HZ BOOKS
华章IT

重量级区块链安全专家联合撰写，知名专家联袂推荐，权威性与实用性毋庸置疑

条分缕析，透视应用层（智能合约）、激励层、网络层、数据层与共识、私钥等维度的安全问题与防御

区块链技术丛书

区块链安全技术指南

黄连金 吴思进 曹锋 季宙栋 ◎ 等编著

机械工业出版社
China Machine Press

区块链
技术丛书

区块链安全技术指南

黄连金 吴思进 曹 锋 季宙栋 马臣云
达 摩 李恩典 徐浩铭 翁俊杰
◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链安全技术指南 / 黄连金等编著 . —北京：机械工业出版社，2018.6
（区块链技术丛书）

ISBN 978-7-111-60036-7

I. 区… II. 黄… III. 电子商务 – 支付方式 – 安全技术 – 指南 IV. F713.361.3-62

中国版本图书馆 CIP 数据核字（2018）第 097642 号

区块链安全技术指南

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：高婧雅　　责任校对：殷　虹
印　　刷：北京市兆成印刷有限责任公司　　版　　次：2018 年 6 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：15.5
书　　号：ISBN 978-7-111-60036-7　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

About the Authors 作者简介

黄连金　硅谷 Dynamic Fintech Group 管理合伙人、联合国旗下世界区块链组织（WBO）首席技术官、美国 ACM Practitioner Board 委员、美国分布式商业应用公司 CEO 和创始人、中国电子学会区块链专家委员、中国人大特聘研究员与讲师、美国 CISSP 专家、CyberVein 总顾问，多个成功区块链项目技术顾问。曾就职于美国 CGI 公司 18 年，任 CGI 安全技术总监、CGI 云安全主管和首席安全架构师等职务，创建了 CGI 联邦身份管理和网络安全能力中心。在 CGI 工作时，曾经为美国联邦政府、金融机构和公用事业公司提供金融、人工智能、区块链、安全等方面的专家咨询。曾多次在国内外大型区块链峰会担任嘉宾、评委、培训专家。

吴思进　33 复杂美创始人及 CEO，浙大本科硕士毕业，金融数据专家，精通量化交易及区块链，主导多家世界 500 强区块链项目落地。2014 年申请区块链发明专利，2 项已授权，目前累计申请专利 50 多项，全球区块链专利排名前十，主要区块链项目有供应链金融、供应链管理、积分、钱包、交易所。

曹锋　PCHAIN 发起人，中物联区块链协会首席科学家。中国早期区块链国际专利发明人，ChinaLedger 共同发起人，2016 年完成全球区块链资产收益权转让暨中国区块链金融真实交易。曾担任 IBM 全球下一代人机大战中国区负责人、互联网金融首席科学家、专利评审委员会联合主席；3 次获得 IBM 全球杰出技术成就奖，发表 22 篇国际顶级论文，30 余项美国专利，并担任多个 ACM IEEE 顶级国际会议论坛主席。

季宙栋　Onchain 分布科技首席战略官，本体联合创始人，（工信部）中国区块链技术与产业发展论坛副秘书长，中国电子学会区块链专委会委员，ISO/IEC TC307 中国代表团成员，参与本体论、身份和隐私保护等标准组。作为区块链行业的资深专家，参与了工信部区块链白皮书及相关标准编制工作。

马臣云　北京信任度科技 CEO、信息安全专家、产品管理专家，电子认证与签名行业

15 年从业经验。主要方向是密码学、区块链、身份认证、电子签名。曾获得省部级科技进步二等奖（国家密码局）、首都五一劳动奖章、全国五一劳动奖章等，是电子签章技术、基于人脸识别的身份认证安全技术、互联网金融个人借贷电子合同安全技术等标准的起草人。著有《精通 PKI 网络安全认证技术与编程实现》。网络 ID：非著名信息安全砖家。

达摩　BOX.LA 项目发起人，原唯链 COO，参与了众多知名区块链项目的早期投资。

李恩典　美国分布式商业应用公司董事与中国区总裁、深圳市微风智联科技有限公司董事长、区块链软件和金融行业应用研发专家。15 年以上金融安全研发经验，在区块链存储、大数据平台、物联网平台和金融系统核心等领域均有领先的技术成果和丰富的产品技术实战经验，并拥有近 10 项相关领域发明专利。

徐浩铭　CyberVein 数脉链项目技术负责人，负责区块链平台架构和搭建。曾就职于欧洲微软研发中心，负责 Office 项目开发。毕业于英国剑桥大学，主要研究方向为机器学习在生物信息学领域的应用；曾在美国卡内基 - 梅隆大学访学，主要研究方向为机器视觉在无人驾驶中的应用；曾在美国杜克大学访学，研究领域为深度学习在生物医学工程中的应用。在 SCI 和 EI 检索杂志上发表多篇文章。

翁俊杰　IBM 10 余年开发及解决方案经验，第一批 Fabric 应用开发者，NEO 核心开发者之一，Onchain DNA 联盟链的架构设计与核心开发人员，Ontology（本体）区块链开发团队负责人。在票据、供应链、积分、征信、数据交易、共享金融等多个领域有区块链应用经验。

Foreword 序一

多边界的区块链安全防守

2018 年是区块链技术（或称分布式账本技术）诞生的第十个年头，人们对它所寄予的厚望正与日俱增。很多人认为区块链技术不仅会对现有的产品、服务、操作系统、商业模式、最佳实践，乃至各行各业带来巨大冲击，甚至可能带来经济运行以及社会组织和治理的大变革。这是因为区块链技术促进了加密技术等方面的科技进步，实现了低成本和实时条件下的超强处理能力，同时为金融服务、医疗保健、物流，以及环境保护等产业的可持续发展提供了无限可能。但更重要的是，区块链技术建立在去中心化共识、开源、透明和社区参与这些原则之上。这些基本原则才是这一技术具有革新性潜能的根本所在。[⊖]

包括联合国和世界银行集团（世行）在内的多边组织已经意识到区块链技术将会对各发展机构及其工作产生深远的影响。这是因为区块链技术能够帮助发展机构减轻对传统银行及其他中介机构的依赖，从而大大降低交易成本；确保援助资金直接转给援助对象，保证专款专用，使整个环节更加透明。鉴于此，世行于 2017 年 6 月建立了区块链实验室，专注研究区块链领域的创新技术，以求更好地服务世行的发展项目。

虽然区块链技术拥有巨大的潜力，但它目前仍面临很多挑战。对于这样一个自动化、去中心化和不断扩展的系统来说，安全性是不容回避的问题。区块链技术在安全性方面面临的挑战包括三方面。首先，虽然区块链技术能够为交易提供高度的完整性（integrity）和透明度（transparency），但是系统设计方面仍亟待加强，才能保证区块链基础设施和平台的机密性（confidentiality）和弹性（resiliency）。其次，不论是共识机制还是“智能合约”，区块链技术都需要依靠开发各种应用软件来实现。因此，软件开发安全方面的最佳实践仍应继续遵守。

⊖ 英国政府首席科学顾问报告：《分布式账本技术：超越“区块”和“链”》（Distributed Ledger Technology: Beyond Block Chain）。

最后，区块链技术需要相应的生态系统来为实践提供完整解决方案。这个生态系统可能会运用包括物联网（IoT）、人工智能和云计算在内的其他新技术。这意味着，所有这些构成区块链生态系统的技术本身的安全问题也需一并考量。

我在世行区块链实验室举办的一次活动中结识了黄连金先生。黄先生是那次活动的特约嘉宾，也是本书的第一作者。当时黄先生在华为技术有限公司担任首席区块链专家，他也是中国区块链安全领域的领军人物。从他那里我了解到，虽然区块链技术还在发展阶段，但在中国已经有一批安全专家开始合作编写一本关于区块链安全问题的著作。这让我惊喜不已，因为一直以来，人们总在创新技术产生之后才亡羊补牢，考虑安全问题。我相信，这本强调安全先行的著作，对确保未来区块链解决方案的可靠性和实用性大有裨益。

本书对区块链技术潜在风险的分析可谓详尽、完备：不仅包括区块链技术本身带来的风险（比如加密技术、身份管理技术、共识技术，以及“智能合约”技术可能涉及的风险），还包括区块链应用方面的风险（例如激励机制、数据安全和网络安全等方面可能面临的风险）。书中不但有对区块链技术各种安全机制的深度解剖，而且有区块链应用遭受攻击的案例分析。这样理论与实际结合，有助于读者学以致用，将对潜在风险的预期和评估置于现实背景之下。

为本书作序，我备感欣慰。据我所知，本书是全球为数不多关注区块链安全问题的专著。借着这则序言，我期待能够让更多的人在区块链及其他革命性技术创新的初期就开始考虑安全问题的重要性。愿更多的研发人员、商业人士以及政策制定者都关注安全问题。我们会因此而更有信心应对未来技术应用（Technology Adoption）过程中的各种挑战。

林儒明

世界银行集团首席信息安全官、区块链实验室负责人

Foreword 序二

区块链安全观之我见

区块链安全观可以从两方面来讨论。技术方面的安全观是本书的主题，遑遑高论，各位看官自可体会；我想从区块链经济模式的安全观方面，谈一些自己的学习体会，以就教于各位作者和读者。

从经济模式来看区块链，我把它分为 4 个层次。

- 最底层是区块链数字身份体系。数字身份包括了身份 ID、社交关系、职业声誉、生活状态等，远比一串身份证号码要更全面、更传神。
- 第二层是密码学账户体系。基于非对称加密算法的分布式账本，非许可、无须 KYC，支持点对点交易，靠算法保证交易安全可靠，坏人无法作恶。
- 第三层是区块链数字货币体系。公有区块链靠算法发行数字货币的一个最主要的目的是为自组织建立一种去中心化的经济激励机制。
- 第四层是商业应用体系。有了前 3 层，任何分布式商业应用项目就有了生存的基础和无限的发展空间。

区块链技术层面的安全，都是为其经济模式的安全运行服务的。无论是保证数据一致性的哈希函数，还是保护隐私的零知识证明；不管是维护账户安全的椭圆曲线加密算法，还是保护数据主权的多方安全计算；直至协调区块链治理的各种共识算法……在分布式、去中心、自组织的区块链世界里，信任关系和安全机制的建立，完全依赖一整套成体系的数学和密码学算法来保证安全、可靠。

传统金融业界有一句名言：无硬件，不安全。其实这句话也完全适用于区块链经济模式。硬件安全不仅仅涉及数字货币“热钱包”“冷钱包”层面的事情，它还可能涉及区块链上金融交易的报文传输等方面。

本书是一本从技术角度讨论区块链安全的著作。在区块链“高烧”发热，热到有可能大热倒灶的今天，一群业界同仁愿意埋头沉心，专注区块链的安全问题，实在是难能可贵！

作为一名非技术背景的区块链信徒，阅读这样一本洋溢着精深技术见解的区块链安全著作，仍然从中学到很多，悟到更多。诚所谓见仁见智，乐山乐水是也！故不论“币圈”“链圈”，无论专业背景，特推荐之，必有收获焉！

肖风

中国万向控股有限公司副董事长、万向区块链实验室董事长兼总经理

Foreword 序三

安全是区块链发展和应用的基石

2008 年，中本聪的论文“比特币：一种点对点的电子现金系统”一经发表，犹如“忽如一夜春风来，千树万树梨花开”。历经十年的迅猛发展，区块链已成为近年来最具革命性的新兴技术之一，并广泛应用于各种社会场景之中。任何事物取得如此之重要地位，必定有其独特魅力。

区块链的魅力在于，它可以利用自律解决社会中靠他律才能解决的问题；区块链的魅力在于，它使参与者都有知情权，信息对等，脱离了只有少数人掌握信息的不平等状态；区块链的魅力在于，它能够做到在现实社会中我们始终倡导和追求的诚信，而不需要人们的长期认知才能达到（其模式自身就存在诚信，不可抵赖）；区块链的魅力在于，它需要大多数伙伴的认同，使人们能够为了一个共同的目标而努力；区块链的魅力在于，它使事物脱离了一成不变的程式化发展趋势，而迎来“百般红紫斗芳菲”的各式发展。其实，区块链的这些魅力并不是其刻意而为之，而是其自身特性决定的。因为独特，所以灿烂。

区块链的这些特殊魅力吸引了社会各界的广泛关注，但是能否长久保鲜而不受摧残也成为我们担心的关键点。区块链的自律，使职能机构失去控制权；区块链的信息共享，使隐私更易暴露；区块链的不可篡改，使可能的错误变成“真实”而存在；区块链的共识，使大多数伙伴的观点无论正确与否都变得“正确”；区块链各具特色的发展模式，使漏洞出现的可能性提高，容易导致应用的浩劫。因此，区块链要真正快速发展和广泛应用，就要不断提高其自身安全性。

黄连金先生作为区块链资深高端专家，经过长年研究积淀，在区块链安全研究成果较少的情况下，他能够领先其他学者研究产出第一批专门的区块链安全著作，可谓独具慧眼。仅从这一点，足以看出他是具有长远眼光和思想前瞻性的专家。有幸提前拜读他的区块链安全

研究成果，使我全面地认识到区块链安全的重要性，对区块链安全有了合理的分类认知，也从中了解到未来区块链安全研究的热点，学到一些有关区块链安全的有效研究手段。阅读时，我能感受到本书行文流畅；在学习到较新的有价值的研究成果的同时，体会到阅读的快乐，创新的热情。为本书写序，备感荣幸。希望更多的人了解区块链，在未来的区块链模式中夯实区块链安全的基石，从而使区块链及其应用更加坚不可摧，更具魅力。

祝烈煌

北京理工大学计算机学院副院长、教授

Preface 前言

为什么要写这本书

这本书的初衷是希望给区块链项目提供一些安全方面的指导来改变目前区块链项目匆匆上线，安全系数不高，安全问题层出不穷的现状，也希望正在开发或将来需要开发的区块链项目在安全方面给予足够的重视。我们认为安全问题会是区块链项目落地的主要绊脚石。一个不注意安全的区块链项目，成功系数不会很高。区块链有很好的安全属性，比如数据不可篡改、数据不会丢失、可利用一些加密技术对数据进行加密等。但是从许多与区块链有关的安全事件可以看出，区块链的安全属性不能保证区块链项目百分之百安全。本书尽量从多个不同的方面，比较系统地对区块链的安全进行分析，并且对区块链项目落地所需要考虑的因素，提供一些建议。

本书特色

本书是为数不多系统性地阐述区块链安全的书。

本书的主要特色是以深入浅出的形式讲解区块链的安全，便于读者更好地理解为什么区块链安全是一个重要的课题，以及如何解决某些区块链的安全问题。

读者对象

本书的读者对象包括：

- 区块链的开发者
- 区块链安全的架构师
- 区块链项目的主要技术负责人
- 其他对区块链安全感兴趣的人

如何阅读本书

在阅读过程中，读者可以根据工作需要将某些章节多读几遍。因为章节与章节之间的依赖性不强，完全可以根据工作需要抽出重点来读。

第 1 章详解区块链的安全属性，主要从保密性、数据完整性、可用性、物理安全性 4 个方面对区块链的安全属性进行详解。在分析过程中，本章穿插了一些实例，使得内容讲解更为直观、易懂。本章所介绍的内容，可以使读者对区块链的安全属性有更深层次的了解，对做好区块链的安全工作具有非常重要的参考价值。

由于区块链的安全性分析极具抽象性，所以第 2 章特意挑选了一些主流数字货币（包括比特币、以太币和 Zcash），对其安全属性进行分析。通过本章的学习，读者可以了解主流数字货币的代码、密码学算法以及“钱包”等，进一步加深对区块链相关安全技术的认识。

第 3 章为应用与智能合约层的安全控制。本章主要从 Web 或者移动客户端应用程序、智能合约，以及身份与访问控制 3 个方面对安全问题进行分析。在当前信息技术快速发展的背景下，移动设备已经成为很多人上网的主要工具。为此，本章从一开始就对 Web 或者移动客户端应用程序的安全性进行了分析，让读者对相关的危险因素有所了解。在智能合约的安全方面，主要从智能合约的概念、安全编码、漏洞、开源工具等几个方面进行了分析，为读者在开发相关内容方面提供了重要的参考。在本章的最后，从多个方面对区块链的身份管理与访问控制进行了分析。通过对这部分内容的学习，读者可以了解在开发区块链的过程中，如何高效、安全地做好身份管理与访问控制等工作。

第 4 章为激励层安全机制设计。本章主要从激励的产生和分配以及激励层安全两方面进行了分析。首先，分别借助比特币、以太币的激励模式对激励的产生和分配进行了分析，可以让读者对区块链激励层的存在有较为直观的认识。在此基础上，本章又从激励模式的安全隐患、安全事件、法律风险以及安全措施等方面，对激励层安全进行了分析，让读者了解安全对激励层的重要性，以及如何设计才能有效避免区块链激励层安全事件的发生。

第 5 章为网络层安全与控制。网络层是区块链的重要组成部分，能否做好安全与控制直接影响区块链的价值。本章主要从 P2P 加密、客户端与节点通信加密、防御 DDoS 攻击 3 个方面进行了分析。通过对本章的学习，读者可以对网络层安全与控制的相关内容有全面的了解。这对开发过程中提高区块链的安全性具有重要指导作用。

第 6 章为数据层与共识安全。数据层是区块链设计的基础部分，是影响区块链能否正常运行的关键。本章主要从区块链数据加密技术、数据传输、区块链交易签名、共识攻击、区块链安全性考虑 5 个方面进行分析。通过本章的学习，读者可以了解关于数据层安全更多的

知识。这对于提高区块链的安全，保障区块链的正常运行具有重要的参考价值。

第 7 章为私钥的安全。本章从私钥的重要性、使用方法、存在的问题等多个方面对私钥的安全进行了全面的分析。通过对本章的学习，读者可以对私钥安全性在区块链技术中的重要性有更深层次的认识，了解如何使用私钥才能有效避免安全问题的出现以及私钥的更新、找回与吊销等。除此之外，本章还对私钥保护的正确“姿势”、硬件钱包等内容做了分析。有了这些内容的指导，读者可以参考、拓展关于保障硬件钱包、移动钱包方面的设计思路，提高区块链的安全性。

除了上述内容，本书还包括 3 个附录。附录 A 介绍的是区块链安全基础概念、原理与分析方法，可以更好地理解区块链。当制定区块链安全性测试标准时，可以适当地参考、借鉴。附录 B 主要介绍 DAG 的基本概念、原理与主流项目，从中可以了解 DAG 给区块链安全带来的价值和影响。附录 C 介绍区块链私钥管理的一种方法，主要用于企业级数字资产的安全。

勘误和支持

本书从不同的角度来阐述区块链安全，抛砖引玉。我们不能说这本书包含了区块链项目落地需要考虑的所有安全因素，因为不可能面面俱到。区块链目前尚处于初级的技术发展阶段，新的安全隐患和新的安全措施会在发展的过程之中不断涌现。我们希望这本书是“活着”的书，通过不断地修订，尽量把新的内容添加到这本书，也欢迎区块链安全专家在这方面给我们多提一些意见。

本书不是从空中楼阁造出来的，我们参阅了大量网络公开的内容，并且引用了很多区块链安全专家在不同新闻媒体或者网络所刊登的内容以及个别面对面的交流信息。对于被引用的内容或者面对面交流的信息，我们尽量与各位专家进行了沟通，并且获得了同意，比如 NEO 创始人、OnChain 创始人及 CEO 达鸿飞，NEO 创始人兼核心开发者张铮文，上交所技术有限责任公司架构师朱立，复杂美 CTO 王志文，元界 CEO 顾颖（初夏虎），元界 CTO 陈浩，公信宝 CEO 黄敏强，Dfinity CEO 丁磊（Tom Ding）等。不过，仍有可能某些内容与网上公开的内容存在类似或雷同之处，在所难免，敬请谅解。如果在阅读本书的过程中发现有类似的内容，请及时与我们联系，我们会在修订版中增加引用的出处。

致谢

在这里，首先要感谢高婧雅编辑，她从一开始便对本书高度重视，在写作过程中不断鼓励我们。在北京的一次会议上，高编辑和我基本上拟订了这本书的架构和一些基本内容，并

且以后又经过几次优化，才有现在这本书的框架。

非常感谢本书所有的作者，他们在百忙之中抽出时间写了这本书，并且经过多次修改。应该说没有这些作者的贡献，就不会有这本书。

感谢深圳市微风智联科技有限公司的李恩典和梁福彬，他们非常有启发意义的讨论和对我负责写作的内容的多次修改，是我完成写作的最大助力。

非常感谢世界银行集团首席信息安全官、区块链实验室负责人林儒明先生，他不仅为本书做序，还在写作过程中不断鼓励我们，多次提供良好的建议。

中国万向控股有限公司副董事长、万向区块链实验室董事长兼总经理肖风博士对本书的构思和一开始的概念提出了很多宝贵意见，给予我们很大的帮助，同时还为本书作序，在此也表示感谢。

北京理工大学计算机学院副院长、网络与信息安全学科方向责任教授祝烈煌也为本书作序，在这里表示诚挚的感谢。

中国电子技术标准化研究院区块链研究室主任李鸣为本书写了推荐语，在此也表示感谢。

本书一共有 9 位作者，在著作委托书的联合签名上，我们第一次使用了区块链技术。感谢北京信任度科技有限公司 CEO 马臣云（也是本书的作者）的大力支持，我们利用该公司的信签电子合同签署平台非常快捷地完成了多人的电子签名。签署后的文档存储在由第三方 CA 机构、司法鉴定中心等组建的可信联盟链上。存证验证地址：http://bc.trustdo.cn/result.html?evidenceId=0x992c316f99baa714006424b6e86a87826dfd6d4cf4af3dbf9a75e3ebb5af6496。

存证有关信息如下。

- 存证地址：0x992c316f99baa714006424b6e86a87826dfd6d4cf4af3dbf9a75e3ebb5af6496。
- 存证时间：2018-03-25 07:47:04。
- 存证内容：fileHash:81e4324b2c842dd05ee977670fba5d6a,fileName: 黄连金 – 吴思进 – 曹锋 – 季宙栋 – 马臣云 – 尚维斯 – 李恩典 – 徐浩铭 – 翁俊杰委托书 .pdf。

黄连金

Contents 目　录