Contents

Preface

The most important contribution in monetary economics in the twenty-first century is the paper "Bitcoin: A Peer-to-Peer Electronic Cash System." It was published via a mailing list for cryptography in 2008 under the pseudonym *Satoshi Nakamoto*. The basic idea of the paper was to create "a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution."

The Bitcoin developers have linked several technological components together to create a virtual asset that is substantially different from any other asset. For the first time, ownership of virtual property is possible without the need for a central authority—a development with the potential to fundamentally change the current financial system and many more areas in business and government.

As with any fundamental innovation, the true potential of this new technology will become apparent only many years—or possibly decades—after it is widely adopted. As of now, the most apparent application is Bitcoin as a virtual asset. It is likely that cryptoassets will emerge as their own asset class and develop into an interesting investment and diversification instrument. Bitcoin itself could, over time, assume a role similar of that of gold.

The aim of this book is to introduce the reader to cryptocurrencies and blockchain technology. The focus is on Bitcoin, but many elements are shared by other blockchain implementations and alternative cryptoassets. As with any fundamental innovation, it is amazing how difficult it is to put the concept into simple words. The question "What is Bitcoin?" opens up a whole spectrum of possible explanations. If Bitcoin is reduced to a monetary asset, such as digital cash, false expectations arise, and Bitcoin may appear uninteresting or even irrelevant. To capture the complexity and potential of Bitcoin and blockchain technology, the reader must be willing to apprehend knowledge from the disciplines of economics, cryptography, and computer science (figure 0.1).

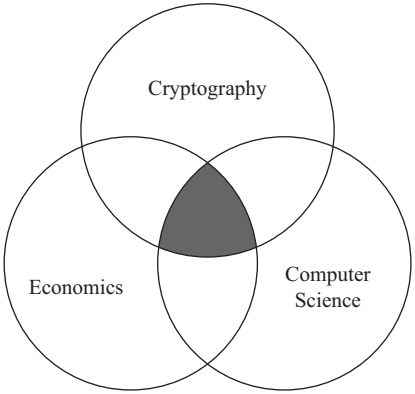

Figure 0.1
Interdisciplinarity of Bitcoin

Bitcoin does not belong to any person or company, nor is it controlled by any single entity. Rather, Bitcoin is an autonomous construct with a multitude of different stakeholders, which shape the system through complex interactions and incentive structures. This independence enables the technology to establish virtual property without the need for a central authority for the first time in history. This achievement is a technological breakthrough.

Before the invention of the Bitcoin blockchain, a consensus about ownership of a virtual asset could only be reached through centralization. In centralized systems, an institution is exclusively endowed with the right of record keeping and hence is responsible for maintaining and establishing property rights. Our current financial infrastructure, for example, relies on centrally managed accounting systems. Centralization creates several problems. With every transaction, user data is collected and centrally stored. This leads to a lack of privacy and creates a central point of attack (so-called data honey pots) as the many recent data breaches show. Further, centralized records can be easily manipulated (internal as well as external), and these play such an important role that they quickly become systemically relevant. Finally, in centralized systems individuals can be excluded from participation, and their assets can be easily confiscated. The decentralized nature of the Bitcoin system makes it immune to many of these problems.

The Bitcoin developers have provided a basic framework which serves as the foundation for a large number of new applications. Analogous to the TCP/IP protocol that enabled the prospering of the internet, Bitcoin technology can be used to represent virtual property in the broadest sense. Virtual claims to real estate, bank money, and company shares are just as conceivable as claims to postal stamps, domain names, or

intellectual property rights. Any real asset can be tokenized and traded worldwide 24/7 without intermediaries on decentralized exchanges. Other applications include smart contracts and autonomous organizations. Finally, because it is very difficult to change records retroactively, the Bitcoin blockchain can be used to serve as proof that a specific data file existed in a particular form at a specific point in time.

The book consists of three parts and eight chapters. The first part of the book is a nontechnical introduction which requires no previous knowledge. Bitcoin was developed with the goal of creating a new kind of monetary unit. Therefore, in chapter 1 we focus on monetary theory to better understand the original motivation behind the Bitcoin system. We discuss the role of money for an economy and analyze the components of value of a monetary unit. We then distinguish between different types of money and study their basic characteristics and control structures. This chapter will help set the stage to understand how cryptocurrencies like Bitcoin are a radical departure from existing monetary instruments. In chapter 2 we begin our analysis of the Bitcoin system, and we introduce blockchain technology by presenting the main building blocks in a nontechnical way. This chapter serves as an overview of the Bitcoin technology that aims to highlight the innovative character of the Bitcoin system.

Part II includes the most challenging chapters of the book and deals mainly with the technical aspects of the Bitcoin system. Chapter 3 introduces the Bitcoin network and differentiates between various types of network participants. We consider the Bitcoin communications protocol, analyze various types of messages, and explain how network participants interact. Chapter 4 explains how Bitcoin units can be assigned to an individual and which principles of mathematics enable a decentralized validation of a transaction's legitimacy. For this purpose, we introduce pseudonyms and expand on the necessary cryptographic foundations. We also present the various transaction types as well as the specific conditions that have to be fulfilled for Bitcoin units to be transmitted. Finally, we look at signature hash types and more recent protocol changes such as Segregated Witness. Chapter 5 explains how transactions find their way into the Bitcoin blockchain and show how the network is able to reach consensus on the current state of the ledger. We study the data structure of blocks; discuss how these blocks are linked together; and analyze the basics of Bitcoin mining, the underlying game theory, and the proof-of-work consensus mechanism.

Part III of the book is dedicated to specific issues and applications. The Bitcoin technology is fascinating and has the potential to radically change the current financial system and many other sectors. Nevertheless, one has to admit that the technology still faces many hurdles. In chapter 6 we take a closer look at some of these challenges and discuss potential solutions. The challenges include high price volatility, scalability,

energy consumption, and regulatory uncertainty. Further, we discuss hot topics such as central bank cryptocurrencies and stablecoins. The Bitcoin blockchain provides an infrastructure that enables numerous non-monetary applications. Chapter 7 discusses alternative applications and is intended to provide an outlook outside the purely monetary area. The applications discussed are decentralized verification and attestation, tokens, smart property, and blockchain contracts (smart contracts). Finally, chapter 8 provides some practical advice on how to get started using Bitcoin. It considers several possibilities for procuring and safeguarding Bitcoin units and indicates some of the risks and errors that users should avoid. It also discusses how to make and receive Bitcoin payments.

Our book is aimed at students and practitioners who would like to familiarize themselves with the subject. The interdisciplinary approach and the technical completeness ensure that it is equally interesting and worth reading for beginners and advanced readers.

We would like to take this opportunity to thank the Förderverein des Wirtschaftswissenschaftlichen Zentrum der Universität Basel and the Federal Reserve Bank of Saint Louis for supporting this project. Further thanks go to the following persons and to all those who supported and accompanied us in the development process of this book: Florian Bitterli, George E. Fortier, Pascal Gantenbein, Stefan Gehrig, Brigitte Guggisberg, Raphael Mani, Marina Markheim, Matthias Mohler, Remo Nyffenegger, Edith Schär, Michèle Schär, Joachim Setlik, and Christopher Waller.