BLOCKCHAIN REVOLUTION

How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World

DON TAPSCOTT

BESTSELLING AUTHOR OF *WIKINOMICS*

AND ALEX TAPSCOTT

BLOCKCHAIN REVOLUTION

HOW THE TECHNOLOGY BEHIND BITCOIN AND OTHER CRYPTOCURRENCIES IS CHANGING THE WORLD

Don Tapscott
and **Alex Tapscott**

Portfolio / Penguin

Portfolio/Penguin
An imprint of Penguin Random House LLC
375 Hudson Street
New York, New York 10014

ISBN 9781101980149 (trade paperback)

Library of Congress Cataloging-in-Publication Data

Names: Tapscott, Don, 1947– author | Tapscott, Alex, author.
Title: Blockchain revolution : how the technology behind bitcoin is changing money, business, and the world / Don Tapscott and Alex Tapscott.
Description: New York : Portfolio, [2016] | Includes bibliographical references and index.
Identifiers: LCCN 2016008427 (print) | LCCN 2016014933 (ebook) | ISBN 9781101980156 (ebook) | ISBN 9781101980132 (hardcover) | ISBN 9780399564062 (international edition) Subjects: LCSH: Electronic funds transfers. | Bitcoin. | Electronic commerce. | Mobile commerce. | Banks and banking—Technological innovations. | Financial institutions—Technological innovations.
Classification: LCC HG1710 (ebook) | LCC HG1710.T385 2016 (print) | DDC 332.1/78—dc23 LC record available at https://lccn.loc.gov/2016008427

First Portfolio/Penguin hardcover edition: May 2016
First Portfolio/Penguin trade paperback edition: June 2018

While the author has made every effort to provide accurate telephone numbers, Internet addresses, and other contact information at the time of publication, neither the publisher nor the author assumes any responsibility for errors, or for changes that occur after publication. Further, the publisher does not have any control over and does not assume any responsibility for author or third-party websites or their content.

Version_2

To Ana Lopes and Amy Welsman for enabling this book,
and for understanding that "it's all about the blockchain."

"A masterpiece. Gracefully dissects the potential of blockchain technology to take on today's most pressing global challenges."
—Hernando De Soto, Economist and President, Institute for Liberty and Democracy, Peru

"The blockchain is to trust as the Internet is to information. Like the original Internet, blockchain has potential to transform everything. Read this book and you will understand."
—Joichi Ito, Director, MIT Media Lab

"In this extraordinary journey to the frontiers of finance, the Tapscotts shed new light on the blockchain phenomenon and make a compelling case for why we all need to better understand its power and potential." **—Dave McKay, President and CEO, Royal Bank of Canada**

"Deconstructs the promise and peril of the blockchain in a way that is at once accessible and erudite. *Blockchain Revolution* gives readers a privileged sneak peak at the future."
—Alec Ross, author, *The Industries of the Future*

"If ever there was a topic for demystification, blockchain is it. Together, the Tapscotts have achieved this comprehensively and in doing so have captured the excitement, the potential, and the importance of this topic to everyone."
—Blythe Masters, CEO, Digital Asset Holdings

"This is a book with the predictive quality of Orwell's *1984* and the vision of Elon Musk. Read it or become extinct."

—Tim Draper, Founder, Draper Associates, DFJ, and Draper University

“Blockchain is a radical technological wave and, as he has done so often, Tapscott is out there, now with son Alex, surfing at dawn. It’s quite a ride.”
—Yochai Benkler, Berkman Professor of Entrepreneurial Legal Studies, Harvard Law School

“If you work in business or government, you need to understand the blockchain revolution. No one has written a more thoroughly researched or engaging book on this topic than Tapscott and Tapscott.” **—Erik Brynjolfsson, Professor at MIT; coauthor of *The Second Machine Age***

“An indispensable and up-to-the-minute account of how the technology underlying bitcoin could—and should—unleash the true potential of a digital economy for distributed prosperity.”
—Douglas Rushkoff, author of *Present Shock* and *Throwing Rocks at the Google Bus*

“Technological change that used to develop over a generation now hits us in a relative blink of the eye, and no one tells this story better than the Tapscotts.”
—Eric Spiegel, President and CEO, Siemens USA

“Few leaders push us to look around corners the way Don Tapscott does. With *Blockchain Revolution* he and his son Alex teach us, challenge us, and show us an entirely new way to think about the future.” **—Bill McDermott, CEO, SAP SE**

“*Blockchain Revolution* is a brilliant mix of history, technology, and sociology that covers all aspects of the blockchain protocol—an invention that in time may prove as momentous as the invention of printing.” **—James Rickards, author of *Currency Wars* and *The Death of Money***

“*Blockchain Revolution* serves as an atlas to the world of digital money, masterfully explaining the current landscape while simultaneously illuminating a path forward toward a more equitable, efficient, and connected global financial system.”
—Jim Breyer, CEO, Breyer Capital

“*Blockchain Revolution* is the indispensable and definitive guide to this world-changing technology.” **—Jerry Brito, Executive Director, Coin Center**

“Incredible. Really incredible. The Tapscotts’ examination of the blockchain as a model for inclusion in an increasingly centralized world is both nuanced and extraordinary.”
—Steve Luczo, Chairman and CEO, Seagate Technology

“Makes a powerful case for blockchain’s ability to increase transparency but also ensure privacy. In the authors’ words, ‘The Internet of Things needs a Ledger of Things.’”
—Chandra Chandrasekaran, CEO and Managing Director, Tata Consultancy Services

“The epicenter of trust is about to diffuse! The definitive narrative on the revolutionary possibilities of a decentralized trust system.”
—Frank D’Souza, CEO, Cognizant

“Identifies a profound new technology movement and connects it to the deepest of human needs: trust. Thoroughly researched and provocatively written. Every serious businessperson and policy maker needs to read *Blockchain Revolution*.”
—Brian Fetherstonhaugh, Chairman and CEO, OgilvyOne Worldwide

“*Blockchain Revolution* sets the table for a wave of technological advancement that is only just beginning.” **—Frank Brown, Managing Director and Chief Operating Office, General Atlantic**

“A must read. You’ll gain a deep understanding of why the blockchain is quickly becoming one of the most important emerging technologies since the Internet.”
—Brian Forde, Director of Digital Currency Initiative, MIT Media Lab

“Blockchain technology has the potential to revolutionize industry, finance, and government—a must read for anyone interested in the future of money and humanity.”

—Perianne Boring, Founder and President, Chamber of Digital Commerce

"When generational technology changes the world in which we live, we are truly fortunate to have cartographers like Don Tapscott, and now his son Alex, to explain where we're going." **—Ray Lane, Managing Partner, GreatPoint Ventures; Partner Emeritus, Kleiner Perkins**

"Don and Alex have written the definitive guidebook for those trying to navigate this new and promising frontier."

—Benjamin Lawsky, Former Superintendent of Financial Services, State of New York; CEO of The Lawsky Group

"*Blockchain Revolution* is an illuminating, critically important manifesto for the next digital age." **—Dan Pontefract, author of *The Purpose Effect*; Chief Envisioner, TELUS**

"The most well-researched, thorough, and insightful book on the most exciting new technology since the Internet. A work of exceptional clarity and astonishingly broad and deep insight."
—Andreas Antonopoulos, author of *Mastering Bitcoin*

"*Blockchain Revolution* beautifully captures and illuminates the brave new world of decentralized, trustless money."

—Tyler Winklevoss, Cofounder, Gemini and Winklevoss Capital

"A fascinating—and reassuring—insight into a technology with the power to remake the global economy. What a prize. What a book!"

—Paul Polman, CEO, Unilever

CONTENTS

PART III: Promise and Peril

ACKNOWLEDGMENTS

This book came from the meeting of two minds and two life trajectories. Don had been leading a $4 million syndicated research program called Global Solution Networks (GSN) at the Rotman School of Management, University of Toronto. The initiative was investigating new, networked models of global problem solving and governance. He researched how the Internet was governed by a multistakeholder ecosystem and became interested in digital currencies and their governance. Meanwhile, Alex was an executive with the investment bank Canaccord Genuity. He noticed the growing enthusiasm for early-stage bitcoin and blockchain companies in 2013 and began leading his firm's efforts in the space. During a father-son ski trip to Mont-Tremblant in early 2014, we brainstormed over dinner about collaborating on this topic, and Alex agreed to lead a research project on the governance of digital currencies, culminating in his white paper, titled *A Bitcoin Governance Network*. The more we dug into the issues, the more we concluded that this could be the next big thing.

Meanwhile our agent, Wes Neff at the Leigh Bureau, along with Don's publisher Adrian Zackheim at Portfolio/Penguin (*Wikinomics*, *Macrowikinomics*), was encouraging Don to formulate a new book concept. When Alex's paper became widely recognized as leading thinking in this area, Don approached Alex to be his coauthor. Adrian, to his credit, made us an offer we couldn't refuse and the book never went to auction, as is normally the case.

We then made what in hindsight was a smart decision. We approached the best book editor we knew, Kirsten Sandberg, formerly of

Harvard Business School Press, and asked her to edit our book proposal. She did a spectacular job and our collaboration was so effortless that we asked her to be a full-time member of the book research team. Kirsten participated with us in more than one hundred interviews and collaborated in real time as we tried to understand the myriad issues on the table and develop helpful formulations to explain this extraordinary set of developments to a nontechnical audience. She helped us bring the story to life. In that sense, she was our coauthor and this book would not have appeared, at least in its current comprehensible form, without her. For that, and for all the stimulation and laugh lines, we are very grateful. Our heartfelt thanks to the people below who generously shared their time and insights with us and without whom this book would not be possible. In alphabetical order:

Jeremy Allaire, Founder, Chairman, and CEO, Circle
Marc Andreessen, Cofounder, Andreessen Horowitz
Gavin Andresen, Chief Scientist, Bitcoin Foundation
Dino Angaritis, CEO, Smartwallet
Andreas Antonopoulos, Author, *Mastering Bitcoin*
Federico Ast, CrowdJury
Susan Athey, Economics of Technology Professor, Stanford Graduate School of Business
Adam Back, Cofounder and President, Blockstream
Bill Barhydt, CEO, Abra
Christopher Bavitz, Managing Director, Cyberlaw Clinic, Harvard Law
School Geoff Beattie, Chairman, Relay Ventures
Steve Beauregard, CEO and Founder, GoCoin
Mariano Belinky, Managing Partner, Santander InnoVentures Yochai
Benkler, Berkman Professor of Entrepreneurial Studies, Harvard Law
School
Jake Benson, CEO and Founder, LibraTax
Tim Berners-Lee, Inventor, World Wide Web
Doug Black, Senator, Canadian Senate, Government of Canada
Perriane Boring, Founder and President, Chamber of Digital
Commerce David Bray, 2015 Eisenhower Fellow and Harvard
Visiting Executive in Residence
Jerry Brito, Executive Director, Coin Center
Paul Brody, Americas Strategy Leader, Technology Group, EY (formerly IoT at IBM)
Richard G. Brown, CTO, R3 CEV (former Executive Architect for Industry Innovation and Business Development, IBM)

Vitalik Buterin, Founder, Ethereum
Patrick Byrne, CEO, Overstock
Bruce Cahan, Visiting Scholar, Stanford Engineering; Stanford
Sustainable Banking Initiative
James Carlyle, Chief Engineer, MD, R3 CEV
Nicolas Cary, Cofounder, Blockchain Ltd.
Toni Lane Casserly, CEO, CoinTelegraph
Christian Catalini, Assistant Professor, MIT Sloan School of
Management Ann Cavoukian, Executive Director, Privacy and Big
Data Institute, Ryerson University
Vint Cerf, Co-creator of the Internet and Chief Internet Evangelist,
Google Ben Chan, Senior Software Engineer, BitGo
Robin Chase, Cofounder and Former CEO, Zipcar
Fadi Chehadi, CEO, ICANN
Constance Choi, Principal, Seven Advisory
John H. Clippinger, CEO, ID3, Research Scientist, MIT Media
Lab Bram Cohen, Creator, BitTorrent
Amy Cortese, Journalist, Founder, Locavest
J-F Courville, Chief Operating Officer, RBC Wealth
Management Patrick Deegan, CTO, Personal BlackBox
Primavera De Filippi, Permanent Researcher, CNRS and Faculty
Associate at the Berkman Center for Internet and Society at Harvard
Law School Hernando de Soto, President, Institute for Liberty and
Democracy Peronet Despeignes, Special Ops, Augur
Jacob Dienelt, Blockchain Architect and CFO, itBit and
Factom Joel Dietz, Swarm Corp
Helen Disney, (formerly) Bitcoin Foundation
Adam Draper, CEO and Founder, Boost VC
Timothy Cook Draper, Venture Capitalist; Founder, Draper Fisher
Jurvetson Andrew Dudley, Founder and CEO, Earth Observation
Joshua Fairfield, Professor of Law, Washington and Lee University
Grant Fondo, Partner, Securities Litigation and White Collar Defense
Group, Privacy and Data Security Practice, Goodwin Procter LLP
Brian Forde, Former Senior Adviser, The White House; Director,
Digital Currency, MIT Media Lab
Mike Gault, CEO, Guardtime
George Gilder, Founder and Partner, Gilder Technology
Fund Geoff Gordon, CEO, Vogogo
Vinay Gupta, Release Coordinator, Ethereum
James Hazard, Founder, Common Accord

Imogen Heap, Grammy-Winning Musician and Songwriter
Mike Hearn, Former Google Engineer,
Vinumeris/Lighthouse Austin Hill, Cofounder and Chief
Instigator, Blockstream
Toomas Hendrik Ilves, President of Estonia
Joichi Ito, Director, MIT Media Lab
Eric Jennings, Cofounder and CEO, Filament
Izabella Kaminska, Financial Reporter, *Financial Times*
Paul Kemp-Robertson, Cofounder and Editorial Director,
Contagious Communications
Andrew Keys, Consensus Systems
Joyce Kim, Executive Director, Stellar Development
Foundation Peter Kirby, CEO and Cofounder, Factom
Joey Krug, Core Developer, Augur
Haluk Kulin, CEO, Personal BlackBox
Chris Larsen, CEO, Ripple Labs
Benjamin Lawsky, Former Superintendent of Financial Services for the
State of New York; CEO, The Lawsky Group
Charlie Lee, Creator, CTO; Former Engineering Manager,
Litecoin Matthew Leibowitz, Partner, Plaza Ventures
Vinny Lingham, CEO, Gyft
Juan Llanos, EVP of Strategic Partnerships and Chief Transparency
Officer, Bitreserve.org
Joseph Lubin, CEO, Consensus Systems
Adam Ludwin, Founder, Chain.com
Christian Lundkvist, Balanc3
David McKay, President and Chief Executive Officer,
RBC Janna McManus, Global PR Director, BitFury
Mickey McManus, Maya Institute
Jesse McWaters, Financial Innovation Specialist, World Economic
Forum Blythe Masters, CEO, Digital Asset Holdings
Alistair Mitchell, Managing Partner, Generation Ventures
Carlos Moreira, Founder, Chairman, and CEO, WISeKey
Tom Mornini, Founder and Customer Advocate, Subledger
Ethan Nadelmann, Executive Director, Drug Policy
Alliance Adam Nanjee, Head of Fintech Cluster, MaRS
Daniel Neis, CEO and Cofounder, KOINA
Kelly Olson, New Business Initiative, Intel
Steve Omohundro, President, Self-Aware Systems
Jim Orlando, Managing Director, OMERS Ventures

Lawrence Orsini, Cofounder and Principal, LO3 Energy
Paul Pacifico, CEO, Featured Artists Coalition
Jose Pagliery, Staff Reporter, CNNMoney
Stephen Pair, Cofounder and CEO, BitPay Inc.
Vikram Pandit, Former CEO, Citigroup; Coinbase Investor, Portland Square Capital
Jack Peterson, Core Developer, Augur
Eric Piscini, Principal, Banking/Technology, Deloitte Consulting
Kausik Rajgopal, Silicon Valley Office Leader, McKinsey and
Company Suresh Ramamurthi, Chairman and CTO, CBW Bank
Sunny Ray, CEO, Unocoin.com
Caterina Rindi, Community Manager, Swarm Corp
Eduardo Robles Elvira, CTO, Agora Voting
Keonne Rodriguez, Product Lead, Blockchain Ltd.
Matthew Roszak, Founder and CEO, Tally Capital
Colin Rule, Chairman and CEO, Modria.com
Marco Santori, Counsel, Pillsbury Winthrop Shaw Pittman
LLP Frank Schuil, CEO, Safello
Barry Silbert, Founder and CEO, Digital Currency Group
Thomas Spaas, Director, Belgium Bitcoin Association
Balaji Srinivasan, CEO, 21; Partner, Andreessen Horowitz
Lynn St. Amour, Former President, The Internet Society
Brett Stapper, Founder and CEO, Falcon Global Capital
LLC Elizabeth Stark, Visiting Fellow, Yale Law School
Jutta Steiner, Ethereum/Provenance
Melanie Swan, Founder, Institute for Blockchain Studies
Nick Szabo, GWU Law
Ashley Taylor, Conensys Systems
Simon Taylor, VP Entrepreneurial Partnerships, Barclays
David Thomson, Founder, Artlery
Michelle Tinsley, Director, Mobility and Payment Security,
Intel Peter Todd, Chief Naysayer, CoinKite
Jason Tyra, CoinDesk
Valery Vavilov, CEO, BitFury
Ann Louise Vehovec, Senior Vice President, Strategic Projects, RBC Financial Group
Roger Ver, “The Bitcoin Jesus,” Memorydealers KK
Akseli Virtanen, Hedge Fund Manager, Robin Hood Asset
Management Erik Voorhees, CEO and Founder, ShapeShift
Joe Weinberg, Cofounder and CEO, Paycase

Derek White, Chief Design and Digital Officer, Barclays Bank Ted
Whitehead, Senior Managing Director, Manulife Asset
Management Zooko Wilcox-O'Hearn, CEO, Least Authority
Enterprises
Carolyn Wilkins, Senior Deputy Governor, Bank of Canada
Robert Wilkins, CEO, myVBO
Cameron Winklevoss, Founder, Winklevoss Capital
Tyler Winklevoss, Founder, Winklevoss Capital
Pindar Wong, Internet Pioneer, Chairman of VeriFi
Gabriel Woo, Vice President of Innovation, RBC Financial
Group Gavin Wood, CTO, Ethereum Foundation
Aaron Wright, Professor, Cardozo Law School, Yeshiva
University Jonathan Zittrain, Harvard Law School

Also special thanks to a few people who really rolled up their sleeves to help. Anthony Williams and Joan Bigham of the GSN project worked closely with Alex on the original digital currencies governance paper. Former Cisco executive Joan McCalla did deep research for the chapters on the Internet of Things and also Government and Democracy. We received a lot of familial support. IT executive Bob Tapscott spent many days downloading and getting under the hood of the entire bitcoin blockchain to give us firsthand insights on some of the technical issues. Technology entrepreneur Bill Tapscott came up with the revolutionary idea of a blockchain-based personal carbon credit trading system, and technology executive Niki Tapscott and her husband, financial analyst James Leo, have been great sounding boards throughout. Katherine MacLellan of the Tapscott Group (conveniently a lawyer) tackled some of the tougher issues around smart contracts as well as managing the interview process. Phil Courneyeur was on the lookout daily for juicy material, and David Ticoll provided helpful insights about the state of the digital age so far. Wes Neff and Bill Leigh of the Leigh Bureau helped us craft the book concept (how many books is this, guys?). As always (now more than twenty years), Jody Stevens flawlessly managed the administration for the entire project including databases, finances, and document management, as well as the proofreading and production process—a full-time job, in addition to her other full-time jobs at the Tapscott Group.

Special thanks to Dino Mark Angaritis, the CEO of blockchain company Smartwallet; Joseph Lubin, CEO of the Ethereum development studio Consensus Systems; and Carlos Moreira of fast-growing security company WISeKey—who each spent considerable time with us brainstorming ideas. They are each brilliant and so kind to help us out. Now we get to enjoy witnessing the success of each of their businesses in this space. Also big thanks to the great team at Penguin Random House led by our editor Jesse Maeshiro and overseen by Adrian Zackheim.

Most important, we'd like to give our heartfelt thanks to our wives, Ana Lopes (Don) and Amy Welsman (Alex), who more than tolerated our obsession with cracking this big nut over the better part of a year. We are both very fortunate to have such wonderful life partners.

Writing this book has been a joyous experience for both of us and it's fair to say that we loved every minute of it. As someone famous once said, "If two people agree on everything, one of them is unnecessary." We challenged each other daily to test our beliefs and assumptions, and this book is living proof of that healthy and vigorous collaboration. Mind you, collaborating does seem effortless when you share so much DNA and have a shared thirty-year history of exploring the world together. We do hope you find the product of this collaboration important and helpful.

Don Tapscott and Alex Tapscott, January 2016

PREFACE TO THE PAPERBACK EDITION

Don Tapscott and Alex Tapscott

CONTENTS

THE BIG IDEAS

When we wrote *Blockchain Revolution,* we got off to a good start by characterizing blockchain—the underlying technology of cryptocurrencies—as the Internet of value. We explained that, for nearly four decades, we've had the Internet of information. It vastly improved the flow of data within and among firms and people, but it hasn't transformed how we do business. That's because the Internet was designed to move information—not value—from person to person. When we e-mail someone a document, photograph, or audio file, we're really sending a copy of our original. This information is abundant, unreliable, and perishable. Anyone else can copy, change, and send it to somebody else. In many cases, it's legal and advantageous to share these copies.

In contrast, to expedite a business transaction, we cannot e-mail money directly to someone—not just because copying money is illegal but because we can't be 100 percent sure our recipient is who he says he is. Information about identity needs to be scarce, permanent, and unchangeable. So we go through powerful intermediaries to establish trust and maintain integrity. Banks, governments, and even big technology companies confirm our identities and enable us to transfer assets; they clear and settle transactions and keep records of these transfers. But the limitations of these intermediaries—their operational opacity and their vulnerability to hackers, rogue employees, and equally vulnerable suppliers—are becoming more apparent. We need a new way forward.

Blockchain solves the double-spend problem, as cryptographers call it. Now for the first time ever we have a native digital medium for value, through which we can manage, store, and transfer any asset—from money and music to votes and Stradivarius violins—peer to peer in a secure and private way. Trust is achieved not necessarily by intermediaries but by cryptography, collaboration, and clever code. We almost titled the book *The Trust Protocol*.

It seems that *Blockchain Revolution* was a clearer title—it's still a best seller, as of this writing. The response to it has both encouraged and delighted us. It received widespread coverage from such respected media as the *Financial Times*, *Forbes*, *Fortune*, *The Guardian*, *Harvard Business Review*, *Newsweek*, NPR's *All Things Considered*, *Reuters*, *Time*, and *The Wall Street Journal* and was a feature article in *The New York Review of Books* and the subject of a PBS television special.

It's gone global, too—translated into fifteen languages so far and, as of now, a best seller in five Asian languages alone. Don's second TED talk (TED's first on blockchain) has received well over three million views. At 2017
TEDxSanFrancisco, Alex spoke on blockchain and financial services; his has become one of the most watched talks on the topic, too.

When we first published in May 2016, ours was one of a handful of serious books about the topic. Now several important new works have entered the market such as Michael Casey and Paul Vigna's *The Truth Machine*, Chris Burniske and Jack Tatar's *Cryptoassets*, and Primavera De Filippi and Aaron Wright's *Blockchain and the Law*, to name a few.

Our book continues to hold its own as the bestselling book on blockchain. We receive positive comments on a number of its big ideas:

1. The book underscores the importance of identity and the end of digital feudalism. What some called "surfing the Internet," we viewed as "serfing the Internet," throwing off our data for the Internet landowners to expropriate and monetize. The notion of a self-sovereign identity for each of us, with our personal data stored in a virtual black box, is one of the most foundational concepts of our time. Realizing this "Virtual You" through blockchain technologies could restore our control over our own identities, the data we create, and the rest of our rights. No serf surfing, we say.

2. As a thought experiment, we tried to get inside Satoshi's mind and tease out his design principles for blockchain. It turns out there were seven. That chapter (chapter 2) was technical, appealing more to technologists and business engineers. We applied these seven principles to seven domains—financial services (chapter 3), the architecture of the firm (chapter 4), business model innovation (chapter 5), the Internet of Things (chapter 6), economic inclusion (chapter 7), government and

democracy (chapter 8), and the creative industries (chapter 9)—and argued that blockchain would create seven new substructures for a distributed economy.

3. We dubbed the financial services industry a Rube Goldberg contraption, a ridiculously complex system that actually performs eight basic functions. That taxonomy has proven helpful for industry executives and regulators alike. Do take a look at chapter 3 and the Golden Eight. Smart contracts (aka distributed applications) on a blockchain could, in theory, do each of these eight to disintermediate incumbents. Conversely, incumbents could transform their businesses for the better, if they embrace blockchain.

4. Nobel Prize–winning economist Ronald Coase's theory on the firm proved quite applicable to an analysis of blockchain's impact on corporate architecture. We explained how blockchain would radically reduce the transaction costs of search, coordination, contracting, and building trust in an open market. Inexorably, this efficiency will lead to more decentralized models for orchestrating the capabilities needed to create new products, services, and wealth. The new "blockchain business models" that we described hold up well, and many new ones have emerged since the book's publication. Decentralized business models are subject to network effects so that, when the number of nodes increases, so does the network. This in part explains the rapid growth of cryptoassets.

5. Blockchain can help us solve the prosperity paradox, where developed economies grow but the middle class and prosperity for most stagnates. Rather than the usual solution—the redistribution of wealth through taxation—we explained how blockchain could help us *pre*distribute wealth by including billions of people in the global economy. For example, we could protect property rights through immutable land titles, create a true sharing economy through shared, open, and distributed platforms, empower diasporas to remit funds through low-fee mobile payment systems, and endow entrepreneurs with the same capabilities as large companies.

6. Soon most transactions will occur between things, not people. We can instill intelligence into our infrastructure by adding smart devices— sensors, cameras, microphones, global positioning

chips, gyroscopes— that reconfigure themselves according to availability of bandwidth, storage, or other capacity, and therefore resist interruption. Blockchain is critical. This Internet of Things depends on a Ledger of Things to track every node, ensure its security and reliability, record its production and consumption, and schedule and pay for its maintenance or replacement. There are potential applications across every sector.

7. Our work on blockchain applications in government, democracy, and culture has received much attention. Since Donald Trump's inauguration as U.S. president, our insights seem even more prescient. Engaged citizens and dedicated public servants everywhere are exploring how blockchain can help them reinvent government, protect the free press, restore legitimacy to democratic institutions, and find common ground in public discourse on the Internet. The technology also helps not only journalists to quash claims of "fake news" but also creators of such cultural assets as songs and art to receive fair compensation for their work.

8. We were reluctant to include a chapter on leadership and governance, but we're glad we did. The space is full of formal and informal leaders, that is, those with executive roles in start-ups, blockchain consortia, and regulatory bodies, and those whose vision and talent are both compelling and influential. That said, concerted effort to transform obstacles into opportunities has been the most important factor in the blockchain's success thus far. So crucial is blockchain stewardship that the World Economic Forum asked us to write a special report on governance and launched important programs based on that work.

We also cofounded the Blockchain Research Institute (BRI), a think tank on distributed ledger technology, to investigate blockchain use cases, transformative thought leadership, and implementation challenges. The multimillion-dollar program includes some seventy-five projects across ten industry verticals and seven C-suite roles in both public and private sectors. Many of the quotes in this new preface come from the leaders of these projects.

BRI membership consists of large corporations, governments, nonprofits, and members of the start-up community. Some of our founding members include IBM, Accenture, Capgemini, SAP, NASDAQ, CIBC, PepsiCo, Liberty Global, Tencent, Fujitsu, FedEx, Thomson Reuters, and Centrica, along with the governments of several countries. To our delight, our institute's editor-in-chief is Kirsten Sandberg, who was the original editor of *Blockchain Revolution*.

Notwithstanding all this goodness, a lot of water has gone under the bridge. While the book holds up well, we wanted to report on our latest discoveries in this new edition. Rather than revise the whole manuscript, we are consolidating our findings in this new preface and an afterword. This new material derives from our ongoing research, investments in the space, and speaking engagements around the world. We welcome your feedback (www.blockchainresearchinstitute.org/contact-us).

CRYPTOASSETS AND THE NEW REVOLUTION IN FINANCIAL SERVICES

When *Blockchain Revolution* went to print in May 2016, the entire cryptoasset market had a value of $9 billion. Ethereum had just crossed $1 billion in network value, becoming the second blockchain unicorn (after bitcoin). These were early days. Had the cryptoasset market been a public company, it would barely have cracked the S&P 500 index.[1] Fewer than two years later, the cryptoasset market is $420 billion in size.[2]

This explosion of value in cryptoassets has captured the imagination of developers, entrepreneurs, nongovernment organizations, and the media, not to mention governments, central banks, the investing public, and regulators. It has also thrust these digital assets (and the underlying blockchain technology), once the domain of a few passionate technologists, into mainstream interest. It has made enthusiasts euphoric, Nobel laureates skeptical, and old-school billionaires dyspeptic.[3] Charlie Munger of Berkshire Hathaway went so far as to call bitcoin "noxious poison."[4](Is there any other kind of poison?)

Vitalik Buterin, Ethereum's inventor, captured the dissonance in late 2017 when the cryptoasset market cap hit half a trillion dollars. He tweeted, "Have We *Earned* It?"[5] "How many unbanked people have we banked?"[6] "How much value is stored in smart contracts that actually do anything interesting?"[7] Buterin pointed out that the level of activity is positive, but perhaps not significant enough to warrant the size of the market. "The answer to all of these questions is definitely not zero, and in some cases, it's quite significant," he added. "But not enough to say it's $0.5T levels of significant. Not enough."[8]

To be sure, there is a lot of hype in this market. For every cryptoasset that succeeds, many fail. Scammers have an outsized negative effect on the space as a whole. According to Reuters, "Twitter Inc. will start banning cryptocurrency advertising . . . joining Facebook and Google in a clampdown that seeks to avoid giving publicity to potential fraud or large investor losses."[9] Moreover, the industry must confront serious challenges. How will these technologies scale? How will incumbents react? What will governments and regulators do? We have good reason to believe this industry urgently needs sound regulation to protect investors and thwart fraudsters, or at least hold them accountable for their crimes. Moreover, to continue investing and building in this technology, market participants need to understand the rules of the road. On the other hand, bad regulations (even with the best intentions) can have unintended consequences and stifle innovation. In some countries, multiple regulators with overlapping mandates are sending conflicting messages. Regulators are not in an easy position. Some jurisdictions, such as Switzerland and Singapore, have emerged as favorable locations for companies to locate and operate with positive outcomes for the local economy. By one (informal) estimate, three thousand jobs have been created in the so-called "Crypto Valley" around Zug and Zurich in the past few years. The Crypto Valley Association has over six hundred members. Smaller and nimbler, these jurisdictions have been able to capitalize on a new industry, though they remain the exception, not the norm. For now, the lack of regulatory clarity in general has created uncertainty.

These are such important issues that we dedicated all of chapter 10 to them, "Overcoming Showstoppers: Ten Implementation Challenges." We continue to view them as implementation challenges to overcome. If we look beyond the hype and mania (not to mention fear, uncertainty, and doubt), we see something profound happening. Bitcoin was the first move in a long campaign to create an entirely new technology stack for the Internet, enabling the first native digital medium for value. That's what blockchain is, and it's limited only by our imagination. Some inventors have imagined a whole new asset class with what we think are at least seven types:

Cryptocurrencies (bitcoin, Zcash, Monero, and Dash)

Protocol tokens (ether, ICON, Aion, COSMOS, NEO)

Utility tokens (Golem, BAT, Spank)

Securities tokens (cryptoequities, cryptobonds)

Natural asset tokens

Crypto collectibles (CryptoKitties, Rare Pepe)

Crypto fiat currencies and stablecoins (Fedcoin proposal, Singapore’s Project Ubin, MakerDAO)

We are witnessing one of the largest transformations of wealth in human history, from paper-based analog assets to digital ones. To be sure, $265 billion is a lot of money. But in terms of all the assets in the world—from stocks, bonds, and mortgages to carbon, land, and water—we have barely scratched the surface of what we can create with crypto.

Is this all a bubble? Possibly. Joseph Lubin, CEO of Consensys and cofounder of Ethereum, says, “We will see bubble after bubble in our space, each one with higher highs and higher lows. I think that’s perfectly reasonable. People claim that the dot-com era of boom and bust was destructive, but I would call it creatively destructive.”[10]It may have harmed those looking only to make a quick buck, but it otherwise sorted out the sustainable business models from the unsustainable ones, and it weeded out inefficient operations. Perhaps more important, talent shifted to this new area of the economy, and the excitement of the Internet era precipitated billions of dollars of investment in new technology infrastructure.

However, blockchain differs from the Internet in two important ways. First, where the Internet was a free utility built by a diverse group of stakeholders, many of them volunteers with little financial incentive, blockchain provides huge financial rewards for those who can build successful, scalable, and widely used technology through the appreciation of underlying cryptoassets. The early Internet pioneers probably would have appreciated some upside from building a utility worth trillions of dollars, but that was impossible.

Blockchain is different—creators and early adopters can participate *directly* and *financially* in the growth of the second era of the Internet. As a result, there is no “one blockchain” but an explosion of competing, overlapping, complementary platforms, all driven by incentives.

Second, blockchain is tackling value industries such as financial services and supply chains, far larger than information industries like media and publishing. So not only will the impact be greater but the aggregate value will be, too. The excitement is indeed palpable. But, as the saying goes, sometimes we need a little irrational exuberance to build the future.

1. Cryptocurrencies

When *Blockchain Revolution* came out, bitcoin was worth around $7 billion. Today it's more than twenty-two times that. Bitcoin is the workhorse of the cryptocurrency world and the cryptocurrency that launched a thousand ships. Bitcoin has become: a store of hundreds of billions of dollars of value on the most robust computer network ever formed (and entirely bootstrapped), a secure payment system that enables billions of dollars in daily on-chain transactions, a reserve currency for the burgeoning cryptoasset world, a final settlement layer when it's time to cash out, and a favorite punching bag for every armchair analyst in the world. Paradoxically, bitcoin's meteoric price rise makes it easier, not harder, for new investors to justify stepping in because it has become an asset class too big to ignore. Moreover, the bigger it gets, the more utility it has. With the launch of the Lightning Network and other scaling solutions in 2018, bitcoin may also fulfill the promise of its most ardent supporters and obliterate the need for traditional financial intermediaries (chapter 3).

To wit, consider the recent shift in tone of some of the biggest banks. When *Blockchain Revolution* went to print, most banks were tactfully supporting the potential for blockchain but dismissing bitcoin (and its crypto brethren) out of hand. "Bitcoin bad, blockchain good" became cliché. As late as 2017, Jamie Dimon, CEO of JPMorgan Chase, was calling bitcoin a fraud. (He has subsequently changed his mind.) Times have changed. In February 2018, Goldman Sachs–backed Circle acquired Poloniex, one of the world's largest cryptocurrency exchanges, suggesting that it sees risks and opportunities in cryptoassets. In its 2017 annual report, JPMorgan echoed Bank of America in acknowledging that cryptocurrencies could pose a risk to its business: "Both financial institutions and their non-banking competitors face the risk that payment processing and other services could be disrupted by technologies, such as cryptocurrencies, that require no intermediation."[11]

Taken alone, bitcoin's impact on culture and the economy has been extraordinary. Its endowment to the world will continue to be profound. More recently, an emphasis on privacy has shaped newer entrants in the currency use case for cryptoassets. New cryptocurrencies such as Zcash and other "privacy coins" have emerged that build upon bitcoin's principles but add this new functionality.[12] This is not just the domain of cypherpunks and other Internet communities: JPMorgan integrated Zcash's core anonymity technology (zero knowledge proofs) into its own Quorum blockchain for use cases in a range of asset classes and business functions.[13] That JPMorgan was spending time, energy, and capital pushing the boundaries of this technology's wildest frontier, while its CEO was simultaneously denouncing it, suggests that (at least until recently) the bank's technologists understood the potential of blockchain more than its management did. Another intriguing new entrant is Metronome, which can be "imported and exported across chains," with the initial issuance happening on the bitcoin, Ethereum, Ethereum Classic, and Qtum networks.[14] As we will see in the next section on platforms, interoperability is a big challenge and opportunity in this space. Zcash and Metronome join Dash, Monero, and others vying for market share in the cryptocurrency sphere of this market. But currencies as a use case are the beginning of this story. Consider Ethereum.

2. Platforms

To the outside world looking in, Ethereum and bitcoin could be mistaken for two sides of the same coin—cryptocurrencies designed to function as cash for the Internet. This view couldn't be further from the truth. Whereas bitcoin serves such a purpose, Ethereum is a platform technology, designed from the outset to enable *distributed applications* (DApps), what Nick Szabo calls "an application that runs in a distributed and trust-minimized manner on a blockchain."[15] At the core of distributed applications are smart contracts, software that mimics the logic of a business agreement. Because they are decentralized and running on blockchains, they minimize the need for intermediaries (banks, brokers, lawyers, courts, escrow agents, corporations) to guarantee execution.

The promise of Ethereum was basically theoretical when we were writing the book: it launched only weeks before our first draft had gone to the editor. Yet today, Ethereum's native token (ether) has a market value of $70 billion. More important, Ethereum emerged as the leading platform for ICOs, where a project can raise millions of dollars peer to peer from a global community of investors and supporters. To date, dozens of new distributed applications have been launched on the Ethereum network. In aggregate, some $3 billion have been raised on Ethereum using its ERC-20 protocol, making Ethereum the proto– investment bank for the digital economy. By some estimates, 70 percent of all distributed applications now run on the Ethereum blockchain, giving it powerful network effects that will be hard to dislodge. Ethereum has also galvanized such large enterprises as Microsoft, JPMorgan, and BP, which collectively established the Enterprise Ethereum Alliance in 2017.

As expected, some of these distributed apps have made a great deal of progress, while many others have floundered. For every great start-up that changes the world, countless others fail and most are forgotten. Platforms like Ethereum, however, are largely agnostic to the success of any one distributed application, so long as the next big thing is built on them. The more DApps built on the network, the more demand for the associated platform token, ether. If Ethereum is the city grid, and the DApp is the car, then ether is the fuel, or “gas” in crypto parlance. We pay in ether to use the network for running the smart contract that powers the DApp. But will Ethereum be the platform for the next generation of distributed applications? Will it be one of the core protocols of the new Internet of Value, or will something else take its place? It’s currently the best candidate for a “flippening,” the point at which an alternative blockchain displaces bitcoin as the network with the most participants and most capital.[16] Massive work is under way to expand Ethereum’s capability, including Casper, sharding, and a shift to proof of stake.

A number of other emerging platforms could challenge or complement it. DApp-focused platforms such as NEO (China), ICON (South Korea), and other regional leaders have emerged. Protocols such as Aion designed with large-scale enterprise applications in mind—a huge but generally untapped market—have also emerged, while some of the biggest hype is reserved for still-unreleased protocols like Polkadot and Cosmos, which promise to eliminate scalability and interoperability bottlenecks and unite all blockchains into a giant seamless web of blockchains. All protocols will not succeed, but some will, and those that remedy the showstoppers (chapter 10) will form the backbone of the next era of the Internet.

3. Utility Tokens (App Coins)

In chapter 3, we wrote about Augur, a prediction market designed to harness the wisdom of crowds in order to make markets in virtually anything. To us, Augur illustrated the potential power of blockchain technology. It was also among the first projects to issue funds in a crowdsale on the blockchain. (We dubbed it the "blockchain IPO," but the term never took off. Instead, people latched on to "initial coin offering," a misnomer if ever there was one.) Augur proved a harbinger of what was to come. In 2016, roughly $165 million was raised in ICOs, which was interesting but not really enough to raise eyebrows outside the blockchain community. By 2017, the figure had reached at least $3 billion, perhaps as much as $7 billion. Joe Lubin believes this new fund-raising mechanism is "democratizing the ability for projects to fund themselves either via tokenized securities issued in a global context or by selling utility tokens that provide consumer membership, consumer access to services, or access to scarce resources . . . basically preselling something and using those proceeds to build what you need or to take it from a rudimentary stage to a more sophisticated stage."[17]

Augur's native token is not equity but a utility token required by users to interact with the network—in effect, a programmable blockchain asset that has functionality in the distributed application. Most ICOs in 2018 were "utility tokens," though many were probably also securities. Consider Golem, a decentralized alternative to today's centralized clouds run by such digital conglomerates as Amazon and Apple. Golem aims to harness the power of the billions of devices used daily to distribute computation. For its model to work, it needs an incentive for participation. So in 2017, Golem issued a utility token that allows users to pay and get paid on its platform. If Golem works, it could disrupt cloud computing as we know it.

Another example is Sweetbridge, which originated the concept of a "discount token," where users receive a monthly discount on goods and services as long as they hold the token in a Sweetbridge wallet. "The amount of the discount is controlled by the revenue in the network and the number of discount tokens held in their wallet. This means that discount tokens have an intrinsic value that increases as more customers use the network, says Scott Nelson of Sweetbridge. "Discount tokens change the business from driven by shareholder value to [driven by] customer value, making the customer the center of the focus of a business."[18] Others are pioneering myriad so-called cryptoeconomic models for utility tokens in virtually every industry.

Utility tokens are usually not stand-alone blockchains. Rather, they run on top of platforms like Ethereum, ICON, and EOS. To be clear, the borders between utility tokens and the underlying platform tokens can be porous. After all, protocol tokens also have utility, as with the ether used to pay transaction fees on the Ethereum network. Some protocols today have only one application. Tomorrow, they may have a lot more. Filecoin, a distributed file sharing system, completed its own ICO in the summer of 2017. However, because it is an open network, developers will ultimately be able to build any number of applications on it. Exceptions notwithstanding, we believe most utility tokens will be application-based and run on networks such as Ethereum.

4. Security Tokens

Though not insignificant, the $265 billion cryptoasset market is a small fraction of the value of virtually any other major asset class. The global equity market, for example, is more than $100 trillion. However, the underlying technology of cryptocurrencies, blockchain, is broadly applicable to basically any asset in the world.

The next ten years will see today's cryptoassets lose their monopoly as securities, particularly nonphysical securities like stocks and bonds, migrate to this technology and increasingly dominate the market. After all, why should a stock trade settle T+3 and involve a handful of intermediaries when buyer and seller can conduct the same transaction peer to peer and settle T+0 on a decentralized exchange? Why shouldn't all stocks, bonds, dividends, futures, forwards, swaps, options, and other financial assets exist in purely digital form on blockchains? An "equity token," for example, is not merely a thumbprint on a blockchain representing some off-chain asset but a native digital asset that we can trade peer to peer without custodians, clearinghouses, brokers, exchanges, and banks.

ICOs have already upended venture capital. Wall Street could be next. To wit, Fidelity, Wellington, and other giants of asset management have taken steps to prepare themselves for this brave new world.

While projects and companies like Polymath, Overstock's tZero, the Jibrel Network (a platform for security token offerings using ERC-20), and the Canadian Securities Exchange build out the technology infrastructure for such a historic transformation, the industry awaits the regulatory infrastructure to give it clarity. This gulf between technology and rule setting creates what legal scholar and blockchain expert Primavera De Filippi calls a "regulatory lag" or "governance gap," which "has resulted in the destabilization of traditional mechanisms of adjudication and rule-making, and the erosion of public confidence in the 'state of play'—that is, what is permissible and what is not."[19] Security tokens could help bridge this divide by defining themselves by what they are *not.*

They are *not* cryptocurrencies, protocols, or utility tokens but “digital bearer assets” (securities) native to blockchains. The offspring of ICOs, *security token offerings* (STOs), will become ubiquitous in venture capital and financial services more generally.

This great migration of value from analog to digital will transform the roles of markets and intermediaries as we know them.

5. Natural Asset Tokens and Commodity Tokens

Natural assets such as water, carbon, and air are foundational to the economy and essential for life on earth. However, with the exception of some nascent carbon trading schemes, these assets have largely remained immune to market based forces. This has led to overuse and exploitation of these resources, with costs borne by society in the form of what economists call “negative externalities.” Sociologist Garrett Hardin describes this as the tragedy of the commons—a situation where a shared common resource is depleted because there is no system to govern its use or consumption.

Michael Casey, coauthor of *The Truth Machine*, uses the work of Hardin as a jumping-off point to examine the role of blockchain in helping to solve this problem of governance. He writes, “With the advent of blockchain technology and the cryptocurrencies, cryptotokens, and other digital assets that it has engendered, we may be moving toward a model of programmable money that can deliver a more automated system of internal governance over common resources.” Indeed, in much the same way that we can tokenize technology protocols, applications, and securities, so too can we tokenize physical assets in the real world. “The great promise of the token economy is that it might solve the Tragedy of the Commons,” writes Casey.[20]

Mostly, entrepreneurs and enterprises have applied this concept to traditional commodities with established markets, such as gold, oil, natural gas, etc. Indeed, it’s true that we can apply the same principle of security tokens to physical commodities like these. Replicating the business logic of an oil-futures contract on the blockchain is feasible as blockchain start-up Nuco demonstrated with the TMX Group, owner of the Toronto Stock Exchange. Even though someone still needs to take physical possession when the contract expires, we can still simplify the mechanism of clearing and settling a trade in an underlying physical asset. In many ways, we could use a token backed by gold as a less volatile and more liquid medium of exchange (see section 7). For example, the Royal Mint partnered with the Chicago Mercantile Exchange to create Royal Mint Gold, a digital gold token backed by physical gold held in the Royal Mint's vaults.[21]

To be sure, we have opportunities to streamline and simplify existing markets. However, as with all technologies, the bigger opportunities are in new and previously impossible use cases. To wit, today's carbon trading schemes create a marketplace for carbon and reward companies for good behavior, allowing them to earn credits for reducing their carbon footprint. If companies can be rewarded for good behavior, why can't people? As it exists today, the market is weighed down by a lack of standards and highly fragmented and regional marketplaces.

Blockchain could change that by aligning incentives with a common and collective goal, such as reducing carbon emissions.[22] Companies like CarbonX (Canada) and Veridium (United States) are tackling this market by tokenizing carbon into fungible liquid tokens. By reducing their footprint, individuals can earn carbon credits redeemable for real value. Compared with cryptocurrencies, utility tokens, and even security tokens, natural asset tokens are a tiny market. Most of what has been proposed is theoretical, and there are real challenges such as government policy and regulations that blockchain alone cannot hope to solve. However, with a massive and untapped underlying market and pressing social, economic, and environmental reasons to move forward, it is only a matter of time before this becomes one of the largest cryptoasset types.

6. Crypto Collectibles: Virtual and IRL

In December 2017, the crypto world caught CryptoKitty fever. CryptoKitties are unique, tradable virtual pets that people can purchase, raise, and even breed with other CryptoKitties. As of January 2018, CryptoKitties had more than 235,000 users and had processed $52 million in transactions. CryptoKitties became so popular that the Ethereum network, on which this particular DApp was running, initially struggled to keep up, surely a sign of both the powerful network effects of popular apps and the current limitations of the underlying platform technology. At its peak, the dearest CryptoKitties were selling for more than $100,000. The phenomenon became personal when a close friend told us that he and a new girlfriend were considering taking their relationship to the next step by breeding their CryptoKitties to create a cryptobaby—surely a novel and modern spin on "Let's get a dog." Such "silly and fun things are important" in engaging people with breakthrough technology, said Elon Musk as he blasted his sports car into space.[23] So it is with CryptoKitties, an example of crypto collectibles.

There are two kinds of crypto collectibles. The first are native digital assets that have no equivalent in real life. CryptoKitties and virtual trading cards (such as Rare Pepe) spring to mind. So, too, do in-game purchases of unique assets of virtually any kind. Artists are applying cryptoeconomics to their virtual art. Art derives much of its value because it is scarce. But the Internet of information allowed us to copy free forms of expression, such as images and songs, ad infinitum, reducing the value to zero and losing track of the original. The blockchain connects the creative work to a unique and scarce token. In *The New York Times*, Scott Reyburn recently wrote, “Will cryptocurrencies be the art market’s next big thing?” He explored a number of artists working solely in the virtual world.[24] The opportunities are tantalizing. As art and other forms of expression increasingly begin as a digital medium, whole new categories of virtual art, collectibles, and other unique assets could explode in value. The second kind of crypto collectible represents a claim on something tangible. Whereas we will eventually have 21 million bitcoin in circulation, each CryptoKitty is *unique*, as is every Rothko, Picasso, Monet, and Pollock. In chapter 9, we wrote about a company called Artlery, which employs an art backed cryptocurrency called the CLIO to register physical artwork in the real world. More have joined the fray, including Dada.nyc.[25] While virtual art is a growing market, the existing art market is enormous. Total sales in 2016 of fine art and antiques was $45 billion.[26] Notoriously opaque, this market is beginning to benefit from the disinfecting sunlight of blockchain. Artwork can get a digital fingerprint through a cryptoasset that allows us to trace, track, and authenticate it.

7. Crypto Fiat Currencies and Stablecoins

In 2017, Venezuela announced that it was launching a new cryptocurrency, dubbed “The Petro,” backed by its vast oil reserves. The reaction from the cryptocurrency community was a mix of dumbfoundedness and anger. Why would a corrupt and antidemocratic government, which had plunged its own currency into a hyperinflationary death spiral, co-opt this technology if not to exploit its association with trust, security, and immutability? According to analysts, it has three strikes against its credibility: there is no evidence that the Petro is actually backed by oil, there is little technical information online about how it works or which blockchain it runs on, and it is controlled by the same people who collapsed the bolívar.[27]

Unbowed by the criticism, the government moved ahead and raised $735 million, according to officials but not corroborated by any other evidence. News of the Petro was quickly followed by reports that lawmakers in Iran and Russia were also considering their own fiat cryptocurrency. All of these countries have three traits in common: they are authoritarian (or deeply undemocratic), they have a lot of oil, and they are under sanctions. So necessity is the mother of invention after all.

Why does this matter? Most obviously, it shows how rogue governments could use their cryptocurrencies to undermine international law, treaties, and sanctions and further destabilize their already weak economies. The Brookings Institution wrote that the Petro would harm other legitimate cryptocurrencies and undermine international sanctions.[28]

More important, it demonstrates that governments can actually do this. In chapter 11, we ruminated on the idea of a government-backed cryptocurrency, though none existed at the time. Indeed, the most promising candidates—august institutions like the Bank of England, Bank of Canada, and Federal Reserve— have made little headway in this regard, with some even backtracking. They should reconsider.

Crypto fiat currencies will probably not be fully decentralized and censorship resistant, like bitcoin. However, implemented properly, they can still make markets more efficient through real-time settlement, improve inclusion by reducing barriers to entry, improve transparency into our institutions, and make central bank policy more effective by improving responsiveness. Consider the example that Bitt is setting in the Caribbean. The company is working with the region’s financial heads to create a digital dollar standard that has a number of benefits to the economy. CEO Gabriel Abed explains, “This is what the Caribbean needs. It’s the entire world in one little melting pot, yet there is no cross-border system for payments. . . . The goal is to enable movement of money between two central banks using smart contracts and digital dollars built by Bitt or others that follow a digital dollar standard.”[29] There are economic and social reasons to make this happen. Abed says, “Remittances are expensive because interregional settlement is not existent. Forty percent of Caribbeans don’t have access to banking. Three percent fees are being taxed by foreign bankers on merchant charges using credit cards.” A digital dollar standard for the region could help alleviate these problems.

Another benefit is price stability. Media of exchange are generally not as volatile as bitcoin has been historically. A crypto fiat currency could help solve this. Some crypto diehards will balk. So be it. We still believe that bitcoin (or something like it) will continue to be a legitimate alternative to fiat currencies.

Stablecoins—cryptocurrencies that try to maintain the same value over time by pegging themselves to some underlying asset, such as a fiat currency or gold, or by managing price through an ever-changing supply—could emerge as a hybrid. Mostly these have been the brainchild of entrepreneurs running private companies. The largest of these today is Tether (USDT). Its creators say that Tether is backed dollar for dollar with USD reserves, though analysts have openly questioned this assertion.[30] Others such as MakerDao, BitCNY, and basecoin (backed by Andreesen Horowitz and other prominent VCs) have also emerged. Stablecoins could gain traction if we assume that existing cryptocurrencies such as bitcoin will remain highly volatile and governments will not create their own fiat currencies. At least for now, both conditions exist, and so stablecoins will continue to be an interesting area of innovation. Still, doubts linger. Stablecoins like Tether "decentralize the dollar but centralized the issuance. You have to trust a single entity who now becomes the monetary authority." Abed asks, "Are you better than the Federal Reserve?"[31]

Ultimately, however, we think governments will move into this market and that the future reserve currencies of the world will likely be a mix of crypto fiat currencies (digital dollars and such) and decentralized cryptocurrencies like bitcoin. Regional hybrids like the digital dollar standard in the Caribbean are likely to succeed, too. Don't count on the Petro joining their ranks.

PERMISSIONED NETWORKS

As we were submitting the final manuscript, forces were coalescing not only around the concept of the Fourth Industrial Revolution but also around special purpose blockchains for industries such as the Industrial Internet of Things.

Ripple, typically one of the three largest cryptoassets by market cap, is an enterprise-friendly alternative to bitcoin, geared toward displacing SWIFT and other global payment networks. Ripple's architecture—relying on a handful of trusted nodes rather than on miners to secure the blockchain—gives it the ability to process more transactions but also makes it more centralized, which, in the eyes of some critics, makes it more vulnerable to attack and capricious and arbitrary behavior. Still, Ripple has been very successful in courting large banks and other potential enterprise users to employ their products and services and, to a lesser extent, use the native token of the network, called XRP.

The Linux Foundation, famous for building ecosystems around open source projects, had been looking at distributed ledger technology for a while. After hearing from several leaders in the space, executive director Jim Zemlin decided that the time had come for Linux to start a blockchain project.

In December 2015, the foundation announced Hyperledger, positioned as a collaborative project to “develop an enterprise grade, open source distributed ledger framework” so that developers could “focus on building robust, industry specific applications, platforms, and hardware systems [that] support business transactions.”[32] The project had “technical and organizational governance structure and 30 founding corporate members,” notably IBM, Fujitsu, DTCC, and Accenture.[33] The Linux Foundation is a good home for open, transparent governance of the software development process and the management of intellectual property provenance and safeguards.

Our book covers public blockchains such as bitcoin and Ethereum, which remain two of the most important platforms today. They are open, meaning that anyone reading this book can conduct transactions, verify transaction data, race to create blocks, and develop distributed applications without anyone else’s permission. Upgrades to the codebase are reached by consensus. Users who don’t agree with particular upgrades (such as the increase of a bitcoin block size) can choose not to adopt it, and the blockchain forks in two. Both bitcoin and Ethereum have forked since we first wrote about them. Hyperledger pioneered the notion of the “consortium” model, which formalizes the governance of such upgrades and consolidates industry expertise around the formulation of standards.

Unlike bitcoin and Ethereum, Hyperledger’s focus is on permissioned blockchains, networks in which verified, nonanonymous nodes can post transactions to the ledger and confirm other transactions. Such networks are typically also read-limited to that same network of verified nodes, but the network could allow a larger audience to read the data. A subset of that network could allow further control over read and write access so that it could use a much simpler form of consensus, one based loosely on a “supermajority vote” of the nodes, rather than on the more CPU-intensive

proof of work (PoW) that bitcoin, ether, and most other coins have used. Such a network could also accommodate a much higher transaction volume than typically provided by PoW blockchains. Many of those building distributed ledger applications for the financial industry and the industrial Internet of Things, for example, prefer this model. It may also prove more valuable for those building certain public-facing applications, such
as educational credentialing, carbon emissions monitoring, or fiat currency administration.

Hyperledger is not alone in building blockchain platforms that allow permissioned use cases and separate the need for a native token or cryptoasset (at least for now). Hashgraph, developed by computer scientist Leemon Baird, does not rely on miners to validate transactions. Instead of bundling transactions into blocks, Hashgraph uses *directed acyclic graphs* to time-sequence transactions on an ongoing basis. Theoretically, this means far faster transaction times, something many enterprises are emphasizing as they embrace this technology. Bloomberg reported that Hashgraph is working with twenty-plus enterprises as well as a number of credit unions in the United States.[34] Whether these new systems will succeed remains to be seen, but the progress of Hashgraph is very encouraging.

Some critics argue that permissioned blockchains are the equivalent of the intranets of the mid-1990s, many of which faded over time as the public Internet grew more robust, secure, and ubiquitous. But this time, blockchain technology enables transactions and management of value—assets owned by persons—and will necessarily have many public and more private forms.

Hyperledger is the fastest-growing project ever hosted by the Linux Foundation. More than two hundred member companies that span numerous industries make up the project and support five blockchain frameworks and four tools/modules.[35] Hyperledger membership is also quite global with 39 percent in Asia Pacific (25 percent in China), 20 percent in Europe, the Middle East, and Africa, and 41 percent spread across North America.

Hundreds of active pilots and proofs of concept (PoCs) are under way with Hyperledger technologies. Many will see production deployment in 2018. Industries as diverse as agriculture, finance, health care, real estate, energy, and diamonds will see blockchain applications disrupt their value chains. Walmart is currently testing blockchain technology for supply chain management. Specifically, it is using Hyperledger Fabric to track and trace pork in China and produce in the

United States.[36]In May 2017, the Danish shipping enterprise Maersk announced completion of its first live blockchain trial, also using Hyperledger Fabric. The PoC aimed to simplify how it sends trillions of dollars' worth of products around the world. Deutsche Börse Group selected three use cases to be based on Hyperledger Fabric, relevant for its core business: cross border collateral movement, posttrade processing, including settlement of securities against cash and asset servicing and provision of (commercial bank)
money on the blockchain, enabling payments, settlement, and asset servicing. Finally, Sony Global Education prototyped a blockchain solution built on Hyperledger Fabric to develop a next-generation credentials platform. The prototype achieved all the needed functionality. Now in phase three, Sony Global Education plans to use the solution to manage the educational data of 250,000 participants in the Global Math Challenge.

Hyperledger brings together a community of organizations and individual developers to develop infrastructural software for blockchain applications. This leads to more effective collaboration, more shared code, and less duplication of effort. Any enterprise or other organization looking to blockchain solutions needs to give it careful consideration.

INTRODUCING THE MENOME: IDENTITY ON THE BLOCKCHAIN

On the subject of identity, it seems we really struck a nerve. In chapter 1, we wrote about enforcing the rights of all individuals to establish their own identities and to capture and control their own data. This is a much bigger idea than the word count allotted to it; the idea of a self-sovereign and inalienable digital identity, an identity that is neither bestowed nor revocable by any central administrator and is enforceable in any context—in person and online— anywhere in the world. It builds on the citizen scientist movement to quantify our selves—the quantified self—by lifelogging our physical activity through a Fitbit or other instrument as well as our virtual activity through our Internet browser or mobile app to learn about our health, our habits, and ourselves.[37]It's a real positive when people become interested enough in their own data to take control of it and use it for the greater good.

We have a greater sense of urgency about developing a distributed self sovereign identity system. Here we need to distinguish between *identity*, which is a social, cultural, and psychological construct, and *identifiers* in a namespace (a 128-bit IP address, a DD Form 214), needed both to participate in and to manage large centralized systems (Google email, Veterans Benefits Administration).[38] Many of us accumulate quite a number of such identifiers in our lifetime, some of them more enduring (a social security number) than others (an employee ID), all generating personal data as we use them. Some of them are inherent (biometric), some are selected (passwords), and some are assigned (resident ID cards).

These are not our identities, which we experience and reveal to others over time as we deem appropriate, and we can do so because we have what developer Moxie Marlinspike calls a *sovereign source authority,* “the actual default design parameter of Human identity, prior to the ‘registration’ process used to inaugurate participation in Society.”[39]Identity is not simply endowed at birth; it is endowed *by* birth. Until now, we haven’t had the means to assert this authority.

An identifier, on the other hand, is only one of many attributes of a person’s identity. There are five problems with identifiers, which several identity projects in the blockchain space are working to solve. We’ll start with the biggest. Before dispensing one of them, most issuers require us first to have some über identifier, often a birth certificate, recognized as authentic by a government. But getting a birth certificate is actually no small feat. According to UNICEF, “the births of around one fourth of children under the age of five worldwide have never been recorded.”[40] Not getting a birth certificate can have life-shattering consequences: these children may have trouble receiving an education or health care. Worse, they may be married off, indentured into labor, or conscripted into the military before they reach the legal age.[41](Is it a coincidence that “children remain the second most commonly detected group of victims of [human] trafficking globally after women, ranging from 25 to 30 percent of the total over the 2012–2014 period”?[42]) As adults, they may not be able to inherit property, vote in elections, or get jobs or passports, let alone bank accounts.[43] The World Bank estimates that 1.5 billion people on the planet lack a legal identifier.[44] The Syrian refugee crisis has underscored the problem of state-based identification.[45] We need to take action now.

So important is seeding identity by providing a trusted form of identification that the United Nations has made it a Sustainable Development Goal (16.9): all participating countries have committed to provide every person with legal identification by 2030.[46] The World Bank’s Identification for Development initiative is designed to support this goal so that more people can participate in the global economy.[47]India has made considerable progress, documenting 99 percent of adults.[48]In a report on peer-to-peer markets, the Blockchain Research Institute highlighted the economic importance of India's efforts. It started with the Aadhaar Act of 2009, which authorized the Unique Identification Authority of India (UIDAI) to create a twelve-digit ID, called an *aadhaar* (meaning "foundation" in Hindi) for every resident.[49] Enrollment agents fanned out to

collect demographic and biometric data and upload them to a repository designed to verify ID instantaneously anytime, anywhere. In April 2016, the National Payments Corporation of India unveiled a unified payment interface that would accept *aadhaar* for payment verification. Anyone with *aadhaar* could use it to complete any transaction, conduct peer-to-peer commerce, and receive government benefits. The plan worked: in November 2017, the UIDAI determined that "*aadhaar* data [are] fully safe and secure, and there has been no data leak or breach at UIDAI."[50]

The UIDAI spoke too soon. In early January 2018, Rachna Khaira, a journalist from *The Tribune* in Jalandhar, received an anonymous offer of unrestricted access to the data behind more than one billion *aadhaar* for only 500 rupees. By typing in a twelve-digit number, she was able to see the personal details associated with it—photo, name, address, phone number, and e-mail. For another 300 rupees, she could create an official-looking *aadhaar* card for that person. The system had been hacked, and one billion records exposed.

So the reality of a government-sourced and -sanctioned identity is a big problem—both administratively and philosophically. Why should any government get to rubber-stamp who we are? We should be establishing our own identities and, as Joe Lubin says, bootstrapping ourselves into economic enfranchisement![51] For those of you who think this is a crazy or ill-advised idea, please allow us to underscore the four other major problems with our current identity regime. One, they are system-centric, system-controlled, and vulnerable to cancellation, forgery, and theft. We're dependent on a system administrator who can freeze access, alter terms of access and usage, or delete our student IDs, health care insurance IDs, or land titles altogether.

Two, all the personal data we create and associate with each identifier (biometrics, college transcript, medical history) reside with and belong to the central system administrator, who may entrust it to untrustworthy vendors or sell some of it to unacceptable third parties without our knowledge. Such a system is opaque. If we want to switch colleges or countries, we bear the responsibility of porting our data from one system to the next—sometimes for a fee—and the rules for doing so are often complex and mercurial. Remember, we're going to be generating more of these data, not less.

Three, nothing about this identifier-centric system is user-friendly. Individuals—or, as noted, government or NGO representatives working on their behalf—have to repeat the registration process to obtain nearly every identifier, provide the same forms of über-identification, and maintain a portfolio of ID numbers, usernames, passwords, and the answers to personal questions. It is a system for the über-organized. It asks us whether we're robots and excludes robots from having their own identification—not good for all those robots that want to buy electricity.

Four, we bear most of the risk and responsibility for cleanup, should hackers break into these central systems and steal our identifiers and our data—but we enjoy none of the rewards of third-party data usage. Consider the legendary breach of Anthem, the largest U.S. health insurer. It agreed "to settle litigation over hacking in 2015 that compromised about 79 million people's personal information for $115 million, which lawyers said would be the largest settlement ever for a data breach."[52] Then it was breached again in October 2017 through one of its vendors, exposing the Medicare and health plan IDs of some 18,000 members.[53] Fool me once.

This is not identity management. This is identifier whack-a-mole. Our identities should be informing our selection and management of identifiers. Instead, these identifiers are deforming our identities. If we don't have them, we get the message that we aren't equal, we don't belong. If we do have them, we get the message to watch our backs, violation is a risk of participation, or privacy is overrated. They become a means of manipulation, conforming us to authoritarian rule. It's a lose-lose-lose-lose-lose situation, multiplied by all the identifiers we need to manage in an increasingly data-rich world.

To bootstrap our identity, we need a model that is distributed among and maintained by the people whose identities it protects so that everyone's incentives align—an identity commons—with clear rights for users to steward their own identity, access (and allow others to access) and monetize their own data, and participate in rule making around the preservation and usage of the commons.[54]It must exist independent of any corporate, government, or other third party, not subject to the agency risk of executives or political parties. It must interoperate with these institutions even as it outlasts them. It must outlive its users and enforce their right to be forgotten, which would mean separating data rights from the actual data so that the rights holder could delete them. And, to be inclusive, it must be user-friendly with a low-tech mobile interface and low-cost dispute resolution.

Here's where blockchain technology comes in. In chapter 2, we wrote about the technical and theoretical groundwork that has been laid—such as the deployment of public key infrastructure and the separation of identification and verification layers from the transaction layer, but we focused more on the principles of privacy design, which is the flip side of this identity coin. We alluded to the challenges to using Pretty Good Privacy and why it wasn't widely adopted. To that discussion, we add the promising work of Zooko Wilcox O'Hearn and his associates at the Zerocoin Electric Coin Company. They launched Zcash, a public blockchain that enables users to conduct transactions while masking their identifiers and the amounts exchanged, compared with the bitcoin blockchain where those data are viewable. Zcash uses what it calls a zero-knowledge proof construction—specifically, a zero-knowledge succinct noninteractive argument of knowledge, or "zk-SNARK" (to which we say, "Gesundheit!")—in which participants can validate transactions and assemble them into a block with zero knowledge about them. Vitalik Buterin told *Fortune*, "I think zk-SNARKs are a hugely important, absolutely game-changing technology. . . . They are the single most under-hyped thing in cryptography right now."[55] We agree: it is an important innovation in privacy.

Let's return to the technology of identity. In *CoinDesk,* veteran developer Christopher Allen wrote a superb overview of the technological "Path to Self Sovereign Identity," from the centralized IANA and ICANN, to the federated Microsoft Passport and Sun Microsystems Liberty Alliance, and then to the user centric but registry-controlled OpenID.[56] With the emergence of blockchain, numerous identity projects have sprung up around the logging, storage, and accessibility of personal data. In chapter 2, we looked at a big one, MIT Media Lab's Enigma and its use of homomorphic encryption and secure multiparty computation, both critical to the identity principles of data minimization and algorithm transparency*:* the data user gets access to only the data needed for a computation but without seeing it, and the data owner can see the algorithms used in processing it. MIT Human Dynamics Group's OpenPDS/SA (for personal data store/safe answers) is a platform for organizing all our personal data streams and allowing people to query our data and get answers but not details.[57]

Blockchain users can already obtain identifiers through such start-ups as Civic, ShoCard, and uPort. We counted at least twenty such companies in the space.[58] The uPort identifier, for example, is a unique and persistent twenty-byte hexadecimal string that is core to uPort's identity system: it serves as the address of a specific type of smart contract known as a *proxy contract*, a piece of special purpose code that executes a complex set of instructions involving identity on the blockchain. The proxy contract is the ultimate mechanism through which a user can digitally sign and verify a transaction, an action, or a claim; manage cryptocurrencies or other tokenized assets; interact with other smart contracts on the Ethereum blockchain; link to the user's off-chain data stored in, say, the distributed InterPlanetary File System; and grant others temporary permission to read or write specific data files in exchange for value.

The uPort system would also work for devices such as driverless cars or 3D printers, virtual entities such as IBM's Watson, or institutions such as the Blockchain Research Institute. For user-friendliness and security, uPort provides a mobile app that holds the user's cryptographic keys. Separating these keys from the proxy contract is another type of smart contract, the *controller contract,* which contains logic for identity recovery: if the device is lost or stolen, the user can replace the private key without having to replace the proxy identifier and all the assets associated with it.[59] So amazing.

Many of these start-ups are collaborating in the Decentralized Identity Foundation (DIF), a consortium consisting of Hyperledger, R3, and Sovrin and incumbents such as Accenture, Microsoft, and IBM. DIF has formed to combine "decentralized identities, blockchain IDs, and zero-trust data stores that are universally discoverable" along the lines of the model of the identity commons we described above.[60]Its working groups are focusing on three big areas— identifiers and discovery, storage and computation of data, and attestation and reputation—with an eye to developing use cases and standards.[61] Separately, Fabian Vogelsteller has put forth "Ethereum request for comment—Issue 725" (ERC-725), a standard that specifies an interface for self-sovereign identity (just as his ERC-20 did for initial coin offerings), where identity resides in a smart contract as it does in uPort.[62]If the standard takes off as the ICO standard did, then we'll make real progress toward realizing this new identity management system, core to the blockchain revolution and the rebalancing of power.

The transition will take time. We expect organizations to take at least two actions to rebuild the trust of those whose data they hold. The first involves data governance. Many large corporations and government agencies have strong governance mechanisms for their hard assets. However, according to Dr. Elizabeth M. Pierce, a program chair for the International Conference on Information Quality hosted by MIT in 2015, "Information assets are often the worst governed, least understood, and most poorly utilized key asset in most firms because [information] is increasingly easy to collect and digitize, has increasing importance in products and services, is very difficult to price, has a decreasing half-life, has increasing security and privacy risk exposure, and is a significant expense in most enterprises."[63]

Dr. Pierce advocates for strong data governance—we couldn't agree more— which she defines as "specifying the decision rights and accountability framework to encourage desirable behaviors in the use of data." She makes an important distinction between data governance and data management: "Governance is about determining who inputs and makes the decisions and how. Management is the process of making and implementing the decisions."[64]

The second involves the discontinuation of practices that collect and store customer data and either destroying these massive customer databases altogether (after returning files and records to customers) or migrating these data to distributed storage systems such as the IPFS and then transferring control to customers.

Consider what Dr. David A. Jaffray is looking to do with patient information. Dr. Jaffray, executive vice president of technology and innovation at the University Health Network and the director of the Techna Institute for the Advancement of Technology for Health, has been involved in the implementation of the patient portal for Toronto's University Health Network. The portal gives patients complete access to their test results, imaging and pathology reports, diagnoses, health care provider's notes from in-person and telephone conversations, health management plans, referrals, and discharge summaries—all of which patients can share as they see fit. The results have been so positive for both patients and medical providers alike that Dr. Jaffray is keen to take the experience to the next level: total patient ownership over this information.

He is working with IBM and Hyperledger to design a blockchain-based pilot project because, for him, it represents a major pivot in thinking about patient data: by putting ownership in the hands of the patients themselves, it obviates a costly complexity of rules, regulations, and contracts among different institutions across jurisdictions—research hospitals, insurance providers, pharmacies, testing sites and laboratories, medical suppliers, drug companies, and National Institutes of Health, to name a few—required to protect patient privacy and security. That it simultaneously solves the data portability problem is a real plus for patients, and it frees them to form communities of interest— member-owned and -governed "health cooperatives," says Dr. Jaffray—around health or medical issues. Through these cooperatives, members could collectively bargain for better prices on specialty drugs in exchange for time-limited access (Dr. Jaffray uses the term "Snapchart") to their collective data on a particular disease.

What interests Dr. Jaffray in particular is the blockchain's ability to support a legal framework for consent at a large scale: through blockchain, patients can not only verify their agreement to share data at a byte level but also track their behavior at a granular level. With these two capabilities, patients can generate unprecedented phenomic data that they can donate or license under very specific terms to medical science, along with their genetic data. Let's call this biodata stream the human *menome*. Human genomics research has been quite useful, of course, but mapping the relationship between genotype and phenotype (e.g., a person's height, weight, health, disease, and fitness over time) will transform our understanding of diet, exercise, occupation, and environment, if not revolutionize medicine altogether. Imagine the health care supply chain of one, tailored to you, and funded in part by your menome.

"It's far more expensive to live a life than to do genetic testing," Dr. Jaffray said. "We need a way for individuals and their heirs to make use of these phenomic data captured over a lifetime."[65] Think of the immortal Henrietta Lacks—both her genes and her phenotypes—except that she now has control over these data, she can decide whether to approve the cultivation of her cells into a cell line, and she can will these data to her family, generation to generation. What an inheritance, potentially a means of transforming how we think of disease to begin with—as an asset, not a liability.

The ability to access and perform data analytics on large sets of (relatively) free data is currently a core competence that bestows competitive advantage; but, as individuals take back control over their data and form their own avatar of data —a *davatar*, if you will—the ability to secure those data sets in a distributed and trust-minimized manner and to help individuals manage and monetize their own data will replace big data analytics as the corporate capability that investors will value. It will remove data as a toxic asset from the corporate balance sheet and make it a fundamental human asset from birth. It will flip the data analytics business model on its head and reward corporations for serving as data brokers on behalf of individuals. We'll see the end of the large centralized data frackers that scrape, hoard, and rent but don't protect these data.

We'll also have a potential solution to the growing fear of mind hacking described by historian Yuval Noah Harari and evidenced by the effectiveness of Cambridge Analytica's psychographic profiling and the Russian manipulation of social media to influence the outcome of the 2016 U.S. presidential election.[66]

Harari writes, "Just as divine authority was legitimized by religious mythologies, and human authority was legitimized by humanist ideologies, so high-tech gurus and Silicon Valley prophets are creating a new universal narrative that legitimizes the authority of algorithms and Big Data."[67]Indeed, Cambridge Analytica received a 2017 David Ogilvy Award for its big data practices from the Advertising Research Foundation.[68] Harari refers to this worldview as "Dataism," whose adherents "perceive the entire universe as a flow of data, see organisms as little more than biochemical algorithms, and believe that humanity's cosmic vocation is to create an all-encompassing data-processing system—and then merge into it."[69]In such a data-bio-mind-meld, we risk the loss of free will.

Others think such fears of human menome hacking are unfounded. "This sort of extremely precise and complete mapping of all human metabolic functions and brain activity is a dream," says Marcelo Gleiser, a theoretical physicist, professor, and director of the Institute for Cross-Disciplinary Engagement at Dartmouth College. "There are limits to what technology can do. Every machine has a precision range and is blind to what goes on beyond what it can probe. To monitor the activity of about eighty-five billion neurons and the flowing of neurotransmitters through trillions of synapses seems highly implausible, even if I wear my science-fiction nerd hat."[70]

We prefer to err on the side of caution and to advocate strongly for self sovereign identities and ownership of all our data through blockchain technology and identity commons.

SMART CONTRACTS COME OF AGE

The use of smart contracts is a big theme of the book—after all, contracts are the building blocks of our identity, economy, and society—and so every chapter highlights potential use cases. In chapter 2, we explain what smart contracts are and how they work. Like traditional contracts, they include incentives—rewards and penalties—for performance in the form of mutually agreeable rules that spell out what happens to assets if certain conditions are met, except that smart contracts can sometimes automate performance (as with the cryptoassets described previously) and call on algorithms and sensors to determine objectively whether those conditions have indeed been met.

Nick Szabo, the father of smart contracts, has come up with the best visual for newcomers to the concept: think of an old-fashioned vending machine as a smart contract, where the terms of a very simple business relationship are programmed into the machine: if the machine has an acceptable type of beverage at an acceptable price, then the buyer selects the beverage and inserts enough coins to cover the price, and the machine verifies the amount, dispenses the chosen beverage, and makes change, if due, for the buyer.[71]In this sense, smart contracts have existed since the first century AD, when the Greek mathematician Hero of Alexandria invented a means of meting out exactly the amount of holy water that worshippers had paid for.[72] Today there are nearly seven million vending machines in the United States alone.[73] We're surrounded by smart contracts.

So they must be legally binding, right? Perhaps. There is no definitive answer yet. Under U.S. common law, for example, parties can express or imply an agreement: they needn't draft or sign a paper contract for the terms to be binding. According legal scholars Primavera De Filippi and Aaron Wright, "Smart contracts memorializing legal agreements are likely to be deemed enforceable under U.S. law. Parties can memorialize their intent using code just as they can with paper; and, to the extent that they set forth recurring performance obligations, smart contracts could even establish a course of performance or dealing."[74] Only time—and courts around the world—will tell.[75]

In chapter 4, we explored how smart contracts could alter the architecture of the firm in Coasian terms of reducing the transaction costs, both shrinking the number of essential employees at the core and expanding the number of gig workers at the edges. Those at the core will work more on retainer-like relationships in ever-changing roles doing whatever the organization needs. Those at the edge will work on more routine tasks that are easy to specify and to verify completion. This transformation will require executives to do what they have most likely never done before. It is what Szabo calls "the most valuable step, but the one traditional scientific management has failed to recognize and take," which is the restructuring of the firm's contractual relationships. We can see why start-ups have an advantage here. Rarely do incumbent firms think about their contract strategy in terms of all the work that needs to be done.

Through smart contracts, we could apply technology strategically to do a greater variety of deals, not just take-it-or-leave-it ones. We could coordinate a greater number of both things and people from a greater diversity of backgrounds across distant legal jurisdictions. We could use cryptocurrencies as a global payment system. In every phase, we could reduce our costs, minimize the need for third-party platforms, and improve productivity, security, and privacy.[76] Szabo points out the scalability of Uber's approach: "Uber substitutes employment with algorithmically negotiated and verified gig work. . . . Since many more people have much more of their labor expended in employment relationships than in spot market relationships, Uber and its similar successors in other logistics industries may be an even bigger deal than eBay and Amazon— and those have been pretty big deals."[77]

Scalability has its downside, if user data aren't secure. Hackers accessed the personal information of 57 million Uber accounts in 2016, but the company didn't disclose the breach until November 2017. Even then, it didn't notify the affected account holders.[78]

Give a blockchain-enabled vending machine wheels, a seat for humans, a trunk for their luggage, mapping software, a global positioning system, and algorithmic pricing, and you've got yourself a driverless and Uber-less ride service (which we call SUber in chapter 6). Blockchain as a Ledger of Things could run each thing's smart contracts—warranties, provenance, registration, insurance, inspection certification, and even operating software written to meet regulatory standards for, say, vehicle emissions. Those contracts could control the operation of that thing. If a machine, a driverless car, or a piece of heavy equipment failed a safety inspection or its liability insurance expired, then the machine could not turn on.

In chapter 5, we talked in theory about a distributed autonomous enterprise that has neither management nor employees; instead, it is a portfolio of smart contracts in the form not of vending machines but of *decentralized applications* that run “on a secure consensus protocol across a network of computers”—in other words, on a blockchain—“rather than on an individual remote computer or centralized server” and that will run properly even if we don’t trust the owners of those computers.[79]

Shortly after the book came out, we witnessed the launch of the first such enterprise called the DAO (for decentralized autonomous organization), which crowdfunded a record-breaking $160 million from tens of thousands of global investors. What distinguished the DAO from all other start-ups was the absence of management in the traditional sense. Created by boutique blockchain development firm Slock.it, the DAO was a smart contract for a token with built in voting rights. Its stakeholders—human beings—could review and vote on proposals curated by a smaller group of stakeholders to determine how the DAO allocated its funds.

Think about that for a moment. There were no agency costs, no information asymmetry between management and stakeholders, because there were no managers. Nor was there moral hazard, where managers could have behaved contrary to stakeholder interests, perhaps taking outsized risks for personal gain in the absence of personal consequences.

Like any corporation, the DAO could invest in new businesses and hire lobbyists or lawyers to represent its interests and advocate on its behalf. Using smart contracts, the DAO could do pretty much what any organization could do, with one important exception: on the blockchain, its agents could not override agreements, mission statements, corporate values, or operating principles without broad stakeholder debate and consensus. That’s huge.

Problems with its contract code ultimately caused it to fail: a hacker exploited flaws in its use of recursion, a Turing-complete feature of Ethereum and not found in Bitcoin Script language.

According to Szabo, “Ethereum has a much larger attack surface than Bitcoin because of its Turing-complete smart contracts language and the relative abundance of applications enabled by high-level languages.” Still, the DAO’s mere existence demonstrated that autonomous entities could raise huge sums of money—peer to peer, without traditional intermediaries. According to Primavera De Filippi and Aaron Wright, “Hundreds of thousands of smart contracts have been deployed since Ethereum’s launch.”[80]

Still, companies are proceeding with caution. They are identifying pilot projects and experimenting in controlled environments. In chapter 6, we outlined new business models appropriate for experimentation. For example, Slock.it worked with MotionWerk to create a peer-to-peer Share&Charge service in Germany. Owners of electric vehicles can share their charging stations with other EV owners through Ethereum-based smart contracts, all of which are 100 percent updatable so that MotionWerk can adjust or respond quickly in an emergency.[81] Users download a Share&Charge app to handle the blockchain driven control of the charging station and accounting.[82] The system is also fully backed by a digital euro to facilitate transaction settlement.[83] Finally, it runs on a public blockchain and so it is transparent and open; anyone can engage directly with it through smart contracts.

In chapter 7, we talk about the use of smart contracts to hold the dispensers of humanitarian aid accountable and to level the playing field for entrepreneurs.

For example, Siemens AG is working with Slock.it to implement a blockchain based DAO that will allow for voting on projects with a social purpose. UNICEF Ventures is testing a multisignature smart contract to make its asset transfers transparent and trackable, since traditional international transactions are often difficult to track.[84]

Knowledge networks will be critical. Creating a smart contract is more difficult than writing a traditional contract because we don't have hundreds of years of experience and many well-worn legal templates yet. According to Alan Majer, founder of Good Robot, "Solidity, a language for coding smart contracts, seems easy to use but is actually quite complex. Users must understand the nitty gritty *anti-patterns*, that is, software design patterns that might be commonly used but can cause code to execute in unintended ways."[85] Competent smart contract developers are rare, with as few as five hundred in the world.[86] Szabo suggests that organizations hire lawyers with computer science backgrounds and software engineers with legal backgrounds. Universities, law schools, and continuing education programs should also be developing coursework and training modules to meet the need for this expertise.

ASSET CHAINS: WHEN BLOCKCHAIN MEETS SUPPLY AND PROCUREMENT

We often get asked, "What is the next big killer app for blockchain?" There is no better candidate than the global supply chain, an industry that runs two thirds of the global economy. Everything we consume is a product of a supply chain. Assets all over the world are extracted, designed, combined, transported, and sold every day through the supply chains that underpin global commerce. While technologies are increasingly disrupting traditional industries, this flow of goods has not been overhauled in years.

In the book, we argue that blockchain holds the potential of decentralizing traditional supply chains and combining them with artificial intelligence, additive manufacturing, and the growing Internet of Things to produce new value networks that scale to the demand of both machines and human beings.

When we were conceiving the Blockchain Research Institute, we began searching for the brightest minds and expert practitioners in this space. At the 2016 TED Summit in Banff, Don met Bettina Warburg and Tom Serres. Bettina was brilliant—her talk has well over three million views. She quoted the work of Nobel Prize–winning economist Douglass North on institutional economics and described blockchain as a new technological institution that would transform the economy and change how we exchange value.

This got us thinking about the unprecedented volume of data that blockchains would be throwing off, enabling us to study large-scale economic systems as never before. Surely a major category of those systems—the global supply chains that manage most of our global trade—would soon be up for change.

We decided to partner with Bettina, Tom, and their company, Animal Ventures, to lead this research. The results have been spectacular.[87] One of our conversations revved up my formulation engine and out popped the phrase *asset chains,* in response to their description of the blockchains that would support the autonomous and distributed management of supply chains.

Their research is foundational and provocative for anyone who deals with assets of some kind—because *every asset has a supply chain*. These new supply chains are autonomous, distributed, and cognitive in the sense that they are learning and bundling what they learn into opportunities for systemic self improvement in efficiency and responsiveness. Cognitive supply chains require “a network state” function that provides a singular universal truth as the basis for what Bettina and Tom call *machine trust*.[88]

Which is where asset chains come it. This new way of thinking provides a framework for machines to participate autonomously in supply chains and the markets they serve. They allow us to unlock the trading capability of machines without human intermediaries.

The work uncovered some extraordinary initiatives using cryptoeconomics and blockchain to bring about this transformation. Consider Sweetbridge, a company that allows any enterprise to do four things that would be impossible without blockchain: pay suppliers and get paid early while decreasing the amount of money tied up in inventory and receivables to zero; obtain low to zero interest rate loans on their own assets without credit checks or loan applications; share underutilized capacity in supply chain assets with other organizations turning unused capacity into a new source of revenue; and incentivize supply chain experts to help optimize supply chains paying for services based on the outcomes that are measured, such as increase in sales and decreases in expense.

It gets better. The Sweetbridge protocols replace the need for letters of credit, trade financing, and working capital in supply chains. Here's how it works. Sweetbridge uses smart contracts to mint a cryptocurrency that is stable and pegged to the fiat currency of the user's choice based on the collateral value of an asset. The protocol acts like a loan that a company grants itself and must pay off in the same cryptocurrency it borrowed. The Sweetbridge protocols convert the value of any asset into a cash equivalent that a company can hold on its balance sheet as cash, trade with other companies as cash, and convert to cash when fiat currency is needed.

Sweetbridge is also the creator of the discount token discussed earlier—a new idea for funding anything from government infrastructure to supply chain assets. Its customers can buy and use these discount tokens themselves or sell them to other customers. According to Scott Nelson, "The more you buy and lock, the greater your discount. The more the network grows, the greater your discount." In essence, customers are "rewarded for growing the network and using the product or service."[89]It incentivizes network loyalty.

The platform also provides a settlement process that can eliminate counterparty risk in supply chains. The process does not require a bank or credit card network for payments because parties can transfer value in minutes on a blockchain. Nor do parties need an intermediary to hold the original asset until the loan is paid off. To sustain liquidity in the network, Sweetbridge has formed an alliance of projects. Members are working together to build supply chains that can identify faster, less costly, and more secure means of getting products to market and then reconfigure themselves to deliver accordingly. Hence, they are cognitive.

Bettina and Tom also explain what leaders should be doing now to prepare their organizations for this inevitable decentralized future. First is to get comfortable with transparency, an integral component of corporate social responsibility and a source of competitive advantage. According to Bettina and Tom, the winners in the decentralized economy will be those who "drive supply chain transparency toward the most accurate network state possible." Second is to cultivate talent, not just lawyer-coders who can program smart contracts but also artist-engineers like Leonardo da Vinci who imbue their designs with humanity. Third is to form coalitions around common goals, one of which is the shared governance of asset chains and the development of standards and best practices.[90] Now is the time to begin.

BLOCKCHAIN AND THE C-SUITE

For the last century, academics and business leaders have shaped the practice of modern management. The main theories, tenets, and behaviors of managers have worked well overall in building corporations—largely hierarchical, insular, and horizontally or vertically integrated. Until now.

In chapters 3 and 4, we discuss how blockchain will bring about profound changes, not just in the nature of firms, but in how they are funded and managed, how they create value, and how they perform basic functions like marketing and accounting. In some cases, algorithms will replace management altogether.

Because blockchain changes the deep structures and architecture of the firm, it will thereby transform our models of management and the roles of the C-suite. Vertical integration may make sense in some situations, but overall networks will become better structures for creating products, services, and value for stakeholders.

Dr. Irving Wladawsky-Berger, a visiting lecturer at MIT's Sloan School of Management, says, "Navigating this balance between hype and promise is a key responsibility of a company's senior management team."[91] So what should the C-suite prepare for? "Executives must decide whether their companies should adopt blockchain early and start experimenting now or wait until the technology matures and risk lagging behind more aggressive competitors."[92]

Chief Executive Officer

Wladawsky-Berger calls blockchain "the Internet of Transactions, a secure system of record for every transaction that has ever occurred" since its inception. He advises CEOs to "figure out how to best communicate, in the simplest way possible, why every company should embrace" blockchain technology. Business strategy becomes a means not only of proving that you "get it," that your organization gets it, but also of associating your brand with the future. This requires consistently telling your blockchain "stories over a variety of communication channels, including press interviews, conferences around the world, IT and financial analyst meetings, Web articles, and lots of client engagements."[93] The CEO sets the tone.

Wladawsky-Berger provides a word of caution about what he calls "a Wild West mentality" in this second era of the Internet, "where leaders send unproductive messages to the effect of 'the rules don't apply to us,' whether they're talking about the principles of economics—'it's all about eyeballs, not revenues'—or the codes of conduct in a civil society, such that sexual harassment, for example, becomes normalized." He sends a strong message to leaders: *"These rules do apply,"* no matter how organizational structure changes.[94]

Since most blockchain initiatives are in the alpha or beta stage, CEOs need to manage expectations, promising only to learn from their experiments and their participation in consortia so that they can anticipate how the future of blockchain will unfold and affect their business.

Chief Information Officer/Chief Technology Officer

CIOs and CTOs have always had to ensure that their organizations incorporated and deployed the right technology at the right time. The Fourth Industrial Revolution centers not only on blockchain but also on machine learning, robotics, the Internet of Things, and even biotechnology.[95] The demands on CIOs and CTOs within an organization will expand from implementing business strategy to formulating it so that it leverages a range of technologies. CIOs and CTOs will need to wear the hats of the visionary and the great communicator so that they can help their peers in the C-suite understand the potential impact of these technologies and move them to action by sharing relevant use cases and suggesting pilot projects.

They will also need to orchestrate innovation across the enterprise. According to Oliver Bussmann, an award-winning CIO and CTO, "Blockchain technology will have a profound impact not only on processes external to the enterprise but also on the architecture stack within the enterprise—generally by moving business logic and processes out of enterprise silos and onto shared blockchains and broader-based ecosystems."[96]

To prepare their organizations, CIOs and CTOs can begin cultivating the necessary skills, talent, and relationships, be they in-house or in the network. There is already a shortage of accomplished blockchain developers and a lack of expertise in smart contracts and blockchain integration. Attending blockchain meetups and participating in relevant consortia can help to make connections.

They should also keep an eye on quantum computing, which uses quantum bits (or "qubits") rather than conventional bits to solve extremely difficult math problems vastly faster than our computers today. We touch on the quantum threat in chapter 10. We have since discovered that it's closer than we originally thought. According to experts at the Institute for Quantum Computing at the University of Waterloo, there's a one-in-seven chance that a quantum computer will be commercially available by 2026. That's less than a decade away! By 2031, the odds become one in two. "The arrival of phenomenally powerful quantum computing will shatter currently deployed public key cryptography and weaken symmetric-key cryptography, thereby undermining the cybersecurity that protects our infrastructure and systems," says Michele Mosca's team at Waterloo. "We cannot assume that blockchains, with their strong reliance on public key cryptography, are immune from this existential threat."[97] CIOs and CTOs should make sure that any blockchain deployed under their watch is quantum-proof.

Chief Human Resources Officer: A Better Way to Engage Talent

Human resources is an area that, when treated properly, can be a strategic asset, not a cost center. As firms move toward contingent labor and operate outside traditional organizational boundaries, the HR function grows more challenging. Perhaps the most immediate concern is diversity. As many have observed, the blockchain movement is overpopulated with men (though many of the best technical minds in the industry are women). In technology, compared with other sectors of the workforce, people of color are underrepresented by 16 to 18 percent, and women hold only 25 percent of all computing jobs.[98] "Everyone in Silicon Valley complains of the gender bias, and perhaps in the blockchain ecosystem even more so," said Pindar Wong, chairman of VeriFi (Hong Kong), former vice-chair of ICANN, and trustee of the Internet Society. "That's unhealthy. We're not getting enough diverse views. Going back to cybernetics' first principles, Ashby's Law of Requisite Variety, we need a variety of viewpoints, be it male, female, gay, straight, old, young, whatever you want to perceive it to be."[99] When problem solving has deadlocked, a key question to ask is, "Do we have enough variety in the room or online?" The goal is to maintain requisite variety to avoid thinking errors, said Wong. "You avoid thinking errors by having a wide variety of views that get equal treatment."[100]

The process of assembling and dispersing a diversity of talent can be far more effective and profitable than the traditional hiring-and-retaining model if HR professionals learn how to leverage blockchain in finding the right people, negotiating all their contracts, implementing the terms, and coordinating their contributions. Andy Spence, founder of Glass Bead Consulting, expects blockchain to transform the HR function in three waves. The first will resolve fundamental issues with recruitment, namely identity management and verification of credentials by querying prospective candidates' black boxes, and payment in nearly real time for output or time worked. The second will provide benefits in the broader talent ecosystem and reduce the number of full-time employment contracts. In the third, he envisages "technology sourcing and executing work projects by bringing in workers and services autonomously."[101]

Spence advises CHROs to "think more in terms of tasks that need to be sourced rather than jobs that need to be filled" and to celebrate portfolio careers, verified career profiles, and the pursuit of digital credentials (aka open badges).

He suggests that "HR can be a pioneer in the new technology—not just blockchain but also artificial intelligence, robotics, and the Internet of Things, all of which could eliminate some jobs and create new ones." Ultimately, HR professionals will need to reimagine their function, since the firm "may no longer require many current HR activities in payroll, corporate learning and development, recruitment, performance management, and benefits administration." Instead, they should focus on enabling self-organizing teams, quantifying and predicting team performance, and safeguarding talent systems so that they remain effective, fair, and inclusive.[102]

Chief Marketing Officer: A Better Way to Engage Customers

Since companies will no longer be able to profile customers online by tracking and capturing their behavior, marketing and sales staff will also need to query prospective consumers' black boxes. Some consumers may allow access to their data in exchange for freebies; others will charge companies a fee to license their data. But the quality of results will increase because companies will find their target audience with greater precision. The nature of the blockchain would prevent the Wells Fargo style of customer abuse.

The upside is an end to intermediary fees and institutional bias. Jeremy Epstein, CEO of Never Stop Marketing, thinks smart contracts will improve SEO performance and price negotiation. Advertisers will know exactly which elements of their ad budgets delivered results: "We will have the opportunity to know the exact cost of attention and subsequent acquisition of an individual customer, eventually at scale," he wrote. "As we move to blockchain-based identity systems, we will witness the arrival of a *pay for attention* model."[103] Epstein described Brave Software's approach: it introduced what it calls a "basic attention token" (BAT) and launched a free Web browser that blocks ads and cookies. Epstein explained: "The token is the mechanism through which an advertiser pays for an individual's attention-based effort. With Brave and the BAT, we will pay end users directly for their attention, instead of the 73 percent of all ad dollars going to Facebook and Google."[104] As noted, retailers and manufacturers could eliminate the cost of warehousing and protecting consumer data.

General Counsel: A New Role for Lawyers in Developing Code

Ronald Coase and his successors argued that a firm was essentially a vehicle for creating long-term contracts when short-term contracts were too much effort to negotiate and enforce. Blockchain facilitates contracting, short- or long-term. Through smart contracts, companies can automate terms and use agents known as *oracles* to refer to external data fields, such as commodity prices and foreign exchange rates. They can trigger alerts and ensure payments.

Because smart contracts are self-enforcing, corporations will not want to enter them lightly. Lawyers and other managers will need to learn how to audit legal templates and make sure the contract software supports what its parties agreed to do. The watch phrase is “Don’t roll your own crypto,” meaning don’t create some new and unproven cryptographic means of securing your smart contracts without publishing it for peer review and outside testing. That’s apparently what IOTA did: it kept its new Curl hash function to itself.[105](IOTA is a blockchain protocol, developed on the concept of a tangle—known also as a directed acyclic graph, as with Hashgraph—to disrupt the Internet of Things. Its team named its hash function Curl.[106]) Cryptographers from Boston-based Commonwealth Crypto and MIT’s Digital Currency Initiative both identified security problems with Curl and found IOTA’s response to their findings equally worrisome.[107] Stick with well-tested methods for creating and running smart contracts, and make sure you have someone on staff who can audit the code of a proposed new blockchain or a DApp behind an ICO.

Lawyers will also need to stay on top of cases involving blockchain, smart contracts, ICOs, and patents, particularly across jurisdictions and in heavily regulated and patent-rich domains such as health care, financial markets, pharmaceuticals, and medical appliances. General counsels will want to understand the patent strategies in the space. According to Thomas M. Isaacson, a lawyer and shareholder of Polsinelli PC, blockchain innovators file patent applications to profit from an invention, to prevent others from using an invention, or to make an invention available to collaborators. The bar is high for receiving a grant. Isaacson writes, “A blockchain patent application must meet three criteria—eligibility, novelty, and nonobviousness. The question of obviousness is rich and deep. Whether a new useful process based on blockchain technology is patent-eligible is not clear-cut. The courts do not favor existing business practices being implemented on generic computers. The more narrow and focused the claims are, the better the chances of getting claims allowed.”[108]

A Fair Deal for Corporate Executives

The year 2017 brought another round of high-profile scandals: bribery charges against Samsung Electronics vice chairman Lee Jae-yong; Uber’s alleged use of “Greyball” software for dodging regulators where it was operating unlawfully; the preventable breach of Equifax, the theft of 145 million records, and the alleged insider trading by the Equifax executive who “dumped his stock before the news [of the breach] went public," according to the SEC's Atlanta Regional Office; the falsification of data by Kobe Steel and Mitsubishi Materials on products sold to clients, and Wells Fargo's admission that it had opened another 1.4 million phony accounts (on top of the 2.1 million already disclosed) and billed some 570,000 consumers for car insurance they didn't need, causing some to default on their car loans.[109] Year after year, executives don't always act with integrity or incentivize employees to act with integrity.

Through smart contracts, owners can hold these executives accountable— they must abide by their commitments as enforced and settled by software. Companies can program relationships and parameters of outcomes so that everyone has a better understanding about what each party has signed up to do and can see whether that party is doing it. With multisignature contracts, shareholders can even vote on high-stakes managerial decisions such as particularly risky investments.

On the blockchain, executives will no longer need to swear that their books are in order once a year; their books will be in order *every ten minutes*, whether executives like it or not. No need for public auditors. The blockchain eliminates human error and prevents fraud in accounting. Shareholders and regulatory agencies alike will be able to examine the books at any point in time. Investors can create their own creditworthy ratings dashboards based on the facts. No more subjective ratings agencies. At last, stakeholders can reward executives for achieving actual results.

GOVERNANCE AND LEADERSHIP FOR THE NEW ERA

Stewarding the Blockchain Revolution

How is this whole blockchain revolution going to play out? As we said in the book, we're of the school that "the future is not something to be predicted: the future is something to be achieved." We argued that, like the first era of the Internet, this blockchain era should *not* be governed by nation-states, state-based institutions, or corporations.

Yes, there is a role for regulation. The first era of the Internet was initially unregulated, but today there are laws in various countries concerning topics ranging from spam and privacy to so-called net neutrality. The second era will require even greater government involvement, because unlike information, it's all about assets—for which there is a clearer public interest.

Still, how we govern the Internet of information as a global resource serves as a model for how to govern this new resource. Rather than relying on governments, blockchain must be primarily self-governed through the bottom up, multistakeholder approach using what we called "global governance networks"—a concept developed in our previous multimillion-dollar program investigating multistakeholder networks for global problem solving and described in chapter 11.[110]

Since then, we have dived deeper into this issue. We hosted a meeting of key players of the blockchain ecosystem at our family lake house in Muskoka, Ontario, Canada—resulting in the creation of the Muskoka Group Manifesto on stewardship of blockchain.[111] We also wrote a white paper commissioned by the World Economic Forum.[112] Faculty members of the Blockchain Research Institute have explored it and produced some helpful material.

We came to some important conclusions for anyone who cares about making blockchain happen. The Internet of information is a network of similar networks. Blockchain is not—it is balkanized at the basic platform or protocol level.

Therefore, unlike the Internet of information, which is a vast network of similar networks, this Internet of value requires stewardship at not just one level but three:

1. Each *platform* needs to govern itself—to develop an ecosystem, standards, and use cases and ensure a robust rollout of its technology. In the last two years, there have been important improvements in this regard, with the bitcoin community forking and implementing different solutions for scalability, the rapid expansion and development of the Lightning Network, Ethereum's crisis management by consensus and planned implementation of proof of stake, and Hyperledger's call for both urgency and moderation around standards.

2. At the *application* level, there have been all kinds of consortia established where companies like FedEx or Pepsi join with industry partners and even competitors to develop standards and common applications. Platforms themselves are encouraging such application level partnerships as reflected by the Enterprise Ethereum Alliance, which works to build application-level standards for companies using Ethereum.

3. At the overall *ecosystem* level, there are networks like the

Blockchain Research Institute conducting research and disseminating knowledge, and advocacy groups like the Global Blockchain Business Council or the Chamber of Digital Commerce.

We can apply our "global solution networks" framework to each of these levels.[113] We urge stakeholders in the space to codify their common ground through standards networks; welcome stakeholders with radically diverse views of what needs to be done through networked institutions; respect members' interests and constraints through advocacy networks; ensure that no one does any harm through watchdog networks; participate in policy debates and coordinate regulation through policy networks; get up to speed through knowledge networks; and keep incentives for mass collaboration in mind through delivery networks.

This is critical work. Whether you are a technology provider or user of this technology, you should care. Think not only about the needs of your own

organization but also about the overall challenges of stewarding the blockchain revolution through the maze and even onslaught of difficulties, from technical challenges to bad legislation.

Profile of a Blockchain Hotbed: Seven Conditions for Success

Silicon Valley has been a modern engine of digital innovation, finance, incubation, and transformation of business models. It's the center of venture capital and entrepreneurship, and it produced FANG (Facebook, Apple, Netflix, and Google). Not so for the second era. ICOs and STOs are replacing venture capital, and leaders of the old have difficulty embracing the new.

It's also unclear as to whether a single global hub for blockchain is feasible. As a technology, blockchain is decentralized by design. Early protocols were developed through cross-border collaboration by creative trailblazers in regions largely outside of Silicon Valley. In the process, hubs of blockchain-based innovation have emerged the world over.

If not the Valley, then where? BRI researchers Hilary Carter and Jill Rundle found that not all blockchain hubs are equal, but leading national ecosystems have many of the following in common.[114]

Incubators and Entrepreneurship

Innovation is nurtured in environments established exclusively for this purpose. In Toronto, incubators such as MaRS, OneEleven, and Ryerson University's DMZ have provided a favorable climate in which blockchain entrepreneurship can flourish. Regions with incubators have an automatic advantage over those without.

Corporate Leadership

Centers of blockchain innovation very often enjoy close ties with established business communities. In areas where corporate entities manifest a culture of curiosity and market positioning as innovators, blockchain developments can especially thrive.

Educational Institutions

Great computer science schools can lead to great blockchain innovation ecosystems. Tip the hat to MIT, the National University of Singapore, ETH Zurich, Stanford University, Middlesex University, the University of Toronto, the University of Waterloo, and York University. The University of California at Berkeley may save Silicon Valley yet with its "Blockchain at Berkeley" program.

Investment Climate

Angel capital, venture capital, and strong financial services industries must have a risk tolerance for this kind of innovation. Through ICOs, entrepreneurs have harnessed blockchain as a distributed financing mechanism to overcome the traditional financial barriers that had prevented many ventures from getting off the ground, though regulatory hurdles must first be overcome.

Government Support

One of the most important things that governments can do is to be model users of the technology itself. Government community-based initiatives can also fund innovation directly. In Hangzhou and Guangzhou, China's government is pouring billions into blockchain development. Canada's supercluster initiative has put a billion dollars into projects with a blockchain component. Israel has produced more unicorns per capita than anywhere.

Regulatory Environment

As we have explained, governments can help or impede innovation. ICOs are a new source of funding. Neither overregulation nor no-regulation is sensible. Free-for-all jurisdictions like Belarus or Ukraine will run into big problems. But banning bitcoin, ICOs, STOs, and cryptocurrency exchanges as many countries are considering will hurt innovation for decades. This is just one of many regulatory issues, not the least of which is taxation.

Communities of Talent

Highly educated populations are an important factor for innovation to take root in any given jurisdiction. How do you initiate a national brain *gain* rather than brain drain? Canada reversed this trend, thanks not only to Donald Trump. In November 2017, Mayor John Tory of the city of Toronto spoke to the Blockchain Research Institute about making Toronto a global technology leader, ensuring that the city attracts talent pools from other countries, and persuading Canadians who have flown south to return home.

Leadership of Nations: The Ten Ahead

The opportunity to lead the blockchain revolution is still an open playing field. Whichever country wins will have an innovation economy for decades ahead. Here are the contenders, listed alphabetically.[115]

Australia

Blockchain innovation is thriving in the land Down Under. There's a burgeoning community of collaborators and advocacy groups, including the Blockchain Association of Australia and the Australian Digital Currency Commerce Association (ADCCA), and innovative apps such as ChronoBank are well ahead of competitors in terms of market positioning. Recently, Australia removed taxes from transactions and trades that are made using bitcoin, and in a historic move, the Australian Securities Exchange (ASX) has announced adoption of blockchain following a two-year test of the technology.

Canada

We could argue that Canada has the biggest ecosystem in the world. Vitalik Buterin left the University of Waterloo to create Ethereum. Some of the world's biggest incubators are headquartered in Toronto. There are five innovative banks working to rethink the financial industry. Some of the world's most promising start-ups, such as Nuco/Aion, Paycase, Tendermint/Cosmos, and Decentral, have strong roots in the Toronto area. Vanbex, Axiom Zen, and Frontier Foundry are based in Vancouver. Quebec, with its cool climate and plentiful energy, is quickly becoming the go-to region for cryptocurrency mining operations. There is strong national government support, and the Bank of Canada is an innovator. We'd argue that Toronto is the global center of thought leadership with the Blockchain Research Institute.

China

China's relationship with blockchain and digital currencies could best be described as complex. The country is able to mobilize vast resources to implement any technology that its leaders view as most beneficial or, conversely, to control tightly those it deems potential threats. Massive government initiatives—including banning ICOs, cryptocurrency exchanges, and the mining of bitcoin itself—have simply impeded entrepreneurship. At the same time, China has openly nurtured other aspects of blockchain innovation, keeping the door open to a blockchain-based fiat currency and other innovations that will drive economic growth.

Dubai (United Arab Emirates)

The Dubai blockchain strategy, led by blockchain innovator Vinay Gupta, was launched in 2016 as an exploration and evaluation of technology innovations that could provide simple and secure transactions to make Dubai a leading city in efficiency. The crown prince has targeted 2020 for all government documentation to be entered on a blockchain. As a gateway to Asia and Africa, Dubai's potential impact on supply chains, transportation initiatives, and government services is enormous.

Estonia

This tiny Baltic nation has demonstrated incredible initiative in blockchain transformation. Nearly all of Estonia's public services have been digitized, including identity. The Estonian data aren’t central, and so major breaches are unlikely; and the underlying blockchain asserts its legitimacy, making medical, school, financial, and government information readily verifiable across platforms —even allowing emergency personnel to access medical records before they reach victims and preregister them en route to the hospital. With the ability to execute smart contracts for remote e-residents, Estonia is displacing the local governments of its subscribers.

Singapore

Singapore was recently identified as the third-largest ICO market (after the United States and Switzerland) and the leading ICO hub in Asia.[116] Like Dubai, the city-state is moving toward its own version of a “Smart Nation,” creating
policies and infrastructure to streamline the adoption of new technology in areas such as health care, fintech, education, autonomous vehicles, and public transit.

Sweden (Stockholm and the “Node” Pole)

In 2016, a project to use blockchain technology for the Swedish Land Registry was proposed after it was determined that the time it takes to conclude a land transaction could be reduced from four months to just a few days. Stockholm is a digital leader among European cities, second only to London as a leading fintech hub. The bitcoin mining community was also quick to take advantage of Sweden’s northern climate to cool their data farms naturally. Boden, a municipality in northern Sweden, calls itself “The Node Pole.”

Switzerland (Zurich and Zug)

Switzerland represents one of the world’s most decentralized political systems, which may be why the decentralized ledger system is seen as an opportunity. Nicknamed “Crypto Valley,” Zug—perhaps in part because of the Swiss tradition of financial privacy and also low corporate tax rates—has attracted bitcoin asset managers, brokers, and currency exchanges, becoming a center for digital money. As the presence of the industry players grew, Zug leaders responded by embracing the technology. City cashiers now take utility payments in bitcoin, and the bitcoin exchange, Bitcoin Suisse, has facilitated $635 million in ICOs.

The Crypto Valley Association facilitates working groups on policy, regulatory development, start-ups, and investments.

United Kingdom (London)

The United Kingdom trails only the United States with 16.7 percent of blockchain start-up activity. Its fintech sector is both vibrant and competitive. The London Blockchain Week, which grew out of an annual conference series, recently focused on government initiatives. Given the high number of identity thefts in the United Kingdom, the government has made new models of identity management a priority. Governor of the Bank of England Mark Carney's Mansion House speech of 2016 also signaled a motivation to advance blockchain applications in financial services as a priority.

United States (New York City and Silicon Valley)

Not surprisingly, the largest market for blockchain development is the United States, with nearly 40 percent of the start-ups in the field. The head start provided by U.S. Internet initiatives is slowly eroding as smaller jurisdictions with fewer regulatory or legacy-system impediments start to gain ground. The legacy power players who have grown up in Silicon Valley, specifically the innovators and venture capitalists who have embraced blockchain technology such as Mark Andreessen and Twitter's Jack Dorsey through his Squarecoin initiative, will likely remain the dominant force in the field.

The ten countries we've listed are showing real leadership. They have, thus far, managed to navigate regulatory and governance uncertainties, giving them an excellent head start in the adoption of blockchain initiatives, in some cases more so than others. There may be no equivalent to Silicon Valley in the second era of the Internet. If economic value can be geographically predistributed by blockchain, and a new economic order realized through sensible regulation, perhaps then, global prosperity centers will simply follow in the technology's decentralized footsteps.

Any country that wants to lead in the second era of the Internet needs to cultivate the seven conditions for success. Consider creating a National Task Force on the Digital Economy, chaired by a well-respected nongovernment leader and consisting of thoughtful and well-respected leaders from business, government, and civil society. Give it six months to hold a national dialogue that engages not only key stakeholders but the population as a whole. Require it to develop an action plan where everyone has a role to play.

What Leaders Can Do

The most exciting development in the past two years has been the emergence of a new generation of leaders for this revolution: the entrepreneurs we've met in visits to thirty countries; the innovative CEOs of major corporations like Fred Smith at FedEx, Jim Smith at Thomson Reuters, and Iain Conn of Centrica; the CFOs, CIOs, and chief legal officers who were curious about the implications for their roles and stepped up to lead; the professionals and managers from every nook of large companies. We've been inspired by central bankers, government regulators, and policy makers who have met the challenge of balancing the innovation, growth, and opportunity that blockchain affords with their ongoing responsibility to steward financial markets. Journalists, academics, and pundits stand on all sides of this issue; and the ones who have discarded their cynicism are inspirations. We've also noted a new generation of "crypto natives" who are growing up with this technology and not only investing but working to develop a career in blockchain.

These are exciting and perilous times. If you are a business leader, we do hope that you will use *Blockchain Revolution* as your playbook, sure, but realize that the rules of the game themselves are changing. You have many other resources at your disposal. Set up Google Alerts for "blockchain," "bitcoin," and other key terms to keep up if you haven't already. Check out Andreessen Horowitz's "Crypto Canon" (a16z.com), which the firm updates constantly.[117] Read *The Truth Machine, Cryptoassets,* and *Blockchain and the Law.* Immerse yourself in "crypto Twitter." Find out who at your company is interested in the technology or already using cryptocurrency. Talk to your chief officers and IT department about the technology's implications. Exchange fiat currency for some bitcoin and then use it to buy something just to see how it works— hundreds of thousands of merchants accept bitcoin.[118]Identify nearby blockchain start-ups, take a field trip to see their operations, and talk with their founders. Invite an expert to speak with your team. Most important, act now. This is your chance to reimagine how you create value. If you don't, someone else will.

Read on and join the revolution!

PART I

SAY YOU WANT A REVOLUTION

CHAPTER 1

THE TRUST PROTOCOL

It appears that once again, the technological genie has been unleashed from its bottle. Summoned by an unknown person or persons with unclear motives, at an uncertain time in history, the genie is now at our service for another kick at the can—to transform the economic power grid and the old order of human affairs for the better. If we will it.

Let us explain.

The first four decades of the Internet brought us e-mail, the World Wide Web, dot-coms, social media, the mobile Web, big data, cloud computing, and the early days of the Internet of Things. It has been great for reducing the costs of searching, collaborating, and exchanging information. It has lowered the barriers to entry for new media and entertainment, new forms of retailing and organizing work, and unprecedented digital ventures. Through sensor technology, it has infused intelligence into our wallets, our clothing, our automobiles, our buildings, our cities, and even our biology. It is saturating our environment so completely that soon we will no longer "log on" but rather go about our business and our lives immersed in pervasive technology.

Overall, the Internet has enabled many positive changes—for those with access to it—but it has serious limitations for business and economic activity. *The New Yorker* could rerun Peter Steiner's 1993 cartoon of one dog talking to another without revision: "On the Internet, nobody knows you're a dog." Online, we still can't reliably establish one another's identities or trust one another to transact and exchange money without validation from a third party like a bank or a government. These same intermediaries collect our data and invade our privacy for commercial gain and national security. Even with the Internet, their cost structure excludes some 2.5 billion people from the global financial system. Despite the promise of a peer-to-peer empowered world, the economic and political benefits have proven to be asymmetrical—with power and prosperity channeled to those who already have it, even if they're no longer earning it. Money is making more money than many people do.

Technology doesn't create prosperity any more than it destroys privacy. However, in this digital age, technology is at the heart of just about everything— good and bad. It enables humans to value and to violate one another's rights in profound new ways. The explosion in online communication and commerce is creating more opportunities for cybercrime. Moore's law of the annual doubling of processing power doubles the power of fraudsters and thieves—"Moore's Outlaws"[1]—not to mention spammers, identity thieves, phishers, spies, zombie farmers, hackers, cyberbullies, and datanappers—criminals who unleash ransomware to hold data hostage—the list goes on.

IN SEARCH OF THE TRUST PROTOCOL

As early as 1981, inventors were attempting to solve the Internet's problems of privacy, security, and inclusion with cryptography. No matter how they reengineered the process, there were always leaks because third parties were involved. Paying with credit cards over the Internet was insecure because users had to divulge too much personal data, and the transaction fees were too high for small payments.

In 1993, a brilliant mathematician named David Chaum came up with eCash, a digital payment system that was "a technically perfect product which made it possible to safely and anonymously pay over the Internet. . . . It was perfectly suited to sending electronic pennies, nickels, and dimes over the Internet."[2]It was so perfect that Microsoft and others were interested in including eCash as a feature in their software.[3] The trouble was, online shoppers didn't care about privacy and security online then. Chaum's Dutch company DigiCash went bankrupt in 1998.

Around that time, one of Chaum's associates, Nick Szabo, wrote a short paper entitled "The God Protocol," a twist on Nobel laureate Leon Lederman's phrase "the God particle," referring to the importance of the Higgs boson to modern physics. In his paper, Szabo mused about the creation of a be-all end-all technology protocol, one that designated God the trusted third party in the middle of all transactions: "All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output."[4] His point was powerful: Doing business on the Internet requires a leap of faith. Because the infrastructure lacks the much-needed security, we often have little choice but to treat the middlemen as if they were deities.

A decade later in 2008, the global financial industry crashed. Perhaps propitiously, a pseudonymous person or persons named Satoshi Nakamoto outlined a new protocol for a peer-to-peer electronic cash system using a cryptocurrency called bitcoin. Cryptocurrencies (digital currencies) are different from traditional fiat currencies because they are not created or controlled by countries. This protocol established a set of rules—in the form of distributed computations—that ensured the *integrity* of the data exchanged among these billions of devices *without going through a trusted third party.* This seemingly subtle act set off a spark that has excited, terrified, or otherwise captured the imagination of the computing world and has spread like wildfire to businesses, governments, privacy advocates, social development activists, media theorists, and journalists, to name a few, everywhere.

"They're like, 'Oh my god, this is it. This is the big breakthrough. This is the thing we've been waiting for,'" said Marc Andreessen, the cocreator of the first commercial Web browser, Netscape, and a big investor in technology ventures. "'He solved all the problems. Whoever he is should get the Nobel Prize—he's a genius.' This is the thing! This is the distributed trust network that the Internet always needed and never had."[5]

Today thoughtful people everywhere are trying to understand the implications of a protocol that enables mere mortals to manufacture trust through clever code. This has never happened before—trusted transactions directly between two or more parties, authenticated by mass collaboration and powered by collective self-interests, rather than by large corporations motivated by profit.

It may not be the Almighty, but a trustworthy global platform for our transactions is something very big. We're calling it the Trust Protocol. This protocol is the foundation of a growing number of global distributed ledgers called blockchains—of which the bitcoin blockchain is the largest. While the technology is complicated and the word *blockchain* isn't exactly sonorous, the main idea is simple. Blockchains enable us to send money directly and safely from me to you, without going through a bank, a credit card company, or PayPal. Rather than the Internet of Information, it's the Internet of Value or of Money. It's also a platform for everyone to know what is true—at least with regard to structured recorded information. At its most basic, it is an open source code: anyone can download it for free, run it, and use it to develop new tools for managing transactions online. As such, it holds the potential for unleashing countless new applications and as yet unrealized capabilities that have the potential to transform many things.

HOW THIS WORLDWIDE LEDGER WORKS

Big banks and some governments are implementing blockchains as distributed ledgers to revolutionize the way information is stored and transactions occur. Their goals are laudable—speed, lower cost, security, fewer errors, and the elimination of central points of attack and failure. These models don't necessarily involve a cryptocurrency for payments.

However, the most important and far-reaching blockchains are based on Satoshi's bitcoin model. Here's how they work.

Bitcoin or other digital currency isn't saved in a file somewhere; it's represented by transactions recorded in a blockchain—kind of like a global spreadsheet or ledger, which leverages the resources of a large peer-to-peer bitcoin network to verify and approve each bitcoin transaction. Each blockchain, like the one that uses bitcoin, is *distributed*: it runs on computers provided by volunteers around the world; there is no central database to hack. The blockchain is *public*: anyone can view it at any time because it resides on the network, not within a single institution charged with auditing transactions and keeping records. And the blockchain is *encrypted*: it uses heavy-duty encryption involving public and private keys (rather like the two-key system to access a safety deposit box) to maintain virtual security. You needn't worry about the weak firewalls of Target or Home Depot or a thieving staffer of Morgan Stanley or the U.S. federal government.

Every ten minutes, like the heartbeat of the bitcoin network, all the transactions conducted are verified, cleared, and stored in a block which is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently time-stamps and stores exchanges of value, preventing anyone from altering the ledger. If you wanted to steal a bitcoin, you'd have to rewrite the coin's entire history on the blockchain in broad daylight. That's practically impossible. So the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the World Wide Web of information, it's the World

Wide Ledger of value—a distributed ledger that everyone can download and run on their personal computer.

Some scholars have argued that the invention of double-entry bookkeeping enabled the rise of capitalism and the nation-state. This new digital ledger of economic transactions can be programmed to record virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, provenance of food, and anything else that can be expressed in code.

The new platform enables a reconciliation of digital records regarding just about everything in real time. In fact, soon billions of smart things in the physical world will be sensing, responding, communicating, buying their own electricity and sharing important data, doing everything from protecting our environment to managing our health. This Internet of Everything needs a Ledger of Everything. Business, commerce, and the economy need a Digital Reckoning.

So why should you care? We believe the truth *can* set us free and distributed trust will profoundly affect people in all walks of life. Maybe you're a music lover who wants artists to make a living off their art. Or a consumer who wants to know where that hamburger meat really came from. Perhaps you're an immigrant who's sick of paying big fees to send money home to loved ones in your ancestral land. Or a Saudi woman who wants to publish her own fashion magazine. Maybe you're an aid worker who needs to identify land titles of landowners so you can rebuild their homes after an earthquake. Or a citizen fed up with the lack of transparency and accountability of political leaders. Or a user of social media who values your privacy and thinks all the data you generate might be worth something—to you. Even as we write, innovators are building blockchain-based applications that serve these ends. And they are just the beginning.

A RATIONAL EXUBERANCE FOR THE BLOCKCHAIN

For sure, blockchain technology has profound implications for many institutions. Which helps explain all the excitement from many smart and influential people. Ben Lawsky quit his job as the superintendent of financial services for New York State to build an advisory company in this space. He told us, "In five to ten years, the financial system may be unrecognizable . . . and I want to be part of the change."[6] Blythe Masters, formerly chief financial officer and head of Global Commodities at JP Morgan's investment bank, launched a blockchain-focused technology start-up to transform the industry. The cover of the October 2015 *Bloomberg Markets* featured Masters with the headline "It's All About the Blockchain." Likewise, *The Economist* ran an October 2015 cover story, "The Trust Machine," which argued that "the technology behind bitcoin could change how the economy works."[7] To *The Economist*, blockchain technology is "the great chain of being sure about things." Banks everywhere are scrambling top level teams to investigate opportunities, some of these with dozens of crackerjack technologists. Bankers love the idea of secure, frictionless, and instant transactions, but some flinch at the idea of openness, decentralization, and new forms of currency. The financial services industry has already rebranded and privatized blockchain technology, referring to it as *distributed ledger technology,* in an attempt to reconcile the best of bitcoin—security, speed, and cost—with an entirely closed system that requires a bank or financial institution's permission to use. To them, blockchains are more reliable databases than what they already have, databases that enable key stakeholders—buyers, sellers, custodians, and regulators—to keep shared, indelible records, thereby reducing cost, mitigating settlement risk, and eliminating central points of failure.

Investing in blockchain start-ups is taking off, as did investing in dot-coms in the 1990s. Venture capitalists are showing enthusiasm at a level that would make a 1990s dot-com investor blush. In 2014 and 2015 alone, more than $1 billion of venture capital flooded into the emerging blockchain ecosystem, and the rate of investment is almost doubling annually.[8] "We're quite confident," said Marc Andreessen in an interview with *The Washington Post,* "that when we're sitting here in 20 years, we'll be talking about [blockchain technology] the way we talk about the Internet today."[9]

Regulators have also snapped to attention, establishing task forces to explore what kind of legislation, if any, makes sense. Authoritarian governments like Russia's have banned or severely limited the use of bitcoin, as have democratic states that should know better, like Argentina, given its history of currency crises. More thoughtful governments in the West are investing considerably in understanding how the new technology could transform not only central banking and the nature of money, but also government operations and the nature of democracy. Carolyn Wilkins, the senior deputy governor of the Bank of Canada, believes it's time for central banks everywhere to seriously study the implications of moving entire national currency systems to digital money. The Bank of England's top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom.[10]

These are heady times. To be sure, the growing throng of enthusiasts has its share of opportunists, speculators, and criminals. The first tale most people hear about digital currencies is the bankruptcy of the Mt. Gox exchange or the conviction of Ross William Ulbricht, founder of the Silk Road darknet market seized by the Federal Bureau of Investigation for trafficking illegal drugs, child pornography, and weapons using the bitcoin blockchain as a payment system. Bitcoin's price has fluctuated drastically, and the ownership of bitcoins is still concentrated. A 2013 study showed that 937 people owned half of all bitcoin, although that is changing today.[11]

How do we get from porn and Ponzi schemes to prosperity? To begin, it's not bitcoin, the still speculative asset, that should interest you, unless you're a trader. This book is about something bigger than the asset. It's about the power and potential of the underlying technological platform.

This is not to say that bitcoin or cryptocurrencies per se are unimportant, as some people have suggested as they scramble to disassociate their projects from the scandalous ventures of the past. These currencies are critical to the blockchain revolution, which is first and foremost about the peer-to-peer exchange of value, especially money.

ACHIEVING TRUST IN THE DIGITAL AGE

Trust in business is the expectation that the other party will behave according to the four principles of integrity: honesty, consideration, accountability, and transparency.[12]

Honesty is not just an ethical issue; it has become an economic one. To establish trusting relationships with employees, partners, customers, shareholders, and the public, organizations must be truthful, accurate, and complete in communications. No lying through omission, no obfuscation through complexity.

Consideration in business often means a fair exchange of benefits or detriments that parties will operate in good faith. But trust requires a genuine respect for the interests, desires, or feelings of others, and that parties can operate with goodwill toward one another.

Accountability means making clear commitments to stakeholders and abiding by them. Individuals and institutions alike must demonstrate that they have honored their commitments and owned their broken promises, preferably with the verification of the stakeholders themselves or independent outside experts. No passing the buck, no playing the blame game.

Transparency means operating out in the open, in the light of day. “What are they hiding?” is a sign of poor transparency that leads to distrust. Of course, companies have legitimate rights to trade secrets and other kinds of proprietary information. But when it comes to pertinent information for customers, shareholders, employees, and other stakeholders, active openness is central to earning trust. Rather than dressing for success, corporations can undress for success.

Trust in business and other institutions is mostly at an all-time low. The public relations company Edelman’s 2015 “Trust Barometer” indicates that trust in institutions, especially corporations, has fallen back to levels from the dismally low period of the 2008 great recession. Edelman noted that even the once impregnable technology industry, still the most trusted business sector, saw declines in the majority of countries for the first time. Globally, CEOs and government officials continue to be the least credible information sources, lagging far behind academic or industry experts.[13] Similarly, Gallup reported in its 2015 survey of American confidence in institutions that “business” ranked second lowest among the fifteen institutions measured; fewer than 20 percent of respondents indicated they had considerable or high levels of trust. Only the U.S. Congress had a lower score.[14]

In the preblockchain world, trust in transactions derived from individuals, intermediaries, or other organizations acting with integrity. Because we often can’t know our counterparties, let alone whether they have integrity, we’ve come to rely on third parties not only to vouch for strangers, but also to maintain transaction records and perform the business logic and transaction logic that powers commerce online. These powerful intermediaries—banks, governments, PayPal, Visa, Uber, Apple, Google, and other digital conglomerates—harvest much of the value.

In the emerging blockchain world, trust derives from the network and even from objects on the network. Carlos Moreira of the cryptographic security company WISeKey said that the new technologies effectively delegate trust— even to physical things. “If an object, whether it be a sensor on a communications tower, a light bulb, or a heart monitor, is not trusted to perform well or pay for services it will be rejected by the other objects automatically."[15] The ledger itself is the foundation of trust.[16]

To be clear, "trust" refers to buying and selling goods and services and to the integrity and protection of information, not trust in all business affairs. However, you will read throughout this book how a global ledger of truthful information can help build integrity into all our institutions and create a more secure and trustworthy world. In our view, companies that conduct some or all of their transactions on the blockchain will enjoy a trust bump in share price. Shareholders and citizens will come to expect all publicly traded firms and taxpayer-funded organizations to run their treasuries, at minimum, on the blockchain. Because of increased transparency, investors will be able to see whether a CEO really deserved that fat bonus. Smart contracts enabled by blockchains will require counterparties to abide by their commitments and voters will be able to see whether their representatives are being honest or acting with fiscal integrity.

RETURN OF THE INTERNET

The first era of the Internet started with the energy and spirit of a young Luke Skywalker—with the belief that any kid from a harsh desert planet could bring down an evil empire and start a new civilization by launching a dot-com. Naïve to be sure, but many people, present company included, hoped the Internet, as embodied in the World Wide Web, would disrupt the industrial world where power was gripped by the few and power structures were hard to climb and harder to topple. Unlike the old media that were centralized and controlled by powerful forces, and where the users were inert, the new media were distributed and neutral, and everyone was an active participant rather than a passive recipient. Low cost and massive peer-to-peer communication on the Internet would help undermine traditional hierarchies and help with the inclusion of developing world citizens in the global economy. Value and reputation would derive from quality of contribution, not status. If you were smart and hardworking in India, your merit would bring you reputation. The world would be flatter, more meritocratic, more flexible, and more fluid. Most important, technology would contribute to prosperity for everyone, not just wealth for the few.

Some of this has come to pass. There have been mass collaborations like Wikipedia, Linux, and Galaxy Zoo. Outsourcing and networked business models have enabled people in the developing world to participate in the global economy better. Today two billion people collaborate as peers socially. We all have access to information in unprecedented ways.

However, the Empire struck back. It has become clear that concentrated powers in business and government have bent the original democratic architecture of the Internet to their will.

Huge institutions now control and own this new means of production and social interaction—its underlying infrastructure; massive and growing treasure troves of data; the algorithms that increasingly govern business and daily life; the world of apps; and extraordinary emerging capabilities, machine learning, and autonomous vehicles. From Silicon Valley and Wall Street to Shanghai and Seoul, this new aristocracy uses its insider advantage to exploit the most extraordinary technology ever devised to empower people as economic actors, to build spectacular fortunes and strengthen its power and influence over economies and societies.

Many of the dark side concerns raised by early digital pioneers have pretty much materialized.[17] We have growth in gross domestic product but not commensurate job growth in most developed countries. We have growing wealth creation and growing social inequality. Powerful technology companies have shifted much activity from the open, distributed, egalitarian, and empowering Web to closed online walled gardens or proprietary, read-only applications that among other things kill the conversation. Corporate forces have captured many of these wonderful peer-to-peer, democratic, and open technologies and are using them to extract an inordinate share of value.

The upshot is that, if anything, economic power has gotten spikier, more concentrated, and more entrenched. Rather than data being more widely and democratically distributed, it is being hoarded and exploited by fewer entities that often use it to control more and acquire more power. If you accumulate data and the power that comes with it, you can further fortify your position by producing proprietary knowledge. This privilege trumps merit, regardless of its origin.

Further, powerful "digital conglomerates" such as Amazon, Google, Apple, and Facebook—all Internet start-ups at one time—are capturing the treasure troves of data that citizens and institutions generate often in private data silos rather than on the Web. While they create great value for consumers, one upshot