity command line	350
APIs, tools, and DApps	350
Applications (DApps and DAOs) developed on Ethereum	350
Tools	351
Supporting protocols	351
Whisper	351
Swarm	352
Scalability, security, and other challenges	353
Trading and investment	353
Summary	354
Chapter 12: Ethereum Development Environment	355
Test networks	356
Setting up a private net	357
Network ID	358
The genesis file	358
Data directory	360
Flags and their meaning	360
Static nodes	361
Starting up the private network	361
Running Mist on private net	367
Deploying contracts using Mist	370

Block explorer for private net / local Ethereum block explorer	375
Summary	378
Chapter 13: Development Tools and Frameworks	379
Languages	381
Compilers	381
Solidity compiler (solc)	381
Installation on Linux	381
Installation on macOS	382
Integrated Development Environments (IDEs)	384
Remix	384
Tools and libraries	387
Node version 7	388
EthereumJS	388
Ganache	389
MetaMask	390
Truffle	393
Installation	394
Contract development and deployment	395
Writing	395
Testing	397
Solidity language	397
Types	398
Value types	398
Boolean	398
Integers	398
Address	399
Literals	400
Integer literals	400
String literals	400
Hexadecimal literals	400
Enums	400
Function types	401
Internal functions	401
External functions	401
Reference types	401
Arrays	401
Structs	402
Data location	402
Mappings	402
Global variables	403
Control structures	403
Events	405
Inheritance	405
Libraries	406
Functions	407
Layout of a Solidity source code file	410
Version pragma	410
Import	410
Comments	411
Summary	411

Chapter 14: Introducing Web3	413
Web3	413
Contract deployment	414
POST requests	421
The HTML and JavaScript frontend	422
Installing web3.js	423
Example	424
Creating a web3 object	426
Checking availability by calling any web3 method	426
Contract functions	427
Development frameworks	430
Truffle	430
Initializing Truffle	430
Interaction with the contract	439
Another example	442
An example project – Proof of Idea	445
Oracles	458
Deployment on decentralized storage using IPFS	460
Installing IPFS	461
Distributed ledgers	464
Summary	464
Chapter 15: Hyperledger	465
Projects under Hyperledger	465
Fabric	466
Sawtooth Lake	466
Iroha	467
Burrow	467
Indy	468
Explorer	468
Cello	468
Composer	469
Quilt	469
Hyperledger as a protocol	469
The reference architecture	470
Requirements and design goals of Hyperledger Fabric	472
The modular approach	472
Privacy and confidentiality	472
Scalability	473
Deterministic transactions	473
Identity	473
Auditability	473
Interoperability	474
Portability	474
Rich data queries	474
Fabric	474
Hyperledger Fabric	475
Membership services	476