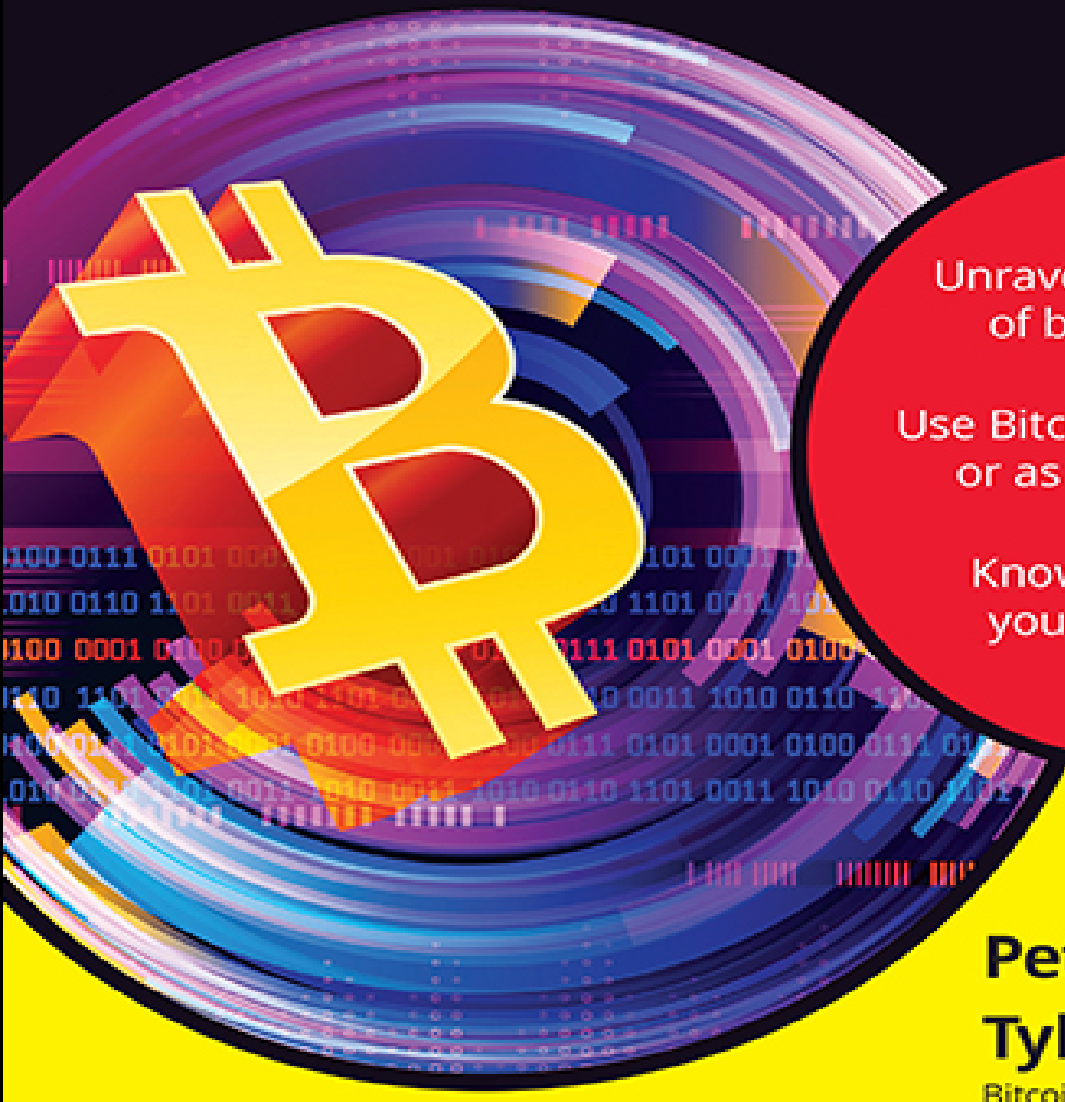
LEARNING MADE EASY

2nd Edition

Bitcoin

for dummies®

A Wiley Brand



Unravel the mysteries of buying Bitcoin

Use Bitcoin for purchases or as an investment

Know how to keep your Bitcoin safe

Peter Kent

Tyler Bain

Bitcoin miners, investors, and educators

Bitcoin

2nd Edition

by Peter Kent and Tyler Bain

for dummies
A Wiley Brand

Bitcoin For Dummies®, 2nd Edition

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

Copyright © 2022 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: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY 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 ANY IMPLIED

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

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.

Library of Congress Control Number: 2022932288

ISBN 978-1-119-60213-2 (pbk); ISBN 978-1-119-60216-3 (ebk); ISBN 978-1-119-60214-9 (ebk)

Bitcoin For Dummies®

To view this book's Cheat Sheet, simply go to www.dummies.com and search for “Bitcoin For Dummies Cheat Sheet” in the Search box.

Table of Contents

- Cover
- Title Page
- Copyright
- Introduction
  - About This Book
  - Foolish Assumptions
  - Icons Used in This Book
  - Beyond the Book
  - Where to Go from Here
- Part 1: Bitcoin Basics
  - Chapter 1: Bitcoin in a Nutshell
    - In the Beginning, There Were … Digital Currencies?
    - The Birth of Bitcoin
    - But Who Is Nakamoto?
    - Understanding What Bitcoin Actually Is
    - Understanding Bitcoin Units
    - Cryptocurrency or Cryptoasset?
    - If There Is No Bitcoin, How Can It Be Valuable?
    - Understanding Bitcoin Benefits

Chapter 2: Bitcoin Tech Explained

- Understanding That There Is No Bitcoin!
- Discovering the Bitcoin Ledger
- Looking at the Bitcoin Distributed, Peer-to-Peer Network
- Using the Bitcoin Blockchain's Blocks of Business
- Finding Out How the Ledger Functions

Part 2: Using Bitcoin

Chapter 3: Buying, Using, and Selling Bitcoin

- Finding the Price of Bitcoin
- Your Options for Acquiring Bitcoin
- "Bitcoin Back" on Credit and Debit Cards
- Earning Your Bitcoin
- Mining Bitcoin
- Finding Bitcoin Everywhere
- Selling Your Bitcoin

Chapter 4: Taking Control of Your Wallet (and Hodling Your Bitcoin)

- What Is a Wallet?
- Exploring Wallet Hardware
- Finding a Wallet
- Setting Up a Bitcoin Wallet
- Using the Lightning Network

Chapter 5: Keeping Your Bitcoin Safe

- Understanding How You Can Lose Control of Your Bitcoin
- Grasping the Goal: Private Key and Seed Protection
- Making a Choice: Custodial or Private Wallet?
- Devising Your Cryptocurrency Safety Plan
- Exploring More Ways to Protect Your Bitcoin (and Everything Else)
- Knowing What Happens When You Kick the Bucket

Chapter 6: Investing in Bitcoin

Bitcoin: Valuable Asset or Bubble About to Burst?
So You Want to Buy Bitcoin…
Hodling II — An Even Better Strategy
The New Frontier — Other Cryptocurrencies
NFTs — What's It All About?

Part 3: Getting Geeky

Chapter 7: Understanding the Bitcoin Network and Bitcoin Mining

The Bitcoin Network
Submitting Transactions
Bitcoin Presets

Chapter 8: Bitcoin Adoption in the Real World

Bitcoin in the Boardroom
Bitcoin in Nations

Chapter 9: Bitcoin Botheration

Bitcoin Is Too Volatile
Governments Ban Bitcoin
Bitcoin: A 21st-Century Ponzi Scheme
The Bitcoin Bubble
Bitcoin Costs Too Much to Use
Bitcoin Security Risks
Bitcoin Energy Usage

Part 4: The Part of Tens

Chapter 10: Ten Tips to Hodl and Stack Sats

Invest in Knowledge, Do Your Homework
Get Off Zero (B)
Lower Your Cost Basis, Buy the Dip
Dry Powder, or Get on Zero ($)?
Run Your Own Bitcoin Node
Secure your Keys, Test Seed Backups
Bitcoin Price-Prediction Models

Bitcoin Technical Analysis, Market Indicators, and Other Tea Leaves
Slow and Steady Wins the Race
Tell Everyone, or Speak Softly?

Chapter 11: Ten Types of Bitcoin Resources

Bitcoin Documentaries
Bitcoin Books
Bitcoin Guides and Walkthroughs
Bitcoin Block Explorers
Bitcoin Data Aggregators
Bitcoin Forums
Bitcoin Volatility Charts
Bitcoin Foundational Documents
Bitcoin Wikis
Bitcoin Data Visualizations

Chapter 12: Ten (Plus One) Thoughts about the Future of Bitcoin

Bitcoiners Love Lindy's Law
Bitcoin's Limited Supply Drives Price
Bitcoin Adoption Coin Rush
Bitcoin Adoption by Corporations
Bitcoin Is Dead!
Bitcoin Boom-and-Bust Cycles
The Halvening and Bitcoin Price
New Bitcoin "Layers"
Bitcoin Will Get Easier
Bitcoin Development and Bitcoin Improvement Proposals
What *Is* the Future of Bitcoin?

Index

About the Authors

Advertisement Page

Connect with Dummies

End User License Agreement

List of Tables

Chapter 1

TABLE 1-1 Bitcoin Units

Chapter 3

TABLE 3-1 $500 Trades Compared

Chapter 6

TABLE 6-1 Gold versus Bitcoin

List of Illustrations

Chapter 1

FIGURE 1-1: How much Bitcoin is needed to buy a share of Apple?

Chapter 2

FIGURE 2-1: Each block’s hash is stored in the next block of data. The hashes c...

FIGURE 2-2: Your browser’s lock icon means that data submitted back to the web ...

FIGURE 2-3: An example of a blockchain explorer tool, found at `https://live.blo`...

FIGURE 2-4: The Bitcoin is associated with an address in the blockchain; the ad...

Chapter 3

FIGURE 3-1: You’re going to have to prove who you are.

FIGURE 3-2: The Coinme wallet.

FIGURE 3-3: The new address shown in the Blockchain.com blockchain explorer.

FIGURE 3-4: Sending Bitcoin from the Coinme web console and smartphone app.

FIGURE 3-5: Let’s buy!

FIGURE 3-6: You’re ready to buy; click Buy Now when you’re sure.

FIGURE 3-7: Sending money from Coinbase to somewhere else.

FIGURE 3-8: Your transaction, still pending.

FIGURE 3-9: Your transaction, in the blockchain explorer.

Chapter 4

FIGURE 4-1: The Cryptotag metal wallet kit (www.cryptotag.io).

FIGURE 4-2: An Ellipal hardware wallet.

FIGURE 4-3: The Blue home screen.

FIGURE 4-4: Picking your wallet type and saving your seed.

FIGURE 4-5: Your wallet, ready for work.

FIGURE 4-6: Advanced options enable you to add more randomness.

FIGURE 4-7: The BlueWallet, ready for a transaction.

FIGURE 4-8: Tell Blue if you want to receive a notification when your Bitcoin a...

FIGURE 4-9: The Electrum connections.

FIGURE 4-10: Your wallet’s addresses.

FIGURE 4-11: The BlueWallet Send screen.

FIGURE 4-12: Choose your miner’s fee.

FIGURE 4-13: Your change addresses.

FIGURE 4-14: Checking out basic wallet info and the export info with a seed.

FIGURE 4-15: The wallet import box.

FIGURE 4-16: Choose an address to access its QR code.

FIGURE 4-17: Create a multi-sig wallet; you choose how many wallets in a group.

FIGURE 4-18: Setting up your vault wallet and getting your first wallet seed.

FIGURE 4-19: Your XPUB QR code.

FIGURE 4-20: The Import screen (on an Android device).

FIGURE 4-21: The Import screen.

FIGURE 4-22: The Import screen (on an Android device).

Chapter 5

FIGURE 5-1: A warning from Coinbase.com?

FIGURE 5-2: What’s going on with the letter a?

FIGURE 5-3: The Google Authenticator app.

Chapter 6

FIGURE 6-1: We’re betting you’re wishing you bought Bitcoin early in 2016 (or e...

FIGURE 6-2: How dollar cost averaging would have worked out over the last three...

FIGURE 6-3: The Bitcoin Rainbow.

FIGURE 6-4: NFT’d art for sale, on Rarible.com.

FIGURE 6-5: $69 million for this NFT-linked collage?

Chapter 7

FIGURE 7-1: A live view of the full listening node count on the Bitcoin network...

Chapter 9

FIGURE 9-1: Average network transaction fees over time, measured in US$ per tra...

FIGURE 9-2: Bitcoin yearly energy estimates (TWh/Year), along with the Bitcoin ...

Chapter 12

FIGURE 12-1: Bitcoin volatility — it’s a wild ride!

FIGURE 12-2: Bitcoin price and the halvenings; is there an association?

Introduction

Welcome to *Bitcoin For Dummies,* 2nd Edition, a book that tells you everything you need to know to get started with the original blockchain-based cryptocurrency (including what *blockchain* and *cryptocurrency* mean).

This is a very strange subject. Bitcoin is perhaps the most valuable asset (there's about a trillion dollars' worth right now) that almost nobody understands. How can you invest in something if you don't understand *what it is?* And make no mistake, most people, even some with thousands of dollars' worth of Bitcoin, don't know what it truly is. Read this book, and that won't be you.

We're firm believers that if you want to be involved in Bitcoin in some way, you need to understand it. Two huge problems come with *not* understanding it:

- **Thousands of Bitcoin owners have had their Bitcoin stolen.** We explain how that happens and how to avoid it.
- **Thousands of Bitcoin owners have "lost" their Bitcoin.** We explain how, how to avoid this, and why the Bitcoin isn't *really* lost (it's just out of reach).

Our job is to break it all down into intelligible, easy-to-digest, bite-sized pieces that ordinary folks like yourself can understand.

About This Book

This book explains, simplifies, and demystifies the world of Bitcoin. You find out what you need to know and do in

order to decide if and how you're going to begin stepping into the beautiful world of Bitcoin.

In this book, we explain the following:

- Where Bitcoin came from (who's this person Satoshi Nakamoto?)
- What Bitcoin actually *is* (and *isn't*)
- The various Bitcoin units, down to the smallest (one-hundred millionth of a Bitcoin)
- How money works (yep, you think you know, but *do you?*)
- How the crypto in cryptocurrency works
- The best places to buy Bitcoin and *how* to do so
- Working with your own crypto wallet (no, this is not where your Bitcoin is stored, but it's critically important nonetheless)
- How to keep your Bitcoin safe from theft and loss
- How to invest in Bitcoin (and maybe other cryptocurrencies)

And plenty more!

Foolish Assumptions

We don't want to assume anything, but we have to believe that if you're reading this book, you already know a few things about the Internet. Bitcoin is a technology that depends on the Internet — no Internet, no Bitcoin. So you need to be tech-aware enough to use some kind of Internet-connected device: a desktop PC or laptop, or maybe just a smartphone. You need to be able to navigate to websites, and download and run software

(not necessarily much software, maybe just a simple crypto wallet you can run on your smartphone).

We explain how to keep your Bitcoin safe, so you'll also need to be able to carry out processes such as loading a password-management program, installing anti-virus software, and doing backups. This isn't rocket surgery or brain science, but if your idea of using a computer is asking your grandkid to find something on the interwebs for you, this book may not be for you!

Icons Used in This Book

This book, like all *For Dummies* books, uses icons to highlight certain paragraphs and to alert you to particularly useful information. Here's a rundown of what those icons mean:

TIP A Tip icon means we're giving you an extra snippet of information that may help you on your way or provide additional insight into the concepts being discussed.

REMEMBER The Remember icon points out information that's worth committing to memory.

TECHNICAL STUFF The Technical Stuff icon indicates geeky stuff that you can skip if you really want to, although you may want to read it if you're the kind of person who likes to have background info.

WARNING The Warning icon helps you stay out of trouble. It's intended to grab your attention to help you avoid a pitfall that may harm your investment.

Beyond the Book

In addition to what you're reading right now, this product also comes with a free access-anywhere Cheat Sheet that covers quick tips and info to help you along the Bitcoin road. To get this Cheat Sheet, simply go to www.dummies.com and search for "Bitcoin For Dummies Cheat Sheet" in the Search box.

Where to Go from Here

Like all good reference tools, this book is designed to be read when needed. It's divided into several parts: background information on what Bitcoin actually *is*; how to actually *use* Bitcoin (buying, selling, and investing); some more details on how the technology functions; and the Part of Tens.

We recommend you start at the beginning and read through sequentially, but if you just want to know how to use wallets, read Chapter 4. If you need to understand where to buy Bitcoin, read Chapter 3. If all you need to understand is what the crypto in cryptocurrency is and how it works, Chapter 2 is for you.

REMEMBER However, Bitcoin is a complex subject. All the topics covered in this book are interrelated. We strongly recommend you read everything in this book before you dive deep into Bitcoin investing. It's essential that you have a strong understanding of everything involved before you start. Don't join the thousands who have lost their Bitcoin. A little knowledge goes a long way!

Part 1

Bitcoin Basics

IN THIS PART ...

Discovering where Bitcoin comes from

Understanding how money works

Learning how Bitcoin uses cryptography

Sending messages to the Bitcoin blockchain

Using private keys to prove Bitcoin ownership

Chapter 1

Bitcoin in a Nutshell

IN THIS CHAPTER

- **» Discovering the history of digital currency**
- **» Finding out about early Bitcoin and its creator**
- **» Understanding what money (and Bitcoin) is and is not**
- **» Exploring the benefits of Bitcoin**

For a mere teenager, the Bitcoin network has certainly had a big impact on the world, transacting more than US$12.4T in 2021 alone. As we write these words, Bitcoin has a *market capitalization* (total value) of $918,705,395,133, which is almost a trillion dollars. (The market cap is the total number of Bitcoins in "circulation" multiplied by the current market price of a single Bitcoin.)

But that's a current low price; just a few weeks prior, it had a combined value of almost 1.3 trillion dollars. By the time you read this, the value may be higher, lower, or the same. That's one of the things about Bitcoin: Its market price can be very volatile, as you'll soon learn if you spend a little time watching the markets.

But the impact we're talking about is not just referring to Bitcoin's current market value. In fact, the market cap of Apple, Inc. is more than three times that of the Bitcoin network. However, a comparison with Apple might be apropos right now. Figure 1-1 shows how much Bitcoin would be needed to buy a single share of Apple stock,

from 2010 through 2021. The value of a single Bitcoin has been increasing against the Apple stock (just as it has, of course, against the U.S. dollar and other governmental currencies).

FIGURE 1-1: How much Bitcoin is needed to buy a share of Apple?

The launch of Bitcoin set off a revolution in blockchain and cryptocurrency. There are now more than 13,000 different cryptocurrencies. (Most, be warned, are essentially valueless and will remain that way.) At the time of writing, the top five cryptocurrencies have a combined market cap of almost 1.7 trillion dollars, and a number of cryptocurrencies have genuinely useful functions beyond merely being used as money or a store of value. It's likely that some of these cryptocurrencies will endure, even if most won't.

But we're here to talk about Bitcoin, so let's begin with a little history. Where did Bitcoin come from, and how did it develop?

In the Beginning, There Were … Digital Currencies?

Blockchain-based cryptocurrencies are pretty new, but digital currencies designed for use online have been around for quite a while. (Don't worry about this *blockchain* thing for the moment; we explain that in not-too-mind-numbing detail in Chapter 2. Just understand for now that a blockchain is a special kind of database, a store of digital data.)

As people started flooding online — the process began in the early 1980s, but really took off in 1994 with the advent of the commercial Internet — it became clear that they were going to need some way to spend money in cyberspace (the first Internet stores opened in that year). Of course, most online transactions today use credit and debit cards — even PayPal and Venmo are essentially enabling such transactions, along with bank transfers — but that wasn't the case in the early days. Many people were concerned about credit-card theft and thus wary of using their numbers online, for instance. (When co-author Peter opened an online store in 1997, he did have a functioning credit-card gateway, but many customers would print out a paper order form and mail a check!)

There was also the issue of *microtransactions*. Surely, in the digital world, it should be possible to pay someone, say, five or ten cents for something, such as access to a video or article. The microtransaction problem has still not been solved (though one might argue that the Bitcoin Lightning network, which we discuss in Chapter 4,

almost gets us there), but nonetheless, that's one of the ideas that drove the development of digital currencies.

And develop they did. In 1983 David Chaum wrote a research paper on the concept of digital currency (*Blind Signatures for Untraceable Payments*), suggesting the use of cryptography to create and manage a digital currency. So even back then, cryptography had a role in digital currencies, although they weren't known as cryptocurrencies back then. When you hear people talk about cryptocurrencies, they are generally talking about this new generation of blockchain-based cryptocurrencies that started with Bitcoin. (We explain more about cryptography and how it relates to cryptocurrencies in Chapter 2.)

Chaum actually launched a cryptography-based digital currency, known as *DigiCash*, in 1990, but these were still very early days. Very few people were online in 1990, and the currency died out by around 1998. What likely hurt digital currencies by the end of the '90s was that the credit-card companies wanted a piece of the online action, and thus went out of their way to assuage consumers' fears of using credit cards online.

Still other digital currencies came along. There was e-gold, a currency backed by real gold, and Millicent, a currency created by a major computing company, Digital Equipment Corporation (DEC). (If you're younger than, say, mid-thirties, you probably won't remember DEC, but it was a big deal. In fact, even IBM had a micropayments division working on digital currencies at the time.)

Then there was NetBill, a project of Carnegie Mellon University, which was later merged into another system, CyberCash, which eventually ended up in the clutches of PayPal. There was Beenz, which had a partnership with MasterCard at one point, First Virtual, CyberCoin, Flooz

(promoted by Whoopi Goldberg, no less!), and various others.

But nothing much *stuck*. Lots of great ideas, but nobody could quite make it all *work*. By the early 2000s, most of these endeavors were moribund (probably ushered along by the dotcom crash of late 2000). There were exceptions. Liberty Reserve, based in Costa Rica, ran from 2006 until 2013, but was shut down after accusations that it was being used to launder billions of dollars of criminal proceeds. And closed systems that work on particular networks, such as China's QQ Coins, are mostly used on the Tencent QQ Messaging service.

But then, there was Satoshi Nakamoto and his magical blockchain.

The Birth of Bitcoin

On November 1, 2008, someone named Satoshi Nakamoto posted a message to a cryptography forum, titled *Bitcoin P2P e-cash paper* (archived at https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html). In his message, Nakamoto announced that he had "been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party."

In other words, he'd created a currency system that worked on a network of peers — computers working together with each equal to the other. With no central power required, no bank or government to act as a "trusted third party" was required.

A comment he made in the post explained his view of the problem with the earlier cryptocurrencies. "A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the

1990s," he said. He believed that these other digital-money systems had a critical weakness, an Achilles heel. "I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system."

TECHNICAL STUFF Nakamoto had previously set up a domain name and a simple website, bitcoin.org, and there he posted a document explaining how all this would work: https://bitcoin.org/bitcoin.pdf. You might want to take a quick look, though it's not essential for your understanding of Bitcoin (it's pretty geeky stuff).

The whitepaper he posted describes how a *blockchain* (a special form of database) could be used to manage the currency. Essentially, the blockchain records a ledger, a record of currency transactions, and because the blockchain is duplicated over numerous computers (the *peers)* and because these peers are all equal, no trust in a central party is required. You may hear Bitcoin described as a "trustless" system. That doesn't mean it can't be trusted; it means that a trusted third party is not required. The trust, in effect, is baked into the system. The mathematics — or mathemagics, as Peter likes to call it — which powers the system means that Bitcoin transactions *can* be trusted, even without a central "power" overseeing the system. (See Chapter 2 for an explanation of why.)

REMEMBER Satoshi Nakamoto (whoever he, she, or it is) didn't use the words *cryptocurrency, blockchain,* or

trustless anywhere in the whitepaper. Those are terms that others applied to the system later.

The idea of blockchain had actually been around for a while — at least since 1991 — in fact, remember David Chaum of DigiCash fame? He had been working with the idea of a blockchain since the early 1990s.

Anyway, Nakamoto didn't stop there. In January of 2009, he/she/it launched the Bitcoin network. Nakamoto released some thirty-thousand lines of code that defined the network protocols and processes necessary to operate this peer-to-peer, decentralized money system. And Bitcoin was born.

Of course, in January of 2009, Bitcoin had essentially no value. Still, the *genesis block* created by Nakamoto (the very first block of data in the blockchain creating the first 50 Bitcoins), along with subsequent blocks of data "mined" by Nakamoto (see Chapter 7), comprise perhaps a million Bitcoins: At current prices, that's $47,369,000,000. Yes, close to 50 billion dollars!

But Who Is Nakamoto?

So who is this Satoshi Nakamoto? Nobody knows. Well, somebody must know, but either they're not saying or they've been unable to convince anybody. In fact, it's not even clear *what* Satoshi Nakamoto is. A man? A woman? A group of collaborators? An organization or firm? We don't know for sure, though most assumptions seem to be that it's a man or a group of two or three people. Perhaps not surprisingly, the most cited targets are generally cryptographers and mathematicians.

There's the actual Satoshi Nakamoto, of course — that was an obvious choice. A Japanese-American resident of California who was born Satoshi Nakamoto, and now

goes by the name Dorian Prentice Satoshi Nakamoto, seems to have some of the skills needed to be *the* Nakamoto, but he denies being the founder of Bitcoin.

Then there's Nick Szabo, a digital-currency enthusiast who has been tagged as Nakamoto but denies it. Elon Musk has been "accused," too, but he denies it (and we personally think he was probably too busy to find the time!). There's Japanese mathematician Shinichi Mochizuki (he denies it), Finnish economic sociologist Dr. Vili Lehdonvirta (denies it), and Irish cryptography student Michael Clear (yep, denies it).

One of the loudest candidates is Craig Wright, an Australian computer scientist. He certainly claims he is Nakamoto, though he's accused by many of carrying out an elaborate fraud. As we write these words, a jury found Wright liable to pay the estate of David Kleiman, a deceased friend and colleague, $100 million for misuse of funds in a joint venture they worked on. But separately, the jury also found that David Kleiman was not a partner in the creation of Bitcoin.

The jury didn't find that Craig Wright *is* Nakamoto, though — only that *if* he is, he doesn't have to share his $50 billion with Kleiman's estate. Not a bad deal. In fact, it's such a good deal that Wright stated that he was *relieved* that all he has to pay is $100 million! Still, the case is not over. Whether Kleiman's estate actually has ownership in the joint-venture company is unclear, and Wright might owe $100 million to his ex-wife. It doesn't settle the question of whether or not Wright actually is Nakamoto. (Wright says that the jury found that he *is* Nakamoto; they didn't.) That won't be settled until Wright — or the *real Satoshi Nakamoto* — moves some of the Bitcoin out of the blockchain addresses owned by Nakamoto.

Regardless, the Bitcoin network has continued to function as designed long after Satoshi Nakamoto mysteriously stopped participating in the network, shortly after claiming Julian Assange and Wikileaks had "kicked the hornets' nest" once they began accepting Bitcoin for donations for their controversial reporting in 2010.

Understanding What Bitcoin Actually Is

So what is Bitcoin? Well, we can tell you what it isn't very quickly. It's not tangible — there's nothing you can touch or hold. You can't taste it or smell it. You can't even see it. In fact — and we explain this in more detail in Chapter 2 — Bitcoin really *isn't*. That is…*there is no Bitcoin.*

What there is, though, is something known as the Bitcoin *ledger* (another word, by the way, that Satoshi Nakamoto didn't use in his famous Bitcoin whitepaper, but that is what the data stored in the Bitcoin blockchain has come to be popularly known as). A ledger is a written record of transactions; your checkbook's little account register is a form of ledger, for instance. (For those of you under 30, a check is a piece of paper you can write a number on, sign your name, and give to someone, and that someone can then give it to their bank and the bank gives them money…an amazingly efficient system.) Or consider a bank statement, showing money coming into and leaving your account. (All too often *leaving*.) That's a form of ledger, too.

So, when Satoshi Nakamoto created the first ever Bitcoin, how did he create it? Well, when we talk about Bitcoin being "created," we're really talking in

shorthand. No Bitcoin *thing* was created. When Nakamoto first "created" Bitcoin, what he really did was to create a set of rules for a ledger in which he *recorded* the creation of Bitcoin. The ledger says, in effect, "50 new Bitcoin were created today." And there you go, Bitcoin exists.

When Nakamoto minted that first "genesis block," the nature of the network was set in computational stone. Buried in the first block of data was a little additional text, words from the front page of that day's *New York Times* (January 3, 2009): "Chancellor on Brink of Second Bailout for Banks." Perhaps this was a hint at Nakamoto's reason for creating the network, as an alternative to what he felt were the corrupt government-managed monetary systems.

The ledger essentially records two things. The first is the *creation* of Bitcoin, which is done through a process called "mining." Nakamoto "mined" those original 50 Bitcoins (however, the first 50 Bitcoins are unspendable due to the nature of the code). Mining continues, and in fact, new Bitcoins are created each time a new block of transactions is added to the Bitcoin blockchain, every ten minutes or so. (Chapter 7 explains how this "mining" process works.)

However, there is a mathematical arrangement to all this: Bitcoins are created on a steady schedule, and every four years or so (during an event quaintly called *the halvening*), the number of Bitcoins created every ten minutes is halved. Right now, 6.25 Bitcoins are created every ten minutes, but sometime in 2024, that will be reduced to 3.125, then again halved four years later, and so on (every four years) until around the year 2140, when the maximum number of Bitcoins will finally be in circulation.

The second thing that the ledger records is what happens to the Bitcoin once it has been created. As we discuss in Chapter 2, all Bitcoin is associated with "addresses" in the blockchain, and as people buy and sell Bitcoin, or use Bitcoin to buy something (essentially the same as selling Bitcoin), the coins get sent from one address in the blockchain to another. The Bitcoin ledger keeps track of where the Bitcoin flows, from address to address to address. Each address is under the control of someone, and thus the blockchain is, in effect, keeping track of who owns what. If the Bitcoin blockchain ledger says the address you control has 2 Bitcoins associated with it, then you control those 2 Bitcoins. (In Chapters 3 and 4, we explain how to exercise this control — that is, how you can transfer your Bitcoin to other addresses in return for governmental fiat currency or for goods and services.)

FIAT CURRENCY?

Hang around in the Bitcoin community long enough and eventually, you'll hear people talking about *fiat* currency, usually disparagingly. A fiat currency is currency by decree, by official order. A fiat currency is one that is issued by a government, without being backed by a commodity such as gold. (To quote Nobel-prize winning economist Paul Krugman, "fiat currencies have underlying value because men with guns say they do.") Most currencies these days are fiat currencies; the "gold standard" generally fell out of favor in the 1930s, during the Great Depression. (Great Britain dropped the gold standard in 1931.) The U.S. dollar used to be pegged to silver, but in 1900, a law was passed linking it to gold. It remained linked to gold through most of the century, until being completely de-linked from gold in 1971 and becoming a fiat currency. (However, in 1934 the U.S. did devalue the dollar against gold; that is, they reduced the weight of gold per dollar.)

The advantage of fiat currency is that it gives governments more control over the money supply. Many economists, probably most, believe that adherence to the gold standard prolonged the Great Depression, as governments were not able to stimulate their economies by increasing the money supply. The disadvantage, according to many true believers in Bitcoin, is that it provides governments with too much control over the money supply!