LEARNING MADE EASY

3rd Edition

# Blockchain

for dummies®
A Wiley Brand

Peek under the hood of tech changing finance

Learn how Blockchain powers cryptocurrency

Launch your own blockchain apps on stable platforms

**Tiana Laurence**
Blockchain pioneer and investor

# Blockchain

# Blockchain

3rd Edition

**by Tiana Laurence**

for dummies®
A Wiley Brand

## Blockchain For Dummies®, 3rd Edition

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: 2023931209

ISBN 978-1-394-15966-6 (pbk); ISBN 978-1-394-15967-3 (ebk); ISBN 978-1-394-15968-0 (ebk)

# 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 may also think that blockchains are just about cryptocurrencies like Bitcoin, but they're 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 and know they're important, but you 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 from 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 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, a smartphone, 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:


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


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.


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.


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, health care, 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 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.

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. Or more commonly now the backbone of the Web3 movement.

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 cryptocurrency. A *cryptocurrency* is a unique bit of data that can be traded between two parties. Public blockchains are open for anyone to participate at any level and usually 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 also known as distributed ledger technology (DLT) tend to be smaller and do not utilize a token or cryptocurrency. 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 the database structure is one of the most important and powerful aspects of blockchains.

All types of blockchains are contributing to what is known as Web3 also referred to as Web 3.0. It is as much a social movement as a new evolution of the World Wide Web. The general idea behind this trend is that individuals are taking ownership of their own data by using tools that decentralization, blockchain technologies, and token-based economics give them. In contrast with Web 2.0, where data and content are controlled by a small group of mega companies such as Apple, Google, and Facebook.

REMEMBER

Blockchains create permanent records and histories of transactions, but nothing is really permanent. The permanence of the record is based on the dependability and health of the network. In the context of blockchains, this means that if a large portion of the blockchain community wanted to change information written to their blockchain, they could. Cryptocurrency is used as a reward to incentivize lots of users to facilitate the healthy function of the network through competition. If the records are changed inappropriately, this is known as a 51 percent attack.

Small networks with few independent minors are vulnerable because it doesn't take much effort to change their information, and powerful miners could do so and gain extra cryptocurrency. Ethereum experienced just this type of attack.

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 works and who can validate transactions.

# 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`.

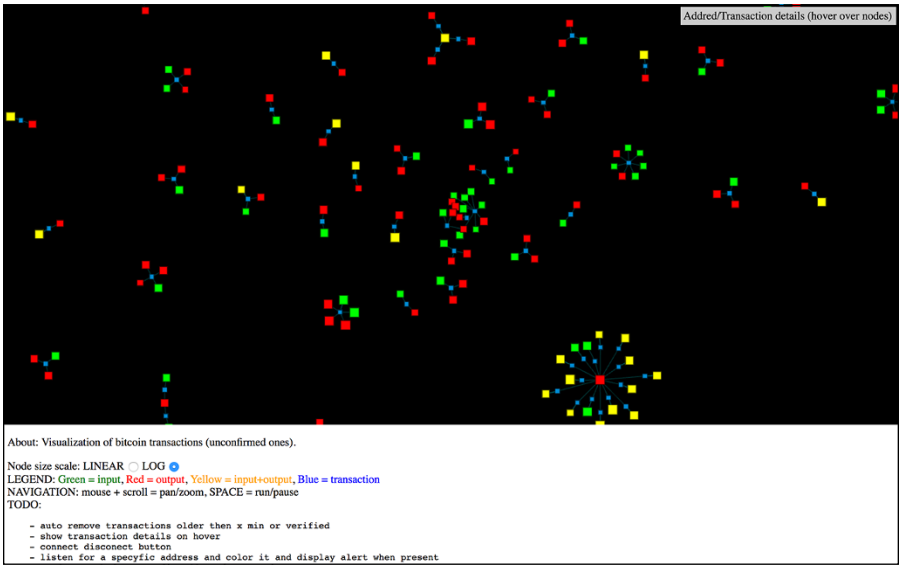


**FIGURE 1-1:** The structure of the Bitcoin blockchain network.

To prevent the network from being corrupted, not only are blockchains decentralized but they often also utilize a cryptocurrency. Blockchain networks produce cryptocurrencies as an incentive to maintain the integrity of the network. Many cryptocurrencies are traded on exchanges like stocks.

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

## Why blockchains matter

Blockchains are recognized as the "fifth evolution" of computing because they're a new trust layer for the Internet. The blockchain space has matured significantly since its inception around 2009. Now individual users have access to higher levels of security and autonomy.

Before blockchains, trust was established by central authorities that would issue certificates. One certificate you may be familiar with is Secure Sockets Layer (SSL). An SSL certificate is the "lock" that you see next to an address in your web browser. It lets you know you're on a secure website. SSL certificates have proven to not be foolproof, however. Certificates have been stolen from the domains of the Central Intelligence Agency (CIA), the U.K.'s Secret Intelligence Service (commonly known as MI6), Microsoft, Yahoo!, Skype, Facebook, and Twitter. Relying on a third party allows for a single point of failure, and hackers have frequently taken advantage of this vulnerability.

Blockchains, on the other hand, establish trust in novel ways. Proof-of-work (POW) blockchains require miners to have a full and accurate history of their transactions to participate on the network. Proof-of-stake (PoS) blockchains create trust by requiring nodes that are processing transactions to "stake" some cryptocurrency that may be forfeited if they're caught defrauding the network. Private blockchains build confidence by distributing data across a network of connected but independent participants that are known by each other and can be held accountable. Each type of blockchain uses a different incentive system to establish trust that each participant in the network will cooperate in keeping a full and unaltered history of each transaction or entry that is made within the database they share.

So, in short, blockchains don't have a single point of attack; they distribute the same replicated date across their network of nodes. Each node adds to the difficulty in tampering with that network's data, at least in theory.

It's very important to note that blockchains are not all equal in their distribution of data control and security. The fifth evolution of the Internet has become progressively more mainstream. More specifically, blockchain-enabled games and nonfungible tokens (NFTs) have generated billions of dollars in sales. They've also impowered a new generation of makers and creatives globally.

The blockchain industry has also renamed itself to Web 3.0. This moniker refers to how people interact online and who controls digital assets and data. For reference, Web 1.0 was a more static Internet experience, where individuals browsed content and built static websites. Web 2.0 is the interactive Internet accessed through commercial portals like Google, Facebook, and Twitter. In the Web 2.0 Internet, data is controlled by commercial entities and privacy is rare for average individual users.

Web 3.0 is a global social movement that pushes back against the egregious privacy violations and fraud that have become ubiquitous online. It also appeals to the entrepreneurial and creative spirit of artists and makers. Web 3.0 software allows users to interact with each other via a sovereign digital identity that each user controls. The user's digital credentials are authenticated via their digital wallet (such as MetaMask), a browser extension, the user's private keys (see Chapter 3).

A user-controlled identity allows average individual users to control their data and privacy. Users also can own digital assets, create new digital assets, and sell them directly. The Internet has enabled digital commerce for a very long time. What makes Web 3.0 special is how elegantly it allows anyone anywhere in the world who has access to a smart device and the Internet to create and transact with any other individual directly.

Global governments have responded strongly to Web 3.0 and have acted quickly to control the inflow and outflow of fiat currency into the blockchain space — for example, requiring Anti–Money Laundering (AML) and Know Your Customer (KYC) verification on individuals moving more than $1,000 of value from one wallet to another.

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.

Blockchains are important because they allow for new efficiency and reliability in the exchange of valuable and private information that once required a third party to facilitate, such as the movement of money and the authenticity of identity. This is a big deal because much of our society and economy has been structured around establishing trust, enforcing trust when it's broken, and third parties that facilitate trust. You can imagine how this simple software can be utilized to fix areas that have proven to not be foolproof, such as voting, supply chain management, money movement, and the exchange of property.