

Praise for *Cryptoassets* and Chris Burniske and Jack Tatar

Anyone with a practical or theoretical interest in financial markets should know about cryptoassets. Burniske and Tatar do an excellent job explaining this brave new world to us.

—HARRY MAX MARKOWITZ, winner of the Nobel Prize in Economics and founder of Modern Portfolio Theory

*Cryptoassets* is an outstanding overview of the state of digital currencies and assets. Highly recommended for those who want to understand where finance is going.

—BALAJI S. SRINIVASAN, CEO of 21.co

and board partner at Andreessen Horowitz

Burniske and Tatar have delivered a seminal guide to what may be the big- gest investment opportunity since the Internet. Informative and actionable, *Cryptoassets* is a must-read for crypto-enthusiasts and capital market investors alike.

—ARTHUR B. LAFFER, chairman of Laffer Associates, member of President Reagan’s Economic Policy Advisory Board, and creator of the Laffer Curve

As we hurtle into a new, decentralized economy, Burniske and Tatar have laid down something of immense importance: a coherent logic, a new science even, for investing in the assets that will define that coming world.

—MICHAEL J. CASEY, senior advisor to the Digital Currency Initiative at MIT Media Lab and coauthor of *The Age of Cryptocurrency*

In this sweeping and lucid work, Burniske and Tatar make a compelling case that cryptoassets are foundational to the second generation of the Internet and represent a once-in-a-generation opportunity for the innovative inves- tor. Required reading for anyone wanting to understand the future of finance, business, and more.

—ALEX TAPSCOTT, CEO of NextBlock Global and coauthor of *Blockchain Revolution*

Poised to be one of the most profound inventions in history, blockchain technol- ogy may change everything—just as the wheel and the Internet did. Chris and Jack will help you understand blockchains and the cryptoassets within them. If you’re a fi ancial advisor, this book will help you serve your clients better.

—RIC EDELMAN, three-time #1 Independent Financial Advisor (*Barron’s*) and *New York Times* bestselling author of

*The Truth About Your Future*

Investors are always seeking new assets to diversify their portfolios, and the emergence of cryptoassets provides such an opportunity. Burniske and Tatar offer the first detailed analysis of cryptoassets from the perspective of a port- folio investment.

—CAMPBELL R. HARVEY, former president of the American Finance Association and professor of finance at the Fuqua School of Business at Duke University

*Cryptoassets* is the definitive guide that comes just in time to introduce you to a radically new era of innovative investment. This book tells you all you need to know to invest in this supreme opportunity of our time: replacing the porous top-down “winner-take-all” Internet with a safe and cornucopian cadastre of trust and opportunity that makes us all potential winners.

—GEORGE GILDER, cofounder of the Discovery Institute and author of *Th Scandal of Money*

The growth and importance of cryptocurrency and cryptocomputing rivals the early growth of the commercial Internet and web, and the technical and economic revolution that will result is perhaps even more significant than the first phase of the Internet. *Cryptoassets* is an excellent introduction to this breakthrough in technology and finance, and a tremendous resource for those eager to get their heads around what can be a daunting and complex subject.

—JEREMY ALLAIRE, CEO and founder of Circle

This is an extremely well-researched and timely “state of the nation” treatise on cryptoassets. I’m excited that the knowledge base of our industry is continuing to expand with such high-quality thought leadership and insights.

—VINNY LINGHAM, cofounder and CEO of [Civic.com,](http://Civic.com/)

Shark on *Shark Tank South Africa*, and board member of the Bitcoin Foundation

Since Bitcoin’s creation, people have been wondering why it and other crypto- assets have any value. Chris Burniske and Jack Tatar give the most compelling case for why, with sharp, detailed analysis that reflects their deep understand- ing of the technology and their strong finance background. Beginners as well as more seasoned crypto investors will find new insights and sensible tips in this practical guide.

—LAURA SHIN, senior editor at *Forbes* and host of *Unchained*

*Cryptoassets* is a fascinating introduction to this new space of the digital econ- omy. The authors surface many historical examples to remind us that in times of excitement, it is even more important to pay attention to the teams and tal- ent behind each project.

—CHRISTIAN CATALINI, Theodore T. Miller Career Development Professor at MIT and assistant professor of technological innovation, entrepreneurship, and strategic management at the Sloan School of Management at MIT

*Cryptoassets* is a must-read for all financial services executives and investors who want to understand the fundamentals and future directions of this bur- geoning new asset class. Delivered by two of the foremost authorities in the nascent, multibillion-dollar space, this is the most extensive guide on crypto- assets currently available.

—SANDRA RO, former head of digitization at CME Group

As renowned industry thought leaders, it’s no surprise that Chris and Jack have delivered what is likely the most thoughtful and in-depth framework for evaluating cryptoassets. Within this book, they’ve rolled up their sleeves to provide helpful historical context and a valuation framework that readers will find intellectually stimulating and illuminating for understanding this rapidly emerging world of cryptoassets.

—SPENCER BOGART, managing director and head of research at Blockchain Capital

Chris is at the forefront of the important work to better understand and ana- lyze this emerging class of assets. In this book, he and Jack have encapsulated years of their thinking in an easy-to-digest manner.

—DAVID KINITSKY, VP of research and innovation at Fidelity Labs

For the uninitiated, the world of cryptocurrencies is fraught with risks and pit- falls. No one should venture into this world without preparation. *Cryptoassets* explains, in simple to understand terms, the full paradigm of Bitcoin and its successor currencies, and it provides everything needed to explore this excit- ing world.

—JOHN MCAFEE, founder of McAfee Associates

A thorough, balanced, and easy read. I would recommend this to anyone who considers building a portfolio of cryptoassets.

—RYAN SELKIS, former director of investments at Digital Currency Group and managing director of CoinDesk

Serious investment professionals should read *Cryptoassets* if they want to understand and value the first new asset class of the twenty-first century. Chris and Jack explain this new-age investment opportunity comprehensively, art- fully, and masterfully.

—CATHERINE WOOD, founder and CIO of ARK Investment Management

A rare combination of quantitative analysis and first principles-based think- ing—this is insightful, original content.

—ADAM WHITE, vice president of Coinbase and general manager of GDAX

In an increasingly digital world, it is only a matter of time until enormous amounts of value are transmitted and secured via blockchains, including the value of music and creative works. *Cryptoassets* makes blockchains accessible to the nontechnical by exploring their varied origin stories, use cases, and fun- damental value. If you’re looking for a grounded, first-principles approach to the next wave of Internet innovation, then this is a great book to read.

—JESSE WALDEN, founder of Mediachain Labs and blockchain lead at Spotify

Chris and Jack show us the future of cryptoassets today. Their outlook is pointed and perceptive. A must-read to understand the next era in wealth and value creation.

—WILLIAM MOUGAYAR, general partner at Virtual Capital Ventures and author of *Th Business Blockchain*

Young, Stanford-trained blockchain analyst and investor Chris Burniske has teamed up with financial planning expert and author Jack Tatar to provide the first comprehensive guide to understanding the fastest growing, most exciting asset class under the sun. While many investors are still waking up to the opportunity, these assets have already provided outsized returns, as the overall market is now hovering around $100 billion, which is 10x from a year ago and 100x from four years ago. Collectively referring to these investments as “cryptoassets,” Burniske and Tatar provide a solid background on how the technology arose, what problems it solves, and how, like the Internet itself, it’s going to have a dramatic impact on not only the venture capital process but on investing itself. Don’t think of rebalancing your portfolio without reading this book.

—MICHAEL TERPIN, founder of Transform Group, organizer of CoinAgenda, and cofounder of BitAngels

While the cryptoasset space has witnessed exponential growth, to achieve its full potential, it has to be broadly integrated into the real world. With consis- tent objectivity and clarity, Chris and Jack’s book details cryptoassets as an asset class, and will prove influential in driving institutional investor adoption of this groundbreaking opportunity.

—JENNIFER ZHU SCOTT, founding partner of Radian Partners and member of the Future of Blockchain Council of the World Economic Forum

*Cryptoassets* provides a great introduction to and overview of the young yet rapidly growing universe of all things blockchain. This industry, asset class, and overall idea will make you ponder why abstract concepts like money, identity, and business function like they do in the world today, and how the innovation we’re seeing will completely reshape the economy of tomorrow. From setting the stage to diving into specific protocols and projects to sharing practical knowledge on how to invest in these emerging assets, Chris and Jack’s combination of expertise and familiarity with the complex topics at hand are testament to why I have considered them some of the best resources through- out my journey of falling deeper and deeper down the crypto rabbit hole.

—ALEX SUNNARBORG, research analyst at CoinDesk and cofounder of Lawnmower.io

From inception to the latest phase, *Cryptoassets* explores the past, present, and future of this new asset class. It’s not a hard read yet delves into much of the detail needed for a complete understanding of the benefits, and risks, of bit- coin, blockchain, and more. Chris and Jack have written a book I highly rec- ommend to investors in this burgeoning field!

—PAT BOLLAND, former business editor at CNBC, CBC, BNN

*Cryptoassets* is the bible for all things crypto. Whether you’re a beginner or expert, you will walk away with a deeper understanding of the entire ecosystem after reading this book.

—GREG ROSEN, principal at BoxGroup

Chris and Jack provide a holistic view of the origin, evolution, and analysis of cryptoassets. It goes through their very short but intense history, talks about methods for analyzing their value, and identifies the ones with potential. I’d recommend it to anyone who wants to dive into investing and understanding how cryptoassets will shape the future of society and the creation of value.

—LUIS CUENDE, cofounder of Aragon and Stampery

Those of us who work in the blockchain industry have long realized that the rise of cryptocurrencies as a legitimate asset class was inevitable. But most traditional investors have been slow on the uptick. Chris was the first buy- side analyst to focus exclusively on this emerging asset class, and Jack was one of the earliest financial journalists to stress its importance. For years, Chris has been working hard to bring Wall Street’s rigorous analytical methodolo- gies to cryptocurrencies, while Jack has been busy explaining the benefits of cryptocurrencies to audiences around the world. Now, with *Cryptoassets*, they describe, as nobody has before, why every investor should incorporate bitcoin, ether, and new blockchain-based assets into their portfolios, and how to ana- lyze these tokens in order to make the right investments.

—TRAVIS SCHER, investment associate at Digital Currency Group

Chris and Jack have written our generation’s *A Random Walk Down Wall Street*. This book is required reading for anyone looking to get involved with and profit from the cryptoassets boom.

—PATRICK ARCHAMBEAU, VP of engineering at CoinDesk and cofounder of Lawnmower.io

Chris and Jack have been fellow travelers in the blockchain space since way before it was a polite cocktail party topic. Over the years, we’ve laughed and marveled together at how the space has evolved. This book could not be more timely in describing an emerging $100+ billion financial market and all of the chaos and promise it brings. The authors capture not only the technical and market analysis you need to know to invest in these projects but also the ethos and excitement of the people pushing the envelope. Savor this book. It’s a time- capsule view of the birth of an amazing technology.

—PETER KIRBY, cofounder and CEO of Factom, Inc.

Burniske and Tatar thread the needle between an approachable guide for new- comers and thought-provoking insights for seasoned investors. I will surely be assigning it to my graduate students as we cover cryptoassets.

—STEPHEN MCKEON, associate professor of finance at the Lundquist College of Business at the University of Oregon

Token-based fund-raising is here to stay, and this book offers the best way to value cryptoassets that I’ve seen. The book provides background and the potential impacts of ICOs, offering insightful knowledge to both those enter- ing the space and experienced investors like myself. I would recommend this book for any crypto reading arsenal!

—PAUL VERADITTAKIT, partner at Pantera Capital

Burniske and Tatar have now given me an easy response when people ask how to get started with cryptoassets—this book!

—ARI PAUL, CIO of BlockTower Capital

This is a seminal work in the evolution of the cryptosphere as digital money moves mainstream. The book covers the full potential and array of what this technology offers in piercing the veil to an Internet of value with all the new innovations and crossovers from the traditional realm of finance. Chris and Jack have brought a wealth of knowledge and cross-disciplinary methods to bear from their respective fields and broken new ground in their analysis of this exciting new space.

—CHARLIE HAYTER, cofounder and CEO of CryptoCompare

*Cryptoassets* is a tour de force. Burniske and Tatar are able to leverage their deep industry experience to condense a complex, continually evolving topic into a concise and informative guide for investors looking to be on the cutting edge of a new asset class. *Cryptoassets* will serve as the entry point to the space for retail investors for years to come.

—PIETER GORSIRA, software engineer at CoinDesk and cofounder of Lawnmower.io

In a world where issuing digital assets becomes as easy as creating a website, Chris and Jack provide a comprehensive guide that will help you separate the wheat from the chaff.

—DEMIAN BRENER, cofounder and CEO of Zeppelin Solutions

As we enter the next great evolution in global financial markets, Chris Burniske and Jack Tatar have authored a unique and much-needed volume. It offers not only a foundational understanding of cryptoassets and digital currencies but also serves as a reference for evaluating and participating in a cryptoasset future. A new asset class has emerged, and *Cryptoassets* is the definitive guide.

—RON QUARANTA, chairman of the Wall Street Blockchain Alliance

This book is very accessible, comprehensive, and easy to read for any size investor. One of its strengths is its ability to be valuable to the novice and the experienced professional alike.

—JARED HARWAYNE-GIDANSKY, founding board member of the Blockchain Association of Australia

Chris and Jack have created a book that not only explains the world of crypto- assets but provides a framework for how to invest in it and become part of what may be the greatest investment opportunity since the Internet.

—NED SCOTT, founder and CEO of Steemit

*Cryptoassets* is an intelligent and well-organized introduction to the world of cryptoassets. The book adapts classic finance pricing models to the challeng- ing task of valuing cryptoassets, offering the reader a solid head start to invest- ing in this new exciting asset class.

—ALESSIO SARETTO, assistant professor of finance at the University of Texas at Dallas

If you want to know how cryptoassets work, get *Mastering Bitcoin* by Andreas Antonopoulos, but if you want to know how and why you should be investing in this new asset class, get yourself a copy of *Cryptoassets*.

—TRON BLACK, investor and principal developer at Medici Ventures

Newcomers often try to wiggle their way into the world of accepted fi ancial tools. Most fail miserably. But cryptocurrency and its accompanying blockchain technology have made their mark and will likely have an ongoing impact on how we all do business. Burniske and Tatar have written an incredibly compre- hensive book that explains what you need to know about this new asset class.

—DOUGLAS GOLDSTEIN, CFP, author of *Rich as a King*

By explaining the various crypto investments, from coins to tokens to commodi- ties, and providing the tools to perform investment analysis, *Cryptoassets* is the best crypto investment novices, professionals, and business leaders can make.

—RON KOCHMAN, former president and CEO of

Volt Information Sciences and cryptoasset angel investor

*Cryptoassets* provides a one-stop shop for learning about this new asset class. You’ll learn about their colorful histories, how to apply fundamental valuation techniques, and practical tips to navigate the at-times turbulent markets.

—MATTHEW GOETZ, CEO of BlockTower Capital

With investing, people always want to know about the next big thing. For curi- ous minds who want to know about emerging technologies or even those who already have an understanding of blockchains, Chris and Jack leave no stone unturned. From the origins, to an explanation of how it works, to what’s next, the reader will leave excited about the possibilities of investing money and time in this exciting adventure.

—TOM SZAKY, founder and CEO of TerraCycle

This book is a must-read for any financial advisor who wants to stay on top of the shifting asset and technological landscape. Advisors would be wise to familiarize themselves with cryptoassets before their innovative clients approach them for an intelligent cryptoasset discussion!

—FRED PYE, president and CEO of 3iQ Corp.

What will a technology that validates the order of entries in an electronic led- ger without a centralized administrator bring? Time will tell. If you can’t wait until then, read Chris and Jack’s book. It will give you a great start.



—FRANCOIS GADENNE, chairman and executive director of the Retirement Income Industry Association

The most complete and informational piece of literature on the subject today. Chris Burniske and Jack Tatar steer the reader through a torrent of unknowns, illuminating the complicated world of cryptoassets and their underlying tech- nology, which will more than likely become our generation’s most important innovation.

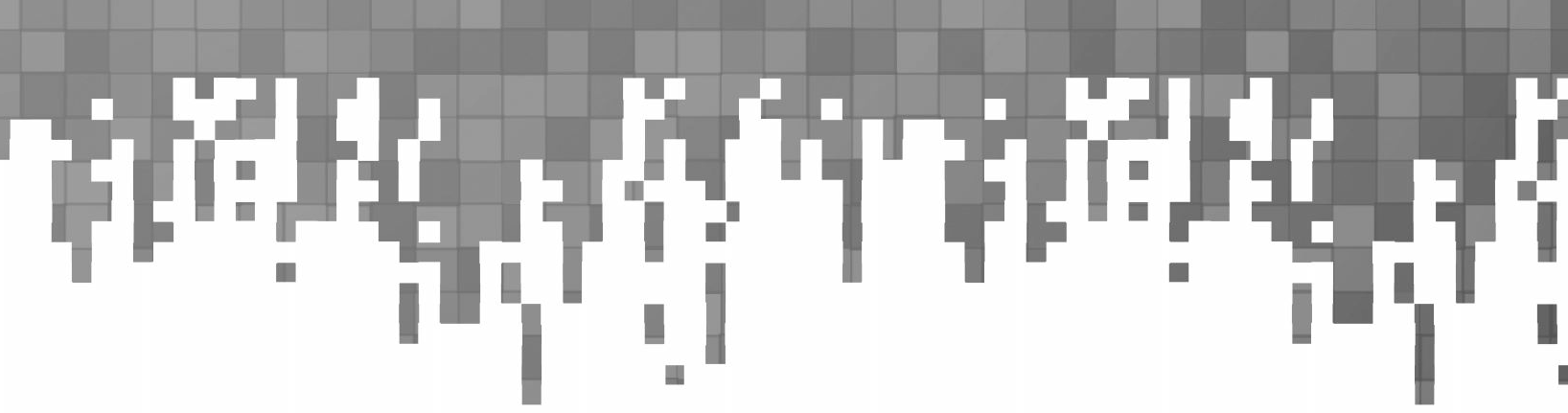
—RYAN LANCELOT, coauthor of *What’s the Deal with Bitcoins?*

A must-read to appreciate the Bitcoin network effect and the wave of innova- tion that it launched through the community of people who played critical roles in creating all the distributed ecosystems that are transforming business models.

—CRISTINA DOLAN, cofounder and COO of InsureX

Crypto trading and the FinTech innovations unlocked by blockchains will do to Wall Street what personal Internet publishing and blogging did to media empires. Th s power shift is inevitable. Capital allocation no longer needs to be managed by powerful institutions which have proven to be corrupt and reck- less. Regulation and regulatory capture is putting the U.S. at risk of losing out in the transition. Chris Burniske and Jack Tatar give you, the individual, the tools to evaluate these new cryptoassets and take advantage of what I believe will be the greatest rebalancing of wealth and power that the world has ever seen.

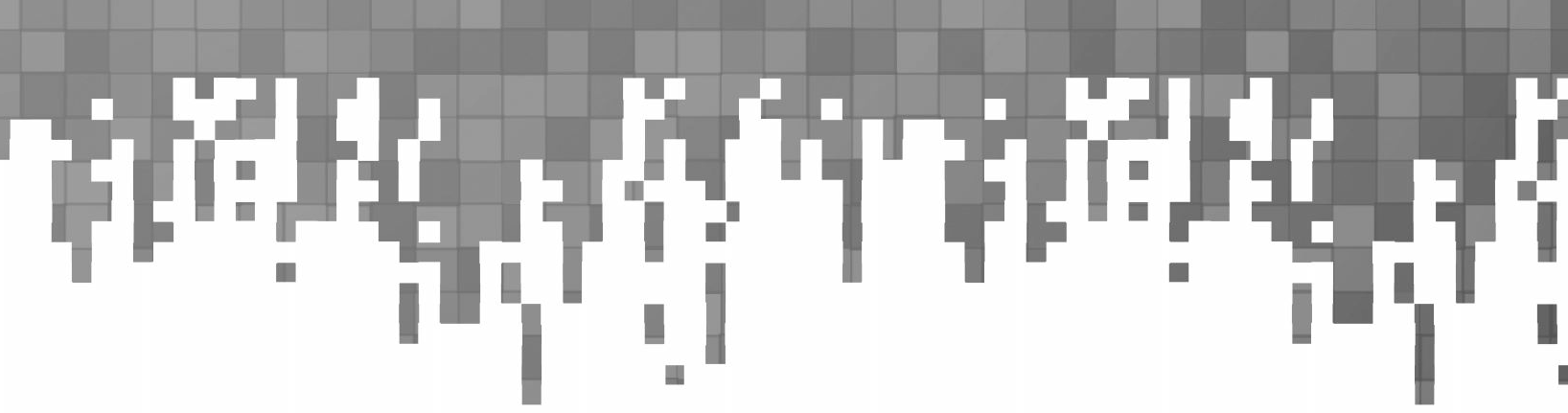
— DR. PATRICK BYRNE, CEO of [Overstock.com](http://Overstock.com/)



# CRYPTOASSETS



*This page intentionally left blank*



**CRYPTOASSETS**

The Innovative Investor’s Guide to Bitcoin and Beyond

CHRIS BURNISKE & JACK TATAR

New York Chicago San Francisco Athens London Madrid Mexico City Milan New Delhi Singapore Sydney Toronto

Copyright © 2018 by Chris Burniske and Jack Tatar. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN: 978-1-26-002668-9 MHID: 1-26-002668-X

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-002667-2, MHID: 1-26-002667-1.

eBook conversion by codeMantra Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at [www.mhprofessional.com.](http://www.mhprofessional.com/)

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that neither the author nor the publisher is engaged in rendering legal, accounting, securities trading, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

*— From a Declaration of Principles Jointly Adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations*

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, dis- seminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education’s prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED “AS IS.” McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUD- ING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPER- LINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANT-

ABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licen- sors do not warrant or guarantee that the functions contained in the work will meet your require- ments or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no respon- sibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

*To Dad, who taught me how to write, and to Mom, who made me believe I could*

—CB

*To Eric and Grace, you are the future*

—JT

*This page intentionally left blank*

**Contents**

[Authors’ Note xi](#_bookmark0)

[Foreword by Brian Kelly xiii](#_bookmark1)

[Acknowledgments xvii](#_bookmark2)

[Introduction xxi](#_bookmark3)

[Part I WHAT](#_bookmark4)

[Chapter 1](#_bookmark5)

[Bitcoin and the Financial Crisis of 2008 3](#_bookmark5)

[Chapter 2](#_bookmark6)

[The Basics of Bitcoin and Blockchain Technology 11](#_bookmark6)

[Chapter 3](#_bookmark7)

[“Blockchain, Not Bitcoin?” 21](#_bookmark7)

[Chapter 4](#_bookmark8)

[The Taxonomy of Cryptoassets 31](#_bookmark8)

[Chapter 5](#_bookmark9)

[Cryptocommodities and Cryptotokens 51](#_bookmark9)

vii

viii CONTENTS

**Part II WHY**

**Chapter 6**

###### The Importance of Portfolio Management and Alternative Assets 69

**Chapter 7**

###### The Most Compelling Alternative Asset

**of the Twenty-First Century 83**

**Chapter 8**

###### Defining Cryptoassets as a New Asset Class 107

**Chapter 9**

###### The Evolution of Cryptoasset Market Behavior 121

**Chapter 10**

###### The Speculation of Crowds and “This Time

**Is Different” Thinking 137**

**Chapter 11**

###### “It’s Just a Ponzi Scheme, Isn’t It?” 155

**Part III HOW**

**Chapter 12**

###### Fundamental Analysis and a Valuation Framework

**for Cryptoassets 171**

**Chapter 13**

###### Operating Health of Cryptoasset Networks

**and Technical Analysis 185**

**Chapter 14**

###### Investing Directly in Cryptoassets:

**Mining, Exchanges, and Wallets 211**

**Chapter 15**

###### “Where’s the Bitcoin ETF?” 231

CONTENTS ix

**Chapter 16**

###### The Wild World of ICOs 247

**Chapter 17**

###### Preparing Current Portfolios for Blockchain Disruption 263

**Chapter 18**

###### The Future of Investing Is Here 279

###### Chris and Jack’s Go-to Crypto Resources 285

**Notes 289**

**Index 309**

*This page intentionally left blank*

## Authors’ Note

hen we started writing this book in December 2016, bitcoin was in the $700s, ether was in the $7s, and the aggregate network value of cryptoassets was just north of $10 billion. Over the ensuing months

W

of writing we watched bitcoin push past $4,000, while ether crossed $400, and the aggregate network value of cryptoassets punched through $100 billion. Cryptoassets went from being esoteric dark web material to mainstream topics of conversation and enthusiasm.

When embarking on our literary journey, we recognized the difficulty in documenting arguably the world’s fastest moving markets. These markets can change as much in a day—up or down—as the stock market changes in a year. Nonetheless, we were continually asked the same question: “What should I read to get the full picture of what’s going on in these markets?” The frequency of this question grew to a clamor as the markets rose through the first half of 2017, and yet information channels remained stubbornly fragmented among Reddit, Twitter, Telegram, Slack, Medium, news sites, and more.

While we recognize the difficulty in covering the *full picture* of the ever- moving cryptoasset markets, we believe that this book provides a comprehen- sive view of the history, technology, and marketplace dynamics of bitcoin and beyond. We have crafted the book to be as evergreen as possible with regard to the background and methodologies laid forth, so that even as the markets change, the book retains its value. We recognize that by the time you read this, some asset prices may seem like the distant past, and some teams may be

xi

xii AUTHORS’ NOTE

indignant that we didn’t cover their story. We couldn’t possibly have covered every price change and every story, or we would never have published the book.

Our hope is to serve as a starting point and means to understanding, so that we can all study and experience this space together. It is a history that is still in its earliest stages of being written.

**Foreword**

hen I first learned about bitcoin, I was convinced it would fail. Based on a few articles and two decades of experience as a skeptical trader,

W

I loudly—and now regrettably—declared on CNBC’s *Fast Money* that bitcoin would not survive. How could it? It was not backed by any entity; it did not have a central bank; it was not accepted for taxes; and it did not have an army to enforce its use. What’s more, it was extremely volatile and had a bad reputation—all of which would contribute surely to its premature demise. I have never been more incorrect in my entire career.

Somewhere in the CNBC archives exists an awkward video of me railing against this “magic Internet money.” If you’re reading this and have access to the video, treat it with the respect it deserves and destroy it! Since those unen- lightened days, I have come to understand that bitcoin—and the blockchain beneath it—is a technological advancement that has the potential to revolu- tionize financial services the same way email did to the post office.

Once I realized that blockchain technology was a disruptive force, I sought out people who shared my view. I met Chris Burniske at the very first Wall Street Blockchain Alliance holiday party, and we immediately found com- mon interest in the potential for blockchain-based assets, or cryptoassets, to become a new asset class for investors. At the time, very few people saw bit- coin’s potential, but Chris did, and it was clear to me that he possessed rare leadership and vision.

xiii

xiv FOREWORD

Jack Tatar is an expert in retirement planning who has spent over two decades in the financial industry and brings a much-needed perspective of finance and investment knowledge to the cryptoasset world. New technology can be confusing and intimidating, but through his engaging writing, Jack possesses the unique ability to distill a complex subject into an easily digestible serving. As a result of their combined perspectives, *Cryptoassets* is a book that will satisfy the most curious minds and engage those approaching the subject for the first time.

Readers will benefit not only from Chris and Jack’s vision but also their deep knowledge of the topic. As the manager of a hedge fund that invests in digital assets, I am constantly researching this asset class’s investment poten- tial, and when I get stumped, my first call is to Chris Burniske. While I am thrilled that Chris is sharing his unique insights in this book, I am selfishly reluctant to lose my secret go-to resource. Layer on Jack’s experience as one of the first financial journalists to write about bitcoin, and you have a powerful combination. Let them be your resource as well.

The beauty of this book is that it takes the reader on a journey from bitcoin’s inception in the ashes of the Great Financial Crisis to its role as a diversifi in a traditional investment portfolio. Those who want to look under the hood of blockchain technology will be thrilled with the skillful description of the elegant architecture that powers this technology, and fi ancial historians, like myself, will fi d the discussion of investment bubbles instructive. Chris and Jack artfully apply fi ancial history lessons to the cryptoasset investment world. Spoiler alert: even though blockchain technology is disrupting traditional fi ancial market structures, fear and greed remain uniquely human traits that can and will fi d a place in cryptoassets. Thankfully, Chris and Jack give readers the tools and knowledge to know what to look out for when bubbles do occur.

Armed with this knowledge, the reader can then use the valuation frame- work laid out in Chapters 12 and 13 to find the most promising cryptoassets. Valuing cryptoassets is done unlike traditional investments; they typically do not have revenue or cash flows and thus present a conundrum for those evaluating their merits. Here, Chris and Jack present groundbreaking work on how to properly value an asset based on the network effect and teams of decentralized developers. Everyone who is even thinking about investing in cryptoassets needs to read these chapters.

One of the most fascinating outcomes of the blockchain revolution is how cryptoassets are disrupting the disruptors. As Chris and Jack explain, the ven- ture capital business model is being turned on its head by crowdfunding efforts

FOREWORD xv

that include initial cryptoasset offerings, or ICOs. Cryptoassets are made of code, and because they easily track and convey ownership, they can be used as fund-raising tools for startups. In the last two years, there has been a wave of entrepreneurs that bypassed venture capitalists and instead chose to raise startup capital via these methods.

As with any new model, there are questions about legality and sustainabil- ity, but the Silicon Valley ethos of “break things first, then ask for forgiveness” has found its way to Wall Street. Professionals who are involved in all aspects of fund-raising—from venture capital to capital markets—will find the dis- cussion of these new methods of raising capital riveting, maybe even a little frightening.

The final chapter of my book *The Bitcoin Big Bang* was titled “Everything You Know About Business Is Wrong,” and it previews what Chris and Jack have identified as a game-changing development in the way capital is raised and distributed. Self-funded, decentralized organizations are a new species in the global economy that are changing everything we know about business. A cryptoasset as the fuel for a decentralized organization not only changes the organizational chart, it also rearranges incentive structures.

These new organizations are altering the way software is developed. Cryptoassets have inverted the value creation structure that worked so well during the development of the Internet. These so-called fat protocols are self- funding development platforms that create and gain value as applications are built on top. This is an entirely new paradigm for open-source projects that incentivizes developers to build socially useful projects.

When I started working on Wall Street, the Internet was something on a computer at the end of the trading desk. Amazon, eBay, and Google did not exist—but within five years, these companies had changed the world. As a greenhorn trader, I was too young and inexperienced to recognize that the Internet was a once-in-a-generation investment opportunity. I was convinced that I would not see another exponential investment opportunity for the rest of my career—until I discovered blockchain technology. Blockchain technol- ogy is one of the most important innovations in the history of finance. It is changing the way we transact, distribute capital, and organize our companies. If you’re like me and missed investing in the Internet, read this book so you can take advantage of the biggest investment opportunity since the Internet.

—BRIAN KELLY, CNBC Contributor and Manager of the BKCM Digital Asset Fund

*This page intentionally left blank*

## Acknowledgments

hanks first and foremost to the best literary partner one could have— the great Karen Lacey. This truly was a three-person production, and we thank you for helping us define, refine, and execute on our vision. Not

T

only did you hone our thinking, but you dove deep down the cryptoasset rab- bit hole too! Anyone looking to work with a gifted and patient literary partner can find Karen a[t www.theuncommonoctopus.co](http://www.theuncommonoctopus.com/)m.

Thanks to our wonderful editor at McGraw-Hill, Casey Ebro, and our liter- ary agent, Marilyn Allen.

Special thanks to all of those in the cryptoasset and financial community who provided ideas, advice, and commentary, especially the awesome trio of Alex Sunnarborg, Patrick Archambeau, and Pieter Gorsira, as well as Charles Bovaird, Balaji Srinivasan, Arthur Laffer, Michael Casey, Alex Tapscott, Ric Edelman, Campbell Harvey, George Gilder, Jeremy Allaire, Vinny Lingham, Laura Shin, Christian Catalini, Sandra Ro, Spencer Bogart, David Kinitsky, John McAfee, Ryan Selkis, Adam White, Jesse Walden, William Mougayer, Michael Terpin, Jennifer Zhu Scott, Pat Bolland, Greg Rosen, Luis Cuende, Travis Scher, Peter Kirby, Stephen McKeon, Paul Veradittakit, Ari Paul, Charlie Hayter, Demian Brener, Ron Quaranta, Jared Harwayne-Gidansky, Ned Scott, Alessio Saretto, Tron Black, Douglas Goldstein, Matthew Goetz, Tom Szaky, Fred Pye, Ryan Lancelot, Cristina Dolan, Ryan Strauss, Jack Hough, and of course to Brian Kelly for his support, friendship, and assistance. We appreci- ate the support of the worldwide cryptoasset community and if we forgot to

xvii

xviii ACKNOWLEDGMENTS

list anyone who was there for us during this journey, please forgive us—it’s because of the crypto-community that this book exists!

—CB and JT

Thanks to Dad, who was a writer himself, and from a young age had me jour- naling, writing summer book reports, and submitting essays to justify the pur- chase of gadgets. He taught me the importance of never having a TV in the house, that all creativity comes at the cost of maintenance, and that excellence should never be compromised.

Thanks to Mom, who has been a fountain of belief and support through the good and the bad. While she may not know much about blockchains (yet), she loves them because I love them. She is the most positive person I know and the one who has taught me how to find silver linings in the clouds. Thanks to my brother, Justin, who resisted the urge to strangle me when Mom was away, and taught me that power doesn’t always have to corrupt.

Thank you to Cathie Wood, who plucked me from a fishmongership and taught me that not all finance is bad. In a few years, Cathie taught me more about economics, the markets, and how the world works than I learned in my time at Stanford. In a world where mentors are increasingly rare, Cathie’s guid- ance has been pivotal in my life. Thank you to Rob Wood, the friendly giant who introduced us.

Thanks to Brett Winton, who has taught me how to approach the most com- plex of problems and that maybe I’m not as dense as I fear. To Joel Monegro, who has been my thematic torchbearer in the world of crypto, thank you. There’s no one I look forward to brainstorming with more than you. Thanks to James Wang, who taught me to love Twitter, and that valuation matters.

Last but not least, thanks to Jack, who has been the driving force behind this book. If not for a fateful lunch at Consensus and Jack’s relentless enthusiasm, this book never would have happened.

—CB

Thanks to the great Harry Markowitz for his advice and insight. One of the wonderful results of this book has been my ability to gain the friendship of this wonderful man. Thanks, Harry! I’m humbled by your assistance.

Special thanks to my bubbie, Stu Sharoff, for taking the dive into this wacky world, his advice on the cover, and for being a brother to me for so many years.

ACKNOWLEDGMENTS xix

Thanks to Stu Rosenberg for also taking the dive and providing such great sup- port and friendship over the years.

Special thanks for my angel investing partner and dear friend, Ron Kochman, for his honest insight into the book and for making this journey so much more entertaining. Also to Steve Katz, who we miss every day.

Thanks to the great John Gioia for his advice and insight throughout the entire process of creating this book. Thanks to Irene Cibas for just being her- self and putting up with John and me for *so* many years. Thanks also to Bill Bonomo, John Barbera, and David Fink for their help and support during the years when I needed it. Of course, thanks to the legendary Sam Kirk for his assistance throughout this process.

To my Mom and Dad, who may not be here physically, but inspire and direct me each and every day.

Most of all, thanks to my family, who put up with me during this process. I couldn’t have done any of it without you. To my children, Eric and Grace, I could never fully articulate how important and valuable your advice and sup- port has been to me. You’re my inspiration for everything.

Finally, to the reason for my being and the love of my life, my Maudee Ann. No one knows better than you what crazy schemes and ideas I’ve had in my life, and you’ve endured them and supported me throughout. I thank God for allowing me the opportunity to live my life with you, and I thank you for, well, everything. I love you more than words can tell . . . always!

And of course, to my terrific coauthor, Chris, who brings intellect, humor, compassion, and honesty to everything he does. The best part of this book was making your friendship.

—JT

*This page intentionally left blank*

## Introduction

ooks, TV shows, and movies have been making futuristic predictions for decades, many of which were originally considered absurd. *Star Trek* featured several that proved to be not so outlandish: the indis-

B

pensable handheld communicators have become today’s smartphones, the personal access display device is now our tablet, and a universal translator exists, of which there are several apps to choose. Edward Bellamy’s enigmati- cally titled 1887 book *Looking Backward* predicted debit and credit cards, and *2001: A Space Odyssey* imagined forms of social media, though nothing on the scale that we currently have. Alvin Toffler’s *Future Shock* gripped readers in the 1970s as it predicted the exponential change destined to shake our society, and issued a warning: “In the three short decades between now and the twenty- first century, millions of ordinary, psychologically normal people will face an abrupt collision with the future.” This future would create “the shattering stress and disorientation that we induce in individuals by subjecting them to too much change in too short a time.”

Exponential change has now become a buzzword, but the power of an expo- nential curve is rarely considered. Each year will entail greater change than the year before. Such a concept differs drastically from a linear rate of change, where the future will change just as quickly as the past did (see Figure I.1.) The two may appear similar in the early days of change, but when the exponential curve starts to inflect it quickly, and at times violently, it distinguishes itself.

xxi

xxii INTRODUCTION

140

Linear (2x)

Exponential (2x)

120

100

80

**Output**

60

40

20

0

1 2 3 4

**Period**

5 6 7

Figure I.1 n Exponential versus linear rates of change

While year 1 exhibits the exact same value for linear and exponential change in Figure I.1, as does year 2, by year 7 an exponential rate has progressed nearly tenfold more than the corresponding seventh period of linear change. We often operate with the rough assumption that the rate of change over the next year or two will be roughly equal to that over the prior years, which is a linear world view. That works for the early stage of change, but not when the exponential curve starts to bend like a hockey stick. Unfortunately, most investment portfo- lios are being managed with a linear world view, with indices that are pegged to the past guiding our future investments. Nothing could be more shortsighted or potentially dangerous in a time of exponential change.

The Internet has irrevocably changed the world, and it continues to do so as developers build on the platform of connection it creates. Thus far, the World Wide Web has been the greatest meta-application to leverage the underlying fiber of the Internet. The indexed web contains at least 4.73 billion pages, near- ing the point where there will be one page for every human.1

The beginning of the Internet is commonly associated with the 1990s, with Tim Berners-Lee stumbling upon the idea of the World Wide Web while trying to create an information management system for CERN, and Marc Andreessen developing the first widely used web browser, which ulti- mately became Netscape. Although the accomplishments of Berners-Lee and Andreessen were linchpins to mainstream adoption, the web and the ability to browse it were the first killer apps built on top of the Internet, not to be conflated with the creation of the Internet itself. We are likely still in the early

INTRODUCTION xxiii

stages of leveraging the potential of the Internet and building meta-applica- tions atop it.

The Internet was fi st conceptualized in the early 1960s to create resilient communication systems that would survive a nuclear attack on the United States. According to one of the Internet’s progenitors, Paul Baran, the key to accom- plishing such resilience was decentralization.2 J. C. R. Licklider proselytized the concept of an “Intergalactic Computer Network,” convincing his colleagues at DARPA—which is responsible for investigating and developing new technolo- gies for the U.S. military—of its importance.3 Leonard Kleinrock, an MIT pro- fessor, was doing work on packet switching—the technology underpinning the Internet—that would lead to the fi st book on the subject: Communication Nets. Ironically, though they were all working on a means to connecting the world, many of the early researchers in this period were unaware of one another.

But their dream has been realized. Every day more than 3.5 billion Google search queries are made,4 18.7 billion text messages are sent (that doesn’t even include WhatsApp and Facebook Messenger, which combine for more than 60 billion messages per day),5 and 269 billion emails are sent.6 Interestingly, how- ever, the Internet has become increasingly centralized over time, potentially endangering its original conception as a “highly survivable system.”

Human ingenuity often surfaces when it’s most needed, and now, a new technology is emerging that returns to the decentralized ethos of the original Internet with the potential to revolutionize our computational and transac- tional infrastructure: blockchain technology. Every second, millions of pack- ets of information are *transacted* between humans and machines using the Internet, and blockchain technology is forcing us to rethink the costs, security, and ownership of these transactions.

Blockchain technology came from Bitcoin. In other words, Bitcoin is the mother of blockchain technology. Bitcoin, with a capital *B*, is a platform that carries upon it programmable money, known as bitcoin with a lowercase

*b*. The technological foundation to this platform is a distributed and digital ledger referred to as a blockchain. In January 2009, when Bitcoin was first released, it embodied the first working implementation of a blockchain the world had seen.

Since then, people have downloaded the open-source software that is Bitcoin, studied its blockchain, and released different blockchains that go far beyond Bitcoin. Blockchain technology can now be thought of as a general purpose technology, on par with that of the steam engine, electricity, and machine learning.

xxiv INTRODUCTION

To quote a May 2016 article in *Harvard Business Review* by Don and Alex Tapscott: “The technology most likely to change the next decade of business is not the social web, big data, the cloud, robotics, or even artificial intelligence. It’s the blockchain, the technology behind digital currencies like bitcoin.”7

Incumbents are sensing the inherent creative destruction, especially within the financial services sector, understanding that winners will grow new mar- kets and feast off the disintermediated. Many startups are eyeing these middle- men with the oft-flickering thought that has been credited to Amazon’s Jeff Bezos: “Your fat margins are my opportunity.”8

If fi ancial incumbents don’t embrace the technology themselves, Bitcoin and blockchain technology could do to banks what cell phones did to tele- phone poles. Nearly every global bank, exchange, custodian, and fi an- cial services provider is part of some blockchain consortium, investing in the potential disruptors or internally building its own team. These players include JP Morgan, Goldman Sachs, Citibank, the New York Stock Exchange, NASDAQ, Banco Santander, Barclays, UBS, South African Reserve Bank, Bank of Tokyo Mitsubishi, Mizuho, China Merchants Bank, Australian Stock Exchange, and more.

Financial incumbents are aware blockchain technology puts on the horizon a world without cash—no need for loose bills, brick-and-mortar banks, or, potentially, centralized monetary policies. Instead, value is handled virtually, through a system that has no central authority figure and is governed in a decentralized and democratic manner. Mathematics force order in the opera- tions. Our life savings, and that of our heirs, could be entirely intangible, float- ing in a soup of secure 1s and 0s, the entire system accessed through comput- ers and smartphones.

Technology providers smell the disruption as well, with Microsoft and IBM most vocally leading the charge. Microsoft provides Blockchain as a Service (BaaS) for developers within its Azure cloud platform. Marley Gray, its direc- tor of technology strategy, has said, “We want, and frankly our customers want, access to every blockchain. It could be two guys in a garage that forked bitcoin and had this genius idea and people want to try that out. We don’t want to have any barriers. We’re open to all. We help even the smallest players onboard.”9

Just as the Internet and World Wide Web changed how we live our lives and interact with others, it also made millionaires out of the innovators who began companies based on these technologies—and the investors who invested in them. Those with the foresight to have bought Google during its “Initial Public

INTRODUCTION xxv

Offering” (IPO) would have seen a 1,800 percent appreciation by August 2016, and those who bought Amazon’s IPO would have seen a 1,827 percent appre- ciation.10

Blockchain architectures and their native assets are well on their way to becoming the next great meta-application to leverage Internet infrastructure. They already provide services that include global currencies, world computers, and decentralized social networks, among hundreds of others.

The native assets historically have been called cryptocurrencies or altcoins, but we prefer the term cryptoassets, which is the term we will use through- out the book. The terms *cryptocurrencies* and *altcoins* convey only a fraction of the innovation that is occurring in the cryptoasset economy. Not all of the 800 existing cryptoassets are currencies. We are not just witnessing the decentral- ized creation of currencies but also of commodities and polished digital goods and services, as blockchains meld technology and the markets to build Web 3.0. It’s early enough in the life of blockchain technology that no books yet have focused solely on public blockchains and their native cryptoassets from the investing perspective. We are changing that because investors need to be aware of the opportunity and armed both to take advantage and protect themselves

in the fray.

Inevitably, innovations of such magnitude, fueled by the mania of mak- ing money, can lead to overly optimistic investors. Investors who early on saw potential in Internet stocks encountered the devastating dot-com bubble. Stock in Books-A-Million saw its price soar by over 1,000 percent in one week simply by announcing it had an updated website. Subsequently, the price crashed and the company has since delisted and gone private. Other Internet-based high fly- ers that ended up crashing include [Pets.com,](http://Pets.com/) Worldcom, and WebVan.11 Today, none of those stocks exist.

Whether specific cryptoassets will survive or go the way of Books-A-Million remains to be seen. What’s clear, however, is that some will be big winners. Altogether, between the assets native to blockchains and the companies that stand to capitalize on this creative destruction, there needs to be a game plan that investors use to analyze and ultimately profit from this new investment theme of cryptoassets. The goal of this book is not to predict the future—it’s changing too fast for all but the lucky to be right—but rather to prepare inves- tors for a variety of futures.

Bitcoin, the most widely known cryptoasset, has been riding a roller coaster. If one had invested $100 in bitcoin in October 2009—the first time an exchange

xxvi INTRODUCTION

rate was established for the nascent digital currency—one would now have over $100 million. In November 2013, if one had invested that same $100 in bitcoin, one would have endured an 86 percent drop by January 2015. There are nearly 800 other stories to tell, considering there are over 800 cryptoassets floating on globally connected and ever-on markets. At the end of 2016, a list of the top 50 included:12

Bitcoin, Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, Dash, MaidSafeCoin, NEM, Augur, Steem, Iconomi, Dogecoin, Factom, Waves, Stellar Lumens, DigixDAO, Zcash, Lisk, Xenixcoin, E-Dinar Coin, Swiscoin, GameCredits, Ardor, BitShares, LoMoCoin, Bytecoin, Emercoin, AntShares, Gulden, Golem, Tether, ShadowCash, Xaurum, Storjcoin, Stratis,

Nxt, Peercoin, I/O Coin, Rubycoin, Bitcrystals, SingularDTV, Counterparty, Agoras Tokens, Siacoin, YbCoin, BitcoinDark, SysCoin, PotCoin, and Global Currency Reserve.

This book will be the first of its kind to dive deep into a number of these. While many have slipped under the mainstream radar, the opportunities they present may be just as great as bitcoin.

We hope to transform today’s intelligent investor into an innovative inves- tor by providing a guide that explains what cryptoassets are, why they should be considered, and how to invest in them. Written by Benjamin Graham, *Th Intelligent Investor* is a seminal work on value investing that Warren Buffet crowned as “the best book about investing ever written.”13 While we can only hope to achieve a fraction of the success Graham had in educating investors, our goals are very similar. We have chosen to focus on an asset class that didn’t exist in Graham’s day, and one that serves as a nice hedge against the exponen- tial change that increasingly will disrupt existing portfolios over time.

One of the keys to Graham’s book was always reminding the investor to focus on the inherent value of an investment without getting caught in the irrational behavior of the markets. Just as he aimed to arm the intelligent investor with the tools to make an investment decision based on fundamental analysis, we hope to do the same for the innovative investor who is considering adding cryptoassets to his or her portfolio.

This is not a get-rich-quick book with the latest hot tips. Rather it’s a book that grounds this new asset class in the context of its own history, common investment strategies, the history of financial speculation, and more. Investors

INTRODUCTION xxvii

who follow through on their interest in cryptoassets and examine them in the context of their overall financial goals and portfolio strategies will become innovative investors.

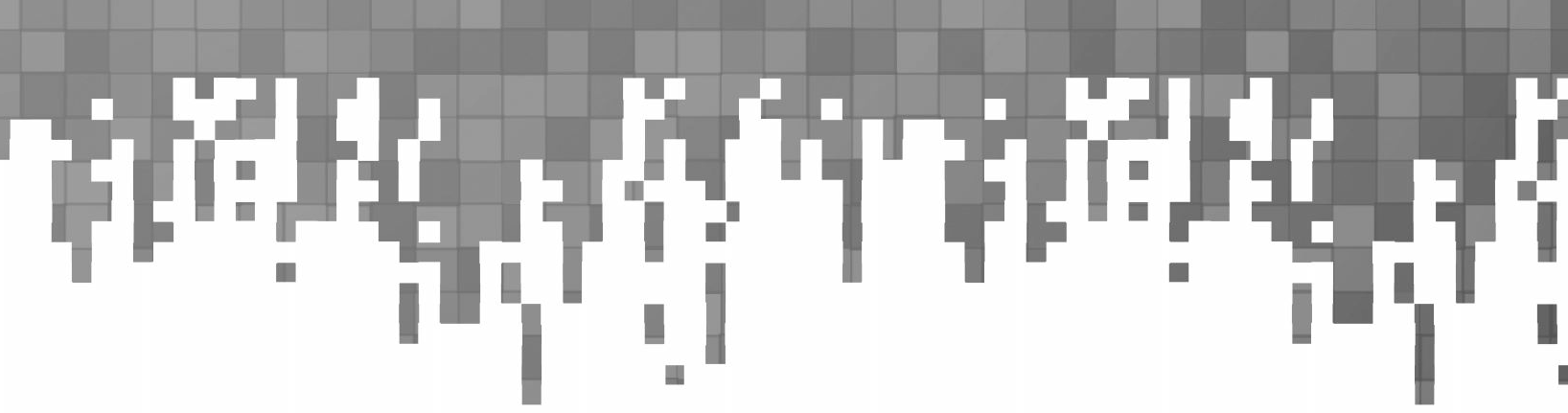
We’ve written this book for the novice and the expert. We’ve divided it into three parts: *What*, *Why*, and *How*. The *What* lays the foundation for this new asset class, providing a concise explanation of the technology and history of cryptoassets. The *Why* dives into why portfolio management matters, as well as why we think this is a whole new asset class that offers great opportunity— as well as great risk. The *How* details how to approach adding a cryptoasset to a portfolio, including a framework for investigating the merits of a new asset, and the logistical grit of acquisition, storage, taxes, and regulation. Each chap- ter effectively can stand alone.

The world of cryptoassets may at times feel like science fiction; we imagine that when the Internet was first explained and discussed, people felt the same way. For many, change sparks fear. We understand that. But it also kindles opportunity, and we hope to prepare the reader to recognize, understand, and act on the opportunities available in the world of cryptoassets.

Tomorrow inevitably becomes today. Exponential change isn’t going away. This book will help the innovative investor not only survive but thrive. Let’s dive in.

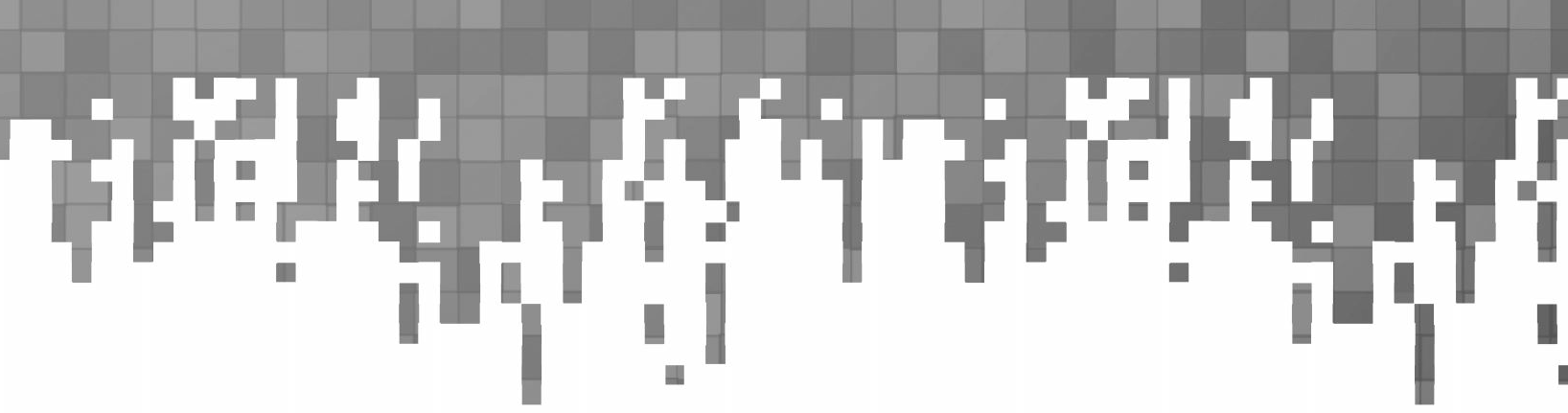


*This page intentionally left blank*



**CRYPTOASSETS**

*This page intentionally left blank*



**Part I**

**WHAT**

*This page intentionally left blank*

## Chapter 1

## Bitcoin and the Financial Crisis of 2008

n 2008, Bitcoin rose like a phoenix from the ashes of near Wall Street col- lapse. In the four months of August to October 2008, an unprecedented series of changes occurred: [Bitcoin.org](http://Bitcoin.org/) was registered, Lehman Brothers filed for the largest bankruptcy in American history, Bank of America bought Merrill Lynch for $50 billion, the U.S. government established the $700 billion Troubled Asset Relief Program (TARP), and Satoshi Nakamoto published a

I

paper that founded Bitcoin and the basis of blockchain technology.1

The entwinement of the financial collapse on the one hand and the rise of Bitcoin on the other is hard to ignore. The financial crisis cost the global economy trillions of dollars and burned bridges of trust between financial titans and the public.2 Meanwhile, Bitcoin provided a system of decentralized trust for value transfer, relying not on the ethics of humankind but on the cold calculation of computers and laying the foundation potentially to obviate the need for much of Wall Street.

WHO IS SATOSHI NAKAMOTO?

Referring to Satoshi as “he” is simply a matter of convenience because to this day no one knows exactly who or even what Satoshi is. He, she, they, or it remains totally anonymous. On a profile page Satoshi created for the P2P Foundation—which he used to communicate with others as he spun up Bitcoin—he wrote that he was a 37-year-old male living in Japan.3

3

4 CRYPTOASSETS

Yet outside of Japan, fact digging has led people to believe Satoshi resided in the United Kingdom, North America, Central America, South America, or even the Caribbean. People point to his impeccable written English or occa- sionally British phrases as proof of U.K. residence,4 while others cite his post- ing patterns as being indicative of living in geographies in Eastern or Central time zones.5 A number of phony Satoshis have appeared, too, as the media is all too eager to present a solution to such a juicy puzzle. An Australian, Craig Wright, claimed to be Satoshi in May 2016 and momentarily grabbed the attention of publications such as *The Economist*6 and *Wired*7 before being debunked.8

Claims of Satoshi’s origin now cover five continents, leading us back to the possibility that maybe Satoshi isn’t even a single person but rather a group of people. The mastery Satoshi showcased across a wide scope of topics— including cryptography, computer science, economics, and psychology—and the ability to communicate it all fluidly seems to support the hypothesis that Satoshi is more than one person. But who would they be? While the mystery may never be solved, Satoshi most certainly was aware of Wall Street’s growing instability.

#### THE FINANCIAL CRISIS OF 2008

For financial titans, 2008 proved a slowly unfolding nightmare. In March of that year, the first major Wall Street institution—Bear Stearns—acquiesced to its demons. After weathering every type of market for 85 years, Bear Stearns was finally dragged under by a slumping housing market. On March 16, JPMorgan Chase & Co. bought it for $2 a share, about 1 percent of the value of its $170 per share price from a year prior.9 To catalyze the deal, the Federal Reserve agreed to facilitate the purchase of $29 billion in distressed assets from Bear Stearns.10 Yet disturbingly, a month after the buyout, John Mack and Lloyd Blankfein, CEOs of Morgan Stanley and Goldman Sachs Group Inc., respectively, told shareholders the housing market crisis was going to be short- lived and nearing a close.11

Much of this crisis was born of irresponsible lending, known as *subprime loans*, to Americans who couldn’t repay their debts. Historically, when a bank issued a loan, the bank was on the hook for ensuring that the borrower repaid the funds. However, in the case of many subprime loans, once these loans were issued to borrowers, they were then packaged, or *securitized*, into complex instruments known as collateralized mortgage obligations (CMOs). These

BITCOIN AND THE FINANCIAL CRISIS OF 2008 5

CMOs were then sold to other investors, effectively passing on the risk like a hot potato through the financial markets, with purchasers lured by the prom- ise of high returns combined with low risk, due to purported diversification.

What people didn’t realize, including Wall Street executives, was how deep and interrelated the risks CMOs posed were. Part of the problem was that CMOs were complex financial instruments supported by outdated financial architecture that blended analog and digital systems. The lack of seamless digi- tal documentation made quantifying the risk and understanding exactly what CMOs were composed of difficult, if not impossible. Furthermore, as these CMOs were spread around the world, global investors were suddenly inter- connected in a web of American mortgages.12 In the summer of 2008, despite the lack of financial transparency but emboldened by access to funds from the Federal Reserve in case of further distress, Richard Fuld Jr., the CEO of Lehman Brothers, eerily claimed, “We can’t fail now.”13

As a storm brewed around unknowing Wall Street executives, Satoshi Nakamoto was busy fleshing out the concept of Bitcoin. On August 18, 2008, [Bitcoin.org,](http://Bitcoin.org/) the home website for information on Bitcoin, was registered.14 Whether as an individual or an entity, what’s now clear is that Satoshi was designing a technology that if existent would have likely ameliorated the toxic opacity of CMOs. Due to the distributed transparency and immutable audit log of a blockchain, each loan issued and packaged into different CMOs could have been documented on a single blockchain. This would have allowed any purchaser to view a coherent record of CMO ownership and the status of each mortgage within. Unfortunately, in 2008 multiple disparate systems—which were expensive and therefore poorly reconciled—held the system together by digital strings.

On the morning of Wednesday, September 10, 2008, Fuld and other senior management faced a different reality from Fuld’s confident summer procla- mation. Management struggled to explain to a group of critical analysts $5.3 billion worth of write-downs on “toxic assets” and a quarterly loss of $3.9 bil- lion.15 The call ended abruptly, and analysts signed off unconvinced of the measures Lehman was taking. The markets had already punished Lehman the day before, dropping its stock price 45 percent, and on Wednesday it dropped another 7 percent.16

Two days later, on Friday afternoon, the CEOs of Merrill Lynch, Morgan Stanley, and Goldman Sachs met at the New York Federal Reserve, along with the Federal Reserve Chairman, the U.S. Treasury Secretary, and the president of the New York Federal Reserve. The afternoon’s topic was what to do about

6 CRYPTOASSETS

Lehman Brothers. It was clear the situation had become critical. Initially it appeared either Barclays or Bank of America would come to the rescue of Lehman Brothers, but that likelihood quickly evaporated.

On Saturday, as the same group met again at the New York Fed, John Thain, Merrill Lynch’s CEO, had an unsettling thought. During the briefing on Lehman’s situation, he realized his company might only be a few steps from the same catastrophe. “This could be me sitting here next Friday,”17 he said. Thain quickly moved to find suitors for Merrill, the most promising option being Bank of America, which had already been in talks to buy Lehman. With talks secretly progressing between Merrill Lynch and Bank of America, Lehman Brothers held Barclays as its only suitor hope.

By Sunday, September 14, Barclays was ready to approve a deal to buy Lehman Brothers. Lehman only needed the U.S. or British government to back its trading balances for a couple of days, enough time for Barclays to conduct a shareholder vote for final approval. Neither government was willing to step in, and the likelihood of a deal began to melt. With only a few hours left until Asian markets opened for trading, the U.S. government questioned Lehman on its only remaining option: bankruptcy.

Harvey Miller, a well-regarded bankruptcy lawyer at Weil, Gotshal & Manges, had been working quietly since Thursday night to lay the groundwork for this worst-case bankruptcy scenario. When asked by a senior Fed official if Mr. Miller felt Lehman was ready to file for bankruptcy, he responded: “This will cause financial Armageddon.”

If Lehman filed for bankruptcy, financial firms that did business with Lehman would also lose billions, potentially triggering a domino effect of bankruptcy.

Later that evening, Bank of America inked a deal to buy Merrill Lynch for

$50 billion, and a couple of hours later, in the early hours of Monday morning, Lehman Brothers filed for Chapter 11 bankruptcy protection, making it the biggest bankruptcy in U.S. history. So came to an end a 164-year-old firm born from a dry-goods store that had evolved into the fourth largest U.S. investment bank. It signaled the end of an era.18

Lehman’s bankruptcy and Merrill’s buyout proved to be only the beginning. On Tuesday, the Federal Reserve Bank of New York was authorized to lend up to $85 billion to the American International Group (AIG), the biggest insurer in America, as the behemoth organization began to teeter.19 It was mid- September and darker clouds loomed on the horizon for Wall Street and global financial markets.

BITCOIN AND THE FINANCIAL CRISIS OF 2008 7

#### THE BIRTH OF BITCOIN

Six and a half weeks later, on October 31, 2008, Satoshi released the Bitcoin white paper, which serves as the genesis for every single blockchain imple- mentation deployed today and forevermore. In the concluding paragraph of his foundational paper, Satoshi wrote: “We have proposed a system for elec- tronic transactions without relying on trust.”20

By the time he released the paper, he had already coded the entire system. In his own words, “I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper.”21 Based on historical estimates, Satoshi likely started formalizing the Bitcoin concept sometime in late 2006 and started coding it around May 2007. In this same time span, many regulators began to believe that the U.S. housing market was overextended and likely in for a rough ride.22 It’s hard to believe someone with such breadth of knowledge as Satoshi would be working in isolation from what he was wit- nessing in global financial markets.

The day after publishing his white paper, Satoshi sent an email to “The Cryptography Mailing List” with a link to his paper.23 The list was composed of subscribers focused on cryptography and its potential applications. Satoshi’s email sparked a chain of responses.

On Friday, November 7, 2008, in reply to his increasingly passionate group of followers, he wrote: “You will not find a solution to political problems in cryptography . . . but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.”24 It’s clear from this quote that Satoshi was not creating Bitcoin to slip seamlessly into the existing gov- ernmental and financial system, but instead to be an alternative system free of top-down control, governed by the decentralized masses. Such decentralized autonomy was foundational to the early days of the Internet as well, where each node on the network was an autonomous agent that corresponded with other agents through shared protocols.

On November 9, the Bitcoin project was registered on [SourceForge.net,](http://SourceForge.net/) a website geared toward facilitating open-source software development. In response to a growing number of inquiries and interest on The Cryptography Mailing List, Satoshi wrote on November 17: “I’ll try and hurry up and release the source code as soon as possible to serve as a reference to help clear up all these implementation questions.”25

8 CRYPTOASSETS

Then Satoshi went quiet for a couple months as Wall Street continued to crumble. The Emergency Economic Stabilization Act of 2008 had done little to ameliorate the meltdown that ensued after Lehman’s bankruptcy. Passed by Congress and signed by President George W. Bush on October 3, the emer- gency act had established the $700 billion TARP. As a result of TARP, the U.S. government acquired preferred stock in hundreds of banks as well as massive companies such as AIG, General Motors, and Chrysler. The stock didn’t come for free, though. It took $550 billion in investments to stabilize those teetering mammoths.26

In the opening moments of Bitcoin’s life as a public network, Satoshi made clear he was attuned to the failings of the global financial system. In the first instance of recording information on Bitcoin’s blockchain, Satoshi inscribed: “The Times 03/Jan/2009 Chancellor on brink of second bailout of banks,”27 in reference to an article that appeared in the British publication *Th Times* on the U.K.’s likely need to assist more banks in staying afloat.28 Many years later people would realize that one of the most powerful use cases of blockchain technology was to inscribe immutable and transparent information that could never be wiped from the face of digital history and that was free for all to see. Satoshi’s choice first to employ this functionality by inscribing a note about bank bailouts made it clear he was keen on never letting us forget the failings of the 2008 financial crisis.

#### AN ALTERNATIVE FINANCIAL SYSTEM

Nine days after this poignant inscription, the first ever transaction using bit- coin took place between Satoshi Nakamoto and Hal Finney, an early advocate and Bitcoin developer. Nine months later the first exchange rate would be set for bitcoin, valuing it at eight one-hundredths of a cent per coin, or 1,309 bit- coin to the dollar.29 A dollar invested then would be worth over $1 million by the start of 2017, underscoring the viral growth that the innovation was poised to enjoy.

Diving deeper into Satoshi’s writings around the time, it becomes more apparent that he was fixated on providing an alternative financial system, if not a replacement entirely. After the network had been up and running for over a month, Satoshi wrote of Bitcoin, “It’s completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust . . . I think this is the first time we’re trying a decentralized, non-trust-based system.”30

BITCOIN AND THE FINANCIAL CRISIS OF 2008 9

On December 5, 2010, Satoshi showed an unnervingly human side, plead- ing that WikiLeaks not accept bitcoin as a means of payment after major credit card networks had blocked users from supporting the site. Satoshi wrote, “No, don’t ‘bring it on’. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.”31

Shortly thereafter, Satoshi vanished. Some speculate it was for the good of Bitcoin. After all, being the creator of a technology that has the potential to replace much of the current financial system is bound eventually to invoke the wrath of powerful government and private sector forces. By disappearing into the ether, Satoshi removed the head of Bitcoin, and with it a single point of failure. In his wake stands a network with thousands of access points and millions of users.

Wall Street, on the other hand, suffered from many points of failure. When the dust settled, the U.S. government had spent well beyond the $700 billion initially secured for TARP. In all, $2.5 trillion was injected into the system, not to mention $12.2 trillion committed to reinstall faith in the fidelity of financial institutions.32

While Wall Street as we knew it was experiencing an expensive death, Bitcoin’s birth cost the world nothing. It was born as an open-source technol- ogy and quickly abandoned like a motherless babe in the world. Perhaps, if the global financial system had been healthier, there would have been less of a community to support Bitcoin, which ultimately allowed it to grow into the robust and cantankerous toddler that it currently is.

#### WELCOME TO THE WORLD THAT BITCOIN CREATED

Since Satoshi disappeared, Bitcoin has unleashed a tidal wave of disruption and rethinking of global financial and technological systems. Countless deri- vations of Bitcoin have been created—systems such as Ethereum, Litecoin, Monero, and Zcash—all of which rely on blockchain technology, Satoshi’s gift to the world. At the same time, many financial and technological incumbents have moved to embrace the technology, creating confusion around all the innovation unfolding and what is most relevant to the innovative investor. The next chapter will involve solidifying understanding of blockchain technology, Bitcoin, bitcoin, cryptoassets, and where the investment opportunities await.

*This page intentionally left blank*

## Chapter 2

## The Basics of Bitcoin and Blockchain Technology

t’s time to crystallize the difference between Bitcoin, Bitcoin’s blockchain, bitcoin with a lowercase *b*, blockchain technology, and other related but distinct concepts. At first blush, this space appears jargon heavy, deterring many from even attempting to understand it. In reality, there are only a few for- eign concepts, encapsulated in recently invented words, which unfortunately keep people out. Since these words are used frequently when people talk about different applications of Bitcoin or blockchain technology, the space appears impenetrable—but it’s not. All that’s required is a concerted effort to nail down the key concepts, which then become the mental scaffolding that will support

I

understanding of the many applications of blockchain technology.

Bitcoin with an uppercase *B* refers to the software that facilitates the trans- fer and custody of bitcoin the currency, which starts with a lowercase *b*.

* Bitcoin equals software.
* bitcoin equals currency.

Much of this book will use Bitcoin (with a capital *B*) as the starting point. Bitcoin is the genesis of the blockchain movement. It is common to compare newly created blockchains with Bitcoin’s because Bitcoin’s blockchain is the longest standing point of reference. Therefore, understanding the basics of Bitcoin is critical.

However, to truly understand Bitcoin, one has to move beyond think- ing of it as some digital Ponzi scheme or shadowy system used by criminals.

11

12 CRYPTOASSETS

Those are stale stories that continue to tumble through the media mill. In July 2016, researchers from the London School of Economics and Political Science, Deutsche Bundesbank (Germany’s central bank), and the University of Wisconsin at Madison released the paper “The Evolution of the Bitcoin Economy.” Three reputable institutions would not waste their time, nor jeop- ardize their reputations, on a nefarious currency with no growth potential.

In that paper, the researchers describe an extensive analysis they performed on Bitcoin’s blockchain and the transactions therein. Below is a summary of what they found:

In this paper, we gather together the minimum units of Bitcoin identity (the individual addresses), and group them into approxi- mations of business entities, what we call “super clusters.” While these clusters can remain largely anonymous, we are able to ascribe many of them to particular business categories by ana- lyzing some of their specific transaction patterns, as observed during the period from 2009–2015. We are then able to extract and create a map of the network of payment relationships among them, and analyze transaction behavior found in each business category. We conclude by identifying three marked regimes that have evolved as the Bitcoin economy has grown and matured: from an early prototype stage; to a second growth stage popu- lated in large part with “sin” enterprise (i.e., gambling, black markets); to a third stage marked by a sharp progression away from “sin” and toward legitimate enterprises.1

Certainly, some of the earliest adopters of Bitcoin were criminals. But the same goes for most revolutionary technologies, as new technologies are often useful tools for those looking to outwit the law. We’ll get into the specifi risks associated with cryptoassets, including Bitcoin, in a later chapter, but it’s clear that the story of bitcoin as a currency has evolved beyond being solely a means of payment for illegal goods and services. Over 100 media articles have jumped at the opportu- nity to declare bitcoin dead,2 and each time they have been proven wrong.

When one considers Bitcoin neutrally in the context of a broader theme of technological evolution, it sits in the sweet spot of key technology trends. For example, the world is increasingly real-time, with people connecting in peer-to-peer manners, empowering and connecting individuals regardless of geographic or socioeconomic birth. Bitcoin fits these thematic molds. It allows

THE BASICS OF BITCOIN AND BLOCKCHAIN TECHNOLOGY 13

a global transaction to be settled in an hour as opposed to a couple of days. It operates in a peer-to-peer manner, the same movement that has driven Uber, Airbnb, and LendingClub to be multibillion-dollar companies in their own realms. Bitcoin lets anyone be their own bank, putting control in the hands of a grassroots movement and empowering the globally unbanked.

However, Bitcoin has done something arguably more impressive than Uber, Airbnb, and LendingClub. Those companies decentralized services that were easily understandable and had precedent for being peer-to-peer. Everyone has had a friend drive them to the airport, or stayed with a relative in another country, or borrowed money from their parents. Decentralizing a currency, without a top-down authority, requires coordinated global acceptance of a shared means of payment and store of value.

Currency originally came about to facilitate trade, allowing society to move past barter and the *double coincidence of wants*. It has evolved over time to be more convenient, resulting in its present paper state. Inherently, that paper has little value other than the fact that everyone else thinks it has value and the government requires it be accepted to fulfill financial obligations. In that sense, it is a usefully shared representation of value. The libertarians in the room would say it’s a *usefully shared illusion* of value, going back to the idea the paper itself is worth little. Bitcoin is a similarly shared representation of value, except it has no physical manifestation and no top-down authority to protect it. Despite these hurdles, the elegance of the mathematics that allow it to func- tion has also allowed it to grow and store billions in value.

#### THE INNER WORKINGS OF BITCOIN’S BLOCKCHAIN

Part of the Bitcoin software involves the building of Bitcoin’s blockchain, which can be thought of as a digital ledger that keeps track of user balances via debits and credits. In this sense, Bitcoin’s blockchain is a database that records the flow of its native currency, bitcoin. What makes this digital ledger special? Bitcoin’s blockchain is a distributed, cryptographic, and immutable data- base that uses proof-of-work to keep the ecosystem in sync. Technobabble?

Sure. But impenetrable technobabble? No.

##### Distributed

Distributed refers to the way in which computers access and maintain Bitcoin’s blockchain. Unlike most databases that rigidly control who can access the

14 CRYPTOASSETS

information within, any computer in the world can access Bitcoin’s block- chain. This feature of Bitcoin’s blockchain is integral to bitcoin as a global currency. Since anyone anywhere can tap into Bitcoin’s blockchain to see the record of debits and credits between different accounts, it creates a system of global trust. Everything is transparent, so everyone is on a level playing field.

WHAT IS CRYPTOGRAPHY?

Initially a scary word, cryptography is the science of secure communication. It involves taking information and scrambling it in such a way that only the intended recipient can understand and use that information for its intended purpose. The process of scrambling the message is encryption, and unscram- bling it is decryption, performed through complex mathematical techniques. Cryptography is the battlefi on which those trying to transmit information securely combat those attempting to decrypt or manipulate the information. More recently, cryptography has evolved to include applications like proving the ownership of information to a broader set of actors—such as public key cryptography—which is a large part of how cryptography is used within Bitcoin. Encryption techniques have been employed for centuries. Julius Caesar used a simple method of encryption during times of war to inform his gener- als of his plans. He would send messages using letters that were three letters after the letter they were supposed to represent. For instance, instead of using the letters ABC in his message, he would write them as DEF and his generals would decrypt them to understand his intended message. Understandably,

this form of encryption did not remain secure for long.3

A more recent example that was the subject of the movie *The Imitation Game* was the effort during World War II of a group of English cryptographers to decode the messages of Nazi Germany, which were encrypted by a coding device called the Enigma machine. Alan Turing, a luminary in machine learn- ing and artificial intelligence, was a major player on the team whose efforts to break the Enigma code ultimately had a debilitating impact on German war strategies and helped to end the war.

Cryptography has become a vital part of our lives. Every time we type in a password, pay with a credit card, or use WhatsApp, we are enjoying the ben- efits of cryptography. Without cryptography, it would be easy for bad actors to steal sensitive information and use it against us. Cryptography makes sure the information can only be used by those for whom it is intended.

THE BASICS OF BITCOIN AND BLOCKCHAIN TECHNOLOGY 15

##### Cryptographic

Every transaction recorded in Bitcoin’s blockchain must be cryptographically verified to ensure that people trying to send bitcoin actually own the bitcoin they’re trying to send. Cryptography also applies to how groups of transac- tions are added to Bitcoin’s blockchain. Transactions are not added one at a time, but instead in “blocks” that are “chained” together, hence the term block- chain. We will go deeper into the specifics of the process in the proof-of-work section that follows, but for now here’s the takeaway: cryptography allows the computers building Bitcoin’s blockchain to collaborate in an automated system of mathematical trust. There is no subjectivity as to whether a transaction is confirmed in Bitcoin’s blockchain: it’s just math. For a deep dive on cryptogra- phy, we highly recommend *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh.

##### Immutable

The combination of globally *distributed* computers that can *cryptographically* verify transactions and the building of Bitcoin’s blockchain leads to an *immu- table* database, meaning the computers building Bitcoin’s blockchain can only do so in an *append only* fashion. *Append only* means that information can only be added to Bitcoin’s blockchain over time but cannot be deleted—an audit trail etched in digital granite. Once information is confirmed in Bitcoin’s blockchain, it’s permanent and cannot be erased. Immutability is a rare feature in a digital world where things can easily be erased, and it will likely become an increasingly valuable attribute for Bitcoin over time.

##### Proof-of-Work

While the previous three attributes are valuable, none of them is inherently new. *Proof-of-work* (PoW) ties together the concepts of a *distributed*, *cryptographic*, and *immutable* database, and is how the distributed computers agree on which group of transactions will be appended to Bitcoin’s blockchain next. Put another way, PoW specifi ally deals with how transactions are grouped in blocks, and how those blocks are chained together, to make Bitcoin’s blockchain.

The computers—or miners as they’re called—use PoW to compete with one another to get the privilege to add blocks of transactions to Bitcoin’s block- chain, which is how transactions are confirmed. Each time miners add a block,

16 CRYPTOASSETS

they get paid in bitcoin for doing so, which is why they choose to compete in the first place.

Competition for a financial reward is also what keeps Bitcoin’s blockchain secure. If any ill-motivated actors wanted to change Bitcoin’s blockchain, they would need to compete with all the other miners distributed globally who have in total invested hundreds of millions of dollars into the machinery necessary to perform PoW. The miners compete by searching for the solution to a cryp- tographic puzzle that will allow them to add a block of transactions to Bitcoin’s blockchain.

The solution to this cryptographic puzzle involves combining four vari- ables: the time, a summary of the proposed transactions, the identity of the previous block, and a variable called the *nonce*.

The nonce is a random number that when combined with the other three variables via what is called a cryptographic hash function results in an output that fits a difficult criteria. The difficulty of meeting this criteria is defined by a parameter that is adjusted dynamically so that one miner finds a solution to this mathematical puzzle roughly every 10 minutes. If all of this seems like drinking water out of a fire hose, that’s okay—it’s that way for everyone at the outset. We’ll cover this process in greater detail in Chapter 4, and then go even deeper in Chapter 14.

The most important part of the PoW process is that one of the four variables is the identity of the previous block, which includes when that block was cre- ated, its set of transactions, the identity of the block before that, and the block’s nonce. If innovative investors keep following this logic, they will realize that this links every single block in Bitcoin’s blockchain together. As a result, no information in any past block, even if it was created years ago, can be changed without changing all of the blocks after it. Such a change would be rejected by the distributed set of miners, and this property is what makes Bitcoin’s block- chain and the transactions therein immutable.

Miners are economically rewarded for creating a new block with a transac- tion that grants them newly minted bitcoin, called a coinbase transaction, as well as fees for each transaction. The coinbase transaction is also what slowly releases new bitcoin into the money supply, but more on that later.

#### A USEFUL ANALOGY FOR BITCOIN’S ECOSYSTEM

To tie everything together using an analogy that will prepare us for a discus- sion of the applications of blockchain technology in Chapter 3 (see Figure 2.1).

THE BASICS OF BITCOIN AND BLOCKCHAIN TECHNOLOGY 17

|  |
| --- |
| End Users |
| Applications |
| Bitcoin Software = Operating System |
| Miners = Hardware |

Figure 2.1 n Bitcoin as a stack of hardware, OS, applications, and end users

It’s helpful to think of the concepts as a stack of hardware, software, applica- tions, and users in relation to a personal computer.

The miners that build Bitcoin’s blockchain with the PoW process are the hardware, just as a MacBook Pro provides the hardware for a personal com- puter. That hardware runs an operating system (OS); in the case of Bitcoin, the operating system is the open-source software that facilitates everything described earlier. Th s software is developed by a volunteer group of developers, just as Linux, the operating system that underlies much of the cloud, is main- tained by a volunteer group of developers. On top of this hardware and operat- ing system combination are applications, just as Safari is an application that runs on an Apple operating system. The applications interface with the Bitcoin operating system, which pushes and pulls information to and from Bitcoin’s blockchain as needed. Lastly, there are the end users that interface with the applications, and someday may have no concept of the hardware or software underneath because all they need to know is how to navigate the applications.

#### PRIVATE VERSUS PUBLIC BLOCKCHAINS

Broadly, there are two types of entities that can own the hardware support- ing blockchains: public and private. The difference between public and private blockchains is similar to that between the Internet and intranets. The Internet is a public resource. Anyone can tap into it; there’s no gatekeeper. Intranets, on the other hand, are walled gardens used by companies or consortiums to transmit private information. Public blockchains are analogous to the Internet, whereas private blockchains are like intranets. While both are useful today, there’s little debate that the Internet has created orders of magnitude more value than intranets. This is despite vociferous proclamations by incumbents

18 CRYPTOASSETS

in the 1980s and 1990s that the public Internet could never be trusted. History is on the side of public networks, and while history doesn’t repeat, it does often rhyme.4

The important distinction boils down to how the entities get access to the network. Remember, a blockchain is created by a distributed system of com- puters that uses cryptography and a consensus process to keep the members of the community in sync. A blockchain is useless in isolation; one might as well use a centralized database. The community of computers building a block- chain can either be public or private, commonly referred to as permissionless or permissioned.

Public systems are ones like Bitcoin, where anyone with the right hardware and software can connect to the network and access the information therein. There is no bouncer checking IDs at the door. Rather, participation in the net- work forms an economic equilibrium in which entities will buy more hard- ware to take part in building Bitcoin’s blockchain if they feel they can make money doing so. Other examples of public blockchains include Ethereum, Litecoin, Monero, Zcash, and so on, which will be discussed in more detail in Chapters 4 and 5.

Private systems, on the other hand, employ a bouncer at the door. Only enti- ties that have the proper permissions can become part of the network. These private systems came about after Bitcoin did, when enterprises and businesses realized they liked the utility of Bitcoin’s blockchain, but weren’t comfortable or legally allowed to be as open with the information propagated among public entities.

These private blockchains have thus far been most widely embraced by the fi ancial services as a means to update IT architecture that hasn’t had a major facelift since preparation for the Y2K bug. Within fi ancial services, these pri- vate blockchains are largely solutions by incumbents in a fi ht to remain incum- bents. While there is merit to many of these solutions, some claim the greatest revolution has been getting large and secretive entities to work together, sharing information and best practices, which will ultimately lower the cost of services to the end consumer.5 We believe that over time the implementation of private blockchains will erode the position held by centralized powerhouses because of the tendency toward open networks. In other words, it’s a foot in the door for further decentralization and the use of public blockchains.

The potential applications of private blockchains extend far beyond the financial services industry. Banks and other monetary intermediaries have most quickly moved to adopt the technology because the use cases are most

THE BASICS OF BITCOIN AND BLOCKCHAIN TECHNOLOGY 19

obvious for a system that specializes in securing transactions. Beyond the financial services industry, others that are exploring the applications of block- chain technology include the music industry, real estate, insurance, healthcare, networking, polling, supply chains, charities, gun tracking, law enforcement, governments, and more.6

Throughout this book, we will focus on public blockchains and their native assets, or what we will define as *cryptoassets*, because we believe this is where the greatest opportunity awaits the innovative investor. Sometimes, crypto- assets have the exact same name as their parent blockchain but with differ- ent capitalization. Other times there’s a slightly different name for the asset. For example, the native asset of Bitcoin’s blockchain is bitcoin, the native asset of Ethereum’s blockchain is ether, the native asset of Litecoin’s blockchain is litecoin, etc.

Many public blockchains are markedly different from one another. Some members of the early Bitcoin community feel the definition of what makes something a blockchain should be very specific, in particular, that any block- chain must use proof-of-work as the means of consensus. We disagree with that exclusive worldview, as there are many other interesting consensus mech- anisms being developed, such as proof-of-stake, proof-of-existence, proof- of-elapsed-time, and so on. Just as machine learning is not just one thing, but composed of the Symbolists, Connectionists, Evolutionaries, Bayesians, and Analogizers, so too can blockchain technology have many flavors. In *The Master Algorithm*,7 Pedro Domingos hypothesizes that all these camps of machine learning—which at times have been bitter rivals—will one day coalesce. The same will likely be true of blockchain technology. If these dis- tributed databases of value are to be truly transformational, they will have to interoperate and value one another.

THE MANY USES OF THE WORD *BLOCKCHAIN*

Despite increased interest in blockchain technology, confusion remains as to what it specifically means due to imprecision in the use of the term. For example, “a blockchain,” “the blockchain,” “blockchain,” and “blockchain technology” can all refer to different things.

Typically, when people say *the blockchain*, they are referring to *the origi- nal*, or Bitcoin’s blockchain. At the risk of redundancy but in pursuit of clarity, we will always use “Bitcoin’s blockchain” instead of “the blockchain.”

20 CRYPTOASSETS

On the other hand, terms such as *a blockchain* and *blockchain technology* typically refer to derivatives of the original that now may have nothing to do with Bitcoin. Meanwhile, *blockchain* is normally used to refer to the concept itself, with no particular implementation in mind. It is the most amorphous, so our least favored of the terms.

## Chapter 3

## “Blockchain, Not Bitcoin?”

n drawing a line between public and private blockchains, we have entered contentious territory that the innovative investor should understand. The difference between these two types of blockchains and the groups that sup- port them is full of tension, because the two camps have different goals for the technology. At the risk of overgeneralizing, private blockchains are backed by incumbents in their respective industries, while public blockchains are backed

I

by the disruptors.

To round out the context within which the innovative investor approaches cryptoassets, it’s important to understand how the world evolved beyond a single blockchain—Bitcoin’s blockchain—to include public and private block- chains. Otherwise, investors may be confused when they hear someone claim that Bitcoin is no longer relevant or that it’s been displaced. Neither of these claims is true, but it’s nonetheless helpful to understand the motivations and rationale behind those that say they are.

#### BITCOIN’S EARLY YEARS

We left Bitcoin in Chapter 1 with Satoshi pleading on December 5, 2010, for WikiLeaks not to accept bitcoin for donations to its site, because bitcoin was still too young and vulnerable to attack. This was about two years after the birth of Bitcoin’s blockchain, during which it had lived a mostly quiet and nerdy life. That was all about to change.

21

22 CRYPTOASSETS

A few months after Satoshi’s plea, a software application was released that would make Bitcoin famous. Launched in February 2011, the Silk Road pro- vided a rules-free decentralized marketplace for any product one could imag- ine, and it used bitcoin as the means of payment. You name it, the Silk Road had it. Gawker put it succinctly in a June 2011 article, “The Underground Website Where You Can Buy Any Drug Imaginable.”1 Clearly, this was one way that Bitcoin developed its dark reputation, though it’s important to know that this was not endorsed by Bitcoin and its development team. The Silk Road was simply making use of this new digital and decentralized currency by building an application atop its platform.

The Gawker article led to the first Google search spike in Bitcoin’s life, as shown in Figure 3.1, and would drive the price of bitcoin from about $10 to

$30 in the span of a week.2 However, the Gawker article jump paled in com- parison to the global Google search volume in March to April 2013, which corresponded with a nearly eightfold increase in price, from roughly $30 to

$230 in about a month. The drivers behind this bitcoin demand were more opaque than the Gawker spike, though many point to the bailout of Cyprus and the associated losses that citizens took on their bank account balances as the core driver. Bitcoin received ample interest for being outside of gov- ernment control, making its holders immune to such events. Bloomberg ran a story on March 25, 2013, with the eye-catching title, “Bitcoin May Be the Global Economy’s Last Safe Haven.”3

While the spring of 2013 was notable, it was a preview for bitcoin’s grand opening to global attention. This came six months later, in November 2013,

100

Bitcoin Rises from

~$30 to $230, 8-Fold in a Month

Gawker Article about the Silk Road, Bitcoin

Rises from ~$10 to $30, 3-Fold in a Week

Bitcoin Crosses $1,000

for First Time, 5-Fold in a Month

75

50

25

0

1 Feb 2009 1 Aug 2013

Figure 3.1 n Google search spikes for the term “bitcoin”

Source: Annotation of Google Search screenshot

“BLOCKCHAIN, NOT BITCOIN?” 23

when increased demand for bitcoin in China along with interest from the U.S. Senate on the innovation led to a stratospheric ascent through $1,000 that grabbed international headlines.4

THE UTILITY OF GOOGLE SEARCH TRENDS

Google search trends are a useful indicator of what is grabbing mainstream attention. The innovative investor can go to <https://trends.google.com/> and explore the patterns of how people are searching for different topics. Google even provides the option to explore search trends by geographical location, giving charts of where interest is spiking, as well as showing what related top- ics are on the rise. For example, after typing in “bitcoin,” investors can look at Google search trends for the last year, or five years, or a custom range, and investigate how Nigeria differs from India. We recommend orienting with this tool even beyond cryptoassets, as it’s a fascinating window into the global mesh of minds.

At this point, bitcoin’s spike captured the attention of the People’s Bank of China, which promptly implemented restrictions on bitcoin’s use, declaring it was “not a currency in the real meaning of the word.”5 The China ruling, com- bined with the FBI’s capture of the creator of the Silk Road, Ross Ulbricht,6 and soon thereafter the collapse of the biggest exchange at the time, Mt. Gox,7 put many bitcoin investors on edge as to its long-term viability in the face of gov- ernment and law enforcement crackdowns.8 Bitcoin’s subsequent price descent through all of 2014, bottoming in January 2015, was volatile, prolonged, and dispiriting for many early adopters who had been drawn to the new concept.

While bitcoin’s price was declining, its developers plowed forward with improving the protocol and building applications atop it. During that time, conversations about the underlying technology gained momentum, as early Bitcoiners9 emphasized that Bitcoin was important not only because of the decentralized currency aspect but also because of the architecture that sup- ported it. This emphasis on the technology supporting Bitcoin came about just as a slew of developers and enterprises began to investigate Bitcoin because of the headlines that had grabbed their attention. Clearly, something was going on, and newcomers to the technology were trying to figure out what.

The trifecta of current Bitcoiners defending and explaining the disruptive potential of Bitcoin’s technology, bitcoin’s price descending dramatically, and

24 CRYPTOASSETS

newcomers investigating the technology led to a seismic shift in the Bitcoin narrative. Newcomers didn’t necessarily see the need for bitcoin in the ways in which they wanted to use blockchain technology, and they felt reaffirmed in their belief by the continued descent of bitcoin’s price through 2014. But to Bitcoiners it had always been “bitcoin *and* blockchain.” The asset, bitcoin, was what incentivized an ecosystem of players—miners, developers, companies, and users—to secure and build upon Bitcoin’s blockchain, delivering means of exchange and store of value services to the world.

Out of this examination of the technology underlying Bitcoin, two move- ments exploded in the blockchain technology space. One was the proliferation of new cryptoassets that supported new public blockchains, like Ethereum. These new public blockchains offered utility outside the realm of Bitcoin. For example, Ethereum’s goal was to serve as a decentralized world computer, whereas Bitcoin aimed to be a decentralized world currency. This diversity has led to tension among players as some of these cryptoassets compete, but this is nothing like the tension that exists between Bitcoin and the second movement. The second movement that exploded on the scene questioned whether bitcoin, or any cryptoasset, was necessary to get the value out of blockchain technology. It is this second movement that we will investigate further in this chapter, as it’s important for the innovative investor to understand why some people will claim bitcoin and other cryptoassets aren’t needed to keep their implementations secure and functioning: welcome to the world of private

blockchains.

**SATOSHI NEVER SAID *BLOCKCHAIN***

The word *blockchain* was not mentioned once in Satoshi’s 2008 white paper. It was early Bitcoin companies that popularized the word within what was then a niche community. For example, [blockchain.info,](http://blockchain.info/) a popular Bitcoin wallet service,10 was launched in August 2011. Satoshi, on the other hand, frequently referred to the system as a “proof-of-work chain.” The closest he came to saying blockchain was with phrases such as “blocks are chained” or a “chain of blocks.” Since Satoshi only places “proof-of-work” directly before “chain,” many early Bitcoiners are adamant that the term blockchain should only be used if it is proof-of-work based. Remember that proof-of-work is a mechanism whereby all the computers building Bitcoin’s blockchain remain in sync on how to construct it.

“BLOCKCHAIN, NOT BITCOIN?” 25

#### BLOCKCHAIN, NOT BITCOIN

Articles like one from the Bank of England in the third quarter of 2014 argued, “The key innovation of digital currencies is the ‘distributed ledger,’ which allows a payment system to operate in an entirely decentralized way, without intermediaries such as banks.”11 In emphasizing the technology and not the native asset, the Bank of England left an open question whether the native asset was needed.

At the Inside Bitcoins conference in April 2015,12 many longtime Bitcoiners commented on how many Wall Street suits were in attendance. While Bitcoin was still king, there were growing whispers of “blockchain not bitcoin,” which was heresy to Bitcoiners.

The term *blockchain*, independent of Bitcoin, began to be used more widely in North America in the fall of 2015 when two prominent financial magazines catalyzed awareness of the concept. First, *Bloomberg Markets* published an article titled “Blythe Masters Tells Banks the Blockchain Changes Everything: The banker who helped give the world credit-default swaps wants to upend finance again—this time with the code that powers bitcoin.”13 In emphasizing “the code that powers bitcoin,” this article quietly questioned the need for the native asset, instead emphasizing the underlying technology. Masters was a well-known and respected figure in financial services, one that people associ- ated with financial innovation. Her choice to join a little-known firm at the time called Digital Asset Holdings, after having been the head of global com- modities at JPMorgan Chase, was reason to believe that blockchain technology was no longer on the fringe of the business world. In the article, a quote from Masters brought everyone to attention: “You should be taking this technology as seriously as you should have been taking the development of the Internet in the early 1990s. It’s analogous to email for money.”

The October 31, 2015, issue of the *Economist* featured “The Trust Machine” on its front cover, and while the article tipped its hat to Bitcoin, its focus was the more broadly applicable “technology behind bitcoin” and used the term *blockchain* throughout.14

The combination of Masters, Bloomberg, and the *Economist* led to a spike in interest in blockchain technology that set off a sustained climb in global Google search volumes for “blockchain” that is still in an upward trend. In the two weeks between October 18 and November 1, 2015, just after Bloomberg and the *Economist* published their articles, global Google search volumes for “blockchain” grew 70 percent (see Figure 3.2).

26 CRYPTOASSETS

120

100

80

60

40

20

0

Dec-11 Feb-12 Apr-12 Jun-12 Aug-12 Oct-12 Dec-12 Feb-13 Apr-13 Jun-13 Aug-13 Oct-13 Dec-13 Feb-14 Apr-14 Jun-14 Aug-14 Oct-14 Dec-14 Feb-15 Apr-15 Jun-15 Aug-15 Oct-15 Dec-15 Feb-16 Apr-16 Jun-16 Aug-16 Oct-16

Figure 3.2 n The rise in Google Search trends for the term “blockchain”

Data sourced from Google Search Trends

Masters’s focus for blockchain technology in financial services is on private blockchains, which are very different from Bitcoin’s blockchain. Pivotal to the current conversation, private blockchains don’t need native assets. Since access to the network is tightly controlled—largely maintaining security through exclusivity—the role of computers supporting the blockchain is different.15 Since these computers don’t have to worry about attack from the outside— they are operating behind a firewall and collaborating with known entities—it removes the need for a native asset that incentivizes the build-out of a robust network of miners.

A private blockchain is typically used to expedite and make existing pro- cesses more efficient, thereby rewarding the entities that have crafted the soft- ware and maintain the computers. In other words, the value creation is in the cost savings, and the entities that own the computers enjoy these savings. The entities don’t need to get paid in a native asset as reward for their work, as is the case with public blockchains.

On the other hand, for Bitcoin to incentivize a self-selecting group of global volunteers, known as miners, to deploy capital into the mining machines that validate and secure bitcoin transactions, there needs to be a native asset that can be paid out to the miners for their work. The native asset builds out support for the service from the bottom up in a truly decentralized manner. Public blockchains are not so much databases as they are system architectures

“BLOCKCHAIN, NOT BITCOIN?” 27

spawned from the bottom up to orchestrate the creation of globally decentral- ized digital services. Over time, miner compensation will shift from the issu- ance of new bitcoin to transaction fees, and if global adoption is great enough, then transaction fees will be sufficient to sustain miners.

The kernel of belief held by many avid proponents of private blockchains is that the native assets themselves (such as bitcoin) are irrelevant; they can be removed from the architecture and the best parts of the technology can remain intact. For the use cases these people are pursuing, that’s true. For pub- lic blockchains, however, it’s not true. Enterprises that have come to explore blockchain technology from the perspective of how they can use it to update their current technology stacks, very much in the form of a database, most often fall into the private blockchain bucket. Many financial services compa- nies are the earliest adopters of this mindset.

Beyond questioning the need for native cryptoassets—which would natu- rally infuriate communities that very much value their cryptoassets—tensions also exist because public blockchain advocates believe the private blockchain movement bastardizes the ethos of blockchain technology. For example, instead of aiming to decentralize and democratize aspects of the existing financial ser- vices, Masters’s Digital Asset Holdings aims to assist existing financial services companies in adopting this new technology, thereby helping the incumbents fight back the rebels who seek to disrupt the status quo.

#### BLOCKCHAINS AS A GENERAL PURPOSE TECHNOLOGY

While we have our beliefs about the most exciting applications of blockchain tech- nology, we don’t ascribe to an exclusive world view. Instead, we believe Bitcoin’s blockchain is one of the most important blockchains in existence, and that it has given birth to a new general purpose technology that goes beyond Bitcoin.

General purpose technologies are pervasive, eventually affecting all con- sumers and companies. They improve over time in line with the deflation- ary progression of technology, and most important, they are a platform upon which future innovations are built. Some of the more famous examples include steam, electricity, internal combustion engines, and information technology.16 We would add blockchain technology to this list. While such a claim may appear grand to some, that is the scale of the innovation before us.

As a general purpose technology, blockchain technology includes private blockchains that are going to have a profound impact on many industries *and* public blockchains beyond Bitcoin that are growing like gangbusters.

28 CRYPTOASSETS

The realm of public blockchains and their native assets is most relevant to the innovative investor, as private blockchains have not yielded an entirely new asset class that is investable to the public.

#### WHERE IS BLOCKCHAIN TECHNOLOGY IN THE HYPE CYCLE?

By now it will be clear to the innovative investor that the blockchain technol- ogy space is still working itself out and will continue to do so for years to come. Captivating technologies have a gravitational pull that brings in new minds with varied perspectives and that will push the boundaries of the technology. The progression of a new technology, and the way it evolves as it gains men- tal mindshare, is at the core of Gartner’s Hype Cycle for Emerging Technologies (Gartner is a leading technology research and advisory firm),17 which displays

five common stages of technology.18

* Innovation Trigger
* Peak of Inflated Expectations
* Trough of Disillusionment
* Slope of Enlightenment
* Plateau of Productivity

First is the Innovation Trigger that brings the technology into the world. While not very visible, just as Bitcoin wasn’t visible in the early years of its life, word spreads and expectations grow. Over time the murmurs gain momentum, building into a crescendo that is Gartner’s second stage, the Peak of Inflated Expectations. The peak represents the height of confusion around the defini- tion of the original technology, because people often apply it optimistically to everything they see. No technology is a panacea.

As companies sprout to life and attempt to transition ideas into reality, shifting from proof-of-concepts to at-scale implementations, it frequently turns out that implementing a new disruptive technology in the wild is much harder than anticipated. The new technology must integrate with many other systems, often requiring a wide-reaching redesign. It also requires retraining of employees and consumers. These difficulties slowly push the technology into the Trough of Disillusionment, as people lament that this technology will never work or is too difficult to deal with.

When enough people have given up, but the loyal keep working in dedica- tion, the technology begins to rise again, this time not with the irrational exu-

“BLOCKCHAIN, NOT BITCOIN?” 29

berance of its early years, but instead with a sustained release of improvements and productivity. Over time the technology matures, ultimately becoming a steady platform in the Plateau of Productivity that provides a base on which to build other technologies.

While it’s hard to predict where blockchain technology currently falls on Gartner’s Hype Cycle (these things are always easier in retrospect), we would posit that Bitcoin is emerging from the Trough of Disillusionment. At the same time, blockchain technology stripped of native assets (private blockchain) is descending from the Peak of Inflated Expectations, which it reached in the summer of 2016 just before The DAO hack occurred (which we will discuss in detail in Chapter 5).

Cryptoassets beyond bitcoin are at different points between the Innovation Trigger and the Trough of Disillusionment. These differ because they came to life at different points after bitcoin and many are still emerging. Suffice it to say, the promise is great, the tensions are high, and opportunity awaits the innovative investor. Let’s now take a tour of the various cryptoassets that cur- rently exist.

*This page intentionally left blank*

## Chapter 4

## The Taxonomy of Cryptoassets

s we’ve seen, bitcoin ignited the cryptoasset revolution, and its success has led to the birth of numerous other permissionless (public) block- chains with their own native cryptoassets. We also refer to these as bit-

A

coin’s digital siblings. As of March 2017, there were over 800 cryptoassets with a fascinating family tree, accruing to a total network value1 of over $24 billion.2 At the time, bitcoin was the largest and most widely transacted of these assets by a wide margin, with a network value of $17 billion, accounting for nearly 70 percent of the total network value of cryptoassets. The next largest cryptoasset by network value was Ethereum’s ether at over $4 billion. Yes, the numbers have changed a lot since. Crypto moves fast.

As the investment landscape for cryptoassets continues to grow beyond bitcoin, it’s vital for the innovative investor to understand the historical con- text, categorization, and applicability of these digital siblings, so that potential investment opportunities can be identified. To this end, we aim to provide a historical grounding of who and what led to the creation of many notable cryptoassets. Through this process, we will also introduce more detailed con- cepts that will go into the innovative investor’s toolset when investigating future cryptoassets.

31

32 CRYPTOASSETS

#### CRYPTOCURRENCIES, CRYPTOCOMMODITIES, AND CRYPTOTOKENS

Historically, cryptoassets have most commonly been referred to as *crypto- currencies*, which we think confuses new users and constrains the conver- sation on the future of these assets. We would not classify the majority of cryptoassets as currencies, but rather most are either digital commodities (*cryptocommodities*), provisioning raw digital resources, or digital tokens (*cryptotokens*), provisioning finished digital goods and services.

A currency fulfills three well-defined purposes: to serve as a means of exchange, store of value, and unit of account. However, the form of currency itself often has little inherent value. For example, the paper bills in people’s wallets have about as little value as the paper in their printer. Instead, they have the illusion of value, which if shared widely enough by society and endorsed by the government, allows these monetary bills to be used to buy goods and services, to store value for later purchases, and to serve as a metric to price the value of other things.

Meanwhile, commodities are wide-ranging and most commonly thought of as raw material building blocks that serve as inputs into finished products. For example, oil, wheat, and copper are all common commodities. However, to assume that a commodity must be physical ignores the overarching “offline to online” transition occurring in every sector of the economy. In an increasingly digital world, it only makes sense that we have digital commodities, such as compute power, storage capacity, and network bandwidth.

While compute, storage, and bandwidth are not yet widely referred to as commodities, they are building blocks that are arguably just as important as our physical commodities, and when provisioned via a blockchain network, they are most clearly defined as *cryptocommodities*.

Beyond cryptocurrencies and cryptocommodities—and also provisioned via blockchain networks—are “fi shed-product” digital goods and services like media, social networks, games, and more, which are orchestrated by *crypto- tokens*. Just as in the physical world, where currencies and commodities fuel an economy to create fi shed goods and services, so too in the digital world the infrastructures provided by cryptocurrencies and cryptocommodities are com- ing together to support the aforementioned fi shed-product digital goods and services*.* Cryptotokens are in the earliest stage of development, and will likely be the last to gain traction as they require a robust cryptocurrency and crypto- commodity infrastructure to be built before they can reliably function.

THE TAXONOMY OF CRYPTOASSETS 33

In summation, we believe that a clearer view of this brave new world of blockchain architecture includes *cryptocurrencies*, *cryptocommodities*, and *cryptotokens*, just as we have had currencies, commodities, and finished goods and services in the preceding centuries. Be it a currency, commodity, or ser- vice, blockchain architectures help provision these digital resources in a dis- tributed and market-based manner.

In this chapter, we focus on the most important cryptocurrencies today, including bitcoin, litecoin, ripple, monero, dash, and zcash. The next chapter covers the world of cryptocommodities and cryptotokens, the development of which has been accelerated by the launch of Ethereum and its value proposi- tion as a decentralized world computer. Besides its status as the number two cryptoasset by network value, Ethereum has also spawned many other crypto- assets that creatively utilize its network.

While we cannot possibly cover all the cryptoassets, we will focus on those we believe will help the innovative investor gain the broadest perspective. To those entrepreneurs and developers who’ve created assets that we’re unable to cover here, we apologize. Many amazing projects were created in the process of writing the book, and if we tried to incorporate them all the book would never have been finished. To that end, we’ve included a listing in the resources section to enable access to information on other cryptoassets.

WHY *CRYPTO*?

Sometimes the word *crypto* makes people shudder, perhaps because they associate it with illicit activity, but that’s a mental bias that is important to overcome. Crypto is simply a tip of the hat to and a shortening of the key technology underlying these systems: cryptography. As discussed in Chapter 2, cryptography is the science of securely transmitting data so that only intended recipients can make use of it. Cryptography is used to ensure that cryptoassets are transferred to the intended recipients securely. Given our digital world and the increasing prevalence of hacks, the secure transmission of resources is paramount, and cryptoassets have such security in spades.

#### THE EVER-EVOLVING NATURE OF CURRENCIES

The pursuit of a decentralized, private, and digital currency predates bitcoin by decades. Bitcoin and its digital siblings are just part of a broader evolu- tion of currencies that has taken place over centuries. At their inception,

34 CRYPTOASSETS

currencies were a solution to ease the impreciseness of barter trade, and for centuries metal coins with material value served as the currencies of choice. Fiat currency was an innovation beyond metal coins, as it was much easier to transport, but the entirety of its value relied upon the government’s stamp of approval and mandate of legal tender. We believe that currency void of any physical representation is the next phase of the evolution, and in our Internet- tethered world an inevitable one.

As innovations underlying the Internet gained steam, so too did the real- ization that we would need a secure form of digital payment. One of Bitcoin’s most famous ancestors was pioneered by a company called DigiCash, led by David Chaum, who remains one of the most famous cryptographers in crypto- asset history. In 1993, prior to Marc Andressen founding Netscape, Chaum invented the digital payment system called ecash. This allowed secure and anonymous payments across the Internet, no matter the amount.3

Clearly, Chaum’s timing could not have been better given the tech boom that followed through the mid- to late-1990s, and his company, DigiCash, had several opportunities for growth, any of which might have made it a household name. However, while Chaum was widely regarded as a technical genius, as a businessperson he left much to be desired. Bill Gates approached Chaum about integrating ecash into Windows 95, which would have immediately given it global distribution, but Chaum refused what was rumored to be a

$100 million offer. Similarly, Netscape made initial inquiries about a relation- ship, but management was quickly turned off by Chaum’s attitude. In 1996, Visa wanted to invest $40 million into the company but were dissuaded when Chaum demanded $75 million (if these reports are correct, it’s clear that the potential price for Chaum’s creation was dropping).4

If all had gone well, DigiCash’s ecash would have been integrated into all our web browsers at the ground floor, serving as the global Internet payment mechanism and potentially removing the need for credit cards in online pay- ments. Sadly, mismanagement ultimately ran DigiCash into the ground, and in 1998 it declared bankruptcy. While DigiCash failed to become a household name, some players will resurface in our story, such as Nick Szabo, the father of “smart contracts,” and Zooko Wilcox, the founder of Zcash, both of whom worked at DigiCash for a time.5

Other attempts were made at digital currencies, payment systems, or stores of value after ecash, like e-gold and Karma. The former ran into trouble with the FBI for serving a criminal element,6 while the latter never gained main-

THE TAXONOMY OF CRYPTOASSETS 35

stream adoption.7 The pursuit of a new form of Internet money drew the atten- tion of present day tech-titans such as Peter Thiel and Elon Musk, both of whom had a hand in founding PayPal. Except for Karma, the problem with all these attempts at digital money was that they weren’t purely decentralized— one way or another they relied on a centralized entity, and that presented the opportunity for corruption and weak points for attack.

#### THE MIRACLE OF BITCOIN

One of the most miraculous aspects of bitcoin is how it bootstrapped support in a decentralized manner. The importance, and diffi ulty, of being the fi st currency to do so cannot be emphasized enough. Until people understand how bitcoin works, they often argue that it has no value as currency because, unlike what they’re used to, you can’t see it, touch it, or smell it.

Paper currency has value because it is mutually agreed upon by members of society that it has value. It’s much easier for society to agree to this with a government involved. Getting a global society to agree that something has value and can be used as a currency without government support and without a physical form is one of the most significant accomplishments in monetary history.

When bitcoin was launched, it had zero value in the sense that it could be used to purchase nothing. The earliest adopters and supporters subjectively valued bitcoin because it was a fascinating computer science and game theory experiment. As the utility of Bitcoin’s blockchain proved itself a reliable facili- tator of Money-over-Internet-Protocol (MoIP),8 use cases began to be built using bitcoin, some of which now include facilitating e-commerce, remit- tances, and international business-to-business payments.

Concurrent with the early development of use cases, investors started to speculate on what future use cases would look like and how much bitcoin those use cases would require. Together, the combination of current use cases and investors buying bitcoin based on the expectation for even greater future use cases creates market demand for bitcoin. How much is a buyer willing to pay for something (the bid), and how much is a seller willing to receive to part with that item (the ask)? As with any market, where the bid and ask meet is where the price is set.

36 CRYPTOASSETS

##### Mathematically Metered Supply

One of the keys to supporting bitcoin’s value was its issuance model. Recall from Chapter 2 that miners—the people running the computers building Bitcoin’s blockchain—are paid each time they append a block of transactions. They are paid in new bitcoin created by a *coinbase transaction* that is included in each block.9 For the first four years of Bitcoin’s life, a coinbase transaction would issue 50 bitcoin to the lucky miner. The difficulty of this proof-of-work process was recalibrated automatically every two weeks with the goal of keep- ing the amount of time between blocks at an average of 10 minutes.10 In other words, 50 new bitcoin were released every 10 minutes, and the degree of dif- ficulty was increased or decreased by the Bitcoin software to keep that output time frame intact.

In the first year of bitcoin running, 300 bitcoin were released per hour (60 minutes, 10 minutes per block, 50 bitcoin released per block), 7,200 bitcoin per day, and 2.6 million bitcoin per year.

Based on our evolutionary past, a key driver for humans to recognize some- thing as valuable is its scarcity. Satoshi knew that he couldn’t issue bitcoin at a rate of 2.6 million per year forever, because it would end up with no scarcity value. Therefore, he decided that every 210,000 blocks—which at one block per 10 minutes takes four years—his program would cut in half the amount of bitcoin issued in coinbase transactions.11 This event is known as a “block reward halving” or “halving” for short.

On November 28, 2012, the first halving of the block reward from 50 bitcoin to 25 bitcoin happened, and the second halving from 25 bitcoin to 12.5 bitcoin occurred on July 9, 2016. The third will happen four years from that date, in July 2020.12 Thus far, this has made bitcoin’s supply schedule look somewhat linear, as shown in Figure 4.1.

However, when we step back and take a longer-term perspective, bitcoin’s supply trajectory looks anything but linear (see Figure 4.2). In fact, by the end of the 2020s it will approach a horizontal asymptote, with annual sup- ply inflation less than 0.5 percent. In other words, Satoshi rewarded early adopters with the most new bitcoin to get suffi t support, and in so doing created a big enough base of monetary liquidity for the network to use. He understood that if bitcoin was a success over time its dollar value would increase, and therefore he could decrease the rate of issuance while still rewarding its supporters.

THE TAXONOMY OF CRYPTOASSETS 37

18,000,000

16,000,000

**Number of Bitcoin Outstanding**

14,000,000

12,000,000

10,000,000

8,000,000

6,000,000

4,000,000

2,000,000

0

Jan-09 Jan-10 Jan-11 Jan-12 Jan-13 Jan-14 Jan-15 Jan-16 Jan-17

**Date**

Figure 4.1 n Bitcoin’s supply schedule (short-term view)

Data sourced from [Blockchain.info](http://Blockchain.info/)

25,000,000

20,000,000

**Number of Bitcoin Outstanding**

15,000,000

10,000,000

5,000,000

0

**Date**

Figure 4.2 n Bitcoin’s supply schedule (long-term view)

Long term, the thinking is that bitcoin will become so entrenched within the global economy that new bitcoin will not need to be issued to continue to gain support. At that point, miners will be compensated for processing transactions and securing the network through fees on high transaction volumes.

It’s common to hear that bitcoin supply will max out at 21 million units by 2140. This is a function of continuing to divide the units of supply released by a factor of two every four years. As of January 1, 2017, already 76.6 percent of bitcoin’s supply had been brought into existence,13 and by the time the next

38 CRYPTOASSETS

block reward halving happens in 2020, 87.5 percent of the bitcoin ever to be minted will be in existence. A few years after 2100, we will reach a supply of 20,999,999 bitcoin, which is effectively 21 million. It is bitcoin’s scarce supply schedule that makes many think of it as digital gold.14

#### THE BIRTH OF ALTCOINS

Within a couple years of launching, it had become clear that bitcoin was the first fully decentralized cryptocurrency to gain significant adoption, but there were some aspects with which people were not fully satisfied. For example, bitcoin’s 10-minute block time meant that, depending on when a consumer hit send, it could take up to 10 minutes, sometimes more, for the transaction to be appended to Bitcoin’s blockchain.

Often this delay was more of an issue for the merchant than the consumer, as the merchants needed to know they were getting paid before they could release a good or service. Others worried about bitcoin’s hash function in the proof-of-work process, because hardware was being created that specialized in this hash function and would lead to increased centralization of the min- ing network. For a decentralized currency, increased centralization of the machines that processed its transactions was concerning. Fortunately, Bitcoin’s protocol is open-source software, which meant developers could download the entirety of its source code and tweak the aspects they felt most needed fixing. When the updated software was ready, the developers released it in a manner similar to how Bitcoin was originally released. The new software oper- ated similarly to Bitcoin, but required its own set of developers to maintain it, miners to provide the hardware, and a separate blockchain to keep track of the debits and credits of the new native asset.

Through this combination of open-source software and ingenious program- mers, many other cryptocurrencies have been brought into existence. Those that are only slight modifications of Bitcoin are often referred to as *altcoins*.

BITCOIN’S FIRST DIGITAL SIBLING

Namecoin15 was the first significant fork away from Bitcoin. Interestingly, it was less about creating a new currency and more about utilizing the immu- table nature of the blockchain, a use case we’ll address more in the next chapter. A website created with Namecoin comes with the .bit domain (as

THE TAXONOMY OF CRYPTOASSETS 39

opposed to [the](http://the.com/) [.com](http://the.com/) domain) and provides security and censorship resistance to those sites registered with it.16

Namecoin grew out of an idea on the Bitcointalk forum in 2010 that focused on BitDNS (DNS stands for domain naming service, which handles all web addresses).17 In 2013, a service called NameID was released that uses the Namecoin blockchain to enable the creation of and access to web- sites that have a Namecoin identity.

Namecoin acts as its own DNS service, and provides users with more control and privacy. As opposed to the typical way in which websites are reg- istered through a government controlled service such as ICANN, a Namecoin site is registered through a service that exists on each computer on the Namecoin network. This improves security, privacy, and speed. To gain a .bit site, one must have namecoin to do so, thus the need for the native asset.

##### Litecoin

While a handful of altcoins were released through 2011, Litecoin was the first that would retain significant value to this day. The cryptocurrency was developed by Charlie Lee, an MIT graduate who was a software engineer at Google. When Lee learned of Bitcoin he quickly understood its power, leading him to mine bitcoin before trying to create his own variants. After the unsuc- cessful launch of Fairbrix in September 2011, Lee tried again with Litecoin in October.18

Litecoin aimed to improve upon Bitcoin in two ways. For one, Litecoin’s block times were 2.5 minutes, four times faster than Bitcoin’s, which would be important for merchants needing faster confirmation of consumer’s payments. Second, Litecoin used a different hash function in the proof-of-work pro- cess—also known as a block hashing algorithm—which tried to make the mining process more accessible to hobbyists. To put it into perspective, in the early years of Bitcoin mining, people used central processing units (CPUs), which are the core chips in personal computers, effectively forcing the com- puters to be used solely for mining purposes. In 2010, people after greater efficiency began using the graphic card (GPU) of an existing computer for the

mining process.

Many, including Lee, anticipated a shift to yet more dedicated and special- ized mining devices called ASICs (application-specific integrated circuits). ASICs required custom manufacturing and specifically designed computers.

40 CRYPTOASSETS

As a result, Lee correctly foresaw that bitcoin mining would ramp beyond the reach of hobbyist miners and their homegrown PCs.

Lee wanted a coin that retained its peer-to-peer roots and allowed users to be miners without the need for specialized and expensive mining units. Litecoin accomplished this by using a block hashing algorithm called *scrypt*, which is memory intensive and harder for specialized chips like ASICs to gain a significant edge upon.

Other than these two tweaks, much of Litecoin remained similar to Bitcoin. The innovative investor will have realized, however, that if blocks are issued four times as fast as bitcoin, then the total amount of litecoin released will be four times greater than that of bitcoin. This is exactly the case, as litecoin will converge upon a fixed 84 million units, whereas bitcoin will converge upon a quarter of that, at 21 million units.19 Lee tweaked the halving characteristics, too, so that a halving occurs at 840,000 blocks, as opposed to bitcoin’s 210,000. As Figure 4.3 shows, this puts litecoin on a similar yet larger supply trajectory than bitcoin. Notably, the annual rates of supply inflation are exactly the same

for the number of years the cryptocurrency is from launch.

It’s important to realize that if bitcoin and litecoin are both being used in similar size markets and therefore have the same size network values, a unit of litecoin will be one-fourth as valuable as a unit of bitcoin because there are four times as many units outstanding. This is an important lesson, because all cryptocurrencies differ in their supply schedules, and thus the direct price of each cryptoasset should not be compared if trying to ascertain the apprecia- tion potential of the asset.

90,000,000

80,000,000

**Number of Coins Outstanding**

70,000,000

60,000,000

50,000,000

40,000,000

30,000,000

20,000,000

10,000,000

0

Litecoin Bitcoin

0 4 8 12 16 20 24 28 32 36 40

**Years from Launch**

Figure 4.3 n The comparative supply schedules of Litecoin and Bitcoin

THE TAXONOMY OF CRYPTOASSETS 41

Litecoin’s network is often used as a testing ground for Bitcoin software updates, given that Litecoin is nimbler than Bitcoin because it stores a fraction of the monetary value. It has also been used as the basis for other cryptoassets. At the start of 2017, litecoin was the fourth largest cryptoasset in terms of network value.20

##### Ripple

Ripple is a cryptocurrency created in 2004 by Ryan Fugger, a web developer from Vancouver, British Columbia. Work on the project actually began before Satoshi and Bitcoin,21 when Fugger was searching for a way to allow commu- nities to create a system of money out of chains of trust. For example, if Alice trusts Bob, and Bob trusts Candace, and Candace trusts Dave, then Alice can send money to Dave (whom she doesn’t know) by first transferring value to Bob, who transfers that same value to Candace, who takes that value and depos- its it in Dave’s account. Using this concept, payments can “ripple” through the network via these chains of trust. Fugger called this concept [RipplePay.com.](http://RipplePay.com/)

While Fugger’s RipplePay did grow to 4,000 users,22 it did not catch fire the way bitcoin did. In August 2012, Fugger was approached by the notable finan- cial innovators Chris Larsen and Jed McCaleb. Larsen had founded E-Loan— one of the first companies to provide access to mortgage loans online—and Prosper, a leader in the peer-to-peer lending space.23 McCaleb was the founder of Mt. Gox, the biggest bitcoin and cryptocurrency exchange in the world at that time.

Fugger announced the partnership: “I believe if anyone can develop the Ripple concept on a global scale, they can. Their system is based on a Bitcoin- style blockchain, much as we have discussed here over the last few years as an interesting possibility, but with a novel miner-less consensus mechanism that allows transactions to be confirmed near instantaneously.”

Interestingly, in November 2012, this statement from Fugger appeared on Bitcoin’s dedicated communication channel, a Reddit-style site called bitcoin- talk, under the heading, “Is Ripple a Bitcoin Killer or Complementer? Founder of Mt. Gox will launch Ripple.”24 This would not be the last time someone asked if a new upstart would be a Bitcoin-killer.

Not long after, in the spring of 2013, it was announced that Larsen and McCaleb’s company that developed the Ripple protocol, then called OpenCoin, had secured funding from prestigious venture capitalists, including Andreessen Horowitz.25 This was a notable development—a sign of approval of the viability

42 CRYPTOASSETS

of cryptocurrency from one of the most revered venture capital firms in the world. OpenCoin would later rebrand as Ripple Labs.

Ripple’s technology did several new things. It didn’t have miners. Instead it utilized a consensus algorithm that relied on trusted subnetworks to keep a broader decentralized network of validators in sync. That’s enough to confuse any innovative investor. What’s important to recognize is that Ripple’s con- sensus algorithm relied on trust of some sort, which was vastly different from Bitcoin’s proof-of-work design that assumed anyone could be a bad actor.

Ripple also used trusted gateways as endpoints for users, and these gate- ways could take deposits and redeem debts in all kinds of asset pairs, including traditional fiat currency. This built off Fugger’s original chains of trust but on a global multi-asset scale. Routing a transaction through Ripple’s network was like sending a packet of information through the Internet, pinging amid con- nected servers.

If users didn’t want to rely on these gateways, Ripple also had its own native cryptocurrency, called ripples, and commonly referred to as XRP. XRP could be used to connect two endpoints in the Ripple network that didn’t have a connection of trust.

But this is where the Ripple team ran into contentious territory, even if the concept was born of good intentions. Since there was no mining process, there was no means to distribute XRP. Instead, 100 billion units of XRP were created and initially held by Ripple Labs (at that time, OpenCoin). While there was, and still is, intent to distribute all this XRP to seed use, as of writing the major- ity of XRP is still under the control of Ripple Labs.

This has led to mistrust of the Ripple protocol from much of the cryptocur- rency community. Vitalik Buterin, who would later go on to create Ethereum, wrote in February 2013 for *Bitcoin Magazine*: “Because of the monetary distri- bution, OpenCoin may well face an uphill battle convincing the community that they can be trusted.”26

Pricing services like CoinCap don’t list XRP’s total available supply as the 100 billion that Ripple lists27 but only include the ripple that has thus far been distributed to the public, which is just north of 37 billion units.28 A word to the wise for the innovative investor: with a new cryptocurrency, it’s always impor- tant to understand how it’s being distributed and to whom (we’ll discuss this further in Chapter 12). If the core community feels the distribution is unfair, that may forever plague the growth of the cryptocurrency.

Ripple has since pivoted away from being a transaction mechanism for the common person and instead now “enables banks to send real-time interna-

THE TAXONOMY OF CRYPTOASSETS 43

tional payments across networks.”29 This focus plays to Ripple’s strengths, as it aims to be a speedy payment system that rethinks correspondent banking but still requires some trust, for which banks are well suited.

##### Dogecoin

A somewhat comic cryptocurrency addition arrived on December 8, 2013 (less than two weeks after bitcoin hit a notable high of $1,242) in the form of dogecoin.30 Dogecoin was launched as a riff off Doge the dog, which *Wired* magazine had pegged as 2013’s meme31 of the year.32 Doge was a Shiba Inu dog whose image with captions of an internal monologue went viral.

Dogecoin was initially floated as a joke. Jackson Palmer, who worked in the marketing department of Adobe’s Sydney offices and was a cryptocur- rency enthusiast, sent the tweet: “Investing in Dogecoin, pretty sure it’s the next big thing.”33 After a positive reception to what was intended as a joke, he bought the domain, [Dogecoin.com.](http://Dogecoin.com/) Jackson’s activity caught the attention of Billy Markus, a Portland, Oregon-based developer who aspired to launch a new cryptoasset. In Markus’s own words: “The first thing I said was, ‘This is so funny.’ Then I said, ‘I should just make this coin.’”34

Markus used Litecoin’s code to derive Dogecoin, thereby making it one more degree of separation removed from Bitcoin. If Litecoin was a child of Bitcoin, then Dogecoin was a grandchild of Bitcoin. A notable variation was that Dogecoin planned to issue a much larger amount of dogecoin than bitcoin or even litecoin. The plan was to have 100 billion dogecoin in circulation after

1.5 years.35 That would equal nearly 5,000 times more coins than bitcoin when it reaches its maximum supply.

Markus’s team later chose to issue roughly 5 billion coins each year, and this created a vastly different supply schedule from those of the deflationary bitcoin and litecoin. Dogecoin mostly gained traction amongst Internet tippers. The supply schedule has kept the value of a single dogecoin to a fraction of a cent, which is suited to its intended use case. As Palmer stated in an early interview:

It’s not taking itself as seriously, it’s not being used by people worrying about whether they’ll become rich . . . It’s something to share for thanks or kudos.36

Palmer’s marketing expertise was another feature that differentiated Dogecoin from other cryptocurrencies at the time. The Dogecoin commu-

44 CRYPTOASSETS

nity raised $50,000 via Dogecoin to send the Jamaican bobsled team to the Olympics; raised another $55,000 via Dogecoin to sponsor a NASCAR driver who raced with the Dogecoin logo at the Talladega Speedway; and raised money to support clean water projects in Kenya via Doge4Water, making the donation via a Twitter-based tip service.37

While Dogecoin may have been launched as a joke, its association with a wildly popular Internet meme, its lighthearted origins, and its savvy focus on slick marketing led to a quick rise, and its network value grew to $70 million only seven weeks after launch.38 But that did not last long. As of March 2017, its network value had dipped to slightly above $20 million.

This bizarre merger of a cryptoasset and pop culture is not surprising con- sidering 2013 was the year that the price of bitcoin ranged from $13 in January to over $1,000 in early December.39 The power and enthusiasm of Dogecoin’s user community shouldn’t be dismissed, even if we encourage the innovative investor to do ample due diligence on it as an investment. While Dogecoin had its flaws, it continues to exist and has taught the cryptocurrency space valuable lessons about gathering community support in an Internet era.

AURORACOIN: ICELAND’S NATIONAL CRYPTOCURRENCY?

Much like the anonymous Satoshi, Auroracoin’s creator also had a ficti- tious name: Baldur Friggjar Óðinsson. Baldur created Auroracoin based on Litecoin’s code and decided to “air-drop” the cryptocurrency to Icelanders with the intent of providing 50 percent of all auroracoin in existence to resi- dents. The hope was that such a distribution would jump-start national use of the cryptocurrency.

A key to Baldur’s plan was his access to the government’s national identi- fication system, which led speculators to believe mistakenly that Auroracoin was sponsored by the Icelandic government. In anticipation of the airdrop, speculators bid Auroracoin’s network value over $1 billion.40

By the time the airdrop began on March 25, 2014, speculators had sobered somewhat, and Auroracoin was hovering just over a $100 million network value. By the end of the month, it would be below $20 million, as citizens receiving Auroracoin moved to sell it on exchanges to turn a profi 41 Along with the drop in price was a loss of confi and enthusiasm for the new cryptocurrency. Few, if any, retailers were willing to accept auroracoin, and it was soon considered a “failed experiment.”42 Some also saw it as a scam

THE TAXONOMY OF CRYPTOASSETS 45

perpetrated by its creator. To this day, auroracoin takes the cake as the crypto- currency with the grandest plan for widespread usage throughout one country. It continues to exist, with a handful of Icelandic developers working to revive the concept and the technology. In 2016, ads began to appear through- out Iceland’s capital city of Reykjavik heralding the return of Auroracoin. As a result, beers in Iceland were being purchased for auroracoin,43 and many other retail establishments began to utilize the cryptocurrency. Then a scandal hit and the prime minister was forced to resign because of his involvement with the Panama Papers.44 This led to the growth in popularity of a political party known as the Pirate Party, which had a favorable view on cryptocurrencies.45 Suddenly there was speculation46 that Iceland could revisit the potential for Auroracoin and its role as a national cryptocurrency.47 As acceptance grows and politics change, it will be interesting to watch what happens next for the

Icelandic cryptocurrency.

Auroracoin is a cautionary tale for both investors and developers. What began as a seemingly powerful and compelling use case for a cryptoasset suf- fered from its inability to provide value to the audience it sought to impact. Icelanders were given a cryptocurrency with little education and means to use it. Unsurprisingly, the value of the asset collapsed and most considered it dead. Nevertheless, cryptocurrencies rarely die entirely, and Auroracoin may have interesting times ahead if its developer team can figure out a way forward.

#### THE RACE FOR PRIVACY: DASH, MONERO, AND ZCASH

While Litecoin, Ripple, and Dogecoin all added elements to the mix of what it meant to be a cryptocurrency, they did not provide the privacy that many early Bitcoin advocates yearned for. It is a common misconception, even for Bitcoin, that it is an anonymous payment network. Bitcoin transactions are *pseudony- mous*, and since every transaction can be seen by any third party, there is a wealth of information for anyone who would like to pinpoint who the partici- pants are. Inarguably, someone who wants to use a currency for illegal activity is better off using cash than bitcoin. With every transaction, bitcoin leaves an indelible digital mark in Bitcoin’s blockchain.

Currently, three notable cryptocurrencies put privacy and anonymity first. In order of launch, they are Dash, Monero, and Zcash. All three pursue this value proposition differently. Monero is likely the most relevant to the inno-

46 CRYPTOASSETS

vative investor, with a sustained record of operations, solid cryptography, and a sound issuance model. While Dash has merits, it has contested origins. Meanwhile, Zcash uses some of the most bleeding-edge cryptography in the world, but it is one of the youngest cryptoassets in the book and suitable only for the most experienced cryptoasset investors.

##### Monero and Its Predecessor, Bytecoin

Monero is a descendent of a lesser-known cryptocurrency called Bytecoin. Bytecoin was crafted quite differently from Bitcoin, using technology known as CryptoNote. Similar to Litecoin’s scrypt, CryptoNote’s block hashing algo- rithm aims to avoid the specialization and therefore centralization of the min- ers supporting the network by requiring an order of operations that favors general purpose chips like the CPUs found in PCs.48 Beyond a focus on more egalitarian proof-of-work, CryptoNote provided untraceable payments, unlinkable transactions, and blockchain analysis resistance.49 Adam Back is considered the inspiration for Satoshi’s proof-of-work algorithm and is pres- ident of Blockstream, one of the most important companies in the Bitcoin space. In March 2014, he tweeted about CryptoNote, saying it was one of the few ideas in the cryptocurrency space outside of Bitcoin that held a “defensible rationale for existence.”50

Some may ask why Monero stole the show from Bytecoin. Bytecoin’s block- chain and the issuance of its currency, bytecoin, started on July 4, 2012, but it did not become widely known until almost two years later when an announce- ment for it appeared on [bitcointalk.org](http://bitcointalk.org/) on March 12, 2014.51 People were intrigued but confused about why the Bytecoin team had taken two years to make it public. Some argued that it was because the developers wanted to make sure the technology was soundly running before drawing more atten- tion. Others argued that something more insidious was at play, called a *premine* (pronounced “pre-mine”).

Bytecoin planned to issue 184.46 billion bytecoin via the mining process, but by the time it was made publicly known, 150 billion bytecoin were already in existence, more than 80 percent of the total supply.52 A classic premine, Bytecoin had quietly released a large amount of the coins in a manner that disadvantaged the broader community. Bitcoin and the permissionless block- chain movement was founded on principles of egalitarian transparency, so premines are widely frowned upon. While they still occur, many are scams that the innovative investor should be wary of. A key differentiator between

THE TAXONOMY OF CRYPTOASSETS 47

a scam and good intent is the communication and rationale of the developer team behind the issuance model.

On April 8, 2014, the [bitcointalk.org](http://bitcointalk.org/) user named “eizh,” who would later become a Monero developer, made the comment, “I’m surprised someone hasn’t started a clone for a fairer distribution and active development.”53 On April 9, 2014, only a month after the public announcement of Bytecoin, an involved user known as “thankful\_for\_today,” made a post to [bitcointalk.org](http://bitcointalk.org/) titled “Bitmonero—a new coin based on CryptoNote technology—launched,” with the intent to launch mining in nine days.54 BitMonero was quickly renamed Monero and often referred to as XMR.

The most defining feature of Monero is its use of *ring signatures*, a crypto- graphic technology that had been evolving since 1991.55 Monero’s ring signa- tures are best explained in the context of Bitcoin. In Bitcoin, to create a trans- action, a known individual signs off on the balance of bitcoin he or she is trying to send. In Monero, a group of individuals signs off on a transaction creating a ring signature, but only one in the group owns that monero. The CryptoNote website puts it succinctly:

In the case of ring signatures, we have a group of individuals, each with their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a mem- ber of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.56

While many are suspicious of such privacy, it should be noted that it has tremendous benefits for fungibility. Fungibility refers to the fact that any unit of currency is as valuable as another unit of equal denomination. A danger for bitcoin, especially for balances known to have been used for illegal activity, is that if an exchange or other service blacklists that balance, then that balance becomes illiquid and arguably less valuable than other balances of bitcoin. While subtle, losing fungibility could be the demise of a digital and distributed currency, hurting the value of all units, not just the ones used for illegal activ- ity. Fortunately, this is one problem that Monero does not have to deal with.

48 CRYPTOASSETS

Monero’s supply schedule is a hybrid of Litecoin and Dogecoin. For monero, a new block is appended to its blockchain every 2 minutes, similar to Litecoin’s

2.5 minutes. Like Dogecoin, however, it will have a small degree of inflation for its entire life beginning in May 2022, when 0.3 monero will be released every minute, totaling 157,680 monero every year. At that time, there will be 18.1 million units of monero outstanding, so inflation in that first year will be only

0.87 percent.57 As we head further into the future, that inflation decreases as the base of monero outstanding increases. Interestingly, in 2040 there will be nearly equivalent units of bitcoin and monero outstanding, and in the period of 2019 to 2027, Monero’s rate of supply inflation will be lower than Bitcoin’s, but in all other periods the opposite is true.58

Expectedly, Monero’s ability to create privacy in transactions was a techno- logical breakthrough that was recognized within the cryptoasset community and the markets. By the end of 2016, Monero had the fifth largest network value of any cryptocurrency and was the top performing digital currency in 2016, with a price increase over the year of 2,760 percent. This clearly demon- strates the level of interest in privacy protecting cryptocurrency. Some of that interest, no doubt, comes from less than savory sources.

##### Dash

Another cryptocurrency targeting privacy and fungibility is Dash. It launched its blockchain a few months before Monero, on January 19, 2014. Its lead developer, Evan Duffield, created Dash by forking the Bitcoin protocol and implementing a coin focused on privacy and speedy settlement of transac- tions. The Dash white paper that Duffield coauthored outlined his intent:

A crypto-currency based on Bitcoin, the work of Satoshi Nakamoto, with various improvements such as a two-tier incen- tivized network, known as the Masternode network. Included are other improvements such as Darksend, for increasing fungibility and InstantX which allows instant transaction confirmation with- out a centralized authority.59

Dash, however, got off to a rocky start. Instead of a premine, it had what is called an *instamine*, where 1.9 million coins were created in the first 24 hours. Considering that three years later, in January 2017, there were just north of 7 million coins, this was a significant error that drastically benefited the com-

THE TAXONOMY OF CRYPTOASSETS 49

puters that supported the Dash network in the first 24 hours, notably Duffield himself.

Duffield reasonably pleaded best intentions, arguing that, “I was working a very challenging day job while working on Dash in the first couple weeks. So I was putting out fires every night, keeping tabs on Dash during the day (while getting yelled at by my boss when he caught me a couple times).”60

From our perspective, if there is a major disruption or error in the launch of a cryptocurrency that significantly skews its distribution, then that crypto- currency should be relaunched. In fact, Duffield easily could have relaunched Dash, especially considering the network was only days old when the insta- mine began to be widely talked about, but he chose not to. It wouldn’t have been unusual to relaunch, given that other cryptocurrencies have done so via the forking of original code. The creators of Monero, for example, specifically chose not to continue building off Bytecoin because the premine distribution had been perceived as unfair.

##### Zcash

The most interest in a cryptocurrency in 2016 was generated by a new crypto- asset called Zcash. The Bitcoin and blockchain community has always been excited by new developments in anonymity and privacy, but Zcash took that excitement to a new level, which upon issuance drove the price through the roof. Like bitcoin’s, zcash’s issuance model was ethical. However, when bitcoin launched from zero units outstanding, next to no one knew about it. When zcash launched from zero units outstanding, it seemed like the entire crypto- universe knew about it, and everyone wanted some.

The scarcity in initial supply combined with the hype pushed the price of zcash to astronomical levels. It quickly reached $1,000 per coin, which at the time was even higher than the price of bitcoin. At one point on Poloniex, a popular cryptoasset exchange, the price reached 1 zcash for 3,299 bitcoin, or almost $2 million at the time.61 However, by the end of 2016, the hysteria had dissipated and zcash was trading in a stable range of $45 to $50.

The Zcash team is led by Zooko Wilcox, whom we have mentioned prior as an early employee at David Chaum’s DigiCash. Through his time at DigiCash and longstanding involvement in cryptography and cryptoassets, Zooko has become one of the most respected members in the community. A key inno- vation of Zcash is the use of a type of zero-knowledge proof, referred to as zk-SNARKs, which allow transactions to be sent between parties without any

50 CRYPTOASSETS

information being revealed other than the validity of the transaction. While it is still early days for Zcash, we are of the belief that the ethics and technology chops of Zooko and his team are top-tier, implying that good things lie in wait for this budding cryptocurrency.

• • •

By the end of 2016, the price of bitcoin had reached a level just below $1,000 (which it broke in January 2017), and there were over 800 cryptoassets in a market that totaled over $17 billion. At that time, the top assets in order of network value were: Bitcoin, Ethereum, Ripple, Litecoin, Monero, Ethereum Classic, and Dash.

The innovative investor may note from this list that Ethereum follows Bitcoin. Its story is one that includes brilliant developers, a wider definition of blockchain technology, and one of the largest hacks on a cryptoasset ecosys- tem to date. In the next chapter, we’ll look at the creation of Ethereum and the significant impact it has and will have on the future of cryptoassets.

## Chapter 5

## Cryptocommodities and Cryptotokens

ryptocurrencies are a powerful vertical of cryptoassets, but as we laid out in the start of the last chapter, only one of three. The other two, cryptocommodities and cryptotokens, are a rapidly growing segment

C

of this budding new asset class. First, let’s look at cryptocommodities.

In some ways, cryptocommodities are more tangible in value than crypto- currencies. For example, the largest cryptocommodity, Ethereum, is a decen- tralized world computer upon which globally accessible and uncensored applications can be built. It’s easy to appreciate the value of using such a com- puter, and therefore Ethereum provides a digitally tangible resource. Paying to use Ethereum’s world computer—also known as the Ethereum Virtual Machine (EVM)—is reminiscent of when schools and libraries had shared computers that students could use. One person could sit down and use a com- puter for a while before moving on, and then another person would come and use it.

The Ethereum Virtual Machine operates somewhat similarly to a shared computer, except it is global in scale and more than one user can operate it at a time. Just as everyone can see Bitcoin transactions from anywhere in the world, anyone can see Ethereum’s programs running from anywhere in the world. While this chapter will dive deep into Ethereum as a cryptocommodity, there are many other budding cryptocommodities, provisioning decentralized

51

52 CRYPTOASSETS

resources like cloud storage, bandwidth, transcoding, proxy re-encryption, and so on.

#### THE IDEA BEHIND ETHEREUM’S WORLD COMPUTER

The founding team of Ethereum and its native asset, ether, weren’t the first to dream of globally distributed computer programs, or what are commonly referred to as smart contracts. For example, Nick Szabo, who was also one of Chaum’s disciples at DigiCash (Chapter 4), had been talking about smart contracts and digital property since the early 1990s. In 1996, he published an article in the magazine *Extropy* on the topic entitled “Smart Contracts.”1

Smart contracts are critical to understand but have a misleading name. The first thing people think of when they hear smart contracts is legal documents that think for themselves, which misses the mark by a wide margin. We believe smart contracts are better thought of as *conditional transactions* because they refer to logic written in code that has “IF this, THEN that” conditions. For example, it can easily be programmed in a smart contract that “IF Jack misses his flight and IF it was the airline’s fault, THEN the airline pays him the cost of the flight.” A vending machine is another commonly used example of a smart contract: “IF the user puts in enough money and IF the user types in the right code, THEN the user gets Doritos.” These conditions can become much more complex, creating conditional waterfalls depending on the process being pro- grammed and the variables that need to be met.

While Szabo had the early vision for smart contracts, the Ethereum team would be the first to create a mainstream and attention-grabbing platform to execute smart contracts in a decentralized manner. At the core of the team is Vitalik Buterin, who many regard as Ethereum’s Satoshi.

Buterin was born in Russia but grew up in Canada. He had the good for- tune of a freethinking father,2 who in February 2011 introduced 17-year-old Buterin to Satoshi’s work and Bitcoin.3 Bitcoin had only been functioning for two years at that point, and no major alternative was in existence. It would not be until October of that year that Charlie Lee would release Litecoin.

It wasn’t long before Buterin fell down the Bitcoin rabbit hole. He quickly became one of the fi st well-known journalists pioneering the world of crypto- assets, even cofounding *Bitcoin Magazine*, which remains one of the best deep dive sites for technical analysis of blockchain architectures. While writing arti- cles that merged sophisticated technical information with an enthusiastic and optimistic style, he used his mathematical prowess to consider how to improve

CRYPTOCOMMODITIES AND CRYPTOTOKENS 53

on the technology. He was, after all, a Bronze medal winner at the International Olympiad in Informatics4 at the age of 18 and could reportedly add three-digit numbers in his head at twice the speed of the average human being.5

To that end, Buterin tinkered with a number of Bitcoin projects that would inform his future work on Ethereum. In a blog post titled “Ethereum: Now Going Public,” he started with a tip of the hat to Bitcoin:

I fi wrote the initial draft of the Ethereum whitepaper on a cold day in San Francisco in November, as a culmination of months of thought and often frustrating work into an area that we have come to call “cryptocurrency 2.0”—in short, using the Bitcoin blockchain for more than just money. In the months leading up to the development of Ethereum, I had the privilege to work closely with several projects attempting to implement colored coins, smart property, and various types of decentralized exchange.6

The projects Buterin references in the last sentence approached the transac- tion of bitcoin using Bitcoin’s blockchain more abstractly. As we have already learned, transacting bitcoin involves the transmission of information that results in a debit or credit of a balance of bitcoin in a user’s address.

In his blog post, Buterin mentions *colored coins*. These involve the marking of an address in Bitcoin with information beyond just the balance of bitcoin in that address. Further identifiers could also be appended to the address, such as information that represented ownership of a house. In transferring that bit- coin in that address to another address, so too went the marker of information about house ownership.

In this sense, by sending bitcoin, the transaction also signified the transac- tion of property rights to a house. There are several regulatory authorities that need to recognize that transfer for this example to become an everyday reality, but the point is to show how all kinds of value can be transmitted through Bitcoin’s blockchain.

COUNTERPARTY: SMART CONTRACTS ON BITCOIN

Counterparty is a cryptocommodity that runs atop Bitcoin, and was launched in January 2014 with a similar intent as Ethereum. It has a fixed supply of

54 CRYPTOASSETS

2.6 million units of its native asset, XCP, which were all created upon launch. As described on Counterparty’s website, “Counterparty enables anyone to write specific digital agreements, or programs known as Smart Contracts, and execute them on the Bitcoin blockchain.”7 Since Bitcoin allows for small amounts of data to be transmitted in transactions and stored on Bitcoin’s blockchain, it becomes the system of record for Counterparty’s more flexible functionality. Since Counterparty relies upon Bitcoin, it does not have its own mining ecosystem.

The reason Bitcoin developers haven’t added extra functionality and flex- ibility directly into its software is that they have prioritized security over com- plexity. The more complex transactions become, the more vectors there are to exploit and attack these transactions, which can affect the network as a whole. With a focus on being a decentralized global currency, Bitcoin devel- opers have decided bitcoin transactions don’t need all the bells and whistles. Instead, other developers can either find ways to build atop Bitcoin’s limited functionality, turning to Bitcoin’s blockchain as a system of record and means of security (e.g., Counterparty), or build an entirely different blockchain system (e.g., Ethereum).

Many were working on building this decentralized future on top of Bitcoin, but it wasn’t easy. The fl bility in adding identifi s to addresses and creating different kinds of transactions was purposefully restricted in Bitcoin for the sake of scalability and security. Bitcoin, after all, was still an experiment. A decentralized currency was enough of a holy grail for Satoshi, and he didn’t have to swallow the whole world in one bite. But Buterin wasn’t satisfi d with Bitcoin as it was and had wide-ranging aspirations for improvements. He wanted a system that was more fl ble and that behaved more like a computer and less like a calculator for debits and credits of bit- coin balances.

Although he invented Ethereum in 2013, Buterin formally announced it in January 2014 at the North American Bitcoin Conference,8 where he was sur- rounded by eager reporters, many of whom had been his colleagues in months past. By that time, he had already garnered the support of over 15 developers and dozens in the community outreach team.9

In Ethereum’s white paper that initially described its inner workings, Buterin’s team made no qualms about their aspirations:

CRYPTOCOMMODITIES AND CRYPTOTOKENS 55

What is more interesting about Ethereum, however, is that the Ethereum protocol moves far beyond just currency. Protocols around decentralized file storage, decentralized computation and decentralized prediction markets, among dozens of other such concepts, have the potential to substantially increase the efficiency of the computational industry, and provide a massive boost to other peer-to-peer protocols by adding for the first time an economic layer.10

Importantly, Buterin did not intend for Ethereum and its native asset, ether, to be a minor variation on Bitcoin’s codebase. This distinguished Ethereum from many of the altcoins that came before it.

By having no affiliation with “coin” in its name, Ethereum was mov- ing beyond the idea of currency into the realm of *cryptocommodities.* While Bitcoin is mostly used to send monetary value between people, Ethereum could be used to send information between programs. It would do so by building a decentralized world computer with a *Turing complete programming language*.11 Developers could write programs, or applications, that would run on top of this decentralized world computer. Just as Apple builds the hard- ware and operating system that allows developers to build applications on top, Ethereum was promising to do the same in a distributed and global system. Ether, the native unit, would come into play as follows:

Ether is a necessary element—a fuel—for operating the distrib- uted application platform Ethereum. It is a form of payment made by the clients of the platform to the machines executing the requested operations. To put it another way, ether is the incen- tive ensuring that developers write quality applications (wasteful code costs more), and that the network remains healthy (people are compensated for their contributed resources).12

Miners of Ethereum would be processing transactions that could transfer not just ether but also information among programs. Just as Bitcoin miners were compensated for supporting the network by earning bitcoin, so too would Ethereum miners by earning ether, and the process would be supported by a similar proof-of-work consensus mechanism.

56 CRYPTOASSETS

#### GETTING ETHEREUM OFF THE GROUND

Buterin understood that building a system from the ground up required a sig- nificant amount of work, and his announcement in January 2014 involved the collaboration of a community of more than 15 developers and dozens of com- munity members that had already bought into the idea. Satoshi’s announce- ment of Bitcoin, in contrast, had involved a quiet mailing of the white paper to a relatively unknown mailing list composed mainly of academics and hard- core cryptographers. The ensuing development of the Bitcoin software before launch mostly involved just two people, Satoshi and Hal Finney.13

Buterin also knew that while Ethereum could run on ether, the people who designed it couldn’t, and Ethereum was still over a year away from being ready for release. So he found funding through the prestigious Thiel Fellowship. Billionaire Peter Thiel, who cofounded PayPal and was Facebook’s first outside investor, created the Thiel Fellowship to reward talented individuals who leave the traditional path of college and pursue immediate ways to make an impact in the world. Winners might conduct scientific research, create a startup, or find other ways to improve society and the world. Thiel Fellowship’s care- fully chosen visionaries receive $100,000 over the course of two years, and the award has been considered more competitive than gaining acceptance to the world’s best universities. In June 2014, Buterin received the Thiel Fellowship14 as a 20-year-old dropping out of the University of Waterloo to pursue his inter- est in Ethereum on a full-time basis.

While Buterin may go down as one of Thiel’s greatest investments, Thiel wasn’t alone in recognizing the potential of Ethereum. In 2014, Buterin was given the World Technology Award in Information Technology Software,15 alongside influential names such as Elon Musk in the Energy category and Walter Isaacson in Media & Journalism.

While the Thiel Fellowship was an indication of what was to come for Buterin, $100,000 wasn’t enough to sustain his team. To that end, from July 23, 2014, to September 2, 2014, they staged a 42-day presale of ether, the crypto- commodity underlying the Ethereum network.16

Ether was sold at a range of 1,337 to 2,000 ether per bitcoin, with 2,000 ether per bitcoin on offer for the first two weeks of the presale and then declin- ing linearly toward 1,337 ether per bitcoin in the latter half of the sale, creating momentum by incentivizing people to buy in at the beginning. Overseeing the legal and financial nuances around this sale was the newly created Ethereum Foundation headquartered in Zug, Switzerland.17

CRYPTOCOMMODITIES AND CRYPTOTOKENS 57

Ethereum’s fund-raising effort was not only innovative and timely, it was also record-breaking. The public invested 31,591 bitcoin, worth $18,439,086, for a total of 60,102,216 ether—an implied rate of $0.31 per ether. At the time, it was the largest single crowdfunding effort.18 Some thought it outrageous that the team supporting a blockchain architecture could raise $18 million without a functioning product, as this was clearly different from Bitcoin’s process.

Venture capital investors (VCs) often invest in ideas and development teams, having faith they will work their way toward success. Ethereum democ- ratized that process beyond VCs. For perspective on the price of ether in this crowdsale, consider that at the start of April 2017, ether was worth $50 per unit, implying returns over 160x in under three years.19 Just over 9,000 peo- ple bought ether during the presale, placing the average initial investment at

$2,000, which has since grown to over $320,000.20

According to the Ethereum white paper, the profits from this sale would be “used entirely to pay salaries and bounties to developers, and invested into various for-profit and non-profit projects in the Ethereum and crypto- currency ecosystem.” In addition to the 60 million ether sold to the public, roughly 6 million was created to compensate early contributors to Ethereum, and another 6 million for long-term reserves of the Ethereum Foundation.

The extra allocation of 12 million ether for the early contributors and Ethereum Foundation has proved problematic for Ethereum over time, as some feel it represented double dipping. In our view, with 15 talented develop- ers involved prior to the public sale, 6 million ether translated to just north of $100,000 per developer at the presale rate, which is reasonable given the market rate of such software developers.

That said, the allocation of capital into founders’ pockets is an important aspect of crowdsales. Called a “founder’s reward,” the key distinction between understandable and a red flag is that the founders should be focused on build- ing and growing the network, not fattening their pockets at the expense of investors. In our opinion, the Ethereum developers were not fattening their pockets, they were putting food on the table. Their modest allocation is a far cry from the antics that some cryptoasset creators have attempted since.

Following the presale, it was a year of development before the Ethereum network went live. During this time, the Ethereum team stayed in close touch with its burgeoning community, releasing proof-of-concepts for the commu- nity to evaluate, organizing conferences, funding projects based on Ethereum, and writing frequent blog updates.21 Perhaps taking note from Dogecoin, the Ethereum team understood the importance of the community in bootstrap-

58 CRYPTOASSETS

ping support for its decentralized system. Although blockchain architectures are cold code, they are warm social networks.

With the money they raised, the Ethereum team was also able to test the network before launch in a way that Satoshi and his small group of support- ers were not able to. Starting at the end of 2014 and for the first half of 2015, the Ethereum Foundation encouraged battle testing of its network, both in a grassroots bug bounty program and in formal security audits that involved professional third-party software security firms.22 The innovative investor should take note of this battle-testing practice, which we also saw with Zcash, as it is an indicator of how seriously core developers take security in their decentralized architectures.

#### ETHEREUM AS A PLATFORM FOR dAPPS

Ethereum’s network with its underlying blockchain went live on July 30, 2015. While much development energy had gone into creating the Ethereum soft- ware, this was the first time that miners could get involved because there was finally a blockchain for them to support. Prior to this launch, Ethereum was quite literally suspended in the ether. Now, Ethereum’s decentralization plat- form was open for business, serving as the hardware and software base for decentralized applications (dApps). These dApps can be thought of as complex smart contracts, and could be created by developers independent of the core Ethereum team, providing leverage to the reach of the technology.

To explain how a dApp works, we’ll use an example from the company Etherisc, which created a dApp for flight insurance to a well-known Ethereum conference. This flight insurance was purchased by 31 of the attendees.23 Figure 5.1 shows a simplified diagram. Using Ethereum, developers can mimic insurance pools with strings of conditional transactions. Open sourcing this process and running it on top of Ethereum’s world computer allows everyday investors to put their capital in an insurance pool to earn returns from the purchasers of insurance premiums that are looking for coverage from certain events. Everyone trusts the system because it runs in the open and is auto- mated by code.

#### WELCOME TO THE AGE OF dAPPS AND CRYPTOTOKENS

Since the launch of Ethereum, a near endless stream of dApps have been released to run on it, many of which have their own native unit. We refer to

CRYPTOCOMMODITIES AND CRYPTOTOKENS 59

**Flight Insurance**

Flight Unsuccessful

Flight Successful

Fault of Airline

Fault of Passenger

No Payment

Payment Made

No Payment

Figure 5.1 n Hypothetical dApp-based flight insurance

many of these dApp native units as cryptotokens, while others refer to them as *appcoins*. A dApp with its own native cryptotoken will use ether as a crypto- commodity to pay the Ethereum network to process certain dApp transac- tions. While many dApps use a cryptotoken, the native units of some dApps should be classified as a cryptocommodity layered on top of Ethereum, like Golem, which aims to be a supercomputer for compute intensive problems. The difference boils down to whether a raw digital resource is being provi- sioned (cryptocommodity) or if the dApp is providing a consumer-facing fin- ished digital good or service (cryptotoken).

Most cryptotokens are not supported by their own blockchain. Often these cryptotokens operate within applications that are built on a cryptocom- modity’s blockchain, such as Ethereum. To continue with the Apple analogy: applications in Apple’s App Store don’t have to build their own operating sys- tems, they run on Apple’s operating system. Due to Ethereum’s wild success, other decentralized world computers have popped up, such as Dfinity, Lisk, Rootstock, Tezos, Waves, and more that can support their own dApps. Just as many altcoins tried to improve upon Bitcoin, these platforms are cryptocom- modities that aim to improve upon Ethereum’s design, thereby attracting their own dApps and associated cryptotokens.

A full list of Ethereum dApps can be seen and explored here: [http://dapps](http://dapps.ethercasts.com/)

[.ethercasts.com/.](http://dapps.ethercasts.com/) The code of many can be investigated in full here: https://live