PREFACE

In writing this book, we wanted to explain the concept and potential of Bitcoin in a more-or-less timeless manner. Boy, was that hard. It would have been much easier to write a book called *The State of Bitcoin Right Now: Please Disregard Everything in This Book One Year After Its Publication.* The core technology behind Bitcoin, as well as the larger technological infrastructure around it, is rapidly evolving as this book goes to press. The debates about the legality, price volatility, and merchant adoption of Bitcoin may already be out of date by 2015, and who knows how they will sound in 2025.

To keep this book relevant for the future, we did our best to focus on those aspects of Bitcoin that will remain important forever, and we tried to cover them in a way that is fun. We hope you will enjoy our approach to this fascinating subject.

Acknowledgments

Chris Wilmer would like to thank his wife Emily Winerock and his family for their patience and early feedback. Conrad Barski would like to thank his wife Lauren Barski and daughter Ava Barski for their support as he was working on this book and for their patience during all the weekends and evenings he spent to get it done.

Special thanks go to Richard Ford Burley, for substantial editorial help in the early drafts of this book, and to Patrick Fuller, for reviewing the programming sections. Many of the great people at No Starch Press helped us to get this book into shape, including Serena Yang, Tyler Ortman, Bill Pollock, and others.

1

WHAT IS BITCOIN?

In the simplest terms, Bitcoin is just another currency. The term *Bitcoin* refers to the entire currency system, whereas *bitcoins* are the basic units of the currency.[1] As with dollars, euros, yen, and gold coins, you can save bitcoins, spend them on goods and services, and exchange them for other currencies. However, Bitcoin is the world's first currency that is both digital and decentralized.

A *digital currency* is one that can be easily stored and used on a computer. By this definition, even dollars can be considered a digital currency, since they can be easily sent to others or used to shop online, but their supply is controlled by a centralized bank organization. In contrast, gold coins are *decentralized*, meaning that no central authority controls the supply of gold in the world. In fact, anyone can dig for gold, create new coins, and distribute them. However, unlike digital currencies, it's not easy to use gold coins to pay for goods (at least not with exact change!), and it's impossible to transfer gold coins over the Internet. Because Bitcoin combines these two

1. Similar to how *renminbi* is name of the Chinese currency, but the *yuan* is the basic unit.

properties, it is somewhat like digital gold. Never before has there been a currency with both these two properties, and its impact on our increasingly digital, globalized world may turn out to be significant.

Sometimes called a stateless currency, Bitcoin is not associated with any nation. However, you should not consider Bitcoin to be in the same category as *private* currencies, hundreds of which have existed in various forms in the past.[2] Private currencies, whether issued by a person, a company, or a nonstate organization, are centrally controlled and run the risk of collapse due to bankruptcy or other economic failure. Bitcoin is not a company, nor does a single person or organization issue or control bitcoins; therefore, it has no central point of failure. For this reason, nobody can inflate the currency supply and create hyperinflation crises, such as those that occurred in post–World War I Germany and more recently in Zimbabwe.[3]

Many people are asking about the motive behind the creation of Bitcoin, so let's explore the currency's purpose.

Why Bitcoin Now?

Until recently, people could not send *digital cash* back and forth to each other in a reliable way without a central mediator. A trusted central mediator such as PayPal can track payments and money transfers in a privately held account ledger, but it wasn't clear how a group of strangers who *do not* trust each other could accomplish the same transactions dependably.[4] Sometimes referred to as the Byzantine Generals' Problem, this fundamental conundrum also emerges in computer science, specifically in how to achieve consensus on a distributed network.

2. For example, in the mid-1800s, banks, companies, churches, and individuals issued hundreds of private currencies in the United States. Eventually, most of these private currencies lost all their value.

3. Between 1921 and 1924, the value of the German mark fell by a factor of more than 10 trillion due to overprinting by the government. In 2008, the government of Zimbabwe printed so much of its currency that in a single year, a loaf of bread increased from $1 to $100 billion. In both cases, any savings that people had in the form of national currency were completely destroyed.

4. To say that something is *decentralized* is more or less equivalent to saying that it is run by a group of strangers who don't necessarily trust each other.

In 2008, the problem was elegantly solved by Bitcoin's inventor, known pseudonymously as Satoshi Nakamoto. Satoshi's significant breakthrough made it possible for a digital currency to exist without relying on a central authority. Satoshi described the solution to the Byzantine Generals' Problem and the invention of Bitcoin in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." But the creation of the software that demonstrated the concept in practice was released a year later.

Although the first version of the software was written by Satoshi, it quickly became a community project as the software was improved and maintained by hundreds of volunteers. Currently, the software is open source, and anyone can read and contribute to it. In January of 2009, the first bitcoins were distributed using the early Bitcoin software, and since then transactions have been running smoothly. Slowly but surely, an increasing number of people have started using Bitcoin, and what began as an experiment is now a multibillion dollar economy that processes hundreds of thousands of transactions per day (and is growing quickly).

The Benefits of Using Bitcoin

Bitcoin is an inherently international currency; anyone can send bitcoins to anyone else in the world, in any amount, almost instantly. In addition, it is becoming increasingly possible to travel the world and spend bitcoins without having to change them into the local currency. Because no middleman is involved, transaction fees are negligible. Unlike with credit cards, which require giving online merchants your personal information, you can use bitcoins to shop online while maintaining your privacy. There is no risk of losing your savings due to runaway inflation because bitcoins were designed to have a fixed supply. Bitcoins are also fundamentally impossible to counterfeit.

As a merchant, you can start accepting bitcoins as payment immediately without filling out tedious paperwork (compared to setting up the credit card transaction process). You can also own bitcoins without anyone else knowing, and no third party or government can seize your money. (The privacy this feature entails may protect the security and freedom of political dissidents living under repressive regimes, for example.)

Thanks to all of its benefits, Bitcoin continues to increase in popularity; however, anyone familiar with Bitcoin will agree the technology behind it is difficult to explain and understand. At first blush, it's hard to grasp how bitcoins are stored, how they are used, or even where they come from.