区块链技术丛书

HZ BOOKS 华章IT

巴比特

区块链底层技术和应用开发的必备用书，中国三大区块链联盟的专家联袂推荐

区块链开发指南

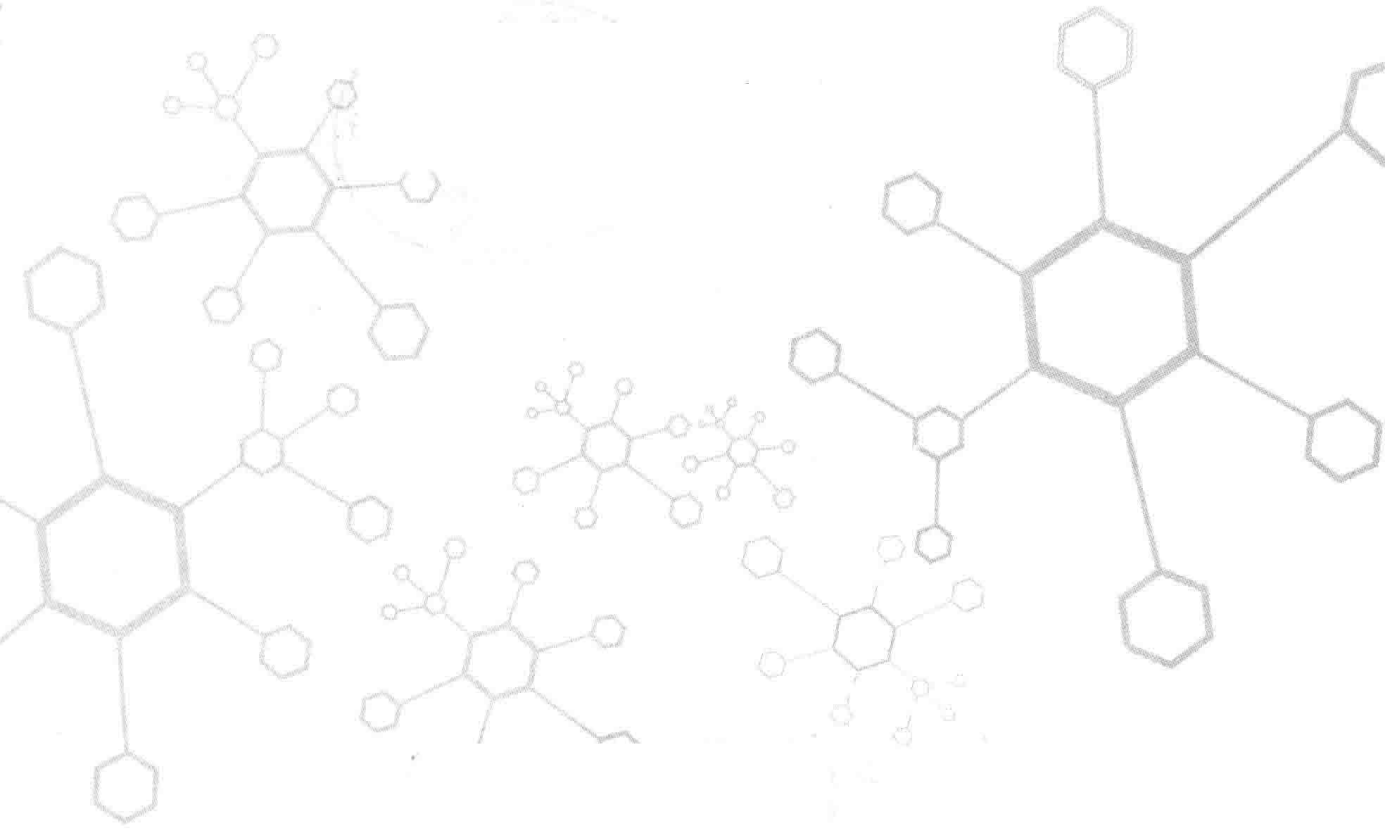
申屠青春 主编
宋波 张鹏 汪晓明 季宙栋 左川民 编著

机械工业出版社
China Machine Press

区块链
技术丛书

区块链开发指南

申屠青春 主编
宋波 张鹏 汪晓明 季宙栋 左川民 编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链开发指南 / 申屠青春主编 . —北京：机械工业出版社，2017.6（2017.7 重印）
（区块链技术丛书）

ISBN 978-7-111-57120-9

I. 区… II. 申… III. 电子商务 – 支付方式 – 指南 IV. F713.361.3-62

中国版本图书馆 CIP 数据核字（2017）第 118975 号

区块链开发指南

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：杨绣国 陈佳媛 责任校对：殷 虹
印 刷：三河市宏图印务有限公司 版 次：2017 年 7 月第 1 版第 2 次印刷
开 本：186mm × 240mm 1/16 印 张：15
书 号：ISBN 978-7-111-57120-9 定 价：59.00 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

Forword 1 推荐序一

区块链的价值实现

区块链和分布式账本技术是全球十大战略技术趋势之一，也是我国金融界、科技界过去一年高度关注的热点之一。毫无疑问，2017 年我国金融界、科技界将会加大在区块链和分布式账本技术领域的投入，同时市场上将会出现几个实际的应用。

深圳市金融科技协会（原深圳市金融信息服务协会）在研究推动区块链和分布式账本技术及应用的过程中，遇到了一批积极探索、深入钻研、大胆应用这门技术的志同道合者，并与微众银行、国信证券、博时基金、富德保险、深证通、银链科技、招银网络、致远速联、中证信用等 25 家金融机构和金融科技企业共同发起并成立了金融区块链合作联盟（深圳）。在这个过程中，我也加深了对申屠青春、姚辉亚、宿旭升等区块链积极推动者的认识，与他们建立了友谊，其中申屠青春就是本书的作者之一。

申屠青春近几年专注于研究区块链技术和应用，技术能力得到了业内的高度认可。他对区块链的热爱程度近乎痴迷，凡是区块链圈内的交流，几乎都有他的身影。对于区块链技术和标准，他都热心地和业内人士进行分享。他为金链盟的筹建和运作做了不少有益的工作，也是成立金链盟的倡议者之一。

自从 2015 年，人们发现了区块链巨大的潜在价值后，区块链技术已经飞速发展了两年多。这两年之中，区块链成为主流金融圈所推崇和研究的创新技术。全球众多大型金融机构都投入了人力财力进行区块链研究，R3、HyperLedger 等大大小小的组织也纷纷成立。我国的反应也很迅速，金链盟、ChinaLedger、工信部区块链联盟快速发展起来。从行业巨头参与的积极性和政府的重视程度来看，我国显然不想在区块链领域落后。

2008 年年底，中本聪在他的论文中提出一个点对点电子支付系统的构想，并且于 2009 年实现了比特币的原型。这个系统可以使地球上的任何人通过互联网以极致的效率进行货币交换和价值传递，无需任何第三方机构。比特币没有发明任何新技术或算法，其中涉及的技术工作量证明、时间戳、公钥体系等早已成熟。神奇的是，中本聪通过对这几项技术的组合

解决了无需可信第三方的数字资产所有权问题。从广义上讲，这些技术和思想的集合正是如今谈论的区块链。

从技术上看，区块链算是一个自由开放、没有固定形式的开源社区。众所周知，Linux 开源社区中，Linus 具有绝对权威来定制发展路线。有趣的是，区块链社区不存在这样一个角色，中本聪在 2010 年就在互联网上消失了，至今也没能确认其真实身份。也就是说，没有任何官方定义区块链该怎么实现，以及未来该怎么样发展。没有方向也许正好说明“一切皆有可能”。

去权威的社区呈现出一种百花齐放的状态，并且涌现出了大量的优秀项目和先进理念。纵览区块链的发展历史，大多创新点可归纳为共识机制、智能合约、隐私安全、可扩展性这几个方面，由于技术实现的灵活性相当大，因此更多的争论和共鸣在于设计理念和哲学上。

共识机制

中本聪在提出以工作量证明（PoW）机制作为共识算法之后，部分人认为耗能过大，于是就有了 Sunny King 设计的“环保”的股权证明（PoS）机制，后续又发展到 Bitshares 改进的股份授权证明（DPoS），并衍生出了更多的类 PoS 机制。从公有链的角度来看，共识算法就是公平和效率孰重孰轻的决策，技术实现不是难点，难点在于如何从社会学、从人性出发去设计激励机制。各种共识算法的支持者都有其合理的理由，不同共识的争论即使到现在也还一直存在。

另一个领域，金融机构的关注点在于效率、不可篡改及对应用的支持，由于不需要链上的代币激励，因而改进的拜占庭容错（PBFT)、PAXOS、RAFT 等传统分布式一致性算法就成为首选。

由此也就形成了两种区块链生态：公有链和联盟链。公有链可以任意加入，联盟链是许可加入，联盟链的用户大多是机构或公司，需要区块链契合自身的业务模式。从共识机制开始，区块链就走向了两条不同的道路，最终双方是竞争还是融合，有待后续观察。

智能合约

对智能合约的探索是出于对比特币区块链低效的脚本系统的不满，该脚本使用的是非图灵完备的堆栈语言，只能实现有限的功能。

一些智能合约研究者一直追求在区块链上运行强大的机器语言，让每个用户都能见证其运行的过程和结果，实现“程序即规则”（Code is Law）的智能环境。从图灵完备的以太坊 EVM、超级账本 ChainCode 到 Chain 平台的 ChainCore，研究者的目标是在有限的存储空间中设计一个完备合约语言和高效的底层虚拟机，甚至将传统开发语言（如 C/C++、Java）移植到

区块链上。效率和安全性的改进依然任重道远，这也是区块链领域最有技术含量的发展方向之一。

隐私安全

区块链中的个人隐私保护是强需求，特别是金融机构要使用的区块链，保护客户隐私是基本的合规条件；但同时还不能产生绝对隐私，必须要让监管者知道交易内容。

隐私安全的研究者大多需要深入掌握密码学知识，这不是一件轻松简单的工作。ZCash使用了零知识证明算法来隐藏交易双方在区块链的信息；比特币使用多输入多输出交易、隐身地址（Stealth address）和其他更多古老的混币方案来保护用户隐私。联盟链将采用数字证书认证用户，隔离一切非相关用户的数据访问。隐私安全是一把双刃剑，技术上满足隐私保护的需要，同时也增加了系统实现的复杂度；在降低透明性的同时，也要让监管更方便。

可扩展性

用户交易数的增多不可避免地会带来区块链数据膨胀的问题，可扩展性解决的是如何尽可能高效地存储不可篡改的区块链数据。业界讨论的焦点放在如下两种方向的解决方案上：

1）从交易层把部分交易迁移到子区块链上运行，即侧链、闪电网络；

2）从减少存储上着手解决，对原始数据进行裁剪分片，研究更安全的瘦客户端，只存储非全量验证数据就可正常工作。

也许从交易层进行分解可以让问题一劳永逸，但这种方法的可靠实现没有理论上那么简单。侧链技术现在正处于原型验证期，到真正实用的程度还需要一段时间。

从上述维度来看，区块链开发是一种综合能力的体现，其开发模式与互联网应用大有不同。传统互联网应用要求快速迭代，不断试错，区块链应用反而在发布前需要细致测试，对未来规划要有清晰的认识，因为一旦上线了就不是开发者能控制的：没有灰度发布、没有回滚下线、试错的成本极高。区块链是一台永不停止的信任机器，任何一次改变都需要通过共识，要明白共识的达成是极其困难的，所以在开发时一定要十分谨慎。

区块链技术的发展还面临着很多的挑战，需要更多的人才加入到探索者的队伍中。区块链开发更是需要复合型人才，分布式网络、分布式计算、密码学、编译原理、经济学等方面的内容都需要涉及，国内缺乏区块链综合技术的教程，这本书来的正当其时。本书各个主题的作者都是相关领域的专家或创业者，他们是对区块链理解最深入的一批人，具有较强的实战经验。书中各章节内容深入浅出，按时间顺序介绍区块链的技术发展，并且加入了大量的代码示例，鼓励读者动手实践，以帮助读者快速掌握区块链的开发技能，是一本值得一读的

实战型好书！

希望大家在阅读本书后有所收获。

邹　胜

2017 年 4 月

邹胜，深圳证券交易所前副总经理、深圳证券通信公司前董事长，拥有 24 年证券金融行业经验，曾领导深交所 IT 和深证通打造了第五代核心交易系统、中国证券期货业南方中心、金融云等业内领先的金融科技基础设施。现任深圳市金融科技协会联席会长，并致力于分布式交易技术在中国证券金融行业的应用推广。

Forword 2 推荐序二

区块链，推动金融代际跃升的新力量

金融为解决信息不对称而生，纵观3000年的发展历程，金融业态的变迁始终围绕着信息如何对称而展开，并基于外界环境的影响在金融化与科技化两个维度上演绎迭代。从金融化维度上看，发展主线围绕着“有中心”与“无中心”展开，哪一种业态更能解决信息对称，在不同的时空下，基于不同的金融工程技术而有不同的呈现，近400年的现代金融史正是一条从“无中心”到“有中心”再到“多中心”进而又可能回到“无中心”的演变轨迹。从科技化维度上看，信息技术的进步对金融业的影响非常敏感，人类历史上每一次信息技术的大提升都会带来金融业态的一次跳跃，尤其是近一百年来，电报、电话、海底电缆、计算机、互联网……无不带来金融业态的深刻变革，变革的指向始终是从“信息不对称”到“信息有限对称”并向着“信息对称”发展。

回顾我国改革开放后40年的金融发展，1997年无疑是至关重要的一年，那一年我国的银行业成功推出了网上银行，以此为标志，中国开始进入互联网金融时代。伴随着互联网这一千年一出的技术革命，金融业态发生着历史性的变革。不论我们以“互联网金融”还是以“金融互联网”来称谓这场变革，都不可否认金融业在解决信息对称的有效性，以及达成信息对称的效率性上，都得到了大幅提升，尤其是在以4G和智能手机为载体的移动金融出现之后，更是如此。

当然在这场长达20年的互联网金融变革中，互联网技术的内在缺陷也日益显现，网上信息的失真、可篡改、无法确权、加密强度低等特性都制约着金融业务的进一步深入，信息量越大反而越限制了信息的有效性，互联网金融开始触及自身发展的瓶颈。如何寻找新一代的替代技术解决信息的“二次不对称”，是金融业下一步演变的关键。

幸运的是，互联网本身也在迭代，并在其中一个迭代方向上出现了区块链技术。BlockChain，从诞生的第一天起就具有信息的真实、不可篡改、可确权、强加密等特征，这在某种意义上正是互联网技术的“扬弃”。而其在物理层和通信协议层与互联网的兼容，更使得

区块链技术的应用成本低、推广简便。

金融业要求信息应真实、安全、准确、权属清晰，因此我们有理由相信，互联网金融下一步演绎的方向是“区块链金融”，在区块链的路径上，继续探索哪一种“中心化形态”更有利于解决信息的对称性和效率性，从而将金融业态推向一个新的高度。

如果我们有能力预测“区块链金融”的发展轨迹，那么我们是否会形成如下这样一些观点。

- 互联网账户的区块链化。互联网金融的效应之一是让每一个金融机构都能平等地接触到终端用户，不受地域、网点、规模所限，重构大中小金融机构在金融领域重要性的自上而下排序的金字塔结构，带有典型的金融领域内的“普惠”特征。然而，这种扁平的平等触达客户的金融结构还需要另一个先决条件，那就是中小金融机构必须用技术手段自证自己的信用，自证安全可靠。显然，这有赖于区块链技术的运用。因此，在线开户、存款、支付、交易等业务整体向区块链平台迁移成为一种必然。
- 支付工具和支付体系的区块链化。以国内支付领域的现状来看，扫码支付替代磁条卡支付的趋势已经确立。然而，扫码支付的安全性始终是各方担忧的焦点。一方面，在二维码的生成与二次传播上如何增强加密强度；另一方面在二维码底层第三方支付的虚拟账户层面或银行的二类账户层面如何增强加密强度，必然会成为区块链技术发挥作用的结合点。此外，从商户收单的领域来看，商户体系只是从围绕银行展开收单和清算转变为围绕第三方支付公司展开，仍是其他“中心”的从属，基于区块链技术构建的以各商户互为中心的、以预付费卡为支付载体的“自收单体系”也将成为支付领域变革的一个重要方向。
- 征信的区块链化。互联网的持续推进引领着全球进入大数据时代，而征信在大数据时代呈现出了完全不同的业务逻辑和规则，但就目前来看，数据的权属问题将构成大数据征信模式最重大的挑战。而数据是谁的、在哪里确权、如何调用、如何计价等问题都可以借助区块链技术加以解决，从这个意义上说，大数据征信的内核是区块链征信。
- 资产证券化的区块链化。资产证券化技术成功解决了基础资产如何变成可交易的金融工具及如何计价交易的难题，从而极大地提升了金融资产的周转效率，因此被视为 20 世纪最重要的金融创新。然而，其基于线下的风险控制流程已难以适应互联网时代对金融效率和信息全面性的要求，因此，资产证券化的互联网模式已成为金融 B2B 领域的重要方向。同样，资产证券化各参与方信息的准确、不可篡改、确权、安全加密等也是 ABS 互联网化必须要面对的问题，也必然要辅助以区块链技术加以解决。
- 金融监管的区块链化。随着金融体系的日益庞大和复杂，如何监管已经成为世界难题。

2008年美国次贷危机诱发的全球金融危机，深刻反映出全球监管的滞后与漏洞。然而，随后出台的一系列监管补救法案，包括多德弗兰克法案、沃克尔法案、新巴塞尔协议等，无一例外仍在延续旧有的“规则性监管”的理念和思路，在所谓的金融杠杆控制上做出各种主观性的设置，全然没有看到在新技术运用上有突破性的理念和方法。基于后互联网时代的一系列信息技术已经完全可以做到实时、同步、自合理性设置、自预测性、自迭代的监管，即“数据性监管”，这也必然会成为下一轮全球金融监管改革的方向。区块链，基于其独特的信息处理属性，无疑会在“数据化监管”方面发挥重要的作用，有效构建监管部门、金融机构、金融客户之间的合理数据纽带。

恰如20世纪90年代末互联网进入应用开发阶段一样，区块链的产业应用同样需要一批具备区块链开发能力的人员、团队、技术组织，如何高效率地普及区块链技术、高效构建区块链技术生态至关重要。申屠青春等人编著的《区块链开发指南》，是一部难得一见的区块链实用著作，系统性地总结和提炼了区块链技术的核心属性，并从开发者的视角予以展开，相信在区块链技术和开发生态构建方面一定会发挥重要作用。也希望有更多区块链领域的技术专家和先行者贡献自身的知识和体会，共同推进区块链这一独特的信息技术，使其更迅速地与金融场景相结合，共同提升我国的金融效率与质量。

曹　彤

国金ABS云创始人

厦门国际金融技术有限公司董事长

中国区块链研究联盟副主任

推荐序三 *Forword 3*

区块链技术的现实和未来

一直以来，科学技术都是推动时代发展的原动力。20 世纪 90 年代，随着互联网的出现，人类的信息传递方式发生了重大改变，引发了新闻媒体行业的革命，促进了电子商务的流行；移动互联网的发展带来的影响更为巨大，激发了社交的变革，带来了更为便捷、高效的包括金融服务、出行服务等在内的各类新型社会服务方式，而且社会的协作模式和运作效率从整体上也发生了深刻的变化，这些正悄然改变着社会。区块链作为近年来新兴的 IT 技术，对任何由第三方机构来进行信用背书的社会协作模式都可能会带来改变，并在金融服务、企业运作、社会生活甚至社会治理等领域引发深远的变革。

区块链是一种去中心化、去信任化的分布式账本技术，由分布式数据存储、点对点传输、共识机制、加密算法等多种技术集合而成。区块链是起源于比特币的底层技术，自 2009 年被提出以后，近年来已成为各大金融机构、IT 公司、投资机构、咨询机构关注的热点，产业界纷纷加大研发投入力度。互联网全面发展以后，已经近乎完美地解决了信息传递的问题，但是还不能自由地实现价值点到点的传递，价值的传递仍然需要中心化的可信第三方来完成，在一些应用场景中仍存在一定的局限性。区块链的出现能够在没有信任基础的双方之间建立信任，完成价值传递，因而被誉为创造信任的机器。由于其具有去中心、去信任及不可篡改的特点，区块链被认为可以应用在多种业务场景中，用来建立信任，提升透明性、可靠性与安全性。目前，区块链的应用已经不只是在数字货币和支付结算领域，在供应链金融、数字资产交易、共享经济、食品安全、慈善等多个领域均有探索，而且还将为云计算、移动互联网、物联网等新一代信息技术的发展带来新的机遇。

当前，区块链一方面带有耀眼的光环，另一方面在现实应用中还存在着很多问题亟待解决，比如：大量冗余存储、共享的数据带来了数据安全和隐私保护等方面的挑战；在去中心化、匿名的区块链系统中，使用私钥管理用户资产，私钥一旦丢失，对应的资产所有权也将丢失，而如今应用对于私钥保护基本上是用软件来实现的，理论上都存在被攻破的可能性；

另外，链上敏感数据的保护与验证也存在一定的矛盾，我们既希望重要的信息对于无关者不可见，又需要相关者在一些场景下验证信息；除此之外，智能合约也存在着一些问题，如现有司法系统对智能合约的理解和接受程度问题，部分定性合同条款难以用代码来表述的问题，代码缺陷对智能合约执行影响的问题等。璞玉亦须雕琢，对于区块链的这些问题还需要进一步探索，还有大量艰苦的工作要做。

对于区块链，业内目前有两种截然相反的态度。一种是过于乐观，看到区块链技术在比特币应用的成功之后，认为区块链技术可以很快地为社会各方面带来翻天覆地的变化。另一种态度则过于悲观，认为区块链存在的问题太多，除了比特币之外再无成功应用，且区块链可以做的工作传统信息技术完全可以解决，甚至更高效。有业内人士担心这又是一个被过度炒作的概念，最终会不了了之。从区块链技术的发展历史来看，来源于比特币的区块链技术，具有无限制加入、匿名机制、公开账本、工作量证明共识算法等技术特点，这些特点比较适合支付结算相关应用，但不具有普适性。后来为了适应不同的应用场景，在比特币平台之后，又陆续出现了多种底层平台，包括致力于打造“世界计算机”的以太坊平台、提供跨行业解决方案的 HyperLedger 项目下的 Fabric 平台、为受监管的金融行业提供专业解决方案的 R3 Corda 平台等，这些平台相互影响并不断发展。目前区块链技术除了影响力最大的比特币之外，大部分应用还处于探索阶段，成功的应用不多，但是从当前各方面的探索中，我们也看到了区块链这种去中心、去信任的价值传递网络的巨大潜力。区块链技术目前尚处在发展的初期阶段，现在最重要的是以务实的态度深入研究，特别是要吃透技术细节，结合实际场景，推动区块链相关应用扎实落地。在这方面，IT 工程师们能够发挥更加积极的作用。

虽然区块链技术仍在发展之中，仍有不少问题需要解决，但是随着基础平台的不断完善，区块链应用将得到快速发展。根据 Gartner 分析报告预测，预计经过 3 到 5 年的发展，区块链应用的落地会出现大规模的增长；未来 10 年左右，整个区块链市场将趋于成熟，广泛应用在智能合约驱动类业务、数字货币业务、机构间和机构内业务及公共记录等领域。目前，已有众多从理论和业务层面探讨区块链的图书和文章，但是技术类图书却非常稀缺。本书对于区块链的开发做了系统的介绍，是献给站在 IT 前沿开拓者的佳作。作为 IT 从业者，此时更需要把握当下，因为未来已来。让我们怀揣梦想，一起努力，共同打造更加完善的区块链服务，用科技创造美好未来！

周天虹

招商银行信息科技部总经理

2017 年 4 月

前　言 Preface

比特币于2009年诞生，在很长一段时间内，人们只知比特币，不知区块链。从2015年开始，区块链像狂风一样席卷全球，倍受金融界和科技界的关注；2015年年底，区块链技术逐渐得到国内金融界和科技界的了解和认同。

区块链行业的蓬勃发展源于区块链有可能给各行业带来巨大的变革。麦肯锡在2016年年初发布报告，指出区块链技术将在未来五年内颠覆众多行业，特别是银行业和保险业；埃森哲预测到2025年，区块链技术每年可帮助全球8大投资银行节省80亿美元至120亿美元的基础设施成本。

全球金融巨头如IBM、高盛、摩根大通、花旗银行、中国平安、瑞银、德勤、毕马威等纷纷布局区块链；区块链初创公司在全球范围内如雨后春笋般崛起，发展速度惊人。从2012年以来，全球区块链创业领域共发生207起融资/并购事件，融资额高达14亿美元。

截至2017年3月，区块链在金融业的落地应用包括跨境支付、清算结算、互助保险、电子票据、商业银行抵押品、贸易金融、数字资产登记、银行间贸易、银行间对账与审计、监管与简化流程、积分、征信、外汇交易市场、证券清算和交割等。

区块链技术还能解决供应链管理、物联网、医疗、军事、政务等领域的很多问题。例如，Warmart试图用区块链保障我国市场的猪肉供应链安全；医疗领域中，生成基于区块链的、不可更改的电子病历、检验报告等用于存证，方便解决医疗纠纷；军事防卫和信息安全化中，区块链技术可实现信息防御平台的现代化；政务中，区块链可以简化文件归档与政府公共档案管理，并且可用来发放政府社保、养老金等社会福利及居民身份存证等。

由此可见，区块链将带来一场巨大的变革。正如德勤的报告中所预言的一样："区块链是一场改变信任的革命，将重塑金融行业。"而它作为一项伟大的技术，不仅仅对于金融行业有革新性，对于其他行业，也会有深远的影响。

而今实施“区块链+”战略所面临的最大难题是：极度缺乏从业人员。很多金融机构和企事业单位对区块链还停留在概念阶段，其开发人员不懂区块链；大部分对区块链技术感兴趣的人，或者想要从事区块链行业的技术人员，未能系统地了解区块链的原理和发展，缺乏区块链开发者应有的知识和技术储备。

为了让更多的开发人员转变成区块链开发者，让更多现有的区块链开发人员系统地理解区块链技术，在区块链领导媒体巴比特的提议和牵头下，成立了《区块链开发指南》编写小组，开始构思、编写本书。

编写小组成员有：银链科技 CEO 申屠青春、深圳大学教授张鹏、币信资深程序员宋波、朝夕网络 CEO 汪晓明、万达网络区块链研发中心总经理季宙栋、华安保险系统架构师左川民、巴比特区块链资深工程师易长军。

本书内容由申屠青春负责组织，共包含六个章节，具体分工如下：申屠青春编写第 1 章和第 2 章的大部分内容，易长军对本部分内容亦有贡献，币信的樊渊文贡献了 1.4.2 节、1.4.3 节和 1.4.4 节，比特大陆的潘志彪贡献了 2.5.2 节、2.5.3 节和 2.5.4 节；张鹏编写第 3 章；宋波编写第 4 章；汪晓明编写第 5 章；季宙栋编写第 6 章的实操部分，左川民编写第 6 章的原理部分。此外，银链科技的林素兰参与第 1 章和第 2 章部分内容的编辑，万达网络的丛宏雷、张梦航参与第 6 章实操部分内容的编写。

本书以比特币、以太坊、Fabric 三种区块链的技术原理和实际操作为主要目标，全书具体内容如下。

第 1 章介绍比特币区块链，包括交易和交易链、区块和区块链、挖矿、矿池、脚本系统、合约应用案例等内容，向读者们介绍区块链基础知识。

第 2 章讲述区块链进阶技术，包括外带数据原理、Counterparty 原理、挖矿算法解析、侧链技术，以及最新的 IBLT、隔离见证、闪电网络等。

第 3 章的主要内容是区块链中使用的密码学基础，包括 Hash 函数、椭圆曲线密码体系、ECDSA 签名、Schnorr 数字签名和 Bloom filter 算法等，向开发者介绍密码学相关算法。

第 4 章是比特币区块链的编译、代码剖析、建立私链及 API 开发等实操内容。

第 5 章介绍以太坊的技术原理，包括以太坊简介、账户管理、交易原理、智能合约等，还涉及搭建私有链，智能合约开发、部署和调用等实操过程。

第 6 章介绍了 IBM 开源的区块链底层技术平台 Fabric 的原理和实操，对 Fabric 系统架构、节点、验证总账、交易背书的基本流程进行了详尽独到的分析，对 Fabric 的私有链建立和配置、链上代码的开发过程进行了详细的描述，为开发者使用 Fabric 提供技术指导。

最后，感谢编写小组各成员的配合和支持，使本书最终得以完本。感谢巴比特的李涛，

时时督促此书的编写；感谢机械工业出版社华章公司的编辑杨绣国为本书顺利出版付出的努力。编写小组期待本书能够在区块链应用开发中给开发者以参考和启发。由于成书仓促，错误之处在所难免，恳请广大读者朋友批评指正。

申屠青春

2017 年 4 月于深圳

Contents 目　录