HZ BOOKS
华章教育

互联网时代的信息安全
创新应用新模式

区块链
技术与应用

朱建明 高胜 段美姣◎等编著

BLOCK CHAIN
TECHNOLOGY AND APPLICATION

机械工业出版社
China Machine Press

区块链

技术与应用

朱建明 高胜 段美姣◎等编著

BLOCK CHAIN

TECHNOLOGY AND APPLICATION

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链技术与应用 / 朱建明等编著 . —北京：机械工业出版社，2017.11

ISBN 978-7-111-58429-2

I. 区… II. 朱… III. 电子商务 – 支付方式 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2017）第 267010 号

随着以比特币为代表的数字货币的崛起，其底层支撑架构——区块链凭借去中心化信用、数据不可篡改等特点，吸引了多国政府部门、金融机构及互联网巨头公司的广泛关注，逐渐成为当前学术界和产业界的热点课题。本书首先简要介绍了密码学、P2P 网络、数据库等区块链技术的基础知识，然后详细介绍了比特币的相关原理与技术，在此基础上重点介绍了区块链技术的原理，最后介绍了区块链技术的应用。本书是第一本系统全面介绍区块链技术的中文教材，目的是使学习者能够掌握区块链的理论与技术，进而从事区块链的开发与应用。

本书可作为计算机、信息管理、电子商务以及管理信息系统等专业的本科生教材和研究生教材。

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：冯小妹　　责任校对：李秋荣

印　　刷：北京诚信伟业印刷有限公司　　版　　次：2018 年 1 月第 1 版第 1 次印刷

开　　本：185mm × 260mm　1/16　　印　　张：20.5

书　　号：ISBN 978-7-111-58429-2　　定　　价：49.00 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）88379210　88361066　　投稿热线：（010）88379007

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjg@hzbook.com

前　言

随着以比特币为代表的数字货币的崛起，其底层支撑架构——区块链凭借去中心化信用、数据不可篡改等特点，吸引了世界许多国家政府部门、金融机构及互联网巨头公司的广泛关注，已经成为当前学术界和产业界的热点课题。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

2016 年 12 月，《国务院关于印发“十三五”国家信息化规划的通知》将区块链写入“十三五”国家信息化规划，将区块链列为重点加强的战略性前沿技术。区块链已经成为国家信息化战略的重要组成部分。

2016 年 9 月，中央财经大学信息学院的朱建明、高胜和段美姣三位老师共同开设了第一门“区块链技术”课程，本书就是在此基础上完成的。本书主要回答四个方面的问题：

第一，为什么要学习和研究区块链技术？从国家战略、技术发展等方面阐述了区块链技术的重要性和区块链技术的应用环境以及面临的问题。

第二，比特币中的区块链技术原理是什么？作为比特币的底层技术，区块链是如何发挥作用的？其技术原理和细节是什么？这一部分给出了详细的介绍。

第三，区块链技术的原理是什么？在比特币区块链技术的基础上，区块链技术又有新的发展，这一部分详细介绍区块链的最新研究成果和技术。

第四，如何应用区块链技术解决实际问题。

全书由朱建明、高胜和段美姣三位老师共同编著。第 1 章由朱建明编写，第 2 章由贾恒越编写，第 3 章由海沫编写，第 4～7 章由段美姣、朱烨辰编写，第 8～10 章由高胜编写，第 11 章案例由布比公司和火币网提供，由付永贵整理。

编者在完成本书的过程中参阅了大量的文献，其中包括专业书籍、学术论文、学位论文、国际标准、国内标准和技术报告等，书中有部分引用已经很难查证原始出处，编者注

明的参考文献仅仅是获得相关资料的文献，没有一一列举出所有的参考文献，在此表示歉意和谢意。

由于编者水平有限，本书不足与疏漏之处在所难免，敬请广大读者批评指正。

作者

2017 年 8 月

目　录

第一部分

基础知识

第1章

绪　论

区块链（blockchain）技术是金融科技（fintech）领域的一项重要技术创新。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，我国也积极探索推动区块链的应用。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

那么，什么是区块链呢？为什么区块链技术引起学术界和产业界的高度重视？本章将回答这些问题。

1.1　区块链概述

最早关于区块链的描述出现在2008年由化名为中本聪（Satoshi Nakamoto）所撰写的论文《比特币：一种点对点的电子现金系统》（*Bitcoin: A Peer-to-peer Electronic Cash System*）中，然而该文重点讨论比特币系统，区块链被描述为用于记录比特币交易的账目历史。在比特币系统成功运行多年后，部分金融机构开始意识到，作为比特币运行的底层支撑技术——区块链实际上是一种极其巧妙的分布式共享账本技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。2014年前后，业界开始认识到区块链技术的重要价值，并通过智能合约技术将其用于数字货币外的分布式应用领域。2015年，《经济学人》（*Economist*）杂志在封面介绍区块链为创造信任的机器，即区

块链可以在没有中央权威机构的情况下，为交易双方建立起信任关系。

1.1.1 为什么关注区块链

2015年以来，区块链技术引起了学术界、产业界的高度重视。下面是有关媒体对区块链的部分报道：

- 区块链——重塑经济与世界。
- 区块链技术有望像互联网一样彻底重塑人类社会活动形态，并实现从目前的信息互联网向价值互联网的转变。
- 互联网已经颠覆世界，区块链却要颠覆互联网。
- 区块链技术已经被视为下一代全球信用认证和价值互联网的基本协议之一。

从这些报道中，可以看出区块链技术的重要性。与此同时，世界各国都加强了区块链技术的研究，将区块链列为国家发展的重要战略。2015年下半年以来，“区块链”这个词开始成为全球各大监管机构、金融机构及商业机构，如摩根士丹利、英国政府、花旗银行等争相讨论的对象。从整体上看，参与讨论的金融机构普遍对区块链技术在改善其中后端流程效率及降低运作成本的可能性上有着较为积极的态度，部分国家政府对推动区块链技术和应用的发展持积极态度。

我国政府也积极支持开展区块链技术的研究和应用。2016年12月在《国务院关于印发“十三五”国家信息化规划的通知》中将区块链写入“十三五”国家信息化规划，将区块链列为重点加强的战略性前沿技术。2016年2月，中国人民银行行长周小川在谈到数字货币相关问题时曾提及，区块链技术是一项可选的技术，并提到中国人民银行部署了重要力量研究探讨区块链应用技术。2017年“两会”上，行长周小川再次表示，数字资产和区块链将产生不可估量的巨大影响。2017年年初，央行数字货币又有新进展，央行推动的基于区块链的数字票据交易平台已测试成功，由央行发行的法定数字货币已在该平台试运行，中国可能成为全球首个发行央行数字货币的国家。

2017年1月，北京市金融工作局、北京市发改委联合印发《北京市“十三五”时期金融业发展规划》强调，要加快云计算、大数据和区块链等金融科技在支付清算、数字货币、财富管理等领域的创新发展与应用。

2016年8月，全球领先的信息技术研究和顾问公司Gartner发布了《Gartner2016年度新兴技术成熟度曲线》，如图1-1所示。2016年，区块链正处于期望膨胀期，距离成熟期5～10年，可见2017年全球区块链技术仍然会保持比较快的发展趋势。

因此，无论从媒体，还是从国家战略和技术发展的角度来看，区块链技术无疑是未来最有发展潜力的技术之一。

比特币作为区块链技术的成功应用示范，其价值变化也进一步说明了区块链技术的重要性。比特币从2009年开始市值已经涨到21 399.00元人民币（2017年8月5日的行情），虽然其中多次反复，出现了多次暴涨暴跌，但是总的趋势是上涨的行情。这也从一个方面反映了社会对区块链技术的信心。

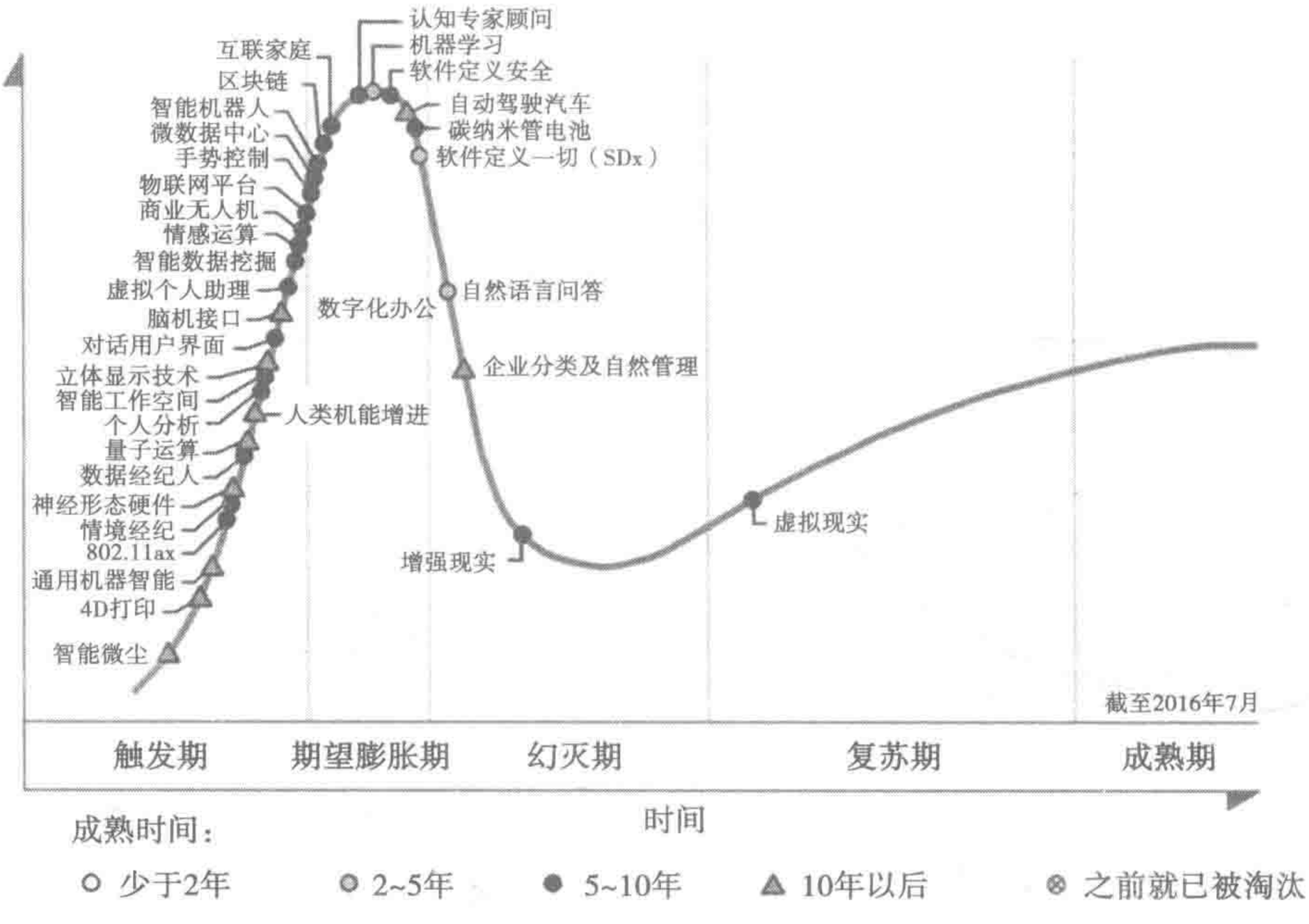

图 1-1　Gartner2016 年度新兴技术成熟度曲线

1.1.2　区块链的特点

2014 年开始，比特币背后的区块链技术受到大家关注，并正式引发了分布式账本（distributed ledger）技术的革新浪潮。区块链实质是由多方参与共同维护一个持续增长的分布式数据库，也被称为分布式共享总账（distributed shared ledger），其核心在于通过分布式网络、时序不可篡改的密码学账本及分布式共识机制建立彼此之间的信任关系，利用由自动化脚本代码组成的智能合约来编程和操作数据，最终实现由信息互联向价值互联的进化。

区块链技术作为创造信任的机器，主要有以下特点：

（1）分布式结构。区块链构建在分布式网络基础之上，账本并不是集中存放在某个服务器或数据中心，也不是由第三方权威机构来负责记录和管理，而是分散在网络中的每一个节点，每一节点都有一个该账本的副本，所有副本同步更新，体现了去中心化的特点。

（2）建立信任。区块链技术通过数学原理和程序算法，使系统运作规则公开透明，实现交易双方在不需要借助第三方权威机构（如央行等）信用背书下通过达成共识建立信任关系。

（3）公开透明。区块链对任何可以上网的人是开放的、透明的。任何人都可以加入区块链，也能查询区块链上的区块记录；同时所有用户看到的是同一个账本，能看到这一账本所发生和记录的每一笔交易。

（4）时序且不可篡改。区块链采用带有时间戳的链式区块结构存储数据，具有极强的可追溯性和可验证性；同时，由密码学算法和共识机制保证了区块链的不可篡改性。

1.1.3 区块链的重要性

随着新一轮产业革命的到来，云计算、大数据、物联网等新一代信息技术在智能制造、金融、能源、医疗健康等行业中的作用愈发重要。从国内外发展趋势和区块链技术发展演进路径来看，区块链技术和应用的发展需要云计算、大数据、物联网等新一代信息技术作为基础设施支撑，同时区块链技术和应用发展对推动新一代信息技术产业发展具有重要的促进作用。图 1-2 说明了区块链与新一代信息技术的关系。

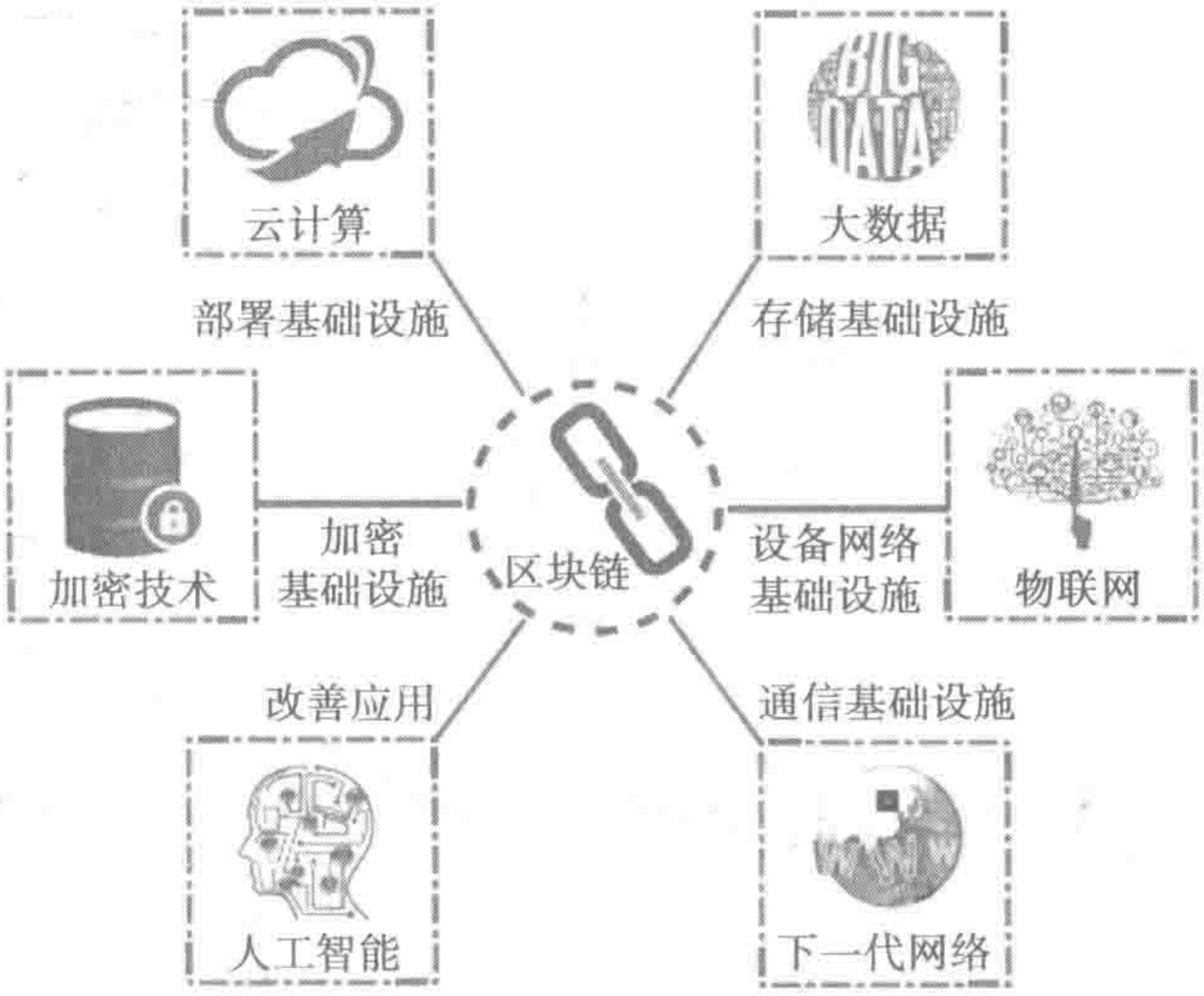

图 1-2 区块链与新一代信息技术的关系

区块链是一种不可篡改的、全历史的数据库存储技术，巨大的区块数据集合包含着每一笔交易的全部历史，随着区块链的应用迅速发展，数据规模会越来越大，不同业务场景区块链的数据融合进一步扩大了数据规模。区块链提供的是账本的完整性，数据统计分析的能力较弱。大数据具备海量数据存储技术和灵活高效的分析技术，极大地提升了区块链数据的价值和使用空间。

1.2 区块链技术的应用

区块链技术是金融科技领域的一项重要技术创新。作为去中心化记账（DLT）平台的核心技术，区块链被认为在资产管理、金融、征信、物联网、经济贸易结算等众多领域都拥有广泛的应用前景。

中本聪在其论文中介绍区块链时指出：“区块链是一种数据结构，也是该电子现金系统（比特币）的核心技术。”该系统的实现原理是：利用区块链让系统中的任意多个节点把一段时间内系统交互的数据，通过密码学算法计算并记录到一个区块（block），并且生成该区块的指纹以用于验证和链接下一个区块，系统所有参与节点共同认定记录的真实性。

1.2.1　区块链技术的应用场景

区块链技术在经济和社会管理系统中存在广泛的应用场景。

1. 数据存储

区块链的高冗余存储（每个节点存储一份数据）、去中心化管理特点使其非常适合存储和保护重要隐私数据，以避免因中心化机构遭受攻击或权限管理不当造成的大规模数据丢失或泄露。目前，利用区块链来存储个人健康数据（如电子病历、基因数据等）是较典型的应用领域。

2. 数字身份验证

OneName 和 BitID 是以区块链为基础提供数字身份服务的典型应用。此类去中心化数字身份验证服务利用了每个比特币用户都有一个比特币钱包的优势（即每个用户都拥有一个唯一的比特币地址），大大提高了用户访问网站的速度，并增强了匿名性和安全性。

3. 数据鉴证

区块链数据具有安全时间戳，由共识节点共同验证和记录，使其可应用于各类数据公证和审计场景。例如，区块链可永久地安全存储由政府机构核发的各类许可证、登记表、执照、证明、认证和记录等，并可在任意时间点方便地证明某项数据的存在性和一定程度上的真实性。包括德勤在内的多家专业审计公司已经部署区块链技术来帮助其审计师实现低成本和高效的实时审计，Factom 公司则基于区块链设计了一套准确的、可核查且不可篡改的审计公证流程与方法。

4. 金融交易

在互联网金融领域，区块链技术已经应用于股权众筹、P2P 网络借贷和互联网保险等业务，同时证券和银行业务也是区块链的重要应用场景。传统证券交易需要经过中央结算机构、银行、证券公司和交易所等中心机构的多重协调，而利用区块链自动化智能合约的特点，能极大地降低成本和提高效率，避免烦琐的中心化清算交割过程，实现方便快捷的金融交易。同时，基于区块链的交融交易可保证即时到账，从而使跨境转账更为快捷、经济和安全，这也是目前 R3CEV 和纳斯达克等各大银行、证券商和金融机构相继投入区块链技术研发的重要原因。

5. 资产管理

区块链在资产管理领域能够实现有形和无形资产的确权、授权和实时监控。对于无形资产来说，可将区块链技术应用于知识产权保护、域名管理、积分管理等业务；而对有形资产来说，通过结合物联网技术为资产设计唯一标识并部署到区块链上，能够形成“数字智能资产”，实现基于区块链的分布式资产授权和控制，这些方向当前均有相关的研究和商业项目被提出。

1.2.2　区块链技术在国外的推广

区块链技术在国外的发展同样是如火如荼，但是与国内多是以研究和探讨应用场景为

主，区块链技术推动多是由中小企业担纲不同，国外区块链技术发展的显著特征是：区块链联盟旨在区块链技术的验证和试验，以及区块链技术标准的制定，区块链技术推动多是由大企业来担纲。

1. R3 区块链联盟

R3 区块链联盟致力于研究和发现区块链技术在金融业中的应用。R3 区块链联盟自 2015 年 9 月份由 9 位发起成员设立，2015 年年底首轮招募 42 家知名国际性银行；2016 年，R3 进一步开放，吸纳非银行金融机构，截至 2016 年 9 月，R3 联盟成员已超过 60 家。进一步，R3 区块链联盟推出自己的产品 Corda，旨在将自身的区块链解决方案打造成全球银行的运作标准。

2. Hyperledger 区块链联盟

超级账本项目是 Linux 基金会管理下的合作项目，目的是要共同建立并维系一个跨产业的、开放的、分布式账本技术平台。截至 2016 年 9 月 30 日，其成员数已达 85 家。Hyperledger 项目是一个“技术驱动”的联盟，在其成员当中，科技公司和金融机构各占三成，另有超过两成的成员是区块链公司，联盟的目标是推动 Hyperledger 成为事实上的工业技术标准。

3. 布局区块链产业的科技巨头

IBM——2016 年年初，IBM InterConnect 创新应用大会上宣布重点投入区块链领域，随后 IBM 公司宣布推出一套用于在 IBM 云上创建、部署、运行和监控区块链应用的“区块链即服务”（BaaS 服务）。IBM 是 HyperLedger 项目的主导者之一，已经向 HyperLedger 项目贡献了 44 000 行代码。

微软——微软宣布向区块链领域开放 Azure 云计算平台，并且已经与以太坊、ConsenSys、Ripple 等多家平台建立了合作关系，其目的在于将 Azure BaaS 平台扩展成一个“认证的区块链市场”，客户既可以直接在 Azure 上部署区块链，也可以间接通过 Azure 在当地的数据中心部署区块链，使用户可以借助自动化设置在 20 分钟之内就能打造一个区块链环境。

亚马逊——亚马逊的云计算商业服务平台亚马逊网络服务（AWS）与投资公司数字货币集团（DCG）合作，为企业提供一个区块链实验环境。亚马逊凭借 AWS 正式进入区块链领域。

谷歌——谷歌在微软、IBM 与亚马逊相继建立区块链技术平台后，于 2016 年也宣布将为银行提供区块链测试服务，正式与 IBM、微软、亚马逊角逐 BaaS 市场。咨询公司 GFT 在其为苏格兰皇家银行集团提供的一个清算及结算的区块链应用的测试中采用了 Google 服务器。

英特尔——2016 年 4 月，英特尔推出一个名为“锯齿湖”（Sawtooth Lake）的用于建造、部署和运行分布式账本的实验性分布式账本平台，并基于该平台向开源超级账本（Hyperledger）区块链项目提供代码贡献。2016 年 6 月，英特尔在以色列特拉维夫市成立了一个开发实验室，致力于研究物联网（IoT）连接设备、云计算、生物识别应用程序以

及区块链技术。

1.2.3　区块链技术的局限性

作为近年来兴起的新技术，区块链仍面临一些制约其进一步发展和广泛应用的障碍，包括底层技术的挑战、潜在的安全隐患以及隐私保护等。

1. 政府监管挑战

区块链技术的兴起对于政府的监管提出了一定挑战，如政府无法按照现行税制收取比特币交易税费。现行的税收结构将被完全颠覆，影响税收及整体经济指标的计算。

2. 运行安全风险

区块链技术目前潜在的最大安全隐患就是 51% 攻击问题，即节点通过掌握全网超过 51% 的算力就有能力成功篡改和伪造区块链数据。据统计，中国大型矿池的算力已占全网总算力的 60% 以上，理论上这些矿池可以通过合作实施 51% 的攻击，从而实现比特币的双重支付。虽然实际系统中为掌握全网 51% 算力所需的成本投入远超成功实施攻击后的收益，但 51% 攻击的安全性威胁是始终存在的。

3. 系统效率及可扩展性问题

比特币区块链目前每秒仅处理 7 笔交易，这极大地制约了区块链技术在金融系统中高频交易场景中的应用（如 VISA 信用卡每秒最多处理 10 000 笔交易）；此外，依据区块链技术的协议设计，当前每个比特币区块的生成时间为 10 分钟，这意味着每笔交易的确认时间为 10 分钟，这在一定程度上限制了比特币在小额交易和时间敏感交易中的使用；最后是容量膨胀问题。区块链要求系统内每个节点保存一份数据备份，这对于日益增长的海量数据存储来说是极为困难的。就比特币区块链而言，完全同步自创世区块至今的区块数据需要约 60GB 存储空间，虽然轻量级节点可部分解决此问题，但适用于更大规模的工业级解决方案仍有待研究。

4. 隐私泄露风险

区块链系统内各节点虽不必公开身份，但也并非完全匿名，而是通过类似电子邮件地址的地址进行标识（如比特币公钥地址）并实现数据传输。虽然地址标识并未直接与用户身份相关联，但区块链数据是完全公开透明的，随着各类反匿名身份甄别技术的发展，仍有可能实现部分重点目标的定位和识别。

思考题

1. 查阅资料，了解区块链的最新进展。
2. 比特币与区块链是什么关系？
3. 针对区块链技术的特点，请举例说明区块链技术的一种应用环境。

参考文献

[1] Nakamoto S. Bitcoin: A Peer-to-peer Electronic Cash System [J], Consulted, 2009.

[2] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. O'Reilly Media Inc., 2014.

[3] Narayanan A, Bonneau J, Felten E, et al. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction [M]. Princeton University Press, 2016.

[4] Morabito V. Business Innovation through Blockchain: The B3 Perspective [M]. Springer, 2017.

[5] Walport M. Distributed Ledger Technology: Beyond Blockchain [R]. Tech Rep, 2016.

[6] 中国区块链技术和产业发展论坛．中国区块链技术和应用发展白皮书，2016.

[7] 袁勇，王飞跃．区块链技术发展现状与展望 [J]. 自动化学报，2016, 42(4): 481-494.

[8] 高航，俞学劢，王毛路．区块链与新经济：数字货币 2.0 时代 [M]. 北京：电子工业出版社，2016.

[9] 谭磊，陈刚．区块链 2.0 [M]. 北京：电子工业出版社，2016.

[10] 赵刚．区块链：价值互联网的基石 [M]. 北京：电子工业出版社，2016.

第 2 章

区块链中的密码学

比特币是一种密码货币，区块链技术的基础是密码学。本章主要介绍在区块链技术中用到的密码算法、数字签名、Hash 函数等。

2.1 密码学概述

密码学（cryptology）起源于保密通信技术，是结合数学、计算机、信息论等学科的一门综合性、交叉性学科。密码学又分为密码编码学（cryptography）和密码分析学（cryptanalysis）两部分。密码编码学主要研究如何设计编码，使得信息编码后除指定接收者外的其他人都不能读懂。密码分析学主要研究如何攻击密码系统，实现加密消息的破译或消息的伪造。这两个分支既相互对立又相互依存，正是由于这种对立统一关系，才推动了密码学自身的发展。

现代密码学主要内容及联系如图 2-1 所示，这些密码技术为信息安全中的机密性、完整性、认证性和不可否认性提供基本的保障，也为 PKI 技术、认证技术等实际应用提供基本的工具，本章主要介绍在区块链技术中所用到的有关密码学知识。

随着计算机科学与技术的蓬勃发展，出现了快速电子计算机和现代数学方法，它们一方面为加密技术提供了新的概念和工具，另一方面也给密码破译者提供了有力的武器，二者相互促进，使密码技术飞速发展。新兴信息技术为密码设计者提供了前所未有的条件，从而可以设计出更加复杂和更为高效的密码体制。

近年来，由于其他相关学科的进步和发展，也出现了一些新兴、交叉性的密码技术。例如，随着量子计算研究热潮的兴起，世界各国对量子密码的研究也广泛地开展起来。量