

# **Beginning Blockchain**

**A Beginner's Guide to Building  
Blockchain Solutions**

**Bikramaditya Singhal  
Gautam Dhameja  
Priyansu Sekhar Panda**

**Apress®**

## ***Beginning Blockchain***

Bikramaditya Singhal  
Bangalore, Karnataka, India

Gautam Dhameja  
Berlin, Berlin, Germany

Priyansu Sekhar Panda  
Bangalore, Karnataka, India

ISBN-13 (pbk): 978-1-4842-3443-3

ISBN-13 (electronic): 978-1-4842-3444-0

<https://doi.org/10.1007/978-1-4842-3444-0>

Library of Congress Control Number: 2018945613

Copyright © 2018 by Bikramaditya Singhal, Gautam Dhameja,  
Priyansu Sekhar Panda

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr  
Acquisitions Editor: Nikhil Karkal  
Development Editor: Laura Berendson  
Coordinating Editor: Divya Modi

Cover designed by eStudioCalamar

Cover image designed by Freepik ([www.freepik.com](http://www.freepik.com))

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail [orders-ny@springer-sbm.com](mailto:orders-ny@springer-sbm.com), or visit [www.springeronline.com](http://www.springeronline.com). Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail [rights@apress.com](mailto:rights@apress.com), or visit [www.apress.com/rights-permissions](http://www.apress.com/rights-permissions).

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at [www.apress.com/bulk-sales](http://www.apress.com/bulk-sales).

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at [www.apress.com/978-1-4842-3443-3](http://www.apress.com/978-1-4842-3443-3). For more detailed information, please visit [www.apress.com/source-code](http://www.apress.com/source-code).

Printed on acid-free paper

# Table of Contents

<b>About the Authors</b> .....	<b>ix</b>
<b>About the Technical Reviewer</b> .....	<b>xi</b>
<b>Acknowledgments</b> .....	<b>xiii</b>
<b>Introduction</b> .....	<b>xv</b>
<b>Chapter 1: Introduction to Blockchain</b> .....	<b>1</b>
Backstory of Blockchain .....	2
What is Blockchain?.....	4
Centralized vs. Decentralized Systems.....	11
Centralized Systems.....	14
Decentralized Systems.....	15
Layers of Blockchain.....	17
Application Layer .....	19
Execution Layer .....	20
Semantic Layer.....	20
Propagation Layer .....	21
Consensus Layer .....	22
Why is Blockchain Important? .....	23
Limitations of Centralized Systems .....	23
Blockchain Adoption So Far.....	24
Blockchain Uses and Use Cases .....	26
Summary.....	28
References .....	29

TABLE OF CONTENTS

**Chapter 2: How Blockchain Works .....31**

- Laying the Blockchain Foundation ..... 32
- Cryptography..... 34
  - Symmetric Key Cryptography ..... 37
  - Cryptographic Hash Functions ..... 55
  - MAC and HMAC..... 76
  - Asymmetric Key Cryptography ..... 78
  - Diffie-Hellman Key Exchange ..... 98
  - Symmetric vs. Asymmetric Key Cryptography ..... 102
- Game Theory ..... 104
  - Nash Equilibrium ..... 107
  - Prisoner’s Dilemma ..... 108
  - Byzantine Generals’ Problem..... 110
  - Zero-Sum Games..... 112
  - Why to Study Game Theory ..... 113
- Computer Science Engineering..... 114
  - The Blockchain ..... 114
  - Merkle Trees ..... 117
- Putting It All Together ..... 122
  - Properties of Blockchain Solutions..... 124
  - Blockchain Transactions ..... 127
  - Distributed Consensus Mechanisms ..... 130
- Blockchain Applications ..... 135
- Scaling Blockchain..... 139
  - Off-Chain Computation ..... 140
  - Sharding Blockchain State ..... 143
- Summary..... 145
- References ..... 146

<b>Chapter 3: How Bitcoin Works</b> .....	<b>149</b>
The History of Money .....	150
Dawn of Bitcoin.....	153
What Is Bitcoin?.....	154
Working with Bitcoins.....	157
The Bitcoin Blockchain.....	159
Block Structure.....	161
The Genesis Block .....	169
The Bitcoin Network.....	172
Network Discovery for a New Node.....	174
Bitcoin Transactions .....	179
Consensus and Block Mining .....	184
Block Propagation .....	193
Putting It all Together.....	195
Bitcoin Scripts.....	195
Bitcoin Transactions Revisited.....	196
Scripts .....	204
Full Nodes vs. SPVs.....	209
Full Nodes.....	209
SPVs .....	210
Bitcoin Wallets .....	212
Summary.....	216
References.....	216
<b>Chapter 4: How Ethereum Works</b> .....	<b>219</b>
From Bitcoin to Ethereum .....	220
Ethereum as a Next-Gen Blockchain .....	221
Design Philosophy of Ethereum.....	223

## TABLE OF CONTENTS

Enter the Ethereum Blockchain.....	224
Ethereum Blockchain.....	225
Ethereum Accounts .....	228
Trie Usage.....	236
Merkle Patricia Tree.....	237
RLP Encoding.....	239
Ethereum Transaction and Message Structure.....	240
Ethereum State Transaction Function.....	245
Gas and Transaction Cost .....	248
Ethereum Smart Contracts.....	253
Contract Creation.....	256
Ethereum Virtual Machine and Code Execution .....	257
Ethereum Ecosystem .....	263
Swarm .....	264
Whisper .....	264
DApp.....	264
Development Components .....	265
Summary.....	265
References.....	266
<b>Chapter 5: Blockchain Application Development .....</b>	<b>267</b>
Decentralized Applications.....	267
Blockchain Application Development.....	269
Libraries and Tools .....	270
Interacting with the Bitcoin Blockchain .....	272
Setup and Initialize the bitcoinjs Library in a <i>node.js</i> Application .....	273
Create Keypairs for the Sender and Receiver.....	274
Get Test Bitcoins in the Sender's Wallet .....	275

Get the Sender’s Unspent Outputs ..... 276

Prepare Bitcoin Transaction..... 278

Sign Transaction Inputs ..... 280

Create Transaction Hex..... 280

Broadcast Transaction to the Network ..... 281

Interacting Programmatically with Ethereum—Sending Transactions ..... 283

    Set Up Library and Connection ..... 284

    Set Up Ethereum Accounts ..... 285

    Get Test Ether in Sender’s Account..... 286

    Prepare Ethereum Transaction ..... 287

    Sign Transaction ..... 288

    Send Transaction to the Ethereum Network ..... 290

Interacting Programmatically with Ethereum—Creating a Smart Contract..... 292

    Prerequisites ..... 292

    Program the Smart Contract..... 293

    Compile Contract and Get Details..... 297

    Deploy Contract to Ethereum Network ..... 302

Interacting Programmatically with Ethereum—Executing Smart  
Contract Functions ..... 307

    Get Reference to the Smart Contract..... 308

    Execute Smart Contract Function ..... 309

Blockchain Concepts Revisited ..... 312

Public vs. Private Blockchains ..... 313

Decentralized Application Architecture ..... 314

    Public Nodes vs. Self-Hosted Nodes ..... 315

    Decentralized Applications and Servers ..... 316

Summary..... 317

References ..... 317

TABLE OF CONTENTS

**Chapter 6: Building an Ethereum DApp .....319**

- The DApp..... 319
- Setting Up a Private Ethereum Network ..... 321
  - Install go-ethereum (*geth*)..... 321
  - Create *geth* Data Directory ..... 322
  - Create a *geth* Account ..... 323
  - Create *genesis.json* Configuration File ..... 324
  - Run the First Node of the Private Network ..... 325
  - Run the Second Node of the Network ..... 329
- Creating the Smart Contract ..... 334
- Deploying the Smart Contract..... 344
  - Setting up *web3* Library and Connection ..... 345
  - Deploy the Contract to the Private Network ..... 345
- Client Application ..... 359
- Summary..... 375
- References..... 375

**Index.....377**



# About the Authors



**Bikramaditya Singhal** is a Blockchain expert and AI practitioner with experience working in multiple industries. He is proficient in Blockchain, Bitcoin, Ethereum, Hyperledger, cryptography, cyber security, and data science. He has extensive experience in training and consulting on Blockchain and has designed many Blockchain solutions. He worked with companies such as WISEKey, Tech Mahindra, Microsoft India, Broadridge, and Chelsio Communications, and he also cofounded

a company named Mund Consulting that focuses on big data analytics and artificial intelligence. He is an active speaker at various conferences, summits, and meetups. He has also authored a book entitled *Spark for Data Science*.

## ABOUT THE AUTHORS



**Gautam Dhameja** is a Blockchain application consultant based out of Berlin, Germany. For most of this decade, he has been developing and delivering enterprise software including Web and Mobile apps, Cloud-based hyper-scale IoT solutions, and more recently, Blockchain-based decentralized applications (DApps). He possesses a deep understanding of the decentralized stack, cloud solutions architecture, and object-oriented design. His

areas of expertise include Blockchain, Cloud-based enterprise solutions, Internet of Things, distributed systems, and native and hybrid mobile apps. He is also an active blogger and regularly speaks at tech conferences and events.



**Priyansu Sekhar Panda** is a research engineer at Underwriters Laboratories, Bangalore, India. He has worked with other IT companies such as Broadridge, Infosys Limited, and Tech Mahindra. His areas of expertise include Blockchain, Bitcoin, Ethereum, Hyperledger, game theory, IoT, and artificial intelligence. Priyansu's current research is on building next-gen applications leveraging Blockchain, IoT, and AI. His major research interests include building Decentralized Autonomous Organizations (DAO), and the security, scalability, and consensus of Blockchains.

# About the Technical Reviewer



**Navin K Manaswi** has been developing AI solutions/products with the use of cutting-edge technologies and sciences related to artificial intelligence for many years. Having worked for consulting companies in Malaysia, Singapore, and the Dubai Smart City project, he has developed a rare skill of delivering end-to-end artificial intelligence solutions. He built solutions for video intelligence, document intelligence, and human-like

chatbots in his own company. Currently, he solves B2B problems in verticals of healthcare, enterprise applications, industrial IoT, and retail in the Symphony AI incubator as Deep Learning-AI Architect. Through this book, he wants to democratize cognitive computing and services for everyone, especially developers, data scientists, software engineers, database engineers, data analysts, and CXOs.

# Acknowledgments

We'd like to thank Nikhil and Divya for their cooperation and support all through and many thanks to Navin for his thorough technical review of this book. We also thank all who have directly or indirectly contributed to this book.

# Introduction

*Beginning Blockchain* is a book for those willing to learn about the technical fundamentals of Blockchain, practical implications, and hands-on development aspects of Blockchain applications. Adequate history, background, and theoretical aspects are covered to help you build a solid foundation for your Blockchain journey, and appropriate development aspects are covered with coding examples to help you jumpstart on Blockchain assignments. The first chapter introduces you to the Blockchain world and sets the context. The second chapter dives deeper into the core components of Blockchain. The third chapter is focused on Bitcoin's technical concepts so what was discussed in the second chapter could be demonstrated with Bitcoin as a cryptocurrency use case of Blockchain. The fourth chapter is dedicated to the Ethereum Blockchain in an effort to demonstrate how Blockchain could be programmed for many more use cases and not limited to just cryptocurrencies. The fifth chapter is where you get the hang of Blockchain development with examples on basic transactions in both Bitcoin and Ethereum. The sixth chapter, as the final chapter, demonstrates the end-to-end development of a decentralized application (DApp). By the end of this chapter, you will have been equipped with enough tools and techniques to address many real-world business problems with applicable Blockchain solutions. Start your journey toward limitless possibilities.