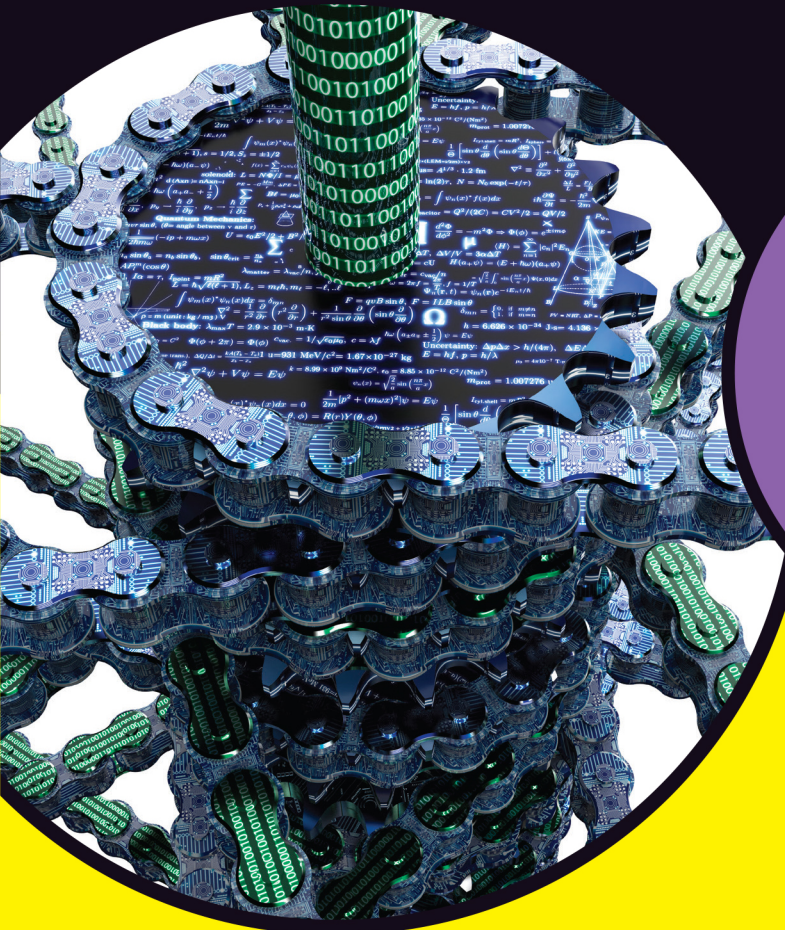


LEARNING MADE EASY



# Blockchain

for  
**dummies**<sup>®</sup>  
A Wiley Brand



Get to know the  
potential of blockchain

Find ways blockchain can  
improve your business

Get tips on enhancing data  
security with blockchain

**Tiana Laurence**

Co-founder of Factom



# Blockchain

for  
**dummies**<sup>®</sup>  
A Wiley Brand





# Blockchain

by Tiana Laurence

for  
**dummies**<sup>®</sup>  
A Wiley Brand

## Blockchain For Dummies®

Published by: **John Wiley & Sons, Inc.**, 111 River Street, Hoboken, NJ 07030-5774, [www.wiley.com](http://www.wiley.com)

Copyright © 2017 by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit <https://hub.wiley.com/community/support/dummies>.

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

Library of Congress Control Number: 2017936813

ISBN 978-1-119-36559-4 (pbk); ISBN 978-1-119-36561-7 (ebk); ISBN 978-1-119-36560-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

# Contents at a Glance

---

|  |     |
|--|-----|
| <b>Introduction</b> .....  | 1   |
| <b>Part 1: Getting Started with Blockchain</b> .....             | 5   |
| CHAPTER 1: Introducing Blockchain .....                          | 7   |
| CHAPTER 2: Picking a Blockchain .....                            | 17  |
| CHAPTER 3: Getting Your Hands on Blockchain .....                | 25  |
| <b>Part 2: Developing Your Knowledge</b> .....                   | 39  |
| CHAPTER 4: Beholding the Bitcoin Blockchain .....                | 41  |
| CHAPTER 5: Encountering the Ethereum Blockchain .....            | 51  |
| CHAPTER 6: Regarding the Ripple Blockchain .....                 | 65  |
| CHAPTER 7: Finding the Factom Blockchain .....                   | 75  |
| CHAPTER 8: Digging into DigiByte .....                           | 89  |
| <b>Part 3: Powerful Blockchain Platforms</b> .....               | 97  |
| CHAPTER 9: Getting Your Hands on Hyperledger .....               | 99  |
| CHAPTER 10: Applying Microsoft Azure .....                       | 109 |
| CHAPTER 11: Getting Busy on IBM Bluemix .....                    | 119 |
| <b>Part 4: Industry Impacts</b> .....                            | 129 |
| CHAPTER 12: Financial Technology .....                           | 131 |
| CHAPTER 13: Real Estate .....                                    | 141 |
| CHAPTER 14: Insurance .....                                      | 151 |
| CHAPTER 15: Government .....                                     | 159 |
| CHAPTER 16: Other Industries .....                               | 171 |
| <b>Part 5: The Part of Tens</b> .....                            | 179 |
| CHAPTER 17: Ten Free Blockchain Resources .....                  | 181 |
| CHAPTER 18: The Ten Rules to Never Break on the Blockchain ..... | 185 |
| CHAPTER 19: Ten Top Blockchain Projects .....                    | 193 |
| <b>Index</b> .....   | 201 |





# Table of Contents

---

|  |    |
|--|----|
| <b>INTRODUCTION</b> .....                                | 1  |
| About This Book .....                                    | 1  |
| Foolish Assumptions .....                                | 2  |
| Icons Used in This Book .....                            | 2  |
| Beyond the Book .....                                    | 3  |
| Where to Go from Here .....                              | 3  |
| <br>   |    |
| <b>PART 1: GETTING STARTED WITH BLOCKCHAIN</b> .....     | 5  |
| <br>   |    |
| <b>CHAPTER 1: Introducing Blockchain</b> .....           | 7  |
| Beginning at the Beginning: What Blockchains Are .....   | 7  |
| What blockchains do .....                                | 8  |
| Why blockchains matter .....                             | 9  |
| The Structure of Blockchains .....                       | 10 |
| Blockchain Applications .....                            | 11 |
| The Blockchain Life Cycle .....                          | 11 |
| Consensus: The Driving Force of Blockchains .....        | 12 |
| Blockchains in Use .....                                 | 14 |
| Current blockchain uses .....                            | 14 |
| Future blockchain applications .....                     | 15 |
| <br>   |    |
| <b>CHAPTER 2: Picking a Blockchain</b> .....             | 17 |
| Where Blockchains Add Substance .....                    | 17 |
| Determining your needs .....                             | 18 |
| Defining your goal .....                                 | 19 |
| Choosing a Solution .....                                | 19 |
| Drawing a blockchain decision tree .....                 | 21 |
| Making a plan .....                                      | 22 |
| <br>   |    |
| <b>CHAPTER 3: Getting Your Hands on Blockchain</b> ..... | 25 |
| Diving into the Bitcoin Blockchain .....                 | 25 |
| Creating your first Bitcoin wallet .....                 | 26 |
| Creating a second Bitcoin wallet .....                   | 27 |
| Generating a Bitcoin vanity address .....                | 27 |
| Transferring your vanity address .....                   | 28 |
| Making an entry into the Bitcoin blockchain .....        | 29 |
| Reading a blockchain entry in Bitcoin .....              | 29 |
| Using Smart Contracts with Bitcoin .....                 | 30 |
| Building your first smart bond .....                     | 31 |
| Checking the status of your contract .....               | 33 |

|   |           |
|---|-----------|
| Building a Private Blockchain with Docker and Ethereum . . . . .    | 34        |
| Preparing your computer . . . . .                                   | 34        |
| Building your blockchain . . . . .                                  | 36        |
| <b>PART 2: DEVELOPING YOUR KNOWLEDGE . . . . .</b>                  | <b>39</b> |
| <b>CHAPTER 4: Beholding the Bitcoin Blockchain . . . . .</b>        | <b>41</b> |
| Getting a Brief History of the Bitcoin Blockchain . . . . .         | 42        |
| Debunking Some Common Bitcoin Misconceptions . . . . .              | 45        |
| Bitcoin: The New Wild West . . . . .                                | 47        |
| Fake sites . . . . .  | 47        |
| No, you first! . . . . .  | 47        |
| Get-rich-quick schemes . . . . .                                    | 48        |
| Mining for Bitcoins . . . . .                                       | 48        |
| Making Your First Paper Wallet . . . . .                            | 49        |
| <b>CHAPTER 5: Encountering the Ethereum Blockchain . . . . .</b>    | <b>51</b> |
| Exploring the Brief History of Ethereum . . . . .                   | 52        |
| Ethereum: The Open-Source World Wide Computer . . . . .             | 53        |
| Decentralized applications: Welcome to the future . . . . .         | 54        |
| The power of decentralized autonomous organizations . . . . .       | 54        |
| Hacking a Blockchain . . . . .                                      | 57        |
| Understanding smart contracts . . . . .                             | 58        |
| Discovering the cryptocurrency Ether . . . . .                      | 58        |
| Getting Up and Running on Ethereum . . . . .                        | 59        |
| Mining for ether . . . . .  | 59        |
| Setting up your Ethereum wallet . . . . .                           | 60        |
| Building Your First Decentralized Autonomous Organization . . . . . | 60        |
| Test net and congress . . . . .                                     | 61        |
| Governance and voting . . . . .                                     | 62        |
| Uncovering the Future of DAOs . . . . .                             | 63        |
| Putting money in a DAO . . . . .                                    | 63        |
| Building smarter smart contracts . . . . .                          | 64        |
| Finding bugs in the system . . . . .                                | 64        |
| <b>CHAPTER 6: Regarding the Ripple Blockchain . . . . .</b>         | <b>65</b> |
| Getting a Brief History of the Ripple Blockchain . . . . .          | 66        |
| Ripple: It's All About Trust . . . . .                              | 67        |
| Seeing How Ripple Differs from Other Blockchains . . . . .          | 68        |
| Unleashing the Full Power of Ripple . . . . .                       | 71        |
| Exercising Caution with Ripple . . . . .                            | 72        |

|   |     |
|---|-----|
| <b>CHAPTER 7: Finding the Factom Blockchain</b>             | 75  |
| A Matter of Trust   | 76  |
| The purpose of the Factom blockchain: Publishing anything   | 77  |
| Incentives of federation                                    | 78  |
| Building on Factom  | 81  |
| Authenticating documents and building identities using APIs | 81  |
| Getting to know the Factoid: Not a normal token             | 81  |
| Anchoring your application                                  | 82  |
| Publishing on Factom  | 82  |
| Building transparency in the mortgage industry              | 84  |
| Verifying physical documents: dLoc with Factom              | 86  |
| <b>CHAPTER 8: Digging into DigiByte</b>                     | 89  |
| Getting Familiar with DigiByte: The Fast Blockchain         | 90  |
| Mining on DigiByte  | 91  |
| Signing Documents on DigiByte's DiguSign                    | 94  |
| Earning DigiBytes While Gaming                              | 95  |
| <b>PART 3: POWERFUL BLOCKCHAIN PLATFORMS</b>                | 97  |
| <b>CHAPTER 9: Getting Your Hands on Hyperledger</b>         | 99  |
| Getting to Know Hyperledger: Dreams of a Hyper Future       | 100 |
| Focusing on Fabric  | 101 |
| Building your system in Fabric                              | 102 |
| Diving into chaincode development                           | 102 |
| Investigating the Iroha Project                             | 104 |
| Introducing Sumeragi: The new consensus algorithm           | 104 |
| Developing mobile apps                                      | 105 |
| Diving into Sawtooth Lake                                   | 106 |
| Exploring the consensus algorithm: Proof of Elapsed Time    | 107 |
| Deploying Sawtooth  | 107 |
| <b>CHAPTER 10: Applying Microsoft Azure</b>                 | 109 |
| Bletchley: The Modular Blockchain Fabric                    | 109 |
| Cryptlets for encrypting and authenticating                 | 111 |
| Utility and Contract Cryptlets and CryptoDelegates          | 112 |
| Building in the Azure Ecosystem                             | 113 |
| Getting Started with Chain on Azure                         | 114 |
| Installing Chain's distributed ledger                       | 115 |
| Creating your own private network                           | 115 |
| Using financial services on Azure's Chain                   | 116 |

|   |            |
|---|------------|
| Deploying Blockchain Tools on Azure . . . . .                     | 116        |
| Exploring Ethereum on Azure . . . . .                             | 116        |
| Cortana: Your analytics machine learning tool . . . . .           | 117        |
| Visualizing your data with Power BI . . . . .                     | 117        |
| Managing your access on Azure's Active Directory . . . . .        | 118        |
| <b>CHAPTER 11: Getting Busy on IBM Bluemix . . . . .</b>          | <b>119</b> |
| Business Blockchain on Bluemix . . . . .                          | 119        |
| Your isolated environment . . . . .                               | 120        |
| Bluemix use cases . . . . .                                       | 121        |
| Watson's Smart Blockchain . . . . .                               | 122        |
| Building Your Starter Network on Big Blue . . . . .               | 124        |
| <br>  |            |
| <b>PART 4: INDUSTRY IMPACTS . . . . .</b>                         | <b>129</b> |
| <br>  |            |
| <b>CHAPTER 12: Financial Technology . . . . .</b>                 | <b>131</b> |
| Hauling Out Your Crystal Ball: Future Banking Trends . . . . .    | 131        |
| Moving money faster: Across borders and more . . . . .            | 133        |
| Creating permanent history . . . . .                              | 134        |
| Going International: Global Financial Products . . . . .          | 135        |
| Border-free payroll . . . . .                                     | 136        |
| Faster and better trade . . . . .                                 | 137        |
| Guaranteed payments . . . . .                                     | 138        |
| Micropayments: The new nature of transactions . . . . .           | 138        |
| Squeezing Out Fraud . . . . .                                     | 139        |
| <br>  |            |
| <b>CHAPTER 13: Real Estate . . . . .</b>                          | <b>141</b> |
| Eliminating Title Insurance . . . . .                             | 141        |
| Protected industries . . . . .                                    | 142        |
| Consumers and Fannie Mae . . . . .                                | 144        |
| Mortgages in the Blockchain World . . . . .                       | 144        |
| Reducing your origination costs . . . . .                         | 145        |
| Knowing your last-known document . . . . .                        | 145        |
| Forecasting Regional Trends . . . . .                             | 146        |
| The United States and Europe: Infrastructure congestion . . . . . | 147        |
| China: First out of the gate . . . . .                            | 148        |
| The developing world: Roadblocks to blockchain . . . . .          | 148        |
| <br>  |            |
| <b>CHAPTER 14: Insurance . . . . .</b>                            | <b>151</b> |
| Precisely Tailoring Coverage . . . . .                            | 151        |
| Insuring the individual . . . . .                                 | 152        |
| The new world of micro insurance . . . . .                        | 153        |
| Witnessing for You: The Internet of Things . . . . .              | 154        |
| IoT projects in insurance . . . . .                               | 155        |
| Implications of actionable big data . . . . .                     | 155        |

|   |            |
|---|------------|
| Taking Out the Third Party in Insurance .....           | 156        |
| Decentralized security .....                            | 156        |
| Crowdfunded coverage .....                              | 156        |
| The implications of DAO insurance.....                  | 157        |
| <b>CHAPTER 15: Government .....</b>                     | <b>159</b> |
| The Smart Cities of Asia .....                          | 159        |
| Singapore satellite cities in India.....                | 161        |
| China's big data problem .....                          | 162        |
| The Battle for the Financial Capital of the World ..... | 163        |
| London's early foresight.....                           | 163        |
| The regulatory sandbox of Singapore .....               | 164        |
| The Dubai 2020 initiative .....                         | 165        |
| Bitlicense regulatory framework: New York City .....    | 167        |
| Securing the World's Borders .....                      | 168        |
| The Department of Homeland Security                     |            |
| and the identity of things .....                        | 168        |
| Passports of the future.....                            | 169        |
| The new feeder document.....                            | 169        |
| <b>CHAPTER 16: Other Industries .....</b>               | <b>171</b> |
| Lean Governments .....                                  | 171        |
| Singapore's Smart Nation project.....                   | 172        |
| Estonia's e-Residency .....                             | 173        |
| Better notarization in China.....                       | 174        |
| The Trust Layer for the Internet .....                  | 174        |
| Spam-free email.....                                    | 175        |
| Owning your identity.....                               | 176        |
| Oracle of the Blockchain.....                           | 176        |
| Trusted authorship .....                                | 177        |
| Intellectual property rights.....                       | 177        |
| <b>PART 5: THE PART OF TENS.....</b>                    | <b>179</b> |
| <b>CHAPTER 17: Ten Free Blockchain Resources .....</b>  | <b>181</b> |
| Factom University .....                                 | 181        |
| Ethereum 101.....                                       | 182        |
| Build on Ripple.....                                    | 182        |
| Programmable Money by Ripple.....                       | 182        |
| DigiKnow.....   | 183        |
| Blockchain University .....                             | 183        |
| Bitcoin Core .....                                      | 183        |
| Blockchain Alliance .....                               | 183        |
| Multichain Blog .....                                   | 184        |
| HiveMind.....   | 184        |

|   |     |
|---|-----|
| <b>CHAPTER 18: The Ten Rules to Never Break on the Blockchain</b> ..... | 185 |
| Don't Use Cryptocurrency or Blockchains to Skirt the Law .....          | 185 |
| Keep Your Contracts as Simple as Possible .....                         | 186 |
| Publish with Great Caution .....  | 187 |
| Back Up, Back Up, Back Up Your Private Keys .....                       | 187 |
| Triple-Check the Address Before Sending Currency .....                  | 189 |
| Take Care When Using Exchanges .....                                    | 189 |
| Beware Wi-Fi .....  | 190 |
| Identify Your Blockchain Dev .....                                      | 190 |
| Don't Get Suckered .....  | 190 |
| Don't Trade Tokens Unless You Know What You're Doing .....              | 191 |
| <b>CHAPTER 19: Ten Top Blockchain Projects</b> .....                    | 193 |
| The R3 Consortium .....   | 193 |
| T ZERO: Overstocking the Stock Market .....                             | 194 |
| Blockstream's Distributed Systems .....                                 | 195 |
| OpenBazaar's Blockchain .....   | 196 |
| Code Valley: Find Your Coder .....                                      | 196 |
| Bitfury's Digital Assets .....  | 197 |
| Any Coin Can ShapeShift .....   | 198 |
| Machine-Payable Apps on 21 .....  | 198 |
| Anonymous Transactions on Dash .....                                    | 199 |
| ConsenSys: Decentralized Applications .....                             | 200 |
| <b>INDEX</b> .....  | 201 |

# Introduction

---

**W**elcome to *Blockchain For Dummies!* If you want to find out what blockchains are and the basics of how to use them, this is the book for you. Many people think blockchains are difficult to understand. They might also think that blockchains are just about cryptocurrencies like Bitcoin, but they're are so much more. Anyone can master the basics of blockchains.

In this book, you find helpful advice for navigating the blockchain world and cryptocurrencies that run them. You also find practical step-by-step tutorials that will build your understanding of how blockchains work and where they add value. You don't need a background in programming, economics, or world affairs to understand this book, but I do touch on all these subjects because blockchain technology intersects all of them.

## About This Book

---

This book explains the basics of blockchains, smart contracts, and cryptocurrencies. You probably picked up this book because you've heard about blockchains, know they're important, but have no idea what they are, how they work, or why you should care. This book answers all these questions in easy-to-understand terms.

This book is a bit different than just about any other blockchain book on the market. It provides a survey of all the key blockchains in the public market, how they work, what they do, and something useful you can try with them today.

This book also covers the landscape of blockchain technology and points out some of the key things to be aware of for your own blockchain projects. Here, you find out how to install an Ethereum wallet, create and execute a smart contract, make entries into Bitcoin and Factom, and earn cryptocurrencies.

You don't have to read the book cover to cover. Just flip to the subject that you're interested in.

Finally, within this book, you may note that some web addresses break across two lines of text. If you're reading this book in print and want to visit one of these web

pages, simply key in the web address exactly as it's noted in the text, pretending as though the line break doesn't exist. If you're reading this as an e-book, you've got it easy — just click the web address to be taken directly to the web page.

## Foolish Assumptions

I don't make many assumptions about you and your experience with cryptocurrency, programming, and legal matters but I do assume the following:

- » You have a computer and access to the Internet.
- » You know the basics of how to use your computer and the Internet.
- » You know how to navigate through menus within programs.
- » You're new to blockchain and you aren't a skilled programmer. Of course, if you are a skilled programmer, you can still get a lot out of this book — you just may be able to breeze past some of the step-by-step guidelines.

## Icons Used in This Book

Throughout this book, I use icons in the margin to draw your attention to certain kinds of information. Here's what the icons mean:



TIP

The Tip icon marks tips and shortcuts that you can use to make blockchains easier to use.



REMEMBER

The Remember icon marks the information that's especially important to know — the stuff you'll want to commit to memory. To siphon off the most important information in each chapter, just skim through these icons.



TECHNICAL  
STUFF

The Technical Stuff icon marks information of a highly technical nature that you can skip over without missing the main point of the subject at hand.



WARNING

The Warning icon tells you to watch out! It marks important information that may save you headaches — or tokens.



## Beyond the Book

---

In addition to the material in the print or e-book you're reading right now, this product also comes with some access-anywhere goodies on the web. Check out the free Cheat Sheet for more on blockchains. To get this Cheat Sheet, simply go to [www.dummies.com](http://www.dummies.com) and type **Blockchain For Dummies Cheat Sheet** in the Search box.

## Where to Go from Here

---

You can apply blockchain technology to virtually every business domain. Right now there is explosive growth in financial, healthcare, government, insurance industries, and this is just the beginning. The whole world is changing and the possibilities are endless.



# 1 Getting Started with Blockchain

## **IN THIS PART . . .**

Discover what blockchains are all about and how they can benefit your organization.

Identify the right type of technology and the four steps to developing and executing an effective blockchain project.

Make your own smart contracts on Bitcoin, and determine where this technology can fit within your organization.

Discover the tools you need to step up and run your own private blockchain on Ethereum.

#### IN THIS CHAPTER

- » Discovering the new world of blockchains
- » Understanding why they matter
- » Identifying the three types of blockchains
- » Deepening your knowledge of how blockchains work

## Chapter **1**

# Introducing Blockchain

Originally, *blockchain* was just the computer science term for how to structure and share data. Today blockchains are hailed the “fifth evolution” of computing.

Blockchains are a novel approach to the distributed database. The innovation comes from incorporating old technology in new ways. You can think of blockchains as distributed databases that a group of individuals controls and that store and share information.

There are many different types of blockchains and blockchain applications. Blockchain is an all-encompassing technology that is integrating across platforms and hardware all over the world.

## Beginning at the Beginning: What Blockchains Are

A blockchain is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties. There are many different types of blockchains.

- » **Public blockchains:** Public blockchains, such as Bitcoin, are large distributed networks that are run through a native token. They're open for anyone to participate at any level and have open-source code that their community maintains.
- » **Permissioned blockchains:** Permissioned blockchains, such as Ripple, control roles that individuals can play within the network. They're still large and distributed systems that use a native token. Their core code may or may not be open source.
- » **Private blockchains:** Private blockchains tend to be smaller and do not utilize a token. Their membership is closely controlled. These types of blockchains are favored by consortiums that have trusted members and trade confidential information.

All three types of blockchains use cryptography to allow each participant on any given network to manage the ledger in a secure way without the need for a central authority to enforce the rules. The removal of central authority from database structure is one of the most important and powerful aspects of blockchains.



REMEMBER

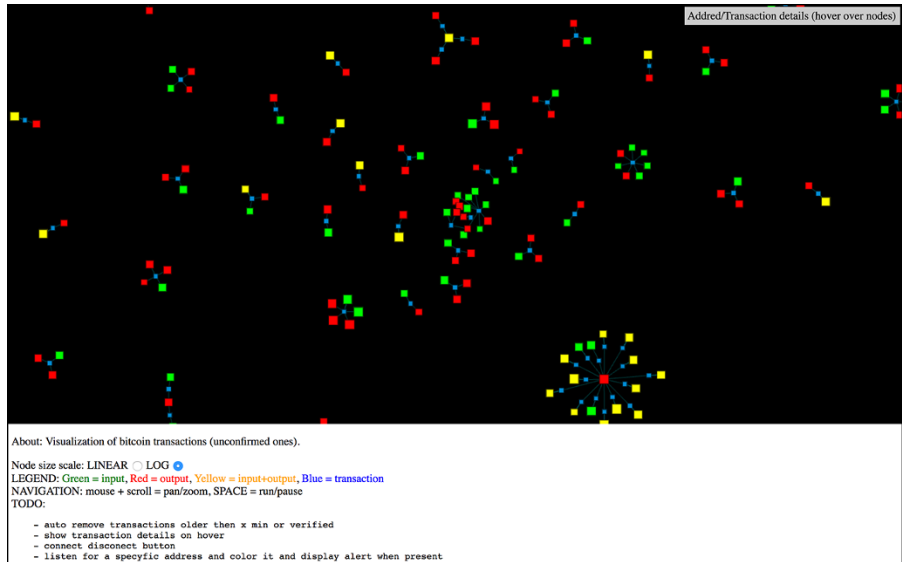
Blockchains create permanent records and histories of transactions, but nothing is really permanent. The permanence of the record is based on the permanence of the network. In the context of blockchains, this means that a large portion of a blockchain community would all have to agree to change the information and are incentivized *not* to change the data.

When data is recorded in a blockchain, it's extremely difficult to change or remove it. When someone wants to add a record to a blockchain, also called a *transaction* or an *entry*, users in the network who have validation control verify the proposed transaction. This is where things get tricky because every blockchain has a slightly different spin on how this should work and who can validate a transaction.

## What blockchains do

A blockchain is a peer-to-peer system with no central authority managing data flow. One of the key ways to removing central control while maintaining data integrity is to have a large distributed network of independent users. This means that the computers that make up the network are in more than one location. These computers are often referred to as *full nodes*.

Figure 1-1 shows a visualization of the structure of the Bitcoin blockchain network. You can see it in action at <http://dailyblockchain.github.io>.



**FIGURE 1-1:**  
The structure of  
the Bitcoin  
blockchain  
network.

To prevent the network from being corrupted, not only are blockchains decentralized but they often also utilize a cryptocurrency. A *cryptocurrency* is a digital token that has a market value. Cryptocurrencies are traded on exchanges like stocks.

Cryptocurrencies work a little differently for each blockchain. Basically, the software pays the hardware to operate. The software is the blockchain protocol. Well-known blockchain protocols include Bitcoin, Ethereum, Ripple, Hyperledger, and Factom. The hardware consists of the full nodes that are securing the data in the network.

## Why blockchains matter

Blockchains are now recognized as the “fifth evolution” of computing, the missing trust layer for the Internet. This is one of the reasons that so many people have become excited about this topic.

Blockchains can create trust in digital data. When information has been written into a blockchain database, it’s nearly impossible to remove or change it. This capability has never existed before.

When data is permanent and reliable in a digital format, you can transact business online in ways that, in the past, were only possible offline. Everything that has stayed analog, including property rights and identity, can now be created and maintained online. Slow business and banking processes, such as money wires

and fund settlements, can now be done nearly instantaneously. The implications for secure digital records are enormous for the global economy.

The first applications created were designed to piggyback on the secure digital value transfer that blockchains enable through the trading of their native tokens. These included things like the movement of money and assets. But the possibilities of the blockchain networks go far beyond the movement of value.

## The Structure of Blockchains

Blockchains are composed of three core parts:

» **Block:** A list of transactions recorded into a ledger over a given period. The size, period, and triggering event for blocks is different for every blockchain.

Not all blockchains are recording and securing a record of the movement of their cryptocurrency as their primary objective. But all blockchain do record the movement of their cryptocurrency or token. Think of the *transaction* as simply being the recording of data. Assigning a value to it (such as happens in a financial transaction) is used to interpret what that data means.

» **Chain:** A hash that links one block to another, mathematically “chaining” them together. This is one of the most difficult concepts in blockchain to comprehend. It’s also the magic that glues blockchains together and allows them to create mathematical trust.

The hash in blockchain is created from the data that was in the previous block. The hash is a fingerprint of this data and locks blocks in order and time.

Although blockchains are a relatively new innovation, hashing is not. Hashing was invented over 30 years ago. This old innovation is being used because it creates a one-way function that cannot be decrypted. A hashing function creates a mathematical algorithm that maps data of any size to a bit string of a fixed size. A bit string is usually 32 characters long, which then represents the data that was hashed. The Secure Hash Algorithm (SHA) is one of some cryptographic hash functions used in blockchains. SHA-256 is a common algorithm that generates an almost-unique, fixed-size 256-bit (32-byte) hash. For practical purposes, think of a hash as a digital fingerprint of data that is used to lock it in place within the blockchain.

» **Network:** The network is composed of “full nodes.” Think of them as the computer running an algorithm that is securing the network. Each node contains a complete record of all the transactions that were ever recorded in that blockchain.



TECHNICAL  
STUFF



The nodes are located all over the world and can be operated by anyone. It's difficult, expensive, and time-consuming to operate a full node, so people don't do it for free. They're incentivized to operate a node because they want to earn cryptocurrency. The underlying blockchain algorithm rewards them for their service. The reward is usually a token or cryptocurrency, like Bitcoin.



TIP

The terms *Bitcoin* and *blockchain* are often used interchangeably, but they're not the same. Bitcoin has a blockchain. The Bitcoin blockchain is the underlying protocol that enables the secure transfer of Bitcoin. The term *Bitcoin* is the name of the cryptocurrency that powers the Bitcoin network. The blockchain is a class of software, and Bitcoin is a specific cryptocurrency.

## Blockchain Applications

Blockchain applications are built around the idea that network is the arbitrator. This type of system is an unforgiving and blind environment. Computer code becomes law, and rules are executed as they were written and interpreted by the network. Computers don't have the same social biases and behaviors as humans do.

The network can't interpret intent (at least not yet). Insurance contracts arbitrated on a blockchain have been heavily investigated as a use case built around this idea.

Another interesting thing that blockchains enable is impeccable record keeping. They can be used to create a clear timeline of who did what and when. Many industries and regulatory bodies spend countless hours trying to assess this problem. Blockchain-enabled record keeping will relieve some of the burdens that are created when we try to interpret the past.

## The Blockchain Life Cycle

Blockchains originated with the creation of Bitcoin. It demonstrated that a group of individuals who had never met could operate online within a system that was desensitized to cheat others that were cooperating on the network.