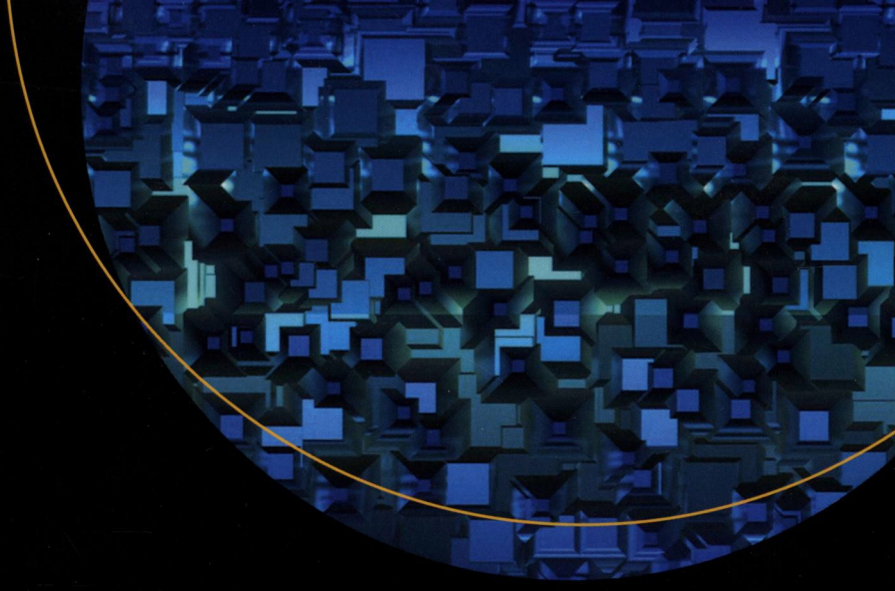


Introducing Ethereum and Solidity

Foundations of Cryptocurrency and Blockchain Programming for Beginners

Chris Dannen

Apress®

FOR PROFESSIONALS BY PROFESSIONALS®

Introducing Ethereum and Solidity

Learn how to use Solidity and the Ethereum project – second only to Bitcoin in market capitalization. Blockchain protocols are taking the world by storm, and the Ethereum project, with its Turing-complete scripting language Solidity, has rapidly become a front-runner. This book presents the blockchain phenomenon in context; then situates Ethereum in a world pioneered by Bitcoin.

See why professionals and nonprofessionals alike are honing their skills in smart contract patterns and distributed application development. You'll review the fundamentals of programming and networking, alongside its introduction to the new discipline of crypto-economics. You'll then deploy smart contracts of your own, and learn how they can serve as a back-end for JavaScript and HTML applications on the Web.

Many Solidity tutorials out there today have the same flaw: they are written for "advanced" JavaScript developers who want to transfer their skills to a blockchain environment. *Introducing Ethereum and Solidity* is accessible to technology professionals and enthusiasts of "all levels." You'll find exciting sample code that can move forward real world assets in both the academic and the corporate arenas. Find out now why this book is a powerful gateway for creative technologists of all types, from concept to deployment.

ISBN 978-1-4842-2534-9
53999
9 781484 225349

US $39.99

User level:
Beginning–Intermediate

SOURCE CODE ONLINE

Apress®
www.apress.com

Dannen

Introducing Ethereum and Solidity

Apress®

Introducing Ethereum and Solidity

Foundations of Cryptocurrency and Blockchain Programming for Beginners

Chris Dannen

Apress®

Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners

Chris Dannen
Brooklyn, New York, USA

ISBN-13 (pbk): 978-1-4842-2534-9 ISBN-13 (electronic): 978-1-4842-2535-6
DOI 10.1007/978-1-4842-2535-6

Library of Congress Control Number: 2017936045

Copyright © 2017 by Chris Dannen

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: Welmoed Spahr
Editorial Director: Todd Green
Acquisitions Editor: Louise Corrigan
Development Editor: James Markham
Technical Reviewer: Massimo Nardone
Coordinating Editor: Nancy Chen
Copy Editor: Sharon Wilkey
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

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`, or visit `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`, or visit `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 `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/9781484225349`. For more detailed information, please visit `http://www.apress.com/source-code`.

Printed on acid-free paper

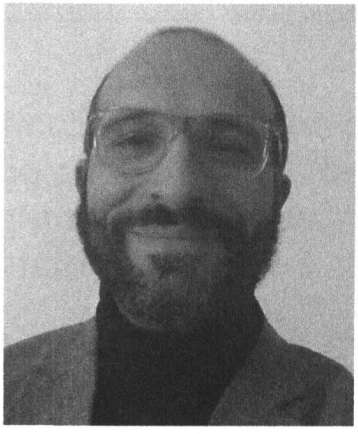
此为试读，需要完整PDF请访问：www.ertongbook.com

Many thanks to Brandon Buchanan, Christopher McClellan, Dr. Solomon Lederer, and the entire Iterative Instinct team for their support and enthusiasm. Thanks also to Joseph Lubin and the team at ConsenSys for acting as a sounding board during the writing of this book.

About the Author

Chris Dannen is a partner and founder at Iterative Instinct, a hybrid investment fund focused on cryptocurrency trading and seed-stage venture investments. He first began working with Bitcoin and Ethereum as a miner, and became gradually more enthralled in researching how smart contracts could be used to automate business logic and create new kinds of experiences with software. He was formerly a corporate strategist for Fortune 500 companies. A self-taught programmer in Objective-C and JavaScript, he holds one computer hardware patent. This is his fourth book. Chris is an avid traveler who has trekked across 20 countries, bicycled from Rome to Barcelona in 30 days, and summited Mount Fuji in under six hours. He was formerly a senior editor at *Fast Company* and today consults on technical content for major publishers such as *Quartz* and *Bloomberg*. He graduated from the University of Virginia and now resides in New York, NY.

About the Technical Reviewer



Massimo Nardone has more than 22 years of experience in security, web/mobile development, and cloud and IT architecture. His true IT passions are security and Android. He has been programming and teaching how to program with Android, Perl, PHP, Java, VB, Python, C/C++, and MySQL for more than 20 years. He holds a master of science degree in computing science from the University of Salerno, Italy.

He has worked as a project manager, software engineer, research engineer, chief security architect, information security manager, PCI/SCADA auditor and senior lead IT security/cloud/SCADA architect for many years. Technical skills include security, Android, cloud, Java, MySQL, Drupal, Cobol, Perl, web and mobile development, MongoDB, D3, Joomla, Couchbase, C/C++, WebGL, Python, Pro Rails, Django CMS, Jekyll, Scratch, and more.

He currently works as chief information security officer (CISO) for CargotecOyj. He worked as visiting lecturer and supervisor for exercises at the Networking Laboratory of the Helsinki University of Technology (Aalto University). He holds four international patents (PKI, SIP, SAML and Proxy areas).

Massimo has reviewed more than 40 IT books for various publishing companies. He is the coauthor of *Pro Android Games* (Apress, 2015).

此为试读,需要完整PDF请访问: www.ertongbook.com

Contents at a Glance

About the Author xix

About the Technical Reviewer xxi

Chapter 1: Bridging the Blockchain Knowledge Gap 1

Chapter 2: The Mist Browser 21

Chapter 3: The EVM 47

Chapter 4: Solidity Programming 69

Chapter 5: Smart Contracts and Tokens 89

Chapter 6: Mining Ether 111

Chapter 7: Cryptoeconomics Survey 139

Chapter 8: Dapp Deployment 149

Chapter 9: Creating Private Chains 159

Chapter 10: Use Cases 165

Chapter 11: Advanced Concepts 173

Index 181

Contents

About the Author xix

About the Technical Reviewer xxi

Chapter 1: Bridging the Blockchain Knowledge Gap 1

Blockchain Roll Call! 1

What Ethereum Does 2

Three Parts of a Blockchain 4

Ethereum Assumes Many Chains 5

This Is a Scam, Just Like Bitcoin! 5

Ether as a Currency and Commodity 6

Gresham's Law 6

The Path to Better Money 7

Cryptoeconomics and Security 7

Back to the Good Old Days 8

Cryptochaos 8

The Power Is in the Protocol 8

You Can Build Trustless Systems 9

What Smart Contracts (Really) Do 10

Objects and Methods for Value 10

Just Add Commerce 11

Content Creation 11

Where's the Data? 12

What Is Mining? 12

Ether and Electricity Prices 12

Going Inside the EVM 13
The Mist Browser 13
Browser vs. Wallet or Keychain 13
Solidity Is Kind of Like JavaScript, But 13
What Ethereum Is Good For 14
A Critical Take 14
State of Smart Contract Development Today 15
Deciding Where You Fit In 16
A Note to New Programmers 17
Ethereum Is Free and Open Source 17
The EVM Is Here to Stay 17
What You Can Build Today 18
Private and Public Chains 18
The Promise of Decentralized Databases 19
What's Next: New Ways of Working 20
Summary 20
Chapter 2: The Mist Browser 21
Wallets as a Computing Metaphor 22
Your Address Is What? 22
Where Is My Ether? 23
The Bank Teller Metaphor 24
In Cryptocurrency, You Hold Your Own Assets 24
Visualizing Ethereum Transactions 24
Breaking with Banking History 26
How Encryption Leads to Trust 26
System Requirements 28

More about Eth.guide and This Book 28
Tools for Developers 29
CLI Nodes 29
Recommended: Using Parity with Geth 30
Finally, into the Mist! 30
Downloading and Installing Mist 30
Configuring Mist 32
Finding Your New Address 36
Sending and Receiving Ether 36
Understanding Ethereum Account Types 38
Backing Up and Restoring Your Keys 39
Using Paper Wallets 40
Using Mobile Wallets 40
Working with Messages and Transactions 42
So, What Is a Blockchain? 43
Paying for Transactions 43
Understanding Denominations 44
Getting Ether 44
Anonymity in Cryptocurrency 45
Blockchain Explorers 45
Summary 46
Chapter 3: The EVM 47
The Central Bank Network of Yesterday 47
What are Virtual Machines, Exactly? 48
The Role of the Ethereum Protocol in Banking 48
Anyone Can Make a Banking Platform 48

What the EVM Does 49
EVM Applications Are Called Smart Contracts 51
The Name "Smart Contracts" 51
The EVM Runs Bytecode 51
Understanding State Machines 51
Digital vs. Analog 51
"State-ments" 52
Data's Role in State 53
How the Guts of the EVM Work 53
The EVM Constantly Checks for Transactions 54
Creating a Common Machine Narrative of What Happened 54
Cryptographic Hashing 55
What Hash Functions (or Hash Algorithms) Do 55
Blocks: The History of State Changes 55
Understanding Block Time 56
The Drawbacks of Short Blocks 56
"Solo Node" Blockchain 56
Distributed Security 57
Mining's Place in the State Transition Function 57
Renting Time on the EVM 58
Hello, Gas 58
Why Is Gas So Important? 59
Why Isn't Gas Priced in Ether? 59
Fees as Regulation 59
Working with Gas 60
Gas Specifics 60
How Gas Relates to Scaling the System 60

此为试读，需要完整PDF请访问：www.ertongbook.com