**Preface 前言**

**Writing the Bitcoin Book 关于本书的写作**

I first stumbled upon bitcoin in mid-2011. My immediate reaction was more or less "Pfft! Nerd money!" and I ignored it for another six months, failing to grasp its importance. This is a reaction that I have seen repeated among many of the smartest people I know, which gives me some consolation. The second time I came across bitcoin, in a mailing list discussion, I decided to read the whitepaper written by Satoshi Nakamoto to study the authoritative source and see what it was all about. I still remember the moment I finished reading those nine pages, when I realized that bitcoin was not simply a digital currency, but a network of trust that could also provide the basis for so much more than just currencies. The realization that "this isn’t money, it’s a decentralized trust network," started me on a four-month journey to devour every scrap of information about bitcoin I could find. I became obsessed and enthralled, spending 12 or more hours each day glued to a screen, reading, writing, coding, and learning as much as I could. I emerged from this state of fugue, more than 20 pounds lighter from lack of consistent meals, determined to dedicate myself to working on bitcoin.

我第一次偶遇比特币是在2011年年中，当时的反应大概是“哈！书呆子的钱嘛！”因为没能领会它的重要性，我忽视它长达六个月之久，而让我稍感宽慰的是，许多我认识的一些聪明绝顶人也是这种反应。在一次邮件列表讨论时，我再次接触到了比特币，于是决定阅读中本聪（Satoshi Nakamoto）写的白皮书，研究比特币的权威解释，看看到底是怎么一回事。我仍记得刚刚读完那九页内容的那一刻，那时我才终于明白了：比特币不单单是一种数字货币，还是一种给货币及其他很多东西提供基础的信任网络。对“不是货币，而是去中心化信任网络”的领悟，让我开启了为期四个月的比特币沉醉之旅。我如饥似渴地寻找任何关于比特币的点滴信息，变得越来越着迷，每天都花上12 个小时以上紧盯屏幕，竭尽所能地不断阅读、写作、学习和编程。从这段着魔的状态中走出来的时候，我的体重由于前期没有规律饮食轻了20 多磅，同时我也坚定了要全心投入比特币事业的决心。

Two years later, after creating a number of small startups to explore various bitcoin-related services and products, I decided that it was time to write my first book. Bitcoin was the topic that had driven me into a frenzy of creativity and consumed my thoughts; it was the most exciting technology I had encountered since the internet. It was now time to share my passion about this amazing technology with a broader audience.

随后的两年，我创立了一系列开发比特币相关服务和产品的公司，之后我决定写我的第一本书。书的主题就是激发了我疯狂的创造力并让我冥思苦想的比特币，它是我在继互联网之后遇到的最为振奋人心的技术。现在是时候跟更广大的读者分享我对这项惊人技术的热情了。

**Intended Audience 目标读者**

This book is mostly intended for coders. If you can use a programming language, this book will teach you how cryptographic currencies work, how to use them, and how to develop software that works with them. The first few chapters are also suitable as an in-depth introduction to bitcoin for noncoders—those trying to understand the inner workings of bitcoin and cryptocurrencies.

本书主要面向程序员。如果你能使用一门编程语言，本书将会告诉你加密货币的原理、使用方法，以及如何开发与之相关的软件。对希望理解比特币及加密货币内在工作机制的非程序员读者们，本书前几章作为对比特币的深入介绍依然适用。

**Why Are There Bugs on the Cover? 封面故事**

The leafcutter ant is a species that exhibits highly complex behavior in a colony super-organism, but each individual ant operates on a set of simple rules driven by social interaction and the exchange of chemical scents (pheromones). Per Wikipedia: "Next to humans, leafcutter ants form the largest and most complex animal societies on Earth." Leafcutter ants don’t actually eat leaves, but rather use them to farm a fungus, which is the central food source for the colony. Get that? These ants are farming!

在群居生物物种中，切叶蚁表现出了高度复杂行为的物种特征。但是，群落中的每一只蚂蚁个体仅仅遵循一些社会互动和化学气味（即信息素）交换的简单规则。维基百科提到：“切叶蚁形成地球上仅次于人类的最为庞大且复杂的动物社会。”实际上，切叶蚁不吃叶子，而是使用叶子制造一种真菌来充当蚁群主要食物来源。意识到了吗？它们在耕作！

Although ants form a caste-based society and have a queen for producing offspring, there is no central authority or leader in an ant colony. The highly intelligent and sophisticated behavior exhibited by a multimillion-member colony is an emergent property from the interaction of the individuals in a social network.

虽然切叶蚁形成的是阶级社会，且依靠蚁后繁衍后代，但是在蚁群中不存在中央集权体制或领导人。通过切叶蚁我们可以看到，群落中数百万成员所展现的高度智能且复杂的行为是社会网络中的个体互动这一性质的凸显。

Nature demonstrates that decentralized systems can be resilient and can produce emergent complexity and incredible sophistication without the need for a central authority, hierarchy, or complex parts.

大自然向我们证明，去中心化体制具有弹性并能创造出意想不到的复杂性和难以想象的精妙，而不需要中央集权体制、等级制度或复杂的组织结构。

Bitcoin is a highly sophisticated decentralized trust network that can support myriad financial processes. Yet, each node in the bitcoin network follows a few simple mathematical rules. The interaction between many nodes is what leads to the emergence of the sophisticated behavior, not any inherent complexity or trust in any single node. Like an ant colony, the bitcoin network is a resilient network of simple nodes following simple rules that together can do amazing things without any central coordination.

比特币网络正是这样一个高度复杂的去中心化的可信网络，能够支撑无数财务流程。然而，比特币网络的每一个节点都遵循着一些简单的数学准则。节点间的相互作用促成引起了组织的复杂行为，而并不是任何某个单一节点自身具有复杂性和可信性。就像蚁群一样，比特币的弹性网络是一个由众多遵循简单准则的简单节点所组成的弹性网络，这些简单的节点准则聚合在一起可以完成惊人的事情，而不需要任何中枢协调。

**Conventions Used in This Book 本书惯例**

The following typographical conventions are used in this book:

本书采用以下排版上的约定:

***Italic***

Indicates new terms, URLs, email addresses, filenames, and file extensions.

***斜体***

指示新的术语、URL链接、email地址、文件名和文件扩展名

***Constant width***

Used for program listings, as well as within paragraphs to refer to program elements such as variable or function names, databases, data types, environment variables, statements, and keywords.

***等宽字***

用于程序清单的显示，也用于段落中涉及的程序要素，如变量或函数名、数据库、数据类型、环境变量、语句和关键字。

***Constant width bold***

Shows commands or other text that should be typed literally by the user.

***等宽粗体***

显示需要由用户输入的命令和其他文字。

***Constant width italic***

Shows text that should be replaced with user-supplied values or by values determined by context.

***等宽斜体***

显示需要由用户提供的或根据上下文环境修改的值。

|  |  |
| --- | --- |
| Tip | This icon signifies a tip or suggestion. |
| Note | This icon signifies a general note. |

|  |  |
| --- | --- |
| Warning | This icon indicates a warning or caution. |

[提示] 表示提示或建议

[说明] 表示一般的说明

[警告] 表示警告或提醒

**Code Examples 代码示例**

The examples are illustrated in Python, C++, and using the command line of a Unix-like operating system such as Linux or macOS. All code snippets are available in the GitHub repository (<https://github.com/bitcoinbook/bitcoinbook>) in the *code*subdirectory of the main repo. Fork the book code, try the code examples, or submit corrections via GitHub.

本书示例是基于类Unix 操作系统（例如Linux 或Mac OS X）的命令行，用Python，C++编程语言来说明的。全部代码段均可在Github 主代码库中的code 子目录获得。读者可以通过GitHub 创建自己的代码分支，尝试书中示例，或者提交代码更正。

All the code snippets can be replicated on most operating systems with a minimal installation of compilers and interpreters for the corresponding languages. Where necessary, we provide basic installation instructions and step-by-step examples of the output of those instructions.

所有代码段在大多数操作系统上都可以通过最小化安装对应语言的编译器和解释器来重现。在必要的地方，本书还提供了基本的安装指令以及每步指令输出的结果。

Some of the code snippets and code output have been reformatted for print. In all such cases, the lines have been split by a backslash (\) character, followed by a newline character. When transcribing the examples, remove those two characters and join the lines again and you should see identical results as shown in the example.

为了便于打印，本书重新格式化了部分代码段和代码输出。在所有此类例子中，每行代码以反斜杠（\）字符和换行符分开。当你需要尝试这些示例时，请删除这两个字符的，把被分隔的两行重连起来，就可以看到与例子中一致的结果了。

All the code snippets use real values and calculations where possible, so that you can build from example to example and see the same results in any code you write to calculate the same values. For example, the private keys and corresponding public keys and addresses are all real. The sample transactions, blocks, and blockchain references have all been introduced in the actual bitcoin blockchain and are part of the public ledger, so you can review them on any bitcoin system.

本书所有代码段尽可能地采用实值计算，因此你可以通过重复构建本书提供的代码示例，用你自己写的代码计算出相同的结果。譬如，书中出现的私钥和对应的公钥及地址也都是真实存在的。示例中的所有交易、区块和区块链均被记录在实际的比特币区块链中，是公共账目的一部分，因而你可以在任何比特币系统中检查它们。

**Using Code Examples 使用代码示例**

This book is here to help you get your job done. In general, if example code is offered with this book, you may use it in your programs and documentation. You do not need to contact us for permission unless you’re reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O’Reilly books does require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product’s documentation does require permission.

本书的目的是帮助你完成工作。总的来说，你可以在你的程序和文档中使用本书的代码示例。除非你要复制代码的关键部分，否则不需要联系我们获得许可。例如，使用程序中的几段代码，或者引用本书及代码来回答问题是不需要获准的；而售卖或分发包含O’Reilly书中代码示例的光盘，或者将大量书中代码合并于你的产品或文档则必须获得我们的许可。

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, and ISBN. For example: “*Mastering Bitcoin* by Andreas M. Antonopoulos (O’Reilly). Copyright 2017 Andreas M. Antonopoulos, 978-1-491-95438-6.”

我们鼓励、但不强制要求您在引用本书时表明出处。书目引用格式通常包括书名、作者、出版商、ISBN。例如:“精通比特币，Andreas•M•Antonopoulos(O’Reilly)。版权2017 Andreas•M•Antonopoulos, 978-1-491-95438-6.”

Some editions of this book are offered under an open source license, such as [CC-BY-NC](https://creativecommons.org/licenses/by-nc/4.0/), in which case the terms of that license apply.

本书某些版本提供了开源许可，如CC-BY-NC，这种情况下,开源许可条款适用。

If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at [permissions@oreilly.com](mailto:permissions@oreilly.com).

如果你觉得你对本书代码示例的使用超出了合理范围或上述许可，请随时与我们联系:permissions@oreilly.com。

**Bitcoin Addresses and Transactions in This Book 书中涉及的比特币地址与交易**

The bitcoin addresses, transactions, keys, QR codes, and blockchain data used in this book are, for the most part, real. That means you can browse the blockchain, look at the transactions offered as examples, retrieve them with your own scripts or programs, etc.

书中的比特币地址、交易、密钥、二维码、区块链数据大部分都是真实的。这就意味着你可以通过脚本或程序等方式在比特币区块链中查看示例中给出的交易。

However, note that the private keys used to construct addresses are either printed in this book, or have been "burned." That means that if you send money to any of these addresses, the money will either be lost forever, or in some cases everyone who can read the book can take it using the private keys printed in here.

然而，需要注意的是创建地址的这些私钥要么写入书中，要么已经被“焚毁”。这就意味着如果你往这些地址中转入比特币的话，这些比特币要么永远丢失，要么被本书的其他读者通过书中给出的私钥拿走。

|  |  |
| --- | --- |
| Warning | DO NOT SEND MONEY TO ANY OF THE ADDRESSES IN THIS BOOK. Your money will be taken by another reader, or lost forever. |

警告:不要给书中给出的任何地址转比特币，否则你的钱将永远消失或被本书其他读者拿走。

**O’Reilly Safari**

|  |  |
| --- | --- |
| Note | [*Safari*](http://oreilly.com/safari) (formerly Safari Books Online) is a membership-based training and reference platform for enterprise, government, educators, and individuals. |

说明：Safari (正式名称为Safari在线书店) 是一个为企业、政府、教育家以及个人提供会员制的培训与参考的平台。

Members have access to thousands of books, training videos, Learning Paths, interactive tutorials, and curated playlists from over 250 publishers, including O’Reilly Media, Harvard Business Review, Prentice Hall Professional, Addison-Wesley Professional, Microsoft Press, Sams, Que, Peachpit Press, Adobe, Focal Press, Cisco Press, John Wiley & Sons, Syngress, Morgan Kaufmann, IBM Redbooks, Packt, Adobe Press, FT Press, Apress, Manning, New Riders, McGraw-Hill, Jones & Bartlett, and Course Technology, among others.

会员可以在该平台获取来自超过250家出版社提供的成千上万的书籍、培训视频、学习路径、交互教程、策划播放列表，这些公司包括：Prentice Hall Professional, Addison-Wesley Professional, MicrosoftPress, Sams, Que, Peachpit Press, Adobe, Focal Press, Cisco Press, John Wiley& Sons, Syngress, Morgan Kaufmann, IBM Redbooks, Packt, Adobe Press, FTPress, Apress, Manning, New Riders, McGraw-Hill, Jones & Bartlett以及CourseTechnology，除此之外还有其他很多公司。

For more information, please visit [*http://oreilly.com/safari*](http://oreilly.com/safari).

要获取更多信息，请访问:<http://oreilly.com/safari>

**How to Contact Us**

Please address comments and questions concerning this book to the publisher:

* O’Reilly Media, Inc.
* 1005 Gravenstein Highway North
* Sebastopol, CA 95472
* 800-998-9938 (in the United States or Canada)
* 707-829-0515 (international or local)
* 707-829-0104 (fax)

To comment or ask technical questions about this book, send email to [*bookquestions@oreilly.com*](mailto:bookquestions@oreilly.com).

For more information about our books, courses, conferences, and news, see our website at [http://www.oreilly.com](http://www.oreilly.com/).

Find us on Facebook: <http://facebook.com/oreilly>

Follow us on Twitter: <http://twitter.com/oreillymedia>

Watch us on YouTube: <http://www.youtube.com/oreillymedia>

**Contacting the Author 联系作者**

You can contact me, Andreas M. Antonopoulos, on my personal site: <https://antonopoulos.com/>

Information about *Mastering Bitcoin* as well as the Open Edition and translations are available on: <https://bitcoinbook.info/>

Follow me on Facebook: <https://facebook.com/AndreasMAntonopoulos>

Follow me on Twitter: <https://twitter.com/aantonop>

Follow me on Linkedin: <https://linkedin.com/company/aantonop>

Many thanks to all my patrons who support my work through monthly donations. You can follow my Patreon page here:<https://patreon.com/aantonop>

你可以在我的个人网站联系我（Andreas M. Antonopoulos）:<https://antonopoulos.com/>

《精通比特币》的信息以及开放版本与翻译的信息可以在此网址获取:<https://bitcoinbook.info/>

请关注我Facebook账号:<https://facebook.com/AndreasMAntonopoulos>

请关注我Twitter账号:<https://twitter.com/aantonop>

请关注我领英账号:<https://linkedin.com/company/aantonop>

特别感谢所有的赞助人，是他们支持我了数月的工作。你可以访问我的赞助人网站：<https://patreon.com/aantonop>

**Acknowledgments 致谢**

This book represents the efforts and contributions of many people. I am grateful for all the help I received from friends, colleagues, and even complete strangers, who joined me in this effort to write the definitive technical book on cryptocurrencies and bitcoin.

这本书的出版浓缩了很多人的努力与付出。在写书的过程中，我很感激来自从朋友、同事、甚至陌生人的帮助，是他们的加入与努力帮助我完成了这本关于数字货币和比特币的纯技术类书籍。

It is impossible to make a distinction between the bitcoin technology and the bitcoin community, and this book is as much a product of that community as it is a book on the technology. My work on this book was encouraged, cheered on, supported, and rewarded by the entire bitcoin community from the very beginning until the very end. More than anything, this book has allowed me to be part of a wonderful community for two years and I can’t thank you enough for accepting me into this community. There are far too many people to mention by name—people I’ve met at conferences, events, seminars, meetups, pizza gatherings, and small private gatherings, as well as many who communicated with me by Twitter, on reddit, on bitcointalk.org, and on GitHub who have had an impact on this book. Every idea, analogy, question, answer, and explanation you find in this book was at some point inspired, tested, or improved through my interactions with the community. Thank you all for your support; without you this book would not have happened. I am forever grateful.

我们不可能将比特币技术与比特币社区区分开，因为这本书不仅是社区的产品，也是比特币技术。我写这本书的工作从始至终都得到了整个社区的鼓励、欢呼、支持与奖励。最重要的是，这本书让我2年来成为这个极好社区的一部分，我无法用言语表达你们接纳我成为社区成员的感谢之情。这写书的过程中有太多的人需要感谢，以至无法用一一列举，这些人包括我在会议、重大事件、研讨会、聚会、比萨聚会以及小型私人集会，同时还有那些在Twitter、reddit、bitcointalk.org以及GitHub上与我联系，并对本书成稿有影响的人。你在本书中找到的每个想法、类比、问题、回答以及解释，都是在我与社区人员沟通交流时产生的，并得到验证和优化的结果。谢谢所有支持过我的人，没有你们的支持将不会有这本书的存在。对此，我将永远心存感激。

The journey to becoming an author starts long before the first book, of course. My first language (and schooling) was Greek, so I had to take a remedial English writing course in my first year of university. I owe thanks to Diana Kordas, my English writing teacher, who helped me build confidence and skills that year. Later, as a professional, I developed my technical writing skills on the topic of data centers, writing for *Network World* magazine. I owe thanks to John Dix and John Gallant, who gave me my first writing job as a columnist at *Network World* and to my editor Michael Cooney and my colleague Johna Till Johnson who edited my columns and made them fit for publication. Writing 500 words a week for four years gave me enough experience to eventually consider becoming an author.

当然，我是经过了很长一段时间才成为作家并编写了第一本书。我的第一语言是希腊语，因此我需要在大学一年级时接受英语写作补习课程。我要感谢我的英语写作老师Diana Kordas，那年是他帮助我建立了自信和写作技能。随后，作为教授，在为《NetworkWorld》杂志撰稿时，我提升了自己在数据中心方面的写作技能。我要感谢John Dix and John Gallant，他们给了我第一份写作方面的工作，让我成为《Network World》杂志的专栏作者，还要感谢我的编辑Michael Cooney和我的同事Johna Till Johnson，是他们帮我编辑我的专栏文章，让它们得以发表。 四年每周500字的写作经验最终给了我足够的信心成为一名作家。

Thanks also to those who supported me when I submitted my book proposal to O’Reilly, by providing references and reviewing the proposal. Specifically, thanks to John Gallant, Gregory Ness, Richard Stiennon, Joel Snyder, Adam B. Levine, Sandra Gittlen, John Dix, Johna Till Johnson, Roger Ver, and Jon Matonis. Special thanks to Richard Kagan and Tymon Mattoszko, who reviewed early versions of the proposal and Matthew Taylor, who copyedited the proposal.

还要感谢那些在我提交本书稿件至 O’Reilly出版社时那些帮助过我的人，他们为我提供参考和稿件审阅。特别要感谢JohnGallant、Gregory Ness、Richard Stiennon、Joel Snyder、Adam B. Levine、Sandra Gittlen、John Dix、Johna Till Johnson、Roger Ver以及Jon Matonis。特别感谢Richard Kagan、Tymon Mattoszko和Matthew Taylor，Richard Kagan、Tymon Mattoszko帮我审阅了本书早期稿件，MatthewTaylor帮我修改了稿件。

Thanks to Cricket Liu, author of the O’Reilly title *DNS and BIND*, who introduced me to O’Reilly. Thanks also to Michael Loukides and Allyson MacDonald at O’Reilly, who worked for months to help make this book happen. Allyson was especially patient when deadlines were missed and deliverables delayed as life intervened in our planned schedule. For the second edition, I thank Timothy McGovern for guiding the process, Kim Cofer for patiently editing, and Rebecca Panzer for illustrating many new diagrams.

感谢《DNS and BIND》的作者Cricket Liu，是他将我介绍给了O’Reilly出版社。还要感谢O’Reilly 的Michael Loukides和Allyson MacDonald，是他们花费数月时间帮助出版本书。当最终稿件因为种种原因未按计划提交而错过出版截止日期时，Allyson表现地特别耐心。对于第2版，我要感谢Timothy McGovern的全程指导、Kim Cofer的耐心编辑以及 RebeccaPanzer帮助插入了许多新图表。

The first few drafts of the first few chapters were the hardest, because bitcoin is a difficult subject to unravel. Every time I pulled on one thread of the bitcoin technology, I had to pull on the whole thing. I repeatedly got stuck and a bit despondent as I struggled to make the topic easy to understand and create a narrative around such a dense technical subject. Eventually, I decided to tell the story of bitcoin through the stories of the people using bitcoin and the whole book became a lot easier to write. I owe thanks to my friend and mentor, Richard Kagan, who helped me unravel the story and get past the moments of writer’s block. I thank Pamela Morgan, who reviewed early drafts of each chapter in the first and second edition of the book, and asked the hard questions to make them better. Also, thanks to the developers of the San Francisco Bitcoin Developers Meetup group as well as Taariq Lewis and Denise Terry for helping test the early material. Thanks also to Andrew Naugler for infographic design.

最初的一些章节的草稿是最难写的部分，因为比特币一个很难说清楚的主题。每次我研究比特币中某个主题时，我还得考虑整体的技术内容。当我努力想将主题说得简单易懂，围绕这样一个密集型技术主题展开叙述时，我不断地被卡住并有点沮丧。最终，我决定以讲述人们使用比特币的故事为主线来编写本书，从而让我可以轻松地编写本书。我要感谢我的导师兼朋友，Richard Kagan，是他帮助我想到了以故事方式来编写此书，让我跨过了编者的阻碍。我要感谢PamelaMorgan，他审阅了本书第一版与第二版的早期草稿的每个章节，并且提出了很好的改进意见，让本书内容质量更高。同时，还要感谢San Francisco比特币开发者组织小组，还要感谢帮助测试早期材料的TaariqLewis和Denise Terry。感谢Andrew Naugler帮助设计信息图标。

During the development of the book, I made early drafts available on GitHub and invited public comments. More than a hundred comments, suggestions, corrections, and contributions were submitted in response. Those contributions are explicitly acknowledged, with my thanks, in [Early Release Draft (GitHub Contributions)](https://github.com/jieming2002/MasterBitcoin2ndCn/blob/master/0.2%20%E5%89%8D%E8%A8%80.asciidoc#github_contrib). Most of all, my sincere thanks to my volunteer GitHub editors Ming T. Nguyen (1st edition) and Will Binns (2nd edition), who worked tirelessly to curate, manage and resolve pull requests, issue reports, and perform bug fixes on GitHub.

在本书编写的过程中，我在GitHub上制作了早期草稿，然后邀请公众对其进行评论。收到了100多条评论、建议、修改和捐赠等方面的回应。那些捐助者在文末的早起发布草稿的GitHub捐助者中进行了公布，并表达了我的感谢之情。真诚地感谢我的GiuHub自愿者编辑Ming T. Nguyen (第1版编辑) and Will Binns (第2版编辑)，他们不辞辛劳地组织、管理和解决GitHub上的pull requests、issue reports，并且执行bug修复工作。

Once the book was drafted, it went through several rounds of technical review. Thanks to Cricket Liu and Lorne Lantz for their thorough review, comments, and support.

当完成草稿撰写后，本书经历了多轮技术审阅与修改。感谢Cricket Liu和Lorne Lantz的全程审阅、评论和支持。

Several bitcoin developers contributed code samples, reviews, comments, and encouragement. Thanks to Amir Taaki and Eric Voskuil for example code snippets and many great comments; Chris Kleeschulte for contributing the Bitcore appendix; Vitalik Buterin and Richard Kiss for help with elliptic curve math and code contributions; Gavin Andresen for corrections, comments, and encouragement; Michalis Kargakis for comments, contributions, and btcd writeup; and Robin Inge for errata submissions improving the second print. In the second edition, I again received a lot of help from many Bitcoin Core developers, including Eric Lombrozo who demystified Segregated Witness, Luke Dashjr who helped improve the chapter on transactions, Johnson Lau who reviewed Segregated Witness and other chapters, and many others. I owe thanks to Joseph Poon, Tadge Dryja, and Olaoluwa Osuntokun who explained Lightning Network, reviewed my writing, and answered questions when I got stuck.

许多比特币开发者贡献了示例代码、审阅、评论和鼓励。感谢Amir Taaki和Eric Voskuil提供了示例代码片段和许多很好的评论。Chris Kleeschulte编写了BitCore附录部分；Vitalik Buterin和Richard Kiss帮助提供椭圆曲线数学解析和实现代码；感谢GavinAndresen对本书的修订、评论和支持；感谢 Michalis Kargakis的评论、捐赠和btcd简介；感谢Robin Inge对本书的勘误，改进了第2版的印刷效果。在第2版中，我再次收到了很多比特币核心开发人员的帮助，包括让隔离见证通俗易懂的Eric Lombrozo，帮助改进交易章节的Luke-Jr，帮助审阅隔离见证和其他章节的JohnsonLau，还有其他很多要感谢的开发者。我深深地感谢帮助解释闪电网络的Joseph Poon、Tadge Dryja和Olaoluwa Osuntokun，他们还帮助我审阅了我的文章，帮助我解答了我无法回答的问题。

I owe my love of words and books to my mother, Theresa, who raised me in a house with books lining every wall. My mother also bought me my first computer in 1982, despite being a self-described technophobe. My father, Menelaos, a civil engineer who just published his first book at 80 years old, was the one who taught me logical and analytical thinking and a love of science and engineering.

我将我的书和深爱之词献给我亲爱的母亲Theresa，她在我们住的房子中的每面墙上放满了书籍。尽管自认为是科技产品排斥着，我母亲还在1982年给我买了第一台电脑。我的父亲Menelaos是一名土木工程师，刚在80岁时出版了他的第一本书，我的父亲是一名科技和工程技术爱好者，他教会了我逻辑思考与分析。

Thank you all for supporting me throughout this journey.

感谢在写书过程中所有支持我的人。

**Early Release Draft (GitHub Contributions)**

Many contributors offered comments, corrections, and additions to the early-release draft on GitHub. Thank you all for your contributions to this book.

Following is a list of notable GitHub contributors, including their GitHub ID in parentheses:

* Akira Chiku (achiku)
* Alex Waters (alexwaters)
* Andrew Donald Kennedy (grkvlt)
* bitcoinctf
* Bryan Gmyrek (physicsdude)
* Casey Flynn (cflynn07)
* cclauss
* Chapman Shoop (belovachap)
* Christie D’Anna (avocadobreath)
* Cody Scott (Siecje)
* coinradar
* Cragin Godley (cgodley)
* Craig Dodd (cdodd)
* dallyshalla
* Darius Kramer (dkrmr)
* David Huie (DavidHuie)
* Diego Viola (diegoviola)
* Dirk Jäckel (biafra23)
* Dimitris Tsapakidis (dimitris-t)
* Dmitry Marakasov (AMDmi3)
* drstrangeM
* Ed Eykholt (edeykholt)
* Ed Leafe (EdLeafe)
* Edward Posnak (edposnak)
* Elias Rodrigues (elias19r)
* Eric Voskuil (evoskuil)
* Eric Winchell (winchell)
* Erik Wahlström (erikwam)
* effectsToCause (vericoin)
* Esteban Ordano (eordano)
* ethers
* fabienhinault
* Frank Höger (francyi)
* Gaurav Rana (bitcoinsSG)
* genjix
* halseth
* Holger Schinzel (schinzelh)
* Ioannis Cherouvim (cherouvim)
* Ish Ot Jr. (ishotjr)
* ivangreene
* James Addison (jayaddison)
* Jameson Lopp (jlopp)
* Jason Bisterfeldt (jbisterfeldt)
* Javier Rojas (fjrojasgarcia)
* Jeremy Bokobza (bokobza)
* JerJohn15
* Joe Bauers (joebauers)
* joflynn
* Johnson Lau (jl2012)
* Jonathan Cross (jonathancross)
* Jorgeminator
* Kai Bakker (kaibakker)
* Lucas Betschart (lclc)
* Magomed Aliev (30mb1)
* Mai-Hsuan Chia (mhchia)
* marcofalke
* Marzig (marzig76)
* Matt McGivney (mattmcgiv)
* Maximilian Reichel (phramz)
* Michalis Kargakis (kargakis)
* Michael C. Ippolito (michaelcippolito)
* Mihail Russu (MihailRussu)
* Minh T. Nguyen (enderminh)
* Nagaraj Hubli (nagarajhubli)
* Nekomata (nekomata-3)
* Philipp Gille (philippgille)
* Robert Furse (Rfurse)
* Richard Kiss (richardkiss)
* Ruben Alexander (hizzvizz)
* Sam Ritchie (sritchie)
* Sebastian Falbesoner (theStack)
* Sergej Kotliar (ziggamon)
* Seiichi Uchida (topecongiro)
* Simon de la Rouviere (simondlr)
* Stephan Oeste (Emzy)
* takaya-imai
* Thiago Arrais (thiagoarrais)
* Thomas Kerin (afk11)
* venzen
* Will Binns (wbnns)
* wintercooled
* wjx
* Wojciech Langiewicz (wlk)
* Yancy Ribbens (yancyribbens)
* yurigeorgiev4