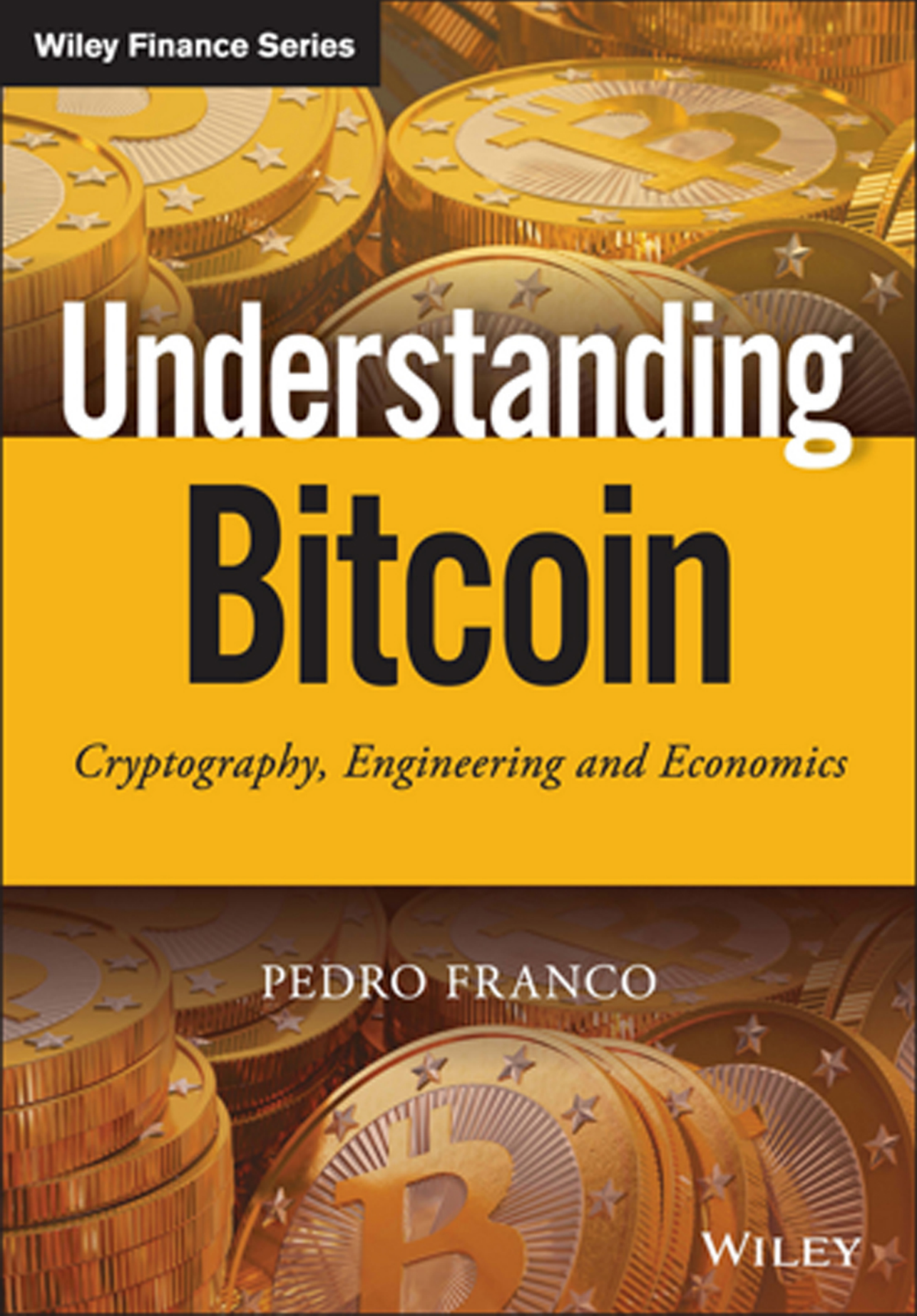
Wiley Finance Series
Understanding
Bitcoin
Cryptography, Engineering and Economics
PEDRO FRANCO
WILEY

Understanding Bitcoin

Cryptography, engineering, and economics

PEDRO FRANCO

WILEY

This edition first published 2015

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

A catalog record for this book is available from the Library of Congress.

A catalogue record for this book is available from the British Library.

ISBN 9781119019169 (hardback/paperback) ISBN 9781119019145 (ebk)
ISBN 9781119019152 (ebk) ISBN 9781119019138 (ebk)

Cover design: Wiley
Cover image: © Shutterstock/Lightboxx

Set in 10 pt Times New Roman by Sparks – www.sparkspublishing.com
Printed in Great Britain by TJ International Ltd, Padstow, Cornwall, UK

Dedicated to Alvaro, Rafael, Luis, and Nayra

Contents

About the Author

Pedro Franco was born in Astorga, Leon (Spain). He holds a MSc in Electrical Engineering from ICAI, a BSc in Economics, and an MBA from INSEAD. Pedro has been a consultant with McKinsey and Boston Consulting Group and a researcher with IIT prior to gaining more than 10 years of experience in financial markets holding Quant and Trading positions in Credit, Counterparty Risk, Inflation, and Interest Rates. He has created various mathematical libraries for financial derivatives, and managed teams of software developers.

The author can be contacted at pfrancobtc@gmail.com.

Acknowledgments

Thanks to Juan Ramirez for helping me gather the courage to write this book.

Thanks to Jon Beracoechea, Manuel Castro, and Robert Smith for exhaustively reviewing an early version of the book and providing many excellent suggestions. Thanks also to Eli Ben-Sasson, Alejandro and Alvaro Franco, Jeff Lim, Jan Pelzl, Stefan Thomas, Evan Schwartz, Rodrigo Serrano, Alena Vranova, and Bob Way for reviewing parts of the book and providing insightful comments.

Finally, thanks to my family for their patience and support; without them this book could not have been written.

Foreword

I have been hoping for some time for a good book covering the technology and ideas behind Bitcoin to be written.

There is certainly a wealth of information about cryptocurrencies, but the field advances rapidly and it is sometimes difficult for the non-initiated to understand the fundamentals and catch up with new developments. This book takes readers to a thorough understanding of the current state-of-the-art cryptocurrencies' technology, as well as its future economic and technological implications, without assuming any previous knowledge of the many fields than constitute Bitcoin. This is an enabling book that empowers the reader to participate in and contribute to this great adventure.

The book clearly exposes many concepts previously mainly known to insiders of the cryptocurrencies' world. It covers a wide range of topics, from the economics or the basic technology (such as elliptic curve cryptography, Merkle trees or the blockchain) to advanced cryptographic concepts (such as non-interactive zero-knowledge proofs), and explores many applications based on these ideas (such as multi-signature wallets or fully anonymous payment systems). All this is accomplished in a book that is very approachable and comprehensible.

Readers new to Bitcoin will surely be surprised by the ingenuity of the technology and the broad range of applications it enables. Those familiar with Bitcoin will find many sections, such as the sections on economics or advanced applications of cryptocurrencies, informative and thought provoking.

I believe Pedro's book will be well received in the business and financial community as well as by the general public, spreading the knowledge about Bitcoin and contributing to this technology crossing the chasm to the early majority.

Jeff Garzik
Bitcoin Core Developer at BitPay, Inc.

Prologue

– What is Bitcoin?
– It's a digital currency.
– Yeah, I get that, but who is behind Bitcoin?
– Nobody.
– What do you mean by nobody? Somebody must be controlling it!
– Nobody is controlling it, it is an algorithm.
– What? You mean like Terminator? So you say the world is going to be taken over by machines?
– Well, not the world, but maybe some businesses.
– Right... (rolling her eyes) But who controls the algorithm? Some mad scientist?
– It's an open source project.
– An open what?
– Yes, free code. You can download it from the internet and do with it whatever you want.
– So you don't have to pay for the "program"?
– Well, it's free as in freedom, not free as in beer.
– What does beer have to do with it?
– The code is not only free in the sense that you can use the program free of charge. It is also free in the sense that you can take the code, modify it, and release a program of your own with it.
– Wait a second! If I can do that then I can make my own bitcoins. What value does a bitcoin have then?
– No, you cannot mint your own bitcoins. What you can do is invent your own currency. And then you have to somehow make it gain acceptance...
– Oh, but this surely is the end of Bitcoin. If you can make as many currencies as you want, none of them would have any value.
– Currencies have value because of social convention. Bitcoin has value because people are willing to give value to it.
– I don't think you are right. Euros or dollars have value, everybody knows that.
– Well if bitcoins do not have value I will gladly accept your bitcoins (smiling).
– Bitcoins are not backed by anything so they cannot have value.
– Neither euros, dollars nor Bitcoin are backed by anything. You can say that all of them are the result of consensual hallucination. They have value because people give value to them. There is not much difference between them in this regard.
– I don't think so. You can buy things with euros or dollars, but what can you buy with bitcoins?

– You can buy almost anything with bitcoins. There are companies that will gladly accept your bitcoins in return for regular currency that you can use to buy anything. Converting bitcoins to sovereign currencies is just a technical interface and many companies provide this service. Besides, you can do things with bitcoins that you cannot do with sovereign currencies.
– Like what?
– For example, you could launch a crowd-funding campaign, just creating a special type of Bitcoin transaction.
– That sounds cool.
– There are many more applications that were impossible until now, such as a car which reads its ownership from the cloud. If you want to buy the car, you just pay the owner with bitcoins and the car knows automatically you are its new owner because it can look it up in Bitcoin's database. And there might be more applications to come that nobody has thought of yet, as was the case (and still is) with the internet.
– I guess I did not think of it that way.
– As they say, a currency is just the first application. The technology allows transferring value securely and in a decentralized way and this can lead to many new cool applications.
– I'm intrigued, I'd like to learn more.
– Great! I believe I have the right book for you...

Preface

Opinions about Bitcoin are highly polarized between enthusiasts and skeptics. The author believes that the point of view of the skeptics is easier to grasp for someone not familiar with Bitcoin's technology. The objective of this book is to present the technology and arguments from both sides of the divide so that readers can form an informed opinion of their own.

What drives the passion of the enthusiasts is that Bitcoin is a technological breakthrough that creates many new and interesting applications. As is often the case with brand new technologies, many future applications of the technology might not be envisioned today. Who could have imagined the success of video streaming services or social networks in 1994? Enthusiasts feel the technology will yield many unforeseen applications for many years to come. The fact that most of these applications are intertwined with monetary economics makes it even more interesting.

The economic and technical aspects of Bitcoin are so intertwined that, in the opinion of this author, they should be tackled together. Arguing about one of them without understanding the other would be like trying to run a car with only one pedal: just pressing the gas or the brake pedal. Sure, the driver could descend a mountain with only the brake pedal, but then she could not go much further. Similarly a driver with only the gas pedal could probably ascend a mountain, but she would be better off not trying to descend it. This book covers the technology behind Bitcoin, ranging from cryptography to software engineering to monetary economics.

References to Bitcoin's source code are scattered throughout the text, especially in the technical sections. These references are intended as clues for readers interested in the implementation of the Bitcoin protocol, but can be safely skipped by other readers.

This book is divided into three parts. The first part serves as an introduction to Bitcoin's technology and philosophy (Chapters 1 and 2). This part will also cover the economic arguments both in favor of and against Bitcoin (Chapter 3) and some business applications (Chapter 4). This part is designed for the time-constrained readers who are mostly interested in the business and economic impact of Bitcoin's technology.

The second part covers in detail how Bitcoin works, starting with public key cryptography (Chapter 5), transactions (Chapter 6) and the blockchain (Chapter 7). The last two chapters expand on related topics: wallets (Chapter 8) and mining (Chapter 9). In this line, two additional great resources for developers are the Developer Guide (Bitcoin Foundation, 2014a) and the Reference Guide (Bitcoin Foundation, 2014b) maintained by the Bitcoin Foundation, and the forthcoming book by Andreas Antonopoulos (Antonopoulos, 2014).

The third part completes the cryptocurrencies landscape. First, digital currency technologies preceding Bitcoin are discussed (Chapter 10). Then alternative cryptocurrencies based on Bitcoin (alt-coins) are covered (Chapter 11) and new applications of cryptocurrencies beyond payment systems are explored (Chapter 12). Most of the action in the cryptocurrencies community is focused on these new applications and Chapter 12 will introduce several of the brand new projects that are being built. Bitcoin is not anonymous, and Chapter 13 explores techniques that can be used to de-anonymize users, as well as technologies that are being built to enable users to counter these techniques and enhance their privacy. The chapter concludes with an introduction to the technology, based on zero-knowledge proofs, to create fully anonymous decentralized digital currencies. The book concludes (Chapter 14) with a discussion of some additional technical topics and the latest developments being discussed in the community.

An earlier version of this book has been registered in the blockchain. The hash of this earlier version is

1324585ce12bdf2c16995835e1ba1a04246592e7755c6c1933419fe80f97f10e

and was registered in the blockchain in transaction

e144275426185d0a0b85e7bdcfdfbbaa6f7f750a522007aeaae6f0f8708838bb.

The blog for this book can be found at understandingbitcoin.blogspot.com.

Madrid, July 2014

PART

One

Introduction and Economics

CHAPTER 1

Foundations

There has been ample media coverage of Bitcoin, and many public figures have been compelled to state their opinion. As Bitcoin is a complex topic, covering cryptography, software engineering and economics, it is difficult to grasp its essence and implications with only a superficial look at it. Thus some commentators might not have a clear picture of how it works and the implications. It is the goal of this book to equip the reader with the knowledge to evaluate the merits of this technology.

Figure 1.1 summarizes some misconceptions around Bitcoin.

Bitcoin is a decentralized digital currency. This means there is no person or institution behind it, either backing it or controlling it. Neither is it backed by physical goods, such as precious metals. This might seem counter-intuitive at first glance: how could it exist if no one controls it? Who created it then? How did the creator lose control over it?

The answer to this seeming paradox is that Bitcoin is just a computer program. How exactly this computer program works is the subject of the second part of this book. The program has a creator (or creators) but his identity is unknown as he released the Bitcoin software using what is believed to be a pseudonym: Satoshi Nakamoto. Bitcoin is not controlled in a tight sense by anyone. The creator did not lose control of it because he

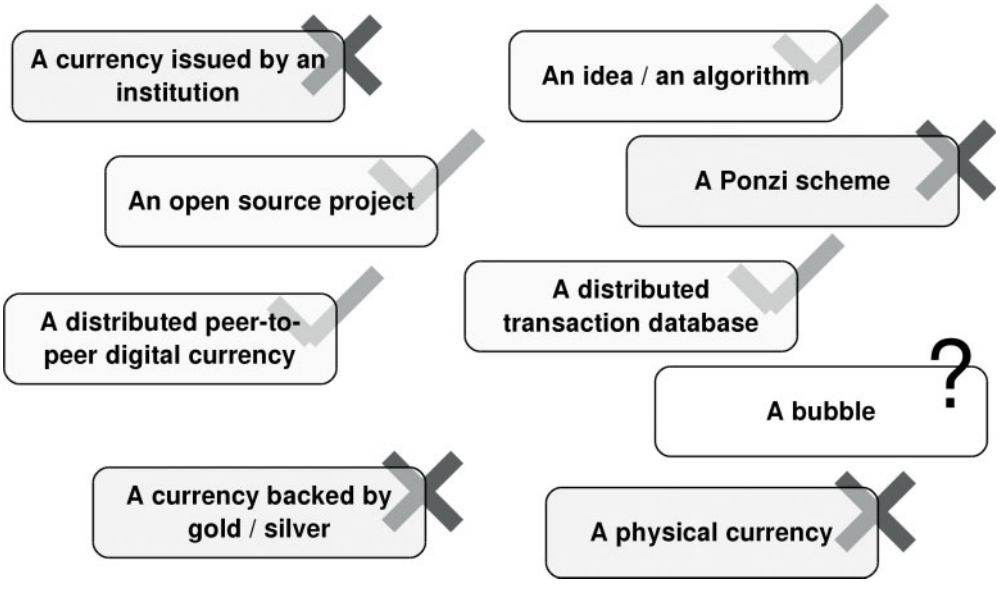

FIGURE 1.1 What Bitcoin is (and isn't)

(she?, they?) never owned the code. The code is **open source** and thus it belongs to the public domain, as will be further explained in section 1.2.

One of the most innovative features of Bitcoin is that it is **decentralized**. There is no central server where Bitcoin is running. Bitcoin operates through a peer-to-peer network of connected computers. Bitcoin is the first digital currency built in a decentralized way, a technological breakthrough. The decentralized nature of Bitcoin will be further explored in section 1.1.

Bitcoin creates its own currency called bitcoin, with a small b. The creation of a currency is integral to how the system operates, as it serves two simultaneous purposes. First, it serves to represent value. Second, issuance of new bitcoins is used to reward operators in the network for securing the distributed ledger. These two functions cannot be unbundled without significantly changing the design.

The heart of the Bitcoin network is a database holding the transactions that have occurred in the past as well as the current holders of the funds. This database is sometimes called a ledger, because it holds the entries representing the owners of the funds. Bitcoin is not the first distributed database to be created. However, the requirements of a financial database are different from those of other applications, such as file sharing or messaging systems. In particular, financial databases must be resilient against users trying to double-spend their funds, which Bitcoin solves elegantly. This is explored in the following sections and in Chapter 2.

Some critics have argued that Bitcoin is a **Ponzi scheme**. **It is not.** In a Ponzi scheme there is a central operator who pays returns to current investors from new capital inflows. First of all, in Bitcoin there is no central operator who can profit from the relocation of funds. Second, there is no mechanism to deflect funds from new investments to pay returns. The only funds recognized in the Bitcoin protocol are bitcoins, the currency. Transfers of bitcoins are initiated by the users at their will: the protocol cannot deflect funds from one user to another. Third, a new investment in Bitcoin is always matched with a disinvestment. Investors who put money into bitcoins usually operate through an exchange where they buy the bitcoins from another investor who is selling her investment. There is simply no new investment flowing into bitcoins: the amount of sovereign currency that has flown into bitcoins exactly matches the amount that has flown out of bitcoins.

However, bitcoin, the currency, can be a bubble. Whether the value of bitcoin crashes, holds, or increases depends on whether bitcoins will be used in the future for different applications. There are several interesting applications for Bitcoin, of which the most straightforward (but not the only) are to serve as a medium of exchange and a store of value. It is too early to tell whether any of these applications will become important in the future. The merits of bitcoins as medium of exchange and store of value are explored in Chapter 3.

Finally, Bitcoin is not just a currency but a whole infrastructure that can be used to transfer value digitally: see section 1.4 and Chapter 12.

1.1 DECENTRALIZED

Most currencies in use today are fiat currencies, where the currency is issued by the government and its supply managed by a central bank.

FIAT MONEY

Most currencies today (Euro, US Dollar) are fiat money. Fiat money does not have intrinsic value, as it is not backed by anything. It is called fiat money because there is a government decree ("fiat") declaring the currency to be legal tender. The acceptance of fiat money depends on expectations and social convention. If confidence in a currency is lost, usually because of irresponsible monetary policy, fiat money can stop being accepted.

Experience has shown that leaving monetary policy in the hands of governments is usually not a good idea, as governments could have an incentive to increase the monetary supply to solve pressing short-term financial problems. This behavior can lead to high inflation and a loss of confidence in the currency.

The conventional solution is to entrust monetary policy to a semi-independent central bank. The central bank is tasked with managing the monetary policy, usually with the goals of economic growth, price stability, and, in some cases, stability of the financial system.

Bitcoin is based on a peer-to-peer network of computers running the software. These computers are called nodes. Participants in the network might be running nodes for different reasons: for profit as in the case of miners (Chapter 9), to manage full-node wallets (Chapter 8), to collect and study information about the network (Chapter 13), or simply as a social good.

Bitcoin's decentralized nature contrasts to the structure of fiat currencies. Central banks make monetary decisions after evaluating evidence gathered from the evolution of the economy. In a decentralized system such as Bitcoin, discretionary decisions are not possible. The original creators of the system have to take most of the decisions upfront at the design phase. These decisions have to be carefully balanced, and take into account the incentives of the different users, otherwise the decentralized system is doomed to fail. In Bitcoin the monetary policy follows a simple rule: the final monetary base is fixed at around 21 million bitcoins and new bitcoins are minted at a planned schedule and paid to users who help secure the network. This serves the double purpose of providing the bitcoins with value due to their scarcity and creating incentives for users to connect to the network and help secure it by providing their computational power.

Control in a centralized system is usually concentrated in an institution or a small group of key people. Thus changes in a centralized system are relatively straightforward to decide and implement. Control in a peer-to-peer network is more subtle: changes in a peer-to-peer network have to be agreed by a majority of the peers at least. But even then, if a strong minority does not agree to a change, implementing the change can be technically challenging as the network runs the risk of a split.

One advantage of the decentralization of power is that changes that are contrary to the interests of most users would be rejected. In contrast, in centralized systems sometimes the outcomes are adverse to most of the participants, as in a currency debasement by excessive printing which usually leads to high inflation.

Another feature of decentralized systems is their resilience. Decentralized systems are robust against attacks either by insiders or by external forces. This feature might have

been critical for the existence of Bitcoin. Earlier centralized attempts to create digital currencies (section 2.1) were forced down by governments. However, to force down a decentralized system, all individual users must be forced down, which is a much harder task. Bitcoin's peer-to-peer nature makes it censorship-resistant, claim its supporters.

The technology to securely (cryptographically) transfer value digitally had been available many years before the creation of Bitcoin (Chapter 10). However, it had always required the creation of a centralized trusted party. Bitcoin not only does not require a central trusted party to operate, but it is also designed to resist the attacks of malicious participants in the peer-to-peer network. As long as these malicious participants do not control a majority of the network these attacks will not succeed (section 7.5).

The main technological breakthrough accomplished by Bitcoin is solving the double-spending problem in a distributed financial database. A double-spend attempt occurs when a user tries to spend some funds twice. All financial systems must reject these attempts. This is relatively straightforward in a centralized system, as transactions are recorded in a central database and future spending attempts are checked against this database first. In a decentralized system, many copies of the database are shared among the peers, and keeping a consistent state of the database is a difficult computational problem[1]. In the context of Bitcoin the problem is how the network can agree on the state of the distributed database when messages between the nodes can be corrupted and there might be attackers trying to subvert the distributed database. Bitcoin gracefully solves this problem (section 2.3 and Chapter 7).

1.2 OPEN SOURCE

Bitcoin is open source software. **Open source** software makes the source code available for anyone to use, modify, and redistribute free of charge. Some well-known open source software products include the Linux and Android operating systems or the Firefox web browser. A large portion of the internet infrastructure runs on less known (but no less important) open source software. The goal of open source is to make software development similar to academic peer-reviewed research. By publishing the source code for anyone to see and check, open source aims to increase the quality of the software.

The difference between open source software and proprietary software lies in their licenses. A proprietary software license grants the right to use a copy of the program to the end user. However, ownership of the software remains with the software publisher. In contrast, an open source license grants the user the right to use, copy, modify, and redistribute the software. The copyright of the software remains with the creator, but the creator of an open source software transfers the rights to the user as long as the obligations of the license are met.

Another difference between proprietary and open source programs is that proprietary programs are usually distributed as compiled binaries. This means that the software is usually distributed in machine language. Users willing to gain knowledge on what the software is doing must interpret the machine code in a time-consuming process called reverse engineering (Eilam, 2005). Most proprietary licenses forbid the use of these reverse

[1] This computational problem is called the Byzantine Generals' problem, introduced in Lamport et al. (1982).

engineering techniques. Thus under a proprietary license the user is usually not allowed to understand or seek knowledge of what the software is actually doing. In contrast, open source software is always distributed with a copy of the source code. A user who wants to understand what the software is doing can just read the source code. Cryptographic open source software has the advantage that it allows users to check that the code does not contain any backdoor or security vulnerabilities[2].

It is unlikely that Bitcoin could have been released under a proprietary license. Had Bitcoin been released as closed-source, its creator could have easily inserted code that deviated from the specification: say, creating new bitcoins and sending them to an address controlled by him. Most users presumably would not have accepted decentralized cryptographic financial software distributed as a compiled binary and with a proprietary license. It is telling that most competing cryptocurrencies (Chapter 11, section 12.7), have either been launched using an open source license or have switched to an open source license.

Open source licenses grant the user the right to use, copy, modify, and redistribute the software. Different licenses may impose different obligations on the users. Broadly speaking, open source licenses belong to one of two families:

- **"Copyleft."** These licenses impose the obligation to distribute derived works under the same license. If a user of the software makes modifications to it, she is obliged to release the modified software under the same license. This is referred to as the share-alike requirement. Thus "copyleft" licenses preserve the open source nature of the software as it is modified. An example of a "copyleft" license is the **GNU Public License** (**GPL**).
- **"Permissive."** These licenses impose very few restrictions on the redistribution of the software, usually just that the derived software acknowledges the original software and retains the copyright notice. Proprietary software that incorporates software released under an open source permissive license retains its proprietary nature as the license usually only requires that the proprietary software includes the copyright notice. Several common open source licenses belong to this family, such as the BSD license, the MIT License or the Apache License. Bitcoin was released under the MIT license.

Proprietary software requires that the company issuing the software maintains and updates it. In contrast, open source software acquires a life of its own once released. It usually does not matter if an original creator decides to stop working on an open source project, as other developers could take it over. For this reason it does not matter who Satoshi Nakamoto is, or that he has moved on. Open source projects are resilient: even if some developers are forbidden or discouraged to work on a project, other developers from all around the world can take over.

---

[2] This should not be interpreted that open source code does not contain security flaws or backdoors. Indeed, many security flaws have been found in open source projects (Green, 2014b; Poulsen, 2014). Open source advocates argue that it is more difficult to include flaws and backdoors into open source programs because there is a higher level of scrutiny, and that these flaws are typically discovered and repaired sooner than similar flaws placed in proprietary software (Raymond, 2001).

Under an open source license it is legitimate to start a new independent software project from a copy of an original project. This process is called **forking**. The threat of a fork can often keep the developers of an open source project honest. If the developers of a project introduce changes that are detrimental to the users of the software, anybody can create a fork, undo those changes and continue the development. Users will most likely follow the fork without the undesired features. Thus forking can be seen as a kill switch that prevents developers from evolving a project against their users. Most large open source projects are rarely forked[3]. Bitcoin is somewhat special in this respect, as it has been forked many times by developers wishing to test new concepts. This has given rise to many alternative cryptocurrencies called alt-coins. Alt-coins will be covered in more detail in Chapter 11.

Open source advocates argue that companies releasing proprietary software often lose the incentive to innovate once a product has achieved a dominant market position. Many software markets behave like natural monopolies where a product with first mover advantage can capture a large market share. Thus innovation in many software categories is low, these advocates suggest. In contrast, if an open source software captures the majority of the market this does not bring about the end of innovation, as anybody can keep on adding improvements to the software. Thus the pace of innovation in open source software can be higher than in closed source software.

One problem facing many open source projects is the **tragedy of the commons**. Although many people benefit from an open source project, few developers might have an incentive to contribute to it. Many open source projects face difficulties in getting appropriate funding or development time. There have been some indications that Bitcoin could be facing this problem (Bradbury, 2014b).

An exposition of the merits of open source software can be found in Raymond (2001).

1.3 PUBLIC ASSET LEDGER

The heart of Bitcoin is a distributed database that holds a copy of the common asset ledger. As this database is distributed, each participant in the network (a node) keeps a copy of it. Copies of this database kept by the different nodes are consistent by design.

On the other hand, every user is in control of her own funds, through a cryptographic private key. When a user wishes to spend some funds, she must use this private key to sign a message that states who she wishes to send the funds to as well as the amount to send. The user broadcasts this signed message to the network, and every participant in the network receives a copy of it. Then each node can independently verify the validity of the message and update its internal database accordingly[4].

---

[3] Most projects are really forked many times by individual users wishing to tinker with them or test new features. However, forks of large open source projects that split the developer base, such as the LibreOffice fork from OpenOffice (Paul, 2011), are rather rare.

[4] The process is actually more involved to prevent double-spending attacks where a user sends different messages to different parts of the network. How Bitcoin prevents double-spending attacks is the subject of Chapter 7.