区块链书系

BLOCKS AND CHAINS:
INTRODUCTION TO BITCOIN,
CRYPTOCURRENCIES,
AND THEIR CONSENSUS MECHANISMS

区块链

比特币、加密货币及其共识机制入门

[奥] 艾尔约书亚·贾德梅尔（Aljosha Judmayer）
尼古拉斯·斯泰福特（Nicholas Stifter）
凯塔琳娜·克罗姆霍兹（Katharina Krombholz）
埃德加·威普尔（Edgar Weippl） 著

魏珺洁 程国建 译

工业出版社
MACHINE PRESS

区块链书系

BLOCKS AND CHAINS:
INTRODUCTION TO BITCOIN,
CRYPTOCURRENCIES,
AND THEIR CONSENSUS MECHANISMS

区块链

比特币、加密货币及其共识机制入门

[奥] 艾尔约书亚·贾德梅尔（Aljosha Judmayer）
尼古拉斯·斯泰福特（Nicholas Stifter）
凯塔琳娜·克罗姆霍兹（Katharina Krombholz）
埃德加·威普尔（Edgar Weippl） 著
魏珺洁 程国建 译

机械工业出版社
CHINA MACHINE PRESS

Part of the Synthesis Lectures on Information Security, Privacy, and Trust Series
Series Editors: Elisa Bertino and Ravi Sandhu
Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms
ISBN: 9781627057165
By Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz ,and Edgar Weippl

图书在版编目（CIP）数据

区块链：比特币、加密货币及其共识机制入门 /（奥）艾尔约书亚·贾德梅尔（Aljosha Judmayer）等著；魏珺洁，程国建译 . —北京：机械工业出版社，2019.1
（区块链书系）
书名原文：Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms
ISBN 978-7-111-61532-3

Ⅰ . ①区… Ⅱ . ①艾… ②魏… ③程… Ⅲ . ①电子商务 – 支付方式 – 研究 Ⅳ . ① F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 277463 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：顾 谦 责任编辑：顾 谦
责任校对：王明欣 封面设计：马精明
责任印制：张 博
三河市宏达印刷有限公司印刷
2019 年 2 月第 1 版第 1 次印刷
145mm × 210mm · 6.25 印张 · 2 插页 · 100 千字
0 001—4 000 册
标准书号：ISBN 978-7-111-61532-3
定价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
电话服务 网络服务
服务咨询热线：010-88361066 机 工 官 网：www.cmpbook.com
读者购书热线：010-68326294 机 工 官 博：weibo.com/cmp1952
010-88379203 金 书 网：www.golden-book.com
封面无防伪标均为盗版 教育服务网：www.cmpedu.com

本书从最基本的定义开始，逐渐深入各类相关技术的原理，最后讲述了区块链及加密货币技术的发展及应用。本书具体结构如下：第1章用一个简单的例子介绍了加密货币；第2章简要介绍了符号和定义；第3章概述了推动比特币发明的密码学历史；第4章讨论了比特币作为现代分布式PoW的加密货币的原型，并强调了区块链和分布式账本技术的基本属性；第5章叙述了以比特币为例的加密货币生态系统的人机交互，并从用户的角度讨论了比特币的可用性、隐私性和安全性；第6章讨论了在分布式容错计算环境中的Nakamoto共识，并强调了对这种新的共识方法建模的发展；第7章介绍了加密货币的未来发展和区块链技术的其他应用。

本书适合区块链及加密货币技术入门读者、相关课程师生以及该领域的研究学者阅读参考。

译者序

自 2008 年比特币作为去中心化的加密货币原型引入以来，加密货币技术领域的人气迅速提高。比特币、加密货币技术、区块链等词几乎家喻户晓。比特币是第一个去中心化的加密货币，其底层技术就是区块链技术。加密货币属于数字货币的一种，它以去中心化的共识机制为基础，使用密码学原理来确保交易安全、控制交易单位。区块链最初用于指代不可变分类账本中的交易汇总和协议，现在它被用作各种加密货币技术的总称。区块链以密码学为基础，通过去中心化的方式集体维护一个可靠数据库。区块链技术已经逐渐应用于各行各业，例如数字货币、金融证券、资产管理、交易支付等领域。

本书从最基本的定义开始，逐渐深入各类相关技术的原理，最后讲述了区块链及加密货币技术的发展及应用。本书具体结构如下：第 1 章用一个简单的例子介绍了加密货币；第 2 章简要介绍了符号和定义；第 3 章概述了推动比特币发明的密码学历史；第 4 章讨论了比特币作为现代分布式 PoW 的加密货币的原型，并强调了区块链和分布式账本技术的基本属性；第 5 章叙述了以比特币为例

的加密货币生态系统的人机交互，并从用户的角度讨论了比特币的可用性、隐私性和安全性；第 6 章讨论了在分布式容错计算环境中的 Nakamoto 共识，并强调了对这种新的共识方法建模的发展；第 7 章介绍了加密货币的未来发展和区块链技术的其他应用。

本书适用于区块链及加密货币技术入门、相关课程的教学以及该领域研究学者借鉴参考。感谢李皎博士对全书的审阅及指正。本书的出版得益于机械工业出版社顾谦老师的推荐与支持，在此特致感谢。由于水平有限，本书可能会有翻译不当之处，请各位读者批评指正。

魏珺洁谨识

2019 年 1 月

原书前言

加密货币和共识分布式账本的新领域，通常被称为区块链，该领域现在越来越多地受到各种不同社团的关注。这些社团非常多样化，其中包括：技术爱好者、活动家团体、各学科的研究人员、初创企业、大型企业、公共机构、银行、金融监管机构、商人、投资者等。科学界对新兴且发展迅速的加密货币和共识分类账本这一领域的适应相对缓慢，这就是为什么在很长一段时间内唯一可用的资源是比特币源代码、博客和论坛帖子、邮件列表及其他在线出版物。引起这种炒作的原始比特币论文在没有任何同行评审的情况下也在网上发布了。遵循比特币论文最初的出版精神，该领域的许多创新都来自社团本身，它们以在线出版和在线对话的形式，而不是以已建立的有同行评审的科学出版物的形式出版。一方面，这种快速自由软件开发的精神，加上加密货币的业务方面，以及当今以市场为中心的行业的利益，产生了大量的出版物、白皮书和样刊；另一方面，这导致了系统化的缺陷以及对这个新领域的理论理解与实践之间的差距。

本书旨在缩小这一差距，并从技术角度对这一广泛领域进行结

构良好的概述。现代加密货币和共识分类账本的原型是比特币及其基本的 Nakamoto（中本聪）共识。因此，本书非常详细地描述了该协议的内部工作原理，并讨论了它与其他派生系统的关系。

关键词：

区块　链　区块链　比特币　加密货币　工作量证明　Nakamoto 共识　共识分类账本

作者简介

Aljosha Judmayer

Aljosha Judmayer 在维也纳技术大学获得了软件工程和互联网计算硕士学位。作为 IT 安全顾问，他在渗透测试方面拥有 5 年以上的经验。目前，他还在奥地利维也纳 SBA 研究所担任 IT 安全研究员，他正在那里攻读加密货币的应用和分布式系统弹性方面的博士学位。他的研究方向包括加密货币技术以及网络和系统安全。

Nicholas Stifter

Nicholas Stifter 拥有维也纳技术大学计算机科学管理硕士学位和软件工程学士学位。他目前正在攻读区块链技术和智能合约的安全性和可维护性方面的博士学位，他的研究兴趣包括 Nakamoto 共识、分布式共识协议和分布式系统主题的计算教育。

Katharina Krombholz

Katharina Krombholz 是奥地利维也纳 SBA 研究所的博士后安

全研究员，也是维也纳技术大学和维也纳应用科学大学 FH 校区的数字取证大学讲师。她以优异的成绩于 2016 年获得博士学位。她的研究方向是可用的安全性、隐私和数字取证。

Edgar Weippl

Edgar Weippl 是奥地利维也纳 SBA 研究所的研究主任和维也纳技术大学的副教授。从维也纳技术大学获得博士学位后，Edgar 在一家研究创业公司工作了两年，然后他在美国威斯康星州伯洛伊特学院担任助理教授一年。2002~2004 年，与软件供应商 ISIS Papyrus 合作，在美国纽约和奥尔巴尼以及德国法兰克福担任顾问。2004 年，他加入了维也纳技术大学并与 A Min Tjoa 和 Markus Klemen 一起创立了奥地利维也纳 SBA 研究所。Edgar 是《计算机与安全》（COSE）编辑委员会成员，组织 ARES 会议并担任 SACMAT 2015 主席、Esorics 2015 主席和 ACM CCS 2016 主席。

原书致谢

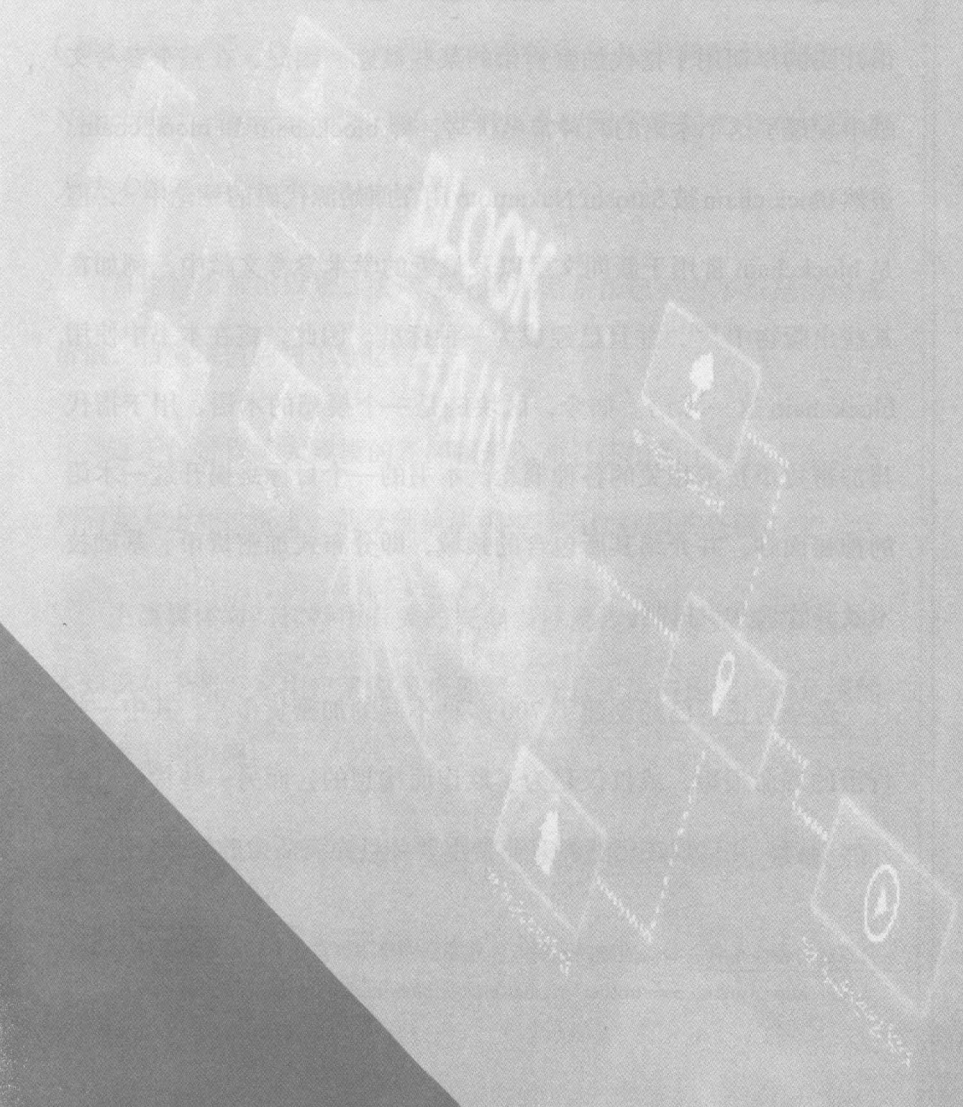
本书涉及的研究由 COMETK1，FFG-Austrian Research Promotion Agency，FFG Bridge Early Stage 846573 A2Bit and FFG Bridge 1858561 SESC 资助。感谢评审专家：Foteini Baldimtsi、Patrick McCorry 和 Jong Ho Won，感谢他们提出了有用的反馈和讨论。

Aljosha Judmayer、Nicholas Stifter、Katharina Krombholz 和 Edgar Weippl

目　录

第1章

入　门



自从 2008~2009 年比特币 [117] 作为去中心化的加密货币的原型引入以来，加密货币技术领域的人气迅速提升。那些以与比特币相同或相似的基本原理为基础的技术通常被称为区块链。区块链本身并不是由 Satoshi Nakamoto 在原始论文中直接引入的 [117]，而是比特币社团的早期用于指代加密货币的某些概念。因此，在整个参考文献中发现了这个术语的两种常见拼写，即 blockchain 和 block chain。虽然 block chain 被 Satoshi Nakamoto 用在原始源代码的评论中[⊖]，但是 blockchain 常用于新闻文章以及最近的学术参考文献中，例如在某些出版物中 [50]，并且已经成为一种标准。因此，将在本书中使用 blockchain 这一术语。如今，区块链是一个模糊的术语，用于指代与加密货币技术相关的各种概念。本书的一个目标是揭开这一术语的神秘面纱，并介绍其所包含的领域，即分布式加密货币、基础技术及其管理共识机制。

迄今为止，已经创建了 700 多种不同的加密货币 [1]。其中一些货币的寿命很短，或仅仅是为了欺诈而构想的，而另一些货币有额外的创新，并且现在仍然拥有非常重要并且充满活力的社团。

⊖ https://github.com/trottier/original-bitcoin/blob/master/src/main.h#L795-L803。

大多数加密货币的机制和基本原则或多或少地源于最初的比特币协议。其中一些加密货币与比特币的不同之处在于它们选择的某些常数，例如目标区块间隔或最终将存在的最大货币单位数。另一些加密货币已经转变成可替代的工作量证明（PoW）算法（如 Litecoin[129]、Dogecoin[128]），它们往往包括了其他的功能（如 Namecoin[2]、Ethereum[66]、Zcash[64]），或使用了不同的分布式共识方法（如 PeerCoin[96]、Ripple[133]）。

自比特币推出以来，去中心化的加密货币已经有了卓越的经济价值，目前市值约为 170 亿美元[⊖]。

这不仅带来了大规模的新闻报道，而且还增加了从技术爱好者到商业人士和投资者，甚至到执法机构等不同社团的兴趣。

主流媒体对与比特币有关的安全事件及传闻的报道表明，其基本知识对于非专家用户来说很难理解，并且无法与传统货币系统的核心模型相协调。

比特币被设计成一种去中心化的加密货币，不依赖于被信任的

⊖ 估值显著上升以及货币汇率的高度波动，使人们难以提供一种不会很快被取代并且看上去不会过时的估计。