

BRIAN KELLY

The Bitcoin Big Bang

How Alternative Currencies Are About to

Change the World

WILEY

THE BITCOIN BIG BANG

THE BITCOIN BIG BANG

*How Alternative Currencies
Are About to Change
the World*

Brian Kelly

WILEY

Cover image: © iStock.com/pixelparticle

Cover design: Wiley

Copyright © 2015 by Brian Kelly. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

ISBN 9781118963661 (Hardcover)

ISBN 9781118963647 (ePDF)

ISBN 9781118963654 (ePub)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

*For my wife, Dawn, this book is a testament to your unwavering
faith in my stupid ideas.*

Contents

Preface	xi
Acknowledgments	xiii
About the Author	xv
Chapter 1 Bitcoin Is a Bubble	1
The Quest to Buy Bitcoin	3
Bitcoin Enlightenment	6
Currencies Are a Matter of Trust	8
What Is Bitcoin?	10
Is It a Currency?	13
It's Revolutionary	17
Chapter 2 Understanding the Digital Gold Rush	19
The Language of Bitcoin	22
How Do I Buy Bitcoin?	26
Who "Gets" It?	30
The Gold Rush Is Just Starting	31
Chapter 3 Bitcoin Is More than Digital Gold	33
Searching for Satoshi	34
The Search	37

	Why Is Satoshi a Genius?	44
	Bigger than Satoshi	46
Chapter 4	Byzantine Generals' Problem	49
	How Does Bitcoin Solve the BGP?	52
	51 Percent Attack	55
	An Elegant Solution	57
Chapter 5	A Decentralized Financial System	59
	Grand De-Central Station	63
	What's at Stake?	69
	Central Banks	72
	Bitcoin Is the Catalyst	73
Chapter 6	What Do You Call a Bitcoin Miner?	75
	A Banker	75
	How Does a Bitcoin Transaction Work?	77
	What Is Cryptography?	78
	Still Want to Be a Miner?	82
	Do We Need Another Bitcoin?	88
Chapter 7	Nautiluscoin—0 to \$1 Million in 60 Days	91
	Creating the Coin	94
	Did It Work?	104
Chapter 8	Building the Nautiluscoin Economy	107
	Dynamic Proof-of-Stake	110
	Other Policy Tools	113
	Alternative to Gold	115
	Money, Made Better	116
	Financial Market Integration	117
	Special Drawing Rights	119
	Why NAUT?	119
Chapter 9	Investing and Trading in Alternative Currencies	121
	A New Investment Class	123
	Valuation	129
	Exchanges	133
	Investment Vehicles	134
	Asset Class Growth	136

Chapter 10 Regulation	139
Regulatory Agencies	140
Challenges to Regulation	147
Pushing on a String	147
Chapter 11 Smart Money: Set It and Forget It	149
Rules of the Road	151
Smart Contracts and Property	152
Ethereum	155
Cryptoequities: A New Type of Investment	160
Decentralized Autonomous Organizations	161
Professor Money	162
Chapter 12 Everything You Know about Business Is Wrong	163
Cryptonomics	166
Growth Share Matrix	169
Learning Curve Effects	171
Porter's Three Generic Strategies	172
Human Resource Management	173
Fueling the Sharing Economy	174
The Future Just Might Work	176
Appendix 1 Department of the Treasury Financial Crimes Enforcement Network Guidance	
<i>FIN-2013-G001</i>	
<i>Issued: March 18, 2013</i>	
<i>Subject: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies</i>	179
Currency vs. Virtual Currency	180
Background	180
Definitions of User, Exchanger, and Administrator	181
Users of Virtual Currency	181
Administrators and Exchangers of Virtual Currency	182
Providers and Sellers of Prepaid Access	185
Dealers in Foreign Exchange	186

Appendix 2 New York State Department of Financial Services Proposed New York Codes, Rules and Regulations

<i>Title 23. Department of Financial Services</i>	
<i>Chapter I. Regulations of the Superintendent of Financial Services</i>	
<i>Part 200. Virtual Currencies</i>	187
Section 200.1 Introduction	188
Section 200.2 Definitions	188
Section 200.3 License	190
Section 200.4 Application	191
Section 200.5 Application Fees	193
Section 200.6 Action by Superintendent	193
Section 200.7 Compliance	195
Section 200.8 Capital Requirements	196
Section 200.9 Custody and Protection of Customer Assets	197
Section 200.10 Material Change to Business	197
Section 200.11 Change of Control; Mergers and Acquisitions	198
Section 200.12 Books and Records	200
Section 200.13 Examinations	201
Section 200.14 Reports and Financial Disclosures	202
Section 200.15 Anti-Money Laundering Program	203
Section 200.16 Cyber Security Program	207
Section 200.17 Business Continuity and Disaster Recovery	210
Section 200.18 Advertising and Marketing	211
Section 200.19 Consumer Protection	212
Section 200.20 Complaints	215
Section 200.21 Transitional Period	215
Index	217

Preface

Very so often I find myself with the insatiable desire to jump off a cliff and think about the consequences later. Some may call it curiosity, while others think I am just plain crazy. I typically relish the skepticism, as I have found that the best opportunities arise when everyone else thinks I am a little nuts. The Bitcoin Big Bang was one of these times—actually, truth be told, this time I was the one who was skeptical. Despite my fear, uncertainty, and doubt, I jumped anyway.

When I began writing *The Bitcoin Big Bang*, it was for selfish reasons: I had bought Bitcoin near the peak and now was in a losing trade and needed to know everything about this “investment.” I figured I could turn my research into a book and learn a few things in the process. I did not know that I had stumbled on one of the most fascinating and promising technological advances since the Internet. When I first heard of Bitcoin, it was through the currency markets, and that is where my journey to Bitcoin Enlightenment began.

I mistakenly assumed that Bitcoin was an interesting new currency that had held little promise. After all, was the U.S. government really going to allow an unregulated currency based on computer code to replace the dollar? What I now realize is that the currency is

not the innovation; the blockchain technology is the game changer. The currency—bitcoin—is a fascinating alternative currency that has the potential to disrupt the global payment networks. However, it is the blockchain technology that is revolutionary.

The concept of the blockchain enables the transfer of secure information over an unsecured network. This may sound like a small step, but it is the first time in human history that this has been possible. The blockchain solves a multidecade-old problem in computer networking, and it can be applied to more than just currencies. It has the potential to end identity theft, create a secure Internet without the need for passwords, and revolutionize the way corporations do business.

When Jeff Bezos left a lucrative job as an investment banker to start an Internet bookstore called Amazon, everyone thought he was crazy. At that time, video stores like Blockbuster were in their prime and smartphones were landlines with an answering machine attached. Today, that same company (Amazon) is a leader in streaming video content to a handheld computer called a smartphone.

I do not know what alternative currencies will look like or accomplish over the next 20 years, but I do know that when a revolutionary technology is born, the world changes.

My goal with the book was to answer four questions:

1. What is Bitcoin, and why is it revolutionary?
2. How does it work?
3. Why are digital currencies a new type of investment?
4. How are alternative currencies going to change the world?

To this end, the book was written with two sections in mind. The first half of the book describes what Bitcoin is and how it works, while the second half illustrates the multiple uses of the blockchain technology and explores the ramifications for investments, business, and government.

An innovative technology was created by an anonymous programmer, who has given it away for free. This creation has spurred a technological explosion similar to the personal computer and the Internet, and, like its predecessors, alternative currencies are about the change the world.

—BK

Acknowledgments

When I began writing this book I thought it would be a solitary endeavor—countless hours writing alone to produce a manuscript that somebody might decide to read. Boy, was I wrong! This book would not exist without the contributions from friends and colleagues.

Let me start by thanking Jeffery Krames, who contacted me four years ago and convinced me I should write a book. It took a while, but this book is a testament to your persistence, patience, and conviction. You always knew I had a book in me.

To the CNBC *Fast Money* production team: thank you for supporting this project and for being an integral part of launching Nautiluscoin. Lisa Villalobos, the multitalented executive producer of *Fast Money*—you were able to take my slides of cryptographic hash functions and economic theory and turn them into a digestible television segment. You make it look easy. Michael Newberg, who was charged with producing a segment on a subject that I was still struggling to comprehend—you skillfully took an esoteric concept and turned it into a television segment that everyone could understand.