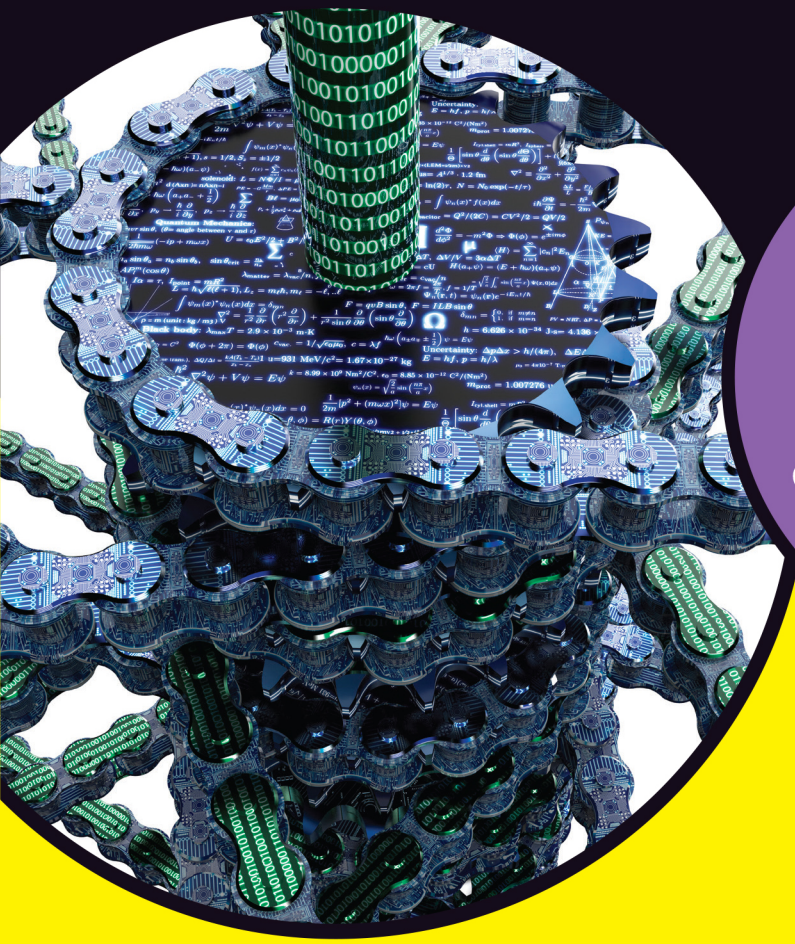
LEARNING MADE EASY

Blockchain

for dummies®

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

Blockchain

by Tiana Laurence

for dummies®
A Wiley Brand

Blockchain For Dummies®

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Published simultaneously in Canada

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

Table of Contents

Introduction

Welcome 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, programing, 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 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`.

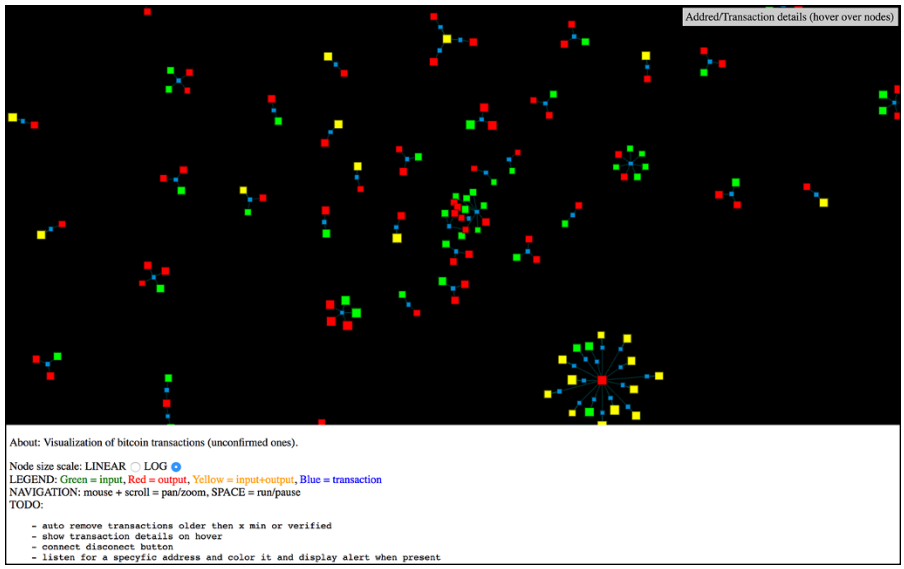


FIGURE 1-1: The structure of the Bitcoin blockchain network.

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.

  
  TECHNICAL STUFF

  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.

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 asses 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.