# 区块链实战

吴为　编著

清華大學出版社
北　京

## 内 容 简 介

本书全景式地描述了互联网前沿技术——区块链，分别从区块链的起源、区块链在全球各个国家的发展现状、区块链的四大核心技术、基于区块链底层技术的数字货币发展现状等角度进行描述。另外，为了更好地理解区块链，本书讲述了区块链在数字货币领域、金融领域、物联网领域、大数据领域、医疗领域、教育领域、公证领域等七个领域的应用。

区块链是一场技术革命。在不久的将来，我们会看到区块链与传统行业的直接较量。而且这是一场不同层面的竞争，传统行业被新技术取代已成必然趋势。所以在一切还未发生之前，关注区块链、参与区块链、应用区块链是至关重要的。

通过阅读本书，读者只需要花费一周的时间就可以理解区块链是什么以及它能干什么，并且理解区块链在各个领域的价值所在。



图书在版编目（CIP）数据

区块链实战 / 吴为著. — 北京：清华大学出版社，2017
ISBN 978-7-302-47589-7

Ⅰ. ①区… Ⅱ. ①吴… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2017）第 146671 号

**责任编辑**：刘 洋
**封面设计**：李召霞
**版式设计**：方加青
**责任校对**：王凤芝
**责任印制**：王静怡

**出版发行**：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 装 者**：三河市金元印装有限公司
**经 销**：全国新华书店
**开 本**：170mm×240mm **印 张**：14.75 **字 数**：262 千字
**版 次**：2017 年 9 月第 1 版 **印 次**：2017 年 9 月第 1 次印刷
**定 价**：49.00 元

产品编号：075513-01

Block chain practice

# 前　言

2017 年 2 月，中国人民银行（简称央行）研究并测试数字票据交易平台的事件轰动了全球，该数字票据交易平台应用的基础技术就是区块链。此外，央行旗下数字货币研究所也在 2017 年上半年正式挂牌成立。这意味着中国人民银行成为全球范围内首个研究数字货币并将数字货币应用于真实生活的中央银行，并率先探索区块链技术在货币发行领域的应用。

那么，央行建立区块链数字票据交易平台对我们的现实生活会产生很大影响吗？答案是肯定的，大家可以想象一下：两三年以后，过年发红包不再是纸质钞票，而是一串串的数字密码，我们可以通过发送邮件、复制到 U 盘里或者通过手机直接将其发送给他人。

关于央行开发数字货币的原因，央行参事盛松成称：“未来的央行数字货币会从多个方面倒逼金融基础设施建设，让我国支付体系进一步完善，支付结算效率进一步提升。更值得一提的是，央行数字货币最后可以构成大数据系统，使经济交易活动的便利性和透明度进一步得到提高，这将有利于货币政策的有效运行和传导。”

在央行的积极带动下，我国各方资本纷纷在区块链行业布局。截至 2016 年年年底，平安银行、招商银行、民生银行都已经加入 R3 区块链联盟。截至 2017 年年初，我国 A 股市场上切入区块链概念的公司已经有 24 家，大部分公司是软件和信息技术提供商。

各大行业巨头公司也不甘落后。其中，万向集团建立了区块链实验室，华为加入了 Linux 基金会领导的超级账本区块链项目。另外，百度、光大投资管理公

司、中金甲子、宜信等机构向一家美国比特币初创公司投资了 6 000 万美元。

从全球范围来看，包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把大把地砸钱，它们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等金融机构还向一家区块链初创公司 Digital Asset 投资 5 000 万美元。

如今，各方都对区块链表示出极大的关注度，区块链技术正在从一片巨大的蓝海转变为一片巨大的红海。那么，区块链凭借什么魅力受到了全球关注呢？以金融业票据清算系统为例，区块链将从以下四个方面发挥作用。

第一，消除了票据中介角色。在应用了区块链技术之后，票据价值可以实现 P2P 无形传递，既不需要特定实物作为连接双方取得信任的证明，也不需要第三方对交易双方价值传递的信息做监督和验证。另外，票据交易双方常常需要通过票据中介来解决信息不对称问题，而借助区块链实现 P2P 交易后，票据中介的现有职能将被消除。

第二，防范票据市场风险。不透明、不规范以及高杠杆错配等潜规则使票据市场的风险频发，参与机构的多样性和逐利性也加大了这一风险。而区块链技术全网公开、数据不可篡改的特性可以防范道德风险；分布式系统无须第三方中介的特性完全避免了人为操作风险；自动控制参与者资产和负债两端平衡且数据公开透明的特性有利于控制市场风险。

第三，建立去中心分布模式的电子商业汇票系统。现有的电子商业汇票系统（Electronic Commercial Draft System，ECDS）是一个中心化系统，其中心为央行，其他银行和企业通过直连或网银代理的方式接入央行的中心化登记和数据交换系统。区块链技术将会改变现有电子商业汇票系统的存储和传输结构，建立去中心分布式模式，还能利用时间戳完整反映票据从产生到毁灭的过程，使每一张票据都可以追溯历史。区块链建立的全新连续“背书”机制将更加真实地反映票据权利的转移过程。

第四，降低了市场监管成本。多样的操作方式使得票据市场的监管变得非常繁杂。监管方式也只能是现场审核，而业务模式和流转则没有全流程的快速审查和调阅手段。

区块链的价值具有无限潜力，不仅仅是在重构票据清算系统方面，也不仅仅是在金融领域。而且区块链红海席卷全球的局势已经基本建立，各种利好也即将降临，那些提前进入区块链行业，提供建设区块链经济最原始资本的人，注定会率先品尝到区块链带来的丰厚回报。

# 本 书 特 色

**1. 内容全面，结构清晰**

本书内容包括区块链的起源、发展、应用以及趋势预测，并重点讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用。而且全书架构清晰，有助于读者形成框架形式的认知。

**2. 案例丰富，实战性强**

本书加入很多真实且具有代表性的案例，使内容更加生动有趣。而且案例的加入使理论知识不再枯燥无味，读者更容易接受其中的观点。另外，本书理论与实战相结合，非常适合没有接触过区块链的读者阅读，帮助他们快速入门，深入理解区块链的价值。

**3. 语言通俗，更接地气**

新概念、新技术类的图书总是被作者包装得高大上，看起来非常有范儿，但实质上却提高了读者的理解门槛。而本书倾向于采用通俗易懂的语言为读者解读深奥的理论，让读者轻松理解与区块链相关的理论、应用等知识。

# 本书内容及体系结构

第 1 章：讲述了区块链起源于比特币，并对比特币的发行规律、价格变化等作出详细报告，有助于读者理解区块链与比特币的关系。

第 2 章：讲述区块链在人类世界的发展现状，包括各国政府对区块链的积极态度、全国各大企业对区块链应用的投资以及 2017 年最热门的 5 家区块链初创公司。

第 3 章：介绍了区块链的四大核心技术，包括具有去中心化创新、数据高度透明、不依赖信任以及信息可回溯性四大特征的分布式账本技术，用户掌握私钥以及匿名的非对称加密和授权技术，参与者共同维护的共识机制、自动控制，以及自动执行数字承诺的智能合约。

第 4 章：讲述了货币的进化历史以及当前三大数字货币（比特币、以太坊和莱特币）的发展现状，还将比特币与以太坊、莱特币作对比，帮助读者了解各自优势。

第 5 ～ 10 章：分别讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用，帮助读者对区块链的价值形成系统

认识。

第 11 章：讲述了区块链技术与物联网、大数据、人工智能等领域深度融合的发展趋势，并分析了区块链将会颠覆传统行业、改变人类世界的发展前景。

## 本书读者对象

- 各领域企业领导、高管
- 金融科技企业工作人员
- 数字货币相关公司工作人员
- 区块链研究以及开发者
- 对区块链以及数字货币感兴趣的其他人群

参与本书编写工作的人员还有梁萍、李改霞、赵丹丹、李恬、曾丽佳、李雪霞、李卫霞、李艳霞、李伟光、李晓青、游万梅、贾云叶、宋佳佳、龚毅、梁现丽、王逊、鲁宗保、李小菊等。

编者

2017 年 5 月

Block chain practice

# 目 录

## 第 1 章　区块链起源



## 第 2 章　区块链——必将颠覆人类世界

## 第 3 章 区块链四大核心技术

## 第 4 章 区块链与数字货币



## 第 5 章 区块链在金融领域的应用

## 第 6 章　区块链在物联网领域的应用



## 第 7 章　区块链在大数据领域的应用

## 第 8 章 区块链在医疗领域的应用



## 第 9 章 区块链在教育领域的应用



## 第 10 章 区块链在公证领域的应用

## 第 11 章 区块链发展趋势分析与预测

Block chain

# 第1章
# 区块链起源

区块链（Blockchain）的本质是一个不依赖第三方、通过自身分布式节点进行数据存储、验证、传递和交流的网络技术方案，正如一个开放的去中心化的分布式记账本，任何人在任何时候都可以采用相同的技术标准生成信息、延伸区块链。当然，大家要想对区块链有深入了解，必须先要知道区块链的起源。

practice

## 1.1
# 区块链的发源——比特币

说到区块链，就不得不提比特币（BitCoin）。比特币诞生于 2008 年，这时还没有人关注区块链。直到 2013 年人们才意识到比特币在没有任何中心化机构运营和管理的情况下，依然稳定地运行了将近 10 年，并且没有出现任何问题。于是，很多人开始注意到比特币的底层技术，即区块链。本节主要介绍区块链与比特币的关系。

### 1.1.1 数字货币的龙头老大——比特币

数字货币包括数字金币和密码货币，这里只讨论密码货币的范畴。密码货币是一种依靠密码技术和教研技术来创建、分发和维持的数字货币，包括比特币、莱特币、维卡币等。其中，比特币是密码货币之首。

事实上，密码货币的历史很悠久，下面来回顾一下密码货币的发展历史。

1982 年，大卫 • 乔姆（David Chaum）最早提出了不可追踪的密码学网络支付系统， 该系统允许一个人发送一串数字到另一个人，而且这个数字可被接收方修改。对加密货币的兴趣以及荷兰历史上对私密性狂热的态度在很大程度上促使大卫 • 乔姆迁移到荷兰。20 世纪 80 年代末期，荷兰成了密码学和数学研究的温床，而大卫 • 乔姆也创立了 DigiCash，并继续构建依托互联网的加密货币的研究。

尽管大卫 • 乔姆的研究引起了媒体前所未有的关注，但最后不幸的是，大卫 • 乔姆和他的公司出现了一些失误，违反了荷兰中央银行的规定。而大卫 • 乔姆作为妥协，不得不同意公司研发的产品卖给银行。这个调整，给 DigiCash 公

司带来一个好的预期——试图通过多家银行来创立一个可行的数字现金领域，但最终在 1998 年破产。

在 DigiCash 引起巨大轰动之后，越来越多的创业者试图在这个领域开创一番成就。1998 年，Wei Dai 发表文章称产生了一种匿名的、分布式的电子现金系统，命名为“b-money”。同一时期内，尼克·萨博（Nick Szabo）也发明了“Bit gold”。Bit gold 与比特币的机制非常相似，用户利用竞争解决“工作量证明问题”，然后通过加密算法将解答的结果串联在一起公开发布，从而构成了一个产权认证系统。

Bit gold 是人们公认的“比特币的前身”。随后，哈尔·芬尼（Hal Finney）在 Bit gold 的基础上开发了“可重复利用的工作量证明”。

以上发生的种种引领大家来到了 2008 年。2008 年，“bitcoin.org”域名被悄悄地匿名注册成功。同年 10 月 31 日，一个自称“中本聪”（Satoshi Nakamoto）的人在密码学网站上发表了名为《比特币：一种点对点的电子货币系统》的论文。10 天之后，开源社区 sourceforge.net 上出现了一个叫 bitcoin 的项目。而世界上首批 50 个比特币诞生于 2009 年年初。

中本聪在搭建完比特币体系后似乎就从互联网上彻底消失了，没有人见过他的真正面目。此后，比特币项目由两个前谷歌工程师维护，但即便是这两个人也声称从未见过中本聪。

2010 年，bitcointalk 论坛上用户之间的自发交易产生了比特币的第一个公允汇率。该交易是一名程序员用 10 000 个比特币购买了一个比萨饼。2011 年，维基解密、自由网、Singularity Institute、互联网档案馆、自由软件基金会以及另外一些组织都开始接受比特币的捐赠。2012 年 10 月，全球比特币付款服务提供商 BitPay 发布报告显示，超过 1 000 家商户通过他们的支付系统来接受比特币的付款。

2012 年 11 月，WordPress 博客平台宣布接受比特币付款，还声称比特币可以帮助肯尼亚、海地和古巴等遭受国际支付系统封锁地区的互联网用户购买服务。2013 年 4 月，海盗湾中文网、EZTV 美剧片源网开始接受比特币捐款。同月，中国四川省遭遇雅安地震，公募基金壹基金宣布接受比特币作为地震捐款。

……

截至 2017 年，比特币已经在全球范围内流行开来。随后，在比特币的带领下，各种密码货币都纷纷崭露头角，走入人们的生活。

### 1.1.2 从“币”到“链”的颠覆

比特币自诞生之后就陆陆续续吸引了世界各个国家的注意。有了比特币之后，只要有网络就可以完成 P2P（个人对个人）交易，不需要借助银行或者其他第三方中介平台。对于投资人来说，比特币就像黄金一样无惧通货膨胀，具有投资价值。

在比特币快速发展的这几年里，与比特币有关的信息一直是人们关注的焦点。比如，比特币价格的涨跌、某快餐店开始接受比特币支付、恐怖分子使用比特币交易、哪个国家政府承认比特币的合法地位，哪个国家反对比特币等。

之后，比特币的发展让其底层技术——区块链——受到了前所未有的关注。人们这才意识到，原来驱动比特币的真正有价值的核心技术是区块链。如果说，比特币对金融秩序的颠覆意义还不够，那么区块链则完全有可能颠覆这个世界。

Chain 公司开发了一个以区块链技术为基础的资产交易平台，该平台可以用于市场上任意类型的资产交易，比如货币交易、股票交易、债券交易等；Counterparty、NXT 和 BitShares 基于区块链技术打造的去中心化交易所可以在脱离传统股票交易所的情况下完成股票发行和交易；Guardtime 正在研究基于区块链技术的工业级网络安全方面的应用；Holbertson 利用区块链技术验证学生的学历，防止学生有学历欺诈行为；Visa 和 DocuSign 致力于通过区块链技术构建汽车租赁市场新商业模式……

未来，如果这些区块链应用全部成为现实并且普遍运用，那么区块链一定会颠覆我们的世界。到时候，如果美国还想试图通过金融封锁的手段制裁一个国家，那么其难度之大可以想象。

区块链之所以具有颠覆意义，是因为它具有以下四个特征，如图 1-1 所示。

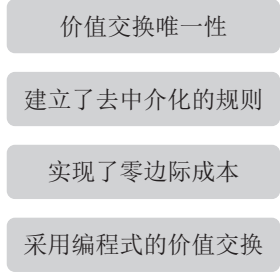


图 1-1　区块链的四大特征

第一个特征是价值交换唯一性。价值交换唯一性解决了互联网 P2P 价值交换时出现的信息传递问题。我们在网上发邮件，发给一个人与发给 100 个人，不会出现明显的成本增加。而通过互联网付款时，我们就只能付给一个人。可见，信息可以无限地复制，但价值交换却需要保持其唯一性。而区块链就能保证价值交换的唯一性。

第二个特征是建立了去中介化的规则。这一规则使得互联网在价值交换中实现了去中介化，在没有第三方平台做担保的情况下，即可用双方都信任的算法保证交易。

第三个特征是实现了零边际成本。因为没有第三方参与，只是通过一个算法使双方建立信任关系，所以这里交易的成本就特别低，基本可以实现交易零成本。

第四个特征是采用编程式的价值交换。假如我们通过基金会做一次捐款，用途是修建学校，那么就可以用区块链数字货币去支付这笔钱。即在区块链上写一个小小的程序，把学校的账户写上去，一起寄给基金会。如果基金会不往指定的学校账户支付这笔钱，那这笔钱基金会永远得不到，也汇不出去。在这里，我们支付的不只是钱，还有一段代码。

以比特币为首的所有基于区块链技术的密码货币都只是区块链技术的第一个重量级应用而已。以区块链技术为基础，已经有越来越多的应用出现在我们的视野里，而它们正在颠覆我们的世界。大家不妨跟笔者一起静待区块链时代的到来。

### 1.1.3　区块链与比特币没有极客说得那么复杂

关于比特币，有种非常夸张的说法是“人类已知金钱的终结”。事实上，很多人对比特币的认知还处于云里雾里的状态。普华永道事务所的消费者调查数据显示，对于比特币熟悉或者非常熟悉的人只有 6%，而 83% 的被调查者表示他们对比特币非常陌生。

与此形成对照的是，“比特币”这一名词的搜索量非常高。以百度指数为例，2017 年 1 月 5 日，“比特币”的用户搜索量达到 80 274 这一峰值。进入 2017 年以来，“比特币”的搜索指数变化曲线如图 1-2 所示。

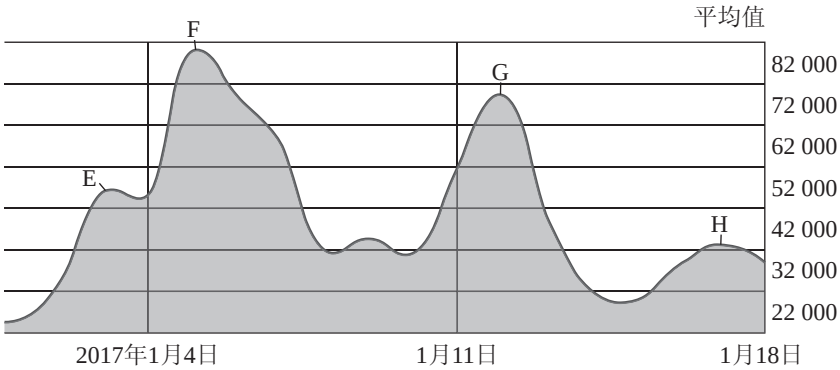


图 1-2 “比特币”的搜索指数变化曲线

那么，比特币到底是什么呢？比特币的本质是一种货币，如果你手上有比特币，就可以按照各外汇市场的汇率用比特币购买商品。也就是说，这和我们用人民币网购以美元标价的产品是一样的。

既然比特币这样简单，为什么大家还是对比特币感到茫然呢？这是因为大部分非技术出身的人认为比特币背后的底层技术区块链是极其复杂的。所以，解释区块链的运作原理是推广比特币的重点和难点。在此之前，几乎没有人会在意银行是如何处理一笔交易的，人们关心的只是账户中的具体交易记录。但是，比特币作为一种未被广泛接受的新事物就必须把一切解释清楚。

众所周知，一本账本必须具有唯一确定性的内容，否则就会有真假之分，从而失去参考意义。所以，记账天然成为一种中心化行为。在技术落后，通信联系不发达的时代，这是必然的选择。在如今的信息时代，中心化的记账方式依然覆盖了社会生活的方方面面。然而，中心化的记账却有一些软肋：一旦这个中心出现问题，如被篡改或者被损坏，整个系统就会面临危机乃至崩溃。另外，整个货币体系作为一个账本系统，也会面临中心控制者滥发导致通货膨胀的风险。

所以说，中心化的记账方式考验中心控制者的能力、参与者对中心者的信任度以及相应的监管法律和手段。那么，有没有可能建立一个不依赖中心以及第三方，但是却可靠的记账系统呢？

区块链解决了这一难题。在互联网信息时代，计算机负责记账，而在记账系统中接入的每一台计算机都是一个“节点”。区块链就是以每个节点的算力

（计算能力）来竞争记账权的一种机制。

在区块链系统中，算力竞赛每十分钟进行一次，每次竞赛的胜利者可获得一次记账的权力，即向区块链这个总账本写入一个新区块的权力。这就导致在一段时间内只有竞争的胜利者才能完成一轮记账，并向其他节点同步增加新的账本信息、产生新的区块。算力竞赛就像购买彩票一样，算力越高就相当于购买的彩票越多，中奖概率越大。

那么，算力竞赛是如何进行的，判定竞赛结果的又是谁呢？区块链的“工作量证明”在这一过程中发挥着重要作用。正如我们早上离开时让保姆打扫房间，晚上回来发现房间一尘不染，尽管我们没有看见保姆工作的过程，但可以确定这些工作已经完成。这就是工作量证明的简单理解，即利用一个人人都能够验证的特定结果确认竞赛参与者完成了相应的工作量。

当然，赢得算力竞赛是有奖励的，即获得比特币。如果没有比特币，节点就没有进行竞争的动力。算力竞赛的奖励也是比特币发行的过程。这种设计是相当精巧的，它将货币的发行与竞争记账机制完美结合到一起，在引入竞争的同时也解决了去中心化货币系统中发行的难题。圈内人士将参与算力竞争试图获得比特币的行为称为“挖矿”。

作为一个记账系统，区块链不仅可以记录以比特币为首的密码货币，还可以记录所有能用数字定义的其他任何资产。

如果你还不明白比特币与你有何关系，那么你只需要知道比特币是另外一种形式的钱就行了。

### 1.1.4　给你一台计算机，你也可以创造比特币

比特币如此神奇，很多人都想知道除了直接用钱购买之外，还有没有其他方法可以获得比特币？答案是肯定的。比特币存在于互联网数字空间中，隐藏在特定算法里，所以只要利用联网的计算机就能挖掘出来。大家口中所说的“挖矿”就是通过计算机设备运算挖掘比特币，那些专门通过“挖矿”寻找比特币的人就是比特币矿工。

从表面上看，“挖矿”是一个非常简单的过程，只需要利用计算机下载比

特币挖矿工具，然后让设备持续运行就能得到比特币，然后确定账户信息取得对比特币的拥有权。但是，比特币在设计之初已经制定好了规则，产生新比特币的算法难度会随着比特币产生速度的变化而变化。也就是说，矿工挖掘比特币的速度越快，算法难度就会越大；反之，难度越小。

根据比特币挖矿原理可知，计算机的运算能力是挖掘比特币的关键。对于大多数矿工来说，只要打开挖矿客户端，然后挂机就可以坐等比特币的产生。目前，常用的“挖矿”工具有 Ufasoft Coin、Guiminer 等。由于越来越多的人涌入“挖矿”行列中，比特币的产生也随着算力的增大而变得缓慢。下面是影响挖矿收益的四大因素，内容如图 1-3 所示。

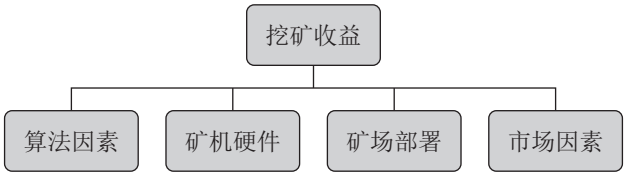


图 1-3　影响挖矿收益的四大因素

### 1. 算法因素

算法因素是比特币本身的特性，不会受到外部因素影响，但是会影响外部因素，包括算法难度调整周期、每区块收益等。

### 2. 矿机硬件

矿机硬件是矿工可以通过人力施加影响，从而提高收益的一个因素。一般来说，硬件因素在短期内几乎没有什么变化，而且可预见性、可操作性较高。例如，矿机速度、功耗、成本等，这些因素主要受上游芯片厂商、矿机组装厂商的影响。

### 3. 矿场部署

矿场指的是比特币矿工团队集体工作的环境。矿场部署是矿场和旷工可以通过人力施加影响，从而提高收益的另一个因素，同样受到上游芯片厂商、矿

机组装厂商的影响，可预见性较高。矿场部署因素包括矿机部署时间、矿场电费、运行保障能力等。

#### 4. 市场因素

比起其他三大因素，市场因素的可预见性较低，但是对挖矿收益的影响非常大。比如，比特币的价格、全网算力增长率、难度增长率等。比特币的价格在短期内波动较小，但是在中长期内何时会出现暴涨暴跌是难以预测的。全网算力和难度增长率在短期内变化幅度会较大，中长期则是会增长趋势。

在影响挖矿收益的四大因素中，算法因素是比特币自身特性，并制约着其他三种因素；矿机硬件的性能和功耗将随着技术升级不断优化；矿场部署的当前趋势是集中化和规模化，通过总量来降低挖矿成本，提升挖矿收益；市场因素受到宏观大环境影响，风险和机遇同时存在。

## 1.2 疯狂的区块链比特币

如果你还没有听说过“比特疯”这个互联网词汇，你就 OUT 了。“比特疯”寓意为“疯狂的比特币”。作为网络虚拟资产，每一个比特币的诞生、消费记录都记录在区块链上，绝不可能造假。随着比特币的流行，比特币已经可以在大多数国家兑换成为国家法币。数量有限而且具有极强的稀缺性是比特币与其他虚拟货币最大的区别。

### 1.2.1 比特币的发行规律

本章 1.1 节已经说过，比特币是与区块链一起被中本聪创造的。比特币的获得依赖于计算机程序计算。如果你有一台配置良好的计算机，并且对计算机程序略知一二，那么你就可以下载一个比特币挖掘软件，这样就能在完成特定

数学程序后获得一定数量的比特币。

比特币的发行有两个明显的特征：首先，与人民币、日元、美元不同，比特币没有固定的发行方，而是通过网络节点计算产生的，只要具备了相应条件，任何人都可以参与制造比特币；其次，比特币的发行是限量限速的，这是因为生产比特币的软件算法计算起来非常困难，而且特解方程组所能得到无限个解中的一组有一定的额度限制，这就决定了比特币不会无限量发行。

现存的比特币数量越多，将来挖掘新币的难度也就越大。截至 2016 年 6 月，现存的比特币大约有 1 566 万个。到 2140 年左右，比特币的产量将达到其上限——2 100 万个，如图 1-4 所示。

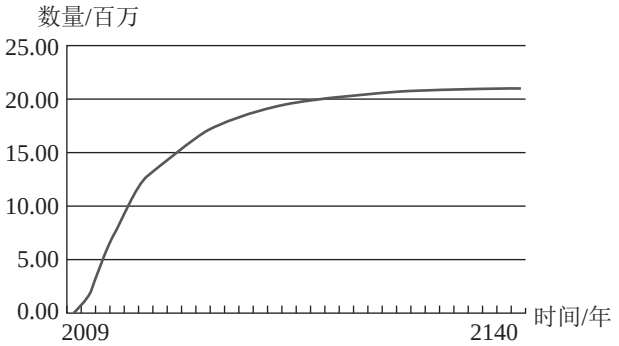


图 1-4　区块链比特币数量变化

生产比特币的算法程序通过四年减半的策略控制比特币的发行速度与发行量。也就是说，在比特币刚诞生的 2009 年 1 月—2012 年 1 月，约有 1 050 万个比特币生成。随后的时间里，每四年生产数值就会降低 50%。因此，在比特币诞生的第 5 ～ 9 年，生产量为 525 万个，在第 10 ～ 13 年，生产量为 262.5 万个，并以此类推。这样，比特币的现存总量永远都不会超过 2 100 万个，而到 2140 年的时候，新的比特币几乎就很难找到了。

### 1.2.2　比特币历史价格变化曲线

试图依靠比特币致富的投资者大有人在，有成功的投资者说：“现在的一枚比特币是一部苹果手机，以后将会成为一栋房子。”据了解，中国是比特币

投资交易最活跃的国家，其次是美国和日本。如图 1-5 所示的是 2009—2016 年比特币在中国日交易量的增长情况。

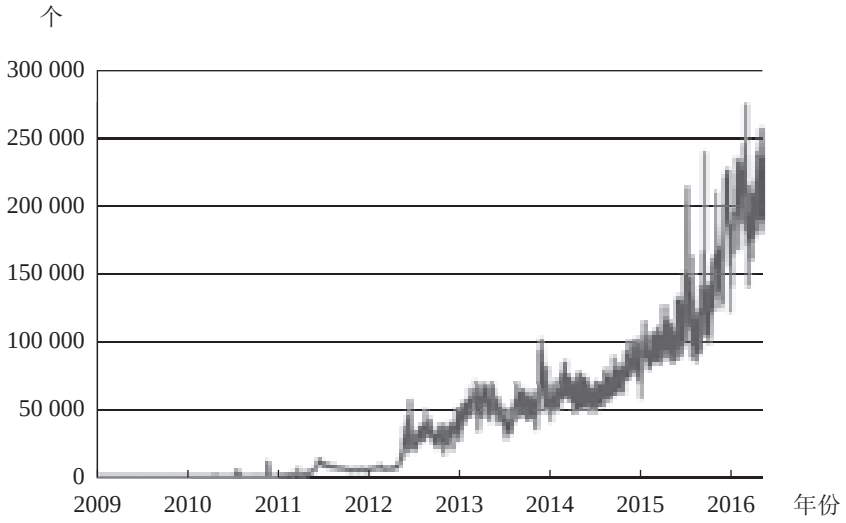


图 1-5　2009—2016 年比特币在中国日交易量的增长情况

在比特币诞生之初，很少有人知道比特币，而且比特币当时没有什么价值。2010 年 5 月 21 日，第一次比特币交易，佛罗里达程序员拉斯洛•豪涅茨（Laszlo Hanyecz） 用 1 万比特币购买了价值 25 美元的比萨优惠券。

自 2013 年塞浦路斯发生金融危机后，比特币的价格开始发生巨大变化。某些欧洲国家的法币大幅贬值，而比特币却突然一路高涨，掀起了炒作热潮并带动了整个数字货币行业的掘金狂潮。由于比特币涨价速度过快，拉斯洛 • 豪涅茨感叹说：“比萨真的很好吃，就是价格有些高。”

2013 年 11 月，比特币攻破 1 000 美元大关，最高时达到 1 200 美元，并一度接近一盎司黄金的价格，综合涨幅超过一万倍，造就了人类历史最大的投资传奇。2014 年之后，比特币市场开始冷静下来，比特币的价值持续降低。

2016 年以来，关于以比特币为代表的数字货币，各国纷纷采取行动。2016 年 1 月 20 日，央行数字货币研讨会在北京召开，并明确表示，央行将争取早日发行央行数字币。与此同时，日本国会也批准有关加密数字货币的新法案，将数字货币视为一种具有货币功能的合法支付形式。另外，作为全球金融

中心之一的英国也宣布发布数字货币 RSCoin 并进行测试。

全球经济大国对去中心化新金融生态的思考，暗含了当前的投资趋势与即将兴起的投资热点。随着各个国家和金融机构相继公布对数字货币的研究进度和相关政策，比特币利好频传，又开始走出一幅波澜壮阔的上涨行情，数字货币也掀起新一轮的投资热潮。截至 2016 年 6 月底，比特币价格维持在 750 美元元附近，如图 1-6 所示的是 2009—2016 年比特币对美元的历史价格变化曲线。

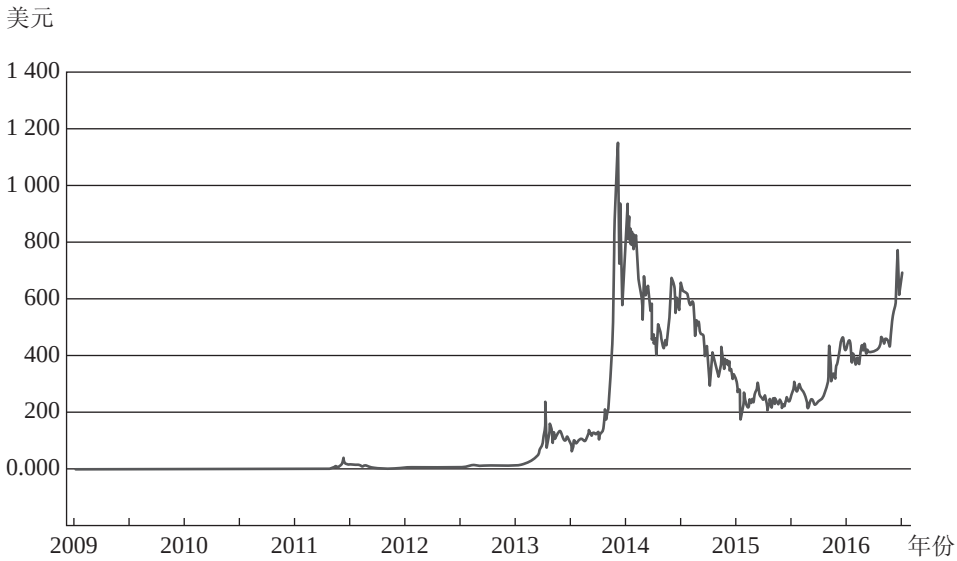


图 1-6　比特币对美元的历史价格变化曲线

看到这里，你是否会感慨比特币的爆发力？

### 1.2.3　价格一个月涨六成，你见过吗?

2016 年 5 月 18 日—6 月 16 日，这是继 2013 年之后，比特币价格迎来第二个“大牛市”。仅仅一个月的时间，比特币的价格暴涨 61.6%。

根据比特币图表网站（bitcoincharts.com）收集的数据，比特币的交易价格从 452.92 美元飙升至 731.89 美元，交易量从 2 608.23 美元上涨到 6 745 美元，交易总价值从 1 184 326.53 美元上涨到 4 860 262.08 美元。

根据比特币当前的市场价格计算，市场上现存的 1 566 万个比特币的市场

规模约为 109.65 亿美元，约合 731.23 亿人民币。

根据比特币的发行规律，从 2016 年开始，比特币又将迎来下一个产量减半时期，这就是比特币价格暴涨的原因。根据比特币开源软件协议的规定，每生产 21 万个区块，生产者获得的比特币奖励就会减半。按照当前计算机平均每天开采 154 个区块的算力计算，截至 2016 年 7 月 10 日，现存区块就会达到 42 万个，这也就意味着达到减半的标准。

根据火币网最新用户调查，有 63% 以上的用户已经从股票市场、贵金属交易以及外汇投资转向了比特币；80% 以上的用户在获悉比特币减半这一消息后对接下来的行情表示看好；还有 13% 的用户将持有比特币当作规避风险的重要手段。

随着区块链技术的发展和成熟，比特币将再次刮起新一轮热潮。仅 2016 年第一季度，全球范围内投资在与比特币和区块链相关的创业公司的风投资金就达到 1.6 亿美元的规模。

## 1.3 区块链比特币的价格来自价值，而非投机

投机是股市中的一个概念，即购买的目的是卖。在货币市场中，英镑和日元是投机的典型代表，吸引了大量投机者进行短线操作。与英镑、日元不同，比特币并不是投机品。因为比特币的总量有限，就像黄金一样有保值功能。众所周知，尽管市场中很少使用黄金作为流通货币，但其市值仍然很高，这不只是因为它能够被制成饰品或金属元件，还因为人们更看重黄金的保值功能，因此愿意买入并持有它，比特币的价值原理也是这样。

### 1.3.1 区块链比特币存储于本地

比特币与虚拟货币有很大的不同，虚拟货币存在于互联网服务器上，而比

特币作为一种字符串，存在于计算机、手机或其他本地硬件设备上。下面一起看比特币与虚拟货币的区别。

虚拟货币是指互联网上非真实的货币，例如，腾讯公司的Q币、Q点、盛大的点券、新浪的微币等。虚拟货币包括网站或应用程序发行的专用货币和游戏币两种。

腾讯公司的Q币就属于网站或应用程序发行的专用货币，可以用来购买QQ会员资格、QQ秀等增值服务，使用比较广泛。与Q币类似的由即时通信工具服务商或门户网站发行的用来购买站内服务的货币都属于这一类虚拟货币。

大多数游戏应用程序都有自己专属的游戏币，而且只能在自身的游戏系统里使用。在游戏里，用户靠打倒敌人、完成签到任务或者直接用钱购买等方式积累游戏币，而用游戏币可购买草药和装备。

比特币是互联网上的数字货币，莱特币、福源币等都属于这种类型的货币。数字货币既可以用于互联网金融投资，也可以作为新式货币用于生活中的某些场景。

如果用户拥有一些比特币的使用权，那么通常需要一个比特币钱包去掌管比特币，例如，PC端的Bitcoin-Qt或者手机端的Bitcoin Wallet。在比特币钱包里，用户会获得一个字符串地址和二维码地址，然后通过这个地址与他人进行比特币交易。

另外，比特币是存储于本地的，所以一旦用户丢失了这个文件，就无法通过网络找到它。然而与实体货币不同的是，比特币是可以备份的，所以用户可以在多个地方保存防止文件丢失。除此以外，用户只要对文件加密，就算别人盗取了比特币文件也难以使用它。

### 1.3.2 网络是区块链比特币的操控者

网络是比特币的操控者，而不是第三方平台。尽管很多用户出于信任担忧选择利用第三方交易平台进行比特币交易，但交易平台起到的作用只是保证两个地址顺利完成，而比特币的实际流通是匿名而且被整个系统记录下来的。因

此，每个人都可以在 Bitcoin-Qt 这样的比特币钱包里看到任意一笔交易，但是你只能看到一笔比特币从 A 流向了 B，却不知道 A 和 B 分别是谁。

网络操控比特币交易涉及一个重要问题，即怎样避免发生双重支付？双重支付指的是一个人用同一笔比特币同时与两个人发生了交易。在实物货币世界，由于人们无法复制黄金、纸币，所以很容易避免双重支付问题。但是在数字货币世界里，比特币需要通过一个机制去确保比特币所有者无法同时与一个以上的人产生交易行为。

为了解决这个问题，比特币引入了“时间戳”概念。在比特币区块链系统中，每笔交易在通过某个节点或钱包产生时，都需要其他节点验证，即每一个节点都能获知每一笔交易的发生，而且它们有一个公认的交易序列。只有大部分节点都认同这笔交易是首次出现的时候，交易才能发生。也就是说，每一笔比特币交易都盖上了“时间戳”，防止重复支付问题。如果有人重复支付，那么时间就会产生矛盾，系统会自动识别为非法交易。根据一定的利益规则，矿工受利益驱动负责为每一笔交易盖“时间戳”。

矿工的利益是每 10 分钟全网只能竞争到的唯一的合法记账权的奖励。谁竞争到了，就可以获得一定数量比特币的奖励。同时，全网其他矿工要同步一致它这个记账，然后竞争下一个区块记账权。

以计算资源为代价，区块链通过全网作证重新建立了信用体系。一些网友已经开始讨论下一代微信可能是什么，下一个阿里巴巴可能是谁等。事实上，下一个巨头最有可能就是一个真正去中心化的系统。

在未来，如果区块链系统的全网公证为我们作证明，那么数据都是无法作假的。比如，将来我们公证自己和爱人的夫妻关系，这将会在几分钟之内成为全网公开的事实。如果有人想要篡改你们的关系，除非他拥有整个系统超过 50% 的算力，但这几乎是不可能的。

### 1.3.3　供小于求决定区块链的超高价值

对于在外地工作的人来说，每年春节来临之前都会因为回家的火车票一票难求而苦恼不已。春运被人们戏称为“人类史上最大规模迁徙”。2017 年春

运与往年相比，形势更加严峻。有媒体报道称，2017 年春运有可能成为“史上最难抢票年”。

上述案例表现了一种供小于求的供求关系。当供小于求时，价格上涨，产品的价格是在产品的市场需求和市场供给两种相反力量的相互作用下形成的。产品的均衡价格指的是该产品的市场需求量和市场供给量相等时的价格。与均衡价格水平相对应的供求数量就是均衡数量。

在供给等其他条件不变的情况下，需求变大，均衡价格则上涨，均衡数量同向变动；在需求等其他条件不变的情况下，供给变动分别引起均衡价格的反方向变动和均衡数量的同方向变动。

晶晶是上海一家鲜花店店主，做鲜花生意十几年了。由于情人节临近，大部分鲜花的价格出现了不同程度的上涨。以销量最好的玫瑰花为例，与几天前相比，每扎 20 枝的玫瑰零售价从 150 元涨至 180 ～ 200 元； 每扎 20 枝的康乃馨零售价从 120 元涨至 150 元；百合的价格基本没有变。业内人士分析，情人节前两天，玫瑰花价格上涨还将继续。玫瑰花的均衡价格上涨的原因是其他条件不变，情人节的来临使玫瑰花的市场需求增加。

总而言之，产品的价格与其需求呈正相关，与其供给呈负相关：供给一定，需求增加，则价格上升，需求减少，则价格下降；需求一定，供给增加，则价格下降，供给减少，则价格上升。如果需求和供给同时发生变化，均衡价格和均衡交易量也会发生变化。需求和供给的同时变化，有同方向变化（需求和供给均增加或均减少）和反方向变化（需求增加而供给减少，或需求减少而供给增加）、变动幅度不同 （需求的增减大于或小于供给的增减）等情况。

匹配上述所说的供求关系，因为比特币的供给总量一定，但是人们对比特币的需求在日益增大，所以区块链的价格将会越来越高。

Block chain

第2章

# 区块链——必将颠覆人类世界

大家应当都听说过这种说法，区块链必将颠覆人类世界。现在很多人都很看好区块链的潜力，但是也担心它遭到各国政府捧杀。而且技术创新领域的成功经验也告诉我们，只有消除政府管控、组织和社会等各个方面的障碍，才有可能真正开创区块链革命。如果对区块链占领高地的过程一无所知，就开始区块链创新是不理性的。下面一起看区块链在全球范围内的发展以及各国政府的态度。

practice

## 2.1
# 区块链的春天——各国积极表态

比特币受到众人追捧后，各国政府更加关注的是比特币的底层技术区块链。当各国政府逐渐认识到区块链在各个领域的巨大潜力后，有些政府甚至已经开始了区块链的应用计划。下面先看一下各国政府对区块链的积极表态。

### 2.1.1 中国央行表态支持区块链

2016 年以来，以比特币为代表的数字货币受到各国关注，各国政府纷纷采取行动。2016 年 1 月 20 日，中国央行数字货币研讨会在北京召开，并表示将争取早日发行央行数字币。

中国央行表示，基于区块链技术的数字货币有望实现去中心化结算。而且通过央行的表态可以发现，央行对区块链技术有着客观、深刻的理解，而且肯定了区块链技术比现有的电子货币优势更大。此前，大家担心政府监管部门不会认可区块链，阻碍区块链的推广，此次表态打消了市场疑虑。与此同时，资本市场对区块链的认可度将会进一步提升。

央行前任副行长王永利指出：“数字货币是应用互联网新技术构建全新的货币体系下的货币，这必将对传统的货币发行、货币政策、清算体系、金融体系等产生极其深刻的影响。同时，新的货币体系与传统货币体系、新的金融体系与传统金融体系如何平稳过渡值得关注。”

截至 2017 年 2 月 4 日，中国央行推动的区块链数字票据交易平台已经测试成功。而且央行旗下的数字货币研究所也将在 2017 年上半年正式挂牌成立。这意味着央行将成为全球范围内首个研究数字货币及真实应用的中央银行，并

率先探索了区块链技术在货币发行领域的应用。

那么，央行建立区块链数字票据交易平台对我们的现实生活有什么影响吗？答案是肯定的，大家可以想象一下：不久，过年发红包不再是纸质钞票，而是一串串的数字密码，我们可以通过发送邮件、复制到 U 盘里或者通过手机将红包直接发送给别人。

你或许会问了，这跟用微信、支付宝发红包不一样吗？需要明确的是，数字货币与电子支付方式的感受类似，但是微信、支付宝等电子支付方式交易时所用的钱都是通过银行账户而来，也就是说即便用支付宝、微信交易，我们使用的依然是银行里的钞票。而数字货币本身就是一种具有支付和流通属性的货币，交易时不需要支付宝、微信等第三方中介。

中国央行为什么要开发数字货币？为什么将票据市场作为数字货币的第一个试点应用场景？区块链靠谱吗？如果你心中存在这些疑惑，那么看看央行参事盛松成如何说。

关于中国央行开发数字货币的原因，盛松成称：“区别于已有的电子形式的本位币，安全芯片、移动支付、可信可控云计算、区块链、密码算法等技术是将来数字货币可能涉及的领域。所以，未来的央行数字货币会从多个方面倒逼金融基础设施建设，让我国支付体系进一步完善，支付结算效率进一步提升。更值得一提的是，央行数字货币最后可以构成大数据系统，让经济交易活动的便利性和透明度进一步提高，这将有利于货币政策的有效运行和传导。”

另外，盛松成还总结了央行开发数字货币的四个好处，如图 2-1 所示。

| | |
|---|---|
| 第一 | 有利于减少洗钱、逃税漏税、逃避资本管制等非法行为 |
| 第二 | 所具有的信息优势使货币指标准确性更高 |
| 第三 | 有利于监管当局进行全面监测和金融风险评估 |
| 第四 | 完善了我国货币政策的利率传导 |

图 2-1　央行开发数字货币的四个好处

第一，数字货币有利于监管当局追踪资金流向，减少洗钱、逃税漏税、逃避资本管制等非法行为。盛松成表示：“现有的数字货币技术不仅可以记录每笔交易，还可以追踪资金流向。与私人数字货币截然相反，监管当局可以采取

可控匿名机制，掌握央行数字货币使用情况，补充现有的监测控制体系，从而增强现有制度的有效性。”

第二，数字货币所具有的信息优势使货币指标准确性更高。对此，盛松成解释说：“央行数字货币形成的大数据系统，不仅有利于提升货币流通速度的可测量度，还有利于更好地计算货币总量、分析货币结构，这将进一步丰富货币指标体系并提高其准确性。”

第三，数字货币有利于监管当局进行全面监测和金融风险评估。盛松成称：“央行数字货币被全社会普遍接受并使用后，整体的经济活动的透明度会大幅度提高，监管当局可以根据不同的需要收集不同机构、不同频率的完整、实时、真实的交易账簿，这就可以为货币政策和宏观审慎政策提供庞大的数据基础。”

第四，数字货币技术完善了我国货币政策的利率传导。盛松成表示：“只有被全社会广泛认可的央行数字货币才可以把此优势辐射给不同的金融市场参与者，进而提升不同金融市场间的资金流动性和单个金融市场的市场流动性。这将降低整个金融体系的利率水平，使利率期限结构更平滑，货币政策利率传导机制更顺畅。”

综上所述，中国央行开发数字货币的目的不仅仅是取代纸币现金流通，还是适应形势发展、紧跟时代潮流，保留货币主权的控制力，对货币发行和货币政策产生积极的服务作用。

### 2.1.2 美国政府机构加快布局区块链技术

前美联储主席本·伯南克（Ben Bernanke）曾经表示，比特币以及其他数字货币有可能与现有的在线支付系统一样拥有长期的前途，未来或许可以建立起一个更快的、更安全的以及更有效率的支付系统。另外，本·伯南克也对数字货币表示担忧，认为数字货币有可能带来执法与监管方面的问题。

2013 年 10 月，美国政府关闭了仅使用比特币交易的在线黑市购物网站丝路（Silk Road）。一个月后，美国国土安全和政府事务委员会召开了一次听证会，对捣毁比特币“地下钱庄”丝路一事展开调查。“丝路”事件导致比特币的价格大幅下降，然而美国联邦政府机构（包括美国司法部和财政部等）在对国土

安全和政府事务委员会的致信中称，“比特币在线支付系统所提供的金融服务是合法的”。

美国政府对比特币金融服务的合法表示肯定，表明他们在对待数字货币上的态度由抵制转向了认可与鼓励，这也使比特币价格再创新高。然而在此之前，美国政府一直强调比特币使洗钱以及其他非法活动更加活跃。下面是美国政府 2016 年在区块链领域的布局。

2016 年 4 月，美国国防部先进项目研究局宣布正在研究基于区块链技术的安全信息系统，用于传播加密信息。

2016 年 6 月，美国国土安全部对六家致力于政府区块链应用开发的公司补贴 60 万美元，让企业研究政府的数据分析、连接设备和区块链。

2016 年 7 月 29 日，22 名美国参议员致函美联储要求对区块链进行指导。

2016 年 9 月 12 日，美国众议院通过了一项要求支持区块链技术的无约束力的决议。

2016 年 9 月 14 日，美国众议院议员大卫 • 施卫克特（David Schweikert）提出区块链被视为解决退伍军人事务部管理问题的解决方案。

2016 年 9 月 28 日，美联储主席珍妮特 • 耶伦（Janet Yellen）透露美国央行正在研究区块链技术。

2017 年 1 月 19 日，据火币区块链研究中心编译，区块链成 2017 年度美国联邦贸易委员会金融会议议题。文章称：“近日，美国联邦贸易委员表示，将会在 3 月 9 日举行一次金融科技集会，部分议程将围绕区块链科技及其对于消费者的影响。据周五发布的消息，金融科技论坛（美国商品贸易第三大监管机构）将会就区块链和人工智能为主题展开讨论。该组织在去年连续举办过两场活动，主题集中在众筹和 P2P（点对点）支付。根据美国联邦贸易委员会，该活动将重点关注区块链及人工智能对于消费者的意义，以及两者的影响。”

金融科技论坛在声明中说道：“我们举办这个为期半天的活动目的是聚集行业参与者、消费群、研究人员和政府代表，审视区块链和人工智能在技术发展进步中被应用于为消费者提供服务、潜在利益及消费者保护等方面的意义。”

美国政府机构加快布局区块链将会带动更多国家拥抱区块链，有利于区块链技术在全球范围内的推进和发展。

### 2.1.3 日本视区块链比特币为现金

2014年6月19日消息称，日本执政党自由民主党（以下简称自民党）表示，暂时不对比特币进行监管。其实，2014年2月25日，全球最大比特币交易平台Mt.Gox正式向法院申请破产保护，估计比特币损失约合4.8亿美元。2015年8月，Mt.Gox的CEO（首席执行官）被捕。日本是第一个遭受巨量比特币损失的国家，此后，日本政府开始考虑比特币监管事宜。

2016年2月29日，日本自民党计划提交认可比特币及其他加密货币货币身份的议案。一旦议案顺利通过，比特币将获得合法的货币地位以及更多的数字货币基础建设投资，同时也将受到更严格的监管并纳税。

日本此项议案是2016年以来首个国家对比特币身份的表态。在此之前，已经有多个国家在2015年对比特币的态度发生了变化。2015年9月，美国商品期货交易委员会（CFTC）正式将比特币纳入大宗商品范围内，并对其进行有序监管。随后，众多不合规的比特币交易平台受到了美国监管机构的制裁。另外，包括英国和瑞士在内的欧洲多个国家等都免除了比特币的增值税。俄罗斯央行也在2015年上半年转变了态度，开始商谈比特币的流通和监管。

2016年5月，日本通过了制定比特币等数字货币规则的资金结算修正案，并将数字货币定义为可用作结算的财产，数字货币与现金进行兑换的交易所将启用登记制度。自此，比特币像现金一样在日本境内流行开来。

日本最大比特币交易所Coincheck的业务发展主管Kagayaki Kawabata表示，资金结算法修正案的实施后将使得比特币成为媒体的新宠儿，推动日本的新趋势。如今，人们已经逐渐改变了旧有的观念，不再仅仅将比特币作为投资工具，而是将比特币用于交易。

截至2017年1月初，在日本大概有5 300个商家及网站支持将比特币作为付款方式，其中99%的商家及网站使用Coincheck付款。与此同时，与2016年1月相比，比特币的月交易金额暴涨了89倍。

在过去，比特币被认为是极客的玩具，但现在它的地位正在发生变化，比特币作为数字货币的合法地位已经被认可。这种观念的转变将会促使越来越多的人使用比特币或其他数字货币进行交易，这也是比特币以及其他数字货币交

易量发生显著增长的主要原因。

Kagayaki Kawabata 对比特币的未来也非常乐观，他认为：“比特币交易量飙升的原因很多，并非偶然事件。尤其是许多大型公司和银行开始对电子货币产生极大的兴趣，并开始尝试区块链技术，预期未来几年电子货币将大幅成长。”

### 2.1.4　英国央行成公认最“积极”央行

在全球范围内，对区块链技术最感兴趣的央行非英国央行莫属。英国央行对区块链技术的研究与探索非常积极。2016 年 1 月，英国央行发表题为《分布式账本技术：超越区块链》的报告。

报告指出，英国央行正在探索类似于区块链技术的分布式账本技术，并且对区块链技术在传统金融业中的应用潜力进行了全方位分析。另外，英国央行认为，去中心化账本技术重新定义了政府和公民之间的数据共享，在改变公共和私人服务领域有着巨大潜力。

与此同时，英国央行已经建立起一个技术团队专门研究区块链，其行长马克·卡尼（Mark Carney）在 2015 年 9 月也曾表示，正在考虑发行数字货币的可能性。

关于数字货币的研究和技术开发，英国央行一直都在秘密进行中。至于发行国家级数字货币的结果是好是坏，还需要用事实进一步验证。

2016 年，英国央行正式宣布创造数字货币的计划，并将该数字货币称作“RSCoin”。 RSCoin 与比特币有很多一样的地方，比如，两者都是使用区块链技术来进行管理的。事实上，区块链对所有的数字货币来说都是必不可少的。

尽管 RSCoin 与比特币的特性相似，但是两者也存在一些区别。其中，最关键的区别是英国央行无法控制比特币的发行与供应，而 RSCoin 的货币供应则是在英国央行内部集中化的。这就意味着英国央行将会创造出 RSCoin 的每个组成部分。这种集中化的货币供应方法要求英国央行必须控制区块链的簿记。

英国央行创造 RSCoin 的目的有两个：一是，通过 RSCoin 使交易活动高效进行，降低交易成本，增大能见度；二是，增强市场信心，并由英国央行对其进行监管，从而降低数字货币带来的不良影响。英国央行之所以有可能对这

种货币进行监管，则是由于区块链技术。

英国央行对数字货币充满了信心，英国央行的一份季度公告表明了其所看重的重点问题。公告称：“数字货币的关键创新在于‘分布式总账’，它允许一种支付系统以一种完全分散化的方式进行运作，不需要银行等中间人。”从这一方面来说，数字货币与当前以电子方式来进行记录的传统货币相差不多。

当前，英国央行将推广 RSCoin，让 RSCoin 在更广泛的范围内得到认可作为主要目标。从这一角度来说，区块链技术的支持是非常重要的。区块链由英国央行控制将会增强使用者对 RSCoin 的信任度。另外，对于以比特币为首的数字货币所面临的数量限制来说，RSCoin 是一种可扩展的解决方案。此前的数字货币在发行总量上受到限制，而 RSCoin 可以随着经济的增长而扩大发行量，这就是 RSCoin 的魅力所在。

比起传统货币，数字货币的货币供应量可以马上受到通货问题的影响，而传统货币的反应较慢。

英国央行积极研究区块链技术，开发数字货币的根本原因在于英国央行试图寻求支付系统的创新，并通过占据区块链技术发展的先机夺回国际金融中心的地位。

另外，银行自动清算业务系统作为英国所有银行进行转账的主要方式，在 2014 年 10 月曾经中断服务长达九个小时。英国银行自动清算业务系统发生的若干次故障也推动了英国央行对区块链技术的探索研究。

无论英国央行积极探索区块链技术的原因是什么，英国央行的行为都对区块链技术在全球范围内的发展起到巨大推动作用。事实上，英国央行已经在某种意义上承认了区块链技术对银行生态系统建设的有利作用。与此同时，我们期待英国央行对区块链的研发取得进一步成果。

## 2.2
# 区块链应用的全球进展

在各国政府积极支持的情况下，区块链在全球范围内的发展现状有着非常

良好的氛围，这也使区块链技术越来越被大众所关注。区块链有着非常强大的生命力，正在由外而内地渗透进各行各业。下面一起看区块链应用的全球进展情况。

### 2.2.1　华尔街各顶级投行对区块链趋之若鹜

高盛集团（Goldman Sachs）是华尔街顶级投行之一，总部在美国纽约。作为世界财富 500 强企业之一，高盛集团的业务范围涵盖投资银行、证券交易和财富管理。高盛在中国香港设有分部，并分别在美国、亚太地区和欧洲 23 个国家和地区设有 41 个办事处。

2016 年年初，高盛发布报告表示，区块链技术已经做好准备要颠覆这个世界。此前，高盛已经和中国 IDG 资本联手向区块链创业公司 Circle Internet Financial 投资 5 000 万美元。

2016 年 5 月底，高盛发布《区块链：将理论应用于实践》报告，展示了区块链将在金融服务、共享经济以及房地产领域如何大显身手。

作为比特币的底层技术，区块链对传统技术的突破在于建立了以 P2P 为基础的去中心化新体系。区块链系统的去中心化使整个网络内的自证明功能成为现实，由中心化的第三方机构进行统一的账簿更新和验证已经成为过去。

行业人士称，比特币是区块链技术的第一个应用，比特币良好的发展状态证明区块链通过去中心化和去信任的方式集体维护一个可靠数据库的方式是可行的。很多华尔街投行都对区块链技术表示相当看好，而高盛只是其中之一。

在长达 88 页的《区块链：将理论应用于实践》报告中，高盛开篇称：“关于区块链技术的讨论，在过去一直都是抽象的，关注的焦点也都是市场去中心化以及去第三方中介的机会，现在我们将关注重点从理论转向实践，研究区块链技术在现实世界中的应用场景。”高盛关注的区块链应用有五个，分别是构建信用体系、实现分布式供电网络、降低房地产交易成本、提高股票交易结算和清算效率、用于客户身份核验。

自 2016 年以来，除了高盛以外，华尔街其他顶级投行也纷纷向区块链技术抛出橄榄枝。前摩根大通高管、信用违约互换（CDS）之母布莱斯 • 马斯特

斯（Blythe Masters）加入数字货币公司 Digital Asset Holdings，出任 CEO；包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把砸钱，它们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等顶级投行还向区块链初创公司 Digital Asset 投资 5 000 万美元。

2016 年 1 月，由 10 多家国外大型银行组成的区块链联盟 R3 CEV 对外宣称已经成功实现了区块链技术，在模拟现实（VR）环境下，区块链技术已经初步实现了银行和银行之间的即时交易。未来金融行业的操作标准很有可能就此诞生。区块链联盟 R3 CEV 成员包括花旗银行、富国银行、汇丰银行、瑞士信贷银行等国际著名银行。

华尔街投行们为何对区块链技术趋之若鹜呢？通过数据分析可知，2016 年第一季度，华尔街投行们的 FICC（固定收益证券、货币及商品期货）主营业务收入总额为 178 亿美元，比 2015 第一季度的 248 亿美元下滑了 28.23%。而对比过去五年，这一主营业务的收入总额更是下滑了 49%。

很明显，华尔街投行们正经历着主业萎缩的艰难时刻。主营业务萎缩带来的负面影响就是必须通过大规模裁员以缩减成本。从 2015 年第一季度到 2016 年第一季度，华尔街投行们的 FICC 部门已经从 19 200 人降至 18 300 人，幅度达 5%；在过去 5 年里，FICC 部门总共裁减了 32% 的员工。

在这种情况下，华尔街投行们都试图通过区块链新技术带来的机遇进行自我拯救。

截至 2016 年，高盛、摩根大通、花旗银行、纳斯达克、瑞银集团、桑坦德银行、巴克莱银行、德勤会计师事务所等都成立了区块链实验室，布局这一领域。区块链技术的应用实验已在证券、银行、审计等行业陆续展开。

瑞银集团区块链技术实验室的 PeterStephens 称：“瑞银集团在区块链上已试验了 20 多项金融应用，包括金融交易、支付结算和发行智能债券等。”瑞银的第一个实验是基于区块链技术的智能债券，接下来，瑞银将在积分卡项目推进区块链应用实验。

德勤亚太区投资管理行业合伙人秦谊表示：“区块链技术解决了审计行业历来在满足公众要求、满足监管部门要求方面的难点，能够保证所有财政数据的完整性、永久性和不可更改性，帮助审计师实现实时审计，提高审计效率。”

另外，纳斯达克已经在私人市场启动了区块链技术在股票市场的应用测试。纳斯达克将会利用区块链技术处理私营公司股票交易的大量非正式系统，比如需要律师手动验证电子表格等。

### 2.2.2　区块链技术应用前景无限扩张

看一下下面的生活场景：我们乘坐的飞机航班是通过微信公众号预定的，飞机降落后我们使用滴滴出行叫到一辆专车，10 分钟后我们到达在美团上预订好的酒店房间，这里地理位置非常好，就在明天开会会场的附近……这种方便快捷的商务旅行生活已经成为一种常态，只要使用当今众多的标志性移动应用就可以实现，比如去哪儿、滴滴出行、美团等。在移动互联网时代，这些应用几乎如影随形。

我们想象一下 10 年后的 2027 年，区块链技术改变了我们的生活，我们可以立即找到提供各种服务的供应商，交易过程更加快捷，不需要借助任何第三方平台。

在未来世界里，区块链使用户获取所有服务的渠道都处于同一个网络中，就像邮件一样采用 P2P 的方式，从而省去加入第三方平台的烦冗手续。而且这个网络中的信息交互都是通过分布式运算引擎上运行的加密算法自动完成的，不会受到任何个体或组织的控制。

在这种环境下，区块链将各种移动应用背后的复杂机制转变成了更完美的系统，帮助用户预订飞机票、订车、订酒店，顺便为用户提供几首你喜爱的音乐。

P2P 基金会的核心成员以及都柏林圣三一学院的讲师 Rachel O’Dwyer 表示：“区块链创造了一种可信的数字货币和会计系统使人们不必向美联储这样的集中式媒介求助。”

非营利公共信托组织 XDI.org 的网络主席菲尔·温德利（Phil Windley）认为：“区块链非常复杂，这是因为人们希望通过区块链技术解决的问题也很复杂。回想一下 20 世纪 80 年代的光景，当时的人们如果想要给一些计算机建立局域网的话，面临的互联网协议也是异常复杂的。当然，与区块链相比，那些协议还是更简单一些，但是在当时的技术背景下，那就与区块链一般复杂。”

对于区块链技术应用普及的时代，菲尔·温德利非常期待：“区块链能够让我们把所有事物都纳入系统，而不需要任何一家公司作为中间人。当然，公司不会因此全部消失，但是有了区块链技术的应用以后，用户就可以随意更改提供商，所有的服务都能互用。代码全部都是开源的，没有任何一个特殊的组织可以独占某些资源。有了区块链以后，我们甚至有能力运营自己的服务器。”

关于区块链的发展与应用，普遍的说法是将其划分为区块链1.0、区块链2.0和区块链3.0三个阶段。区块链1.0是指以比特币为代表的数字货币应用时代；区块链2.0是指区块链技术在股份、债权、版权、产权等金融领域的扩展应用；区块链3.0是指区块链应用扩展到金融行业之外的司法、医疗、物流等各个领域，全面覆盖人类社会生活，实现信息共享，而不再依靠第三方获得或建立信用。

目前，我国对区块链技术的应用尚处于探索阶段，还没有真正应用起来。但随着相关资源的投入越来越大，一些新型的区块链技术公司正在快速成长，不断地促进各行各业的快速发展，让区块链技术的应用初露锋芒。

## 2.3 2017年最热门的5家区块链初创公司

在2015年年底，比特币区块链受到了众人的质疑。因此，2016年对比特币来说是至关重要的一年。在比特币没有被广泛认可的情况下，有5家区块链初创公司大力开展比特币业务，开发比特币相关应用程序项目。对比特币的未来发展产生了巨大影响，成为2017年最热门的5家区块链初创公司。

### 2.3.1 “隐形的比特币公司”——Blockstream

Blockstream是由在比特币领域内做出过重要贡献的比特币爱好者成立的，他们试图通过“侧链”机制来扩展比特币区块链的能力，将比特币的区块链技术应用到包括数字货币、开放资产和智能合约在内的其他资产类型。

2014 年 11 月 18 日，Blockstream 正式宣布获得 2 100 万美元的种子轮融资，资金将会用于探索侧链机制上。

Blockstream 官网的公告显示，此轮融资的投资人分别是 LinkedIn 联合创始人雷德·霍夫曼（Reid Hoffman）、曾投资比特币 API 开发者 Chain 的科斯拉风险投资公司、加拿大种子基金 Real Ventures 等共计 40 位投资者。

Blockstream 的 CEO 奥斯汀·希尔（Austin Hill）表示，Blockstream 之所以能够成功融资是因为高新技术产业逐渐认识到比特币区块链的巨大潜力。奥斯汀·希尔称：“Blockstream 是行业内首家致力于扩大比特币协议层功能的公司。也就是说，公司着眼于侧链的扩展机制，使各种创新在一个开放、可互操作的平台上发生。”

在行业里，Blockstream 算得上是资金最充足的创业公司之一，然而 Blockstream 却自称是“隐形的比特币公司”。

有了充足的发展资金后，Blockstream 开始在后台忙碌，并在 2015 年推出了横幅侧链项目的测试版，并公布了首个商业化产品 Liquid。Liquid 的推出将会缩短比特币交易所之间的资金传输时间。

Blockstream 研究开发的另一个项目是闪电网络（ Lightning Network），即分布式小额支付网络。这种去中心化的系统可以将小额的比特币交易从区块链移除，此做法不仅加快了交易的速度，还降低了发生费用。另外，闪电网络依然实现了当前比特币网络无须依赖第三方信任的特性。

闪电网络将会降低比特币区块链的交易承载负担，从而使它们无法影响比特币区块的总大小。然而这一项目正面临着一些挑战，比如整合比特币核心。一旦这些问题得到解决，当前的区块大小争论将得到缓解，并且增强比特币网络的健壮性。

2016 年 2 月 3 日，Blockstream 对外宣布获得 A 轮融资，募集资金总额为 5 500 万美元。亚洲富豪李嘉诚旗下维港投资、全球保险集团安盛旗下的 AXA Strategic Ventures 以及日本科技公司 Digital Garage 领投了此轮融资。其他投资者还包括由雅虎创始人杨致远创办的 AME Cloud Ventures、Blockchain Capital 等公司。加上 2014 年的 2 100 万美元种子资金，Blockstream 通过两轮融资中共获得 7 600 万美元的资金。

Blockstream 为什么能受到投资人青睐呢？下面一起看投资人是如何看待 Blockstream 的。

领投方维港投资的公司代表 Fraces Kang 认为：“区块链技术重新定义了金融科技内外的生态系统，释放出无限可能。此次投资 Blockstream 意味着我们将会亲眼见证创新的侧链技术诞生，对此，我们感到非常兴奋。”

AXA Strategic Ventures 管理合伙人 Francois Robinet 则说：“区块链技术不但为金融服务带来变革，也会颠覆其他行业。Blockstream 拥有业内最优秀的技术团队，其开放原始码的做法以及所掌握的侧链技术是我们看重的价值所在。这将会使不同区块链之间进行相互操作，提供关键的长期成效，未来有可能会为保险及资产管理业务带来突破。”

AXA Strategic Ventures 的合作伙伴 Manish Agarwal 认为，公共区块链的商业化是未来大势。Manish Agarwal 表示：“我们相信区块链技术具有重塑金融服务环境的巨大潜力，而公共区块链是最关键的部分。我们对比特币这种数字货币感兴趣，而技术是其关键。”

日本科技公司 Digital Garage 的首席传媒官 Rocky Eda 称：“Linux 系统占据了操作系统的半壁江山，我认为区块链也会故事重演，开源社区将会经过多次测试。”

Rocky Eda 还指出：“日本公司经常把侧链技术用在发展奖励点设计或智能合约之类的应用。侧链是区块链技术的应用开发中最好的解决方案，而私有区块链则显得专有而封闭。”

Manish Agarwal 进一步指出：“侧链的价值地位与比特币区块链的本意较为接近，这种特性更能吸引关注区块链技术的投资公司。我相信这种技术中的价值在于它无须信任的特性，我认为开源证明是其中的关键。”

奥斯汀 • 希尔也赞同上述观点，他在一篇博客中写道：“这一轮的融资会为 Blockstream 提供资源，继续打造一个开源的结构，这种结构可能会为全球动态信任打下基础。”

结合当前大部分区块链公司都主张抛弃比特币区块链另起炉灶的形势，Blockstream 此次拿到 5 500 万美元的 A 轮融资令比特币技术开发者看到了希望。当前的区块链技术发展还处于探索阶段，面临着各种技术路线的选择。Blockstream 代表着通过比特币区块链以及其侧链来突破限制，实现更多功能。

总体来说，比特币区块链依然是当前最为安全的区块链，而通过开发侧链可以增强平台的开放性，有利于发掘比特币区块链的更大潜力。

### 2.3.2　在线零售巨头Overstock创造的区块链交易平台——TØ

2015 年 8 月，美国在线零售商 Overstock 的 CEO 帕特里克·伯恩（Patrick Byrne）在美国纳斯达克纽约总部揭露了神秘的区块链交易平台项目 TØ。据悉，Overstock 在 2014 年首次公布了基于区块链的私有和公有股权交易平台。

帕特里克·伯恩解释了的 TØ 的新目标：“我们建立 TØ 平台，在上面交易就是结算，这是一个具有颠覆性的事情。另外，账目的交易和结算也是一体的，它不需要成为各自独立的进程。”

2016 年 4 月， TØ 首次尝试利用区块链技术开启线上股票交易模式。在 Overstock 使用区块链发行私有债券后，TØ 得到美国证券交易委员会（SEC）的批准，发行了公共债券。

下面一起看看票据清算模式的发展史。在纳斯达克证券交易所还没有成立之前，人们为了完成票据的清算，只能骑着自行车，驮着装满债券的包在华尔街上来回奔波。20 世纪 60 年代，美国资本市场经过大规模爆发性增长后迎来了一场危机，骑自行车清算票据的办法已经不能满足当时的市场需求。为了让清算速度赶上交易量，华尔街曾经每周只交易四天，而且每天只有 4 个小时。

1971 年，美国证券交易委员会（sec）召开会议商议如何通过计算机解决票据清算问题。最后，他们讨论出两个方向：一是建立中央对手方 （central counterparty） 的清算模式，即有一个清算中心，所有交易都要从这里经过，从清算中心系统内展开，经纪人全部要接入这个系统；二是在经纪人之间建立点对点的清算模式，纳斯达克证券交易所的成立就是在这一背景下。

对此，帕特里克·拜恩 （patrick byrne） 解释说：“第一个解决方向就好像用计算机来安排调度骑自行车的人一样，虽然使用了计算机，但是仍旧没有解决根本问题。”而第二个解决方向被美国证券交易委员会极力推崇，也成为华尔街直到现在依然采用的模式。

帕特里克·拜恩指出：“真正的清算模式应该将交易和清算两个步骤合二

为一同时完成，而不是现在的净额清算 （net settlement）。尽管一些金融巨头和硅谷科技公司都在开发应用于市场交易的区块链技术，但是要清楚他们在做什么，只需要问一个问题：清算方式是怎样的？如果他们做的仍旧是净额清算，那么他们就是‘在给骑自行车的人打工’。”

一旦真正的区块链去中心化清算模式取代了现在的中心化清算模式，华尔街某些赚钱的不法勾当将难以进行下去。比如“无货沽空”（naked short selling，也叫“裸卖空”），也就是说在交易市场上出售或者声称出售实际并不持有的资产，以实现在未来以较低的价格买入等额资产的目的。

无货沽空对市场交易有着巨大影响，比如德国曾经在 2010 年宣布暂时禁止对 10 家德国银行和保险公司的股票进行无货沽空，从而导致股市大跌。另外，股票借贷（stock loan）、提前交易（front-running）等最赚钱的生意都不再可能。

如果区块链使票据清算模式实现了真正去中心化，那么华尔街将不仅会失去“信息不对称”为其带来的优势，也会失去相应的赚钱能力。可以想象，一旦真正去中心化的清算模式在全球交易市场大规模推广，那些依靠华尔街生存的人就不得不另谋出路。

作为比特币区块链在金融票据领域的应用，TØ 平台将会打破多少传统金融服务，只有时间才能给我们答案，大家拭目以待。

### 2.3.3 比特币消费类应用程序——OpenBazaar

OpenBazzar 是一个运用比特币作技术支撑的比特币消费类应用程序。就像是去中心化的 eBay（线上拍卖及购物网站），OpenBazaar 利用应用程序市场将买家和卖家联系起来，同时用比特币作为交易媒介替代 PayPal 和信用卡。2016 年年底，OpenBazzar 继获得 100 万美元种子资金后，又获得 300 万美元的 A 轮融资。

OpenBazaar 的诞生加速了比特币向分散市场的发展。一旦该应用取得成功，OpenBazaar 将会因为大幅降低各方费用而成为 eBay 的开源竞争对手。

当前的环境下，电子商务离不开中心化服务。以亚马逊、eBay 和其他电商巨头为例，它们对平台上的卖家实施严格监管，并通过收取一定费用盈利。

而且这些公司只接受信用卡和 PayPal 等类似的支付方式，这些支付方式对买家和卖家都收取一定比例的手续费。

另外，这些公司将会获得用户的个人信息。用户面临着信息被盗取或者被卖给他人的风险。在交易过程中，政府和电商公司负责审查所有的交易商品和服务，因此买家和卖家无法做到自由交易。

OpenBazaa 为电子商务带来了另外一种途径，一种让用户掌握权力的途径。OpenBazaar 消除了中心化第三方的角色，将卖家和买家直接联系在一起。由于交易中没有第三方，所以双方都无须支付交易费用。在交易过程中，没有第三方监管，用户可以自主决定是否公开个人信息。

比如，用户 A 想要将使用一年的 iPad5 出售。他首先需要下载 OpenBazaar 客户端，然后在计算机上创建一个产品目录，并标明 iPad5 产品的细节。当用户 A 公布 iPad5 产品的目录后，该目录被发送到 OpenBazaar 的分布式 P2P 网络上。当用户 B 搜索的关键词符合用户 A 设置的“电子产品”“iPad”等关键词时，用户 B 就可以发现用户 A 的商品目录。如果用户 B 不同意用户 A 的报价，可以提出新的报价。

如果两人都同意价格，OpenBazaar 客户端就会使用用户 A 和用户 B 的数字签名为两人创建一个合约，然后将这一合约发送给第三方公证人。如果用户 A 和用户 B 在交易中发生纠纷，公证人就会介入交易。这些公证人和仲裁者与用户 A 和用户 B 一样都是 OpenBazaar 用户。他们既可能是用户 A 的邻居，也可能是用户 B 的朋友，还有可能只是一个陌生人。第三方公证人需要为合约做证，并创建多重签名比特币账户。一旦集齐三个签名中的两个，比特币就会被发送给用户 A。

在这一过程中，用户 B 发送与用户 A 商量好数量的比特币到多重签名地址。用户 A 得到即时通知，确定用户 B 已经发送货款后，就会发出出售的 iPad5，并告诉用户 B 已经发货。几天后，用户 B 收到 iPad5，就会告诉用户 A 已经收到产品，并从多重签名地址释放货款。用户 A 获得了比特币，用户 B 买到了想要的 iPad5，双方都无须支付交易费用，也没有第三方监管交易，用户 A 和用户 B 都得到了想要的结果。

交易中发生纠纷怎么解决呢？与任何网购一样，OpenBazaar 上的交易并

不能保证顺利进行。比如，卖家发错货、没有发货或者产品质量不如预期的好，那该怎么办呢？这时，第三方公证人会介入。只有集齐三把私钥中的两把，才能从多重签名地址中取走货款。而第三方公证人掌握着第三把私钥，所以只要买卖双方没有达成和解或者在第三方公证人判定一方正确之前，多重签名地址中的货款就无法被移动。

那么，如何保证用户对第三方公证人的信任呢？OpenBazaar 设置有一个信誉评分系统，全部用户都有权利对其他用户进行反馈评分。如果一些用户试图交易欺诈，他们的信誉将会受损。如果第三方公证人裁定交易纠纷不够公正，其信誉也会受损。

当用户在 OpenBazaar 平台上购买商品以及选择第三方公证人时，可以通过对方的信誉评分判断他们是否值得信任。当然，OpenBazaar 客户端会通过技术保证评分是合理的，有效防止作弊。具体的步骤非常复杂，但是 OpenBazaar 会处理好这些细节问题。

2016 年 4 月，OpenBazaar 平台正式上线营业，发布了首个完整版本软件并提供下载服务。尽管第一个版本的功能不够丰富，但是该项目充分完成了 18 个月的初期发展，这使数字货币领域为之振奋。

随着完整版本的上线， OpenBazaar 项目负责人表示：“交易本该是免费的。这个想法启发了我们，于是我们花费了两年时间来建设 OpenBazaar 这个平台。从今天开始，世界上任何人，只要能访问互联网，就能使用比特币和 OpenBazaar 来免费交易商品和服务。我们已经迫不及待地想看看大家会如何使用这个工具了。”

### 2.3.4 搭载比特币的社会化媒体平台——Zapchain

Zapchain 是一个搭载比特币的社会化媒体平台，也是备受期待的区块链初创公司之一。Zapchain 做的是整合链上（ on-chain）的比特币微打赏方式，通过革命性的创意促使用户参与高品质的内容创作。

Zapchain 面临的最大挑战在于是否具有可持续发展的能力以及如何避免垃圾用户。据当前的 Zapchain 来说，其避免垃圾用户，遏制垃圾内容的行为已

经出现成效，而且 Zapchain 的用户增长说明其流行度越来越高。

2015 年 11 月 7 日，ZapChain 对外宣布获得 35 万美元的天使轮融资，并公布了与比特币公司（Coinbase）的合作关系，同时推出一个新的数字商品计划。

此轮融资的投资者包括德丰杰（Draper Fisher Jurvetson）合伙人蒂姆·德雷珀（Tim Draper）、Boost VC 创始人兼 CEO 亚当·德雷珀（Adam Draper）以及 Boost 比特币基金。

ZapChain 的首席运营官 Dan Cawrey 表示，这笔资金将被用于平台推广，扩大内容创建者和数字社区成员的范围。

对于投资 ZapChain 的原因，蒂姆·德雷珀解释说：“我投资 ZapChain 是因为该公司是最好的比特币应用之一。ZapChain 使得区块链被用于小额支付，为记者和其他媒体人员带来便利，减少与银行之间的摩擦。”

亚当·德雷珀（Adam Draper）也非常看好 ZapChain，他描绘了 ZapChain 内容货币化愿景背后的大画面。亚当·德雷珀是这样说的：“微交易很可能是网络内容创作者赚钱的新方式，它可能会改变游戏规则。”

与比特币公司展开合作后，用户可以通过 ZapChain 购买和销售比特币，促进 ZapChain 的数字商品销售。音乐家 Talib Kweli 便尝试了利用 ZapChain 销售他的最新专辑《Indie 500》及单曲。

Talib Kweli 在声明中表示：“比特币背后的技术将会帮助人们更容易地获取音乐，并且为音乐家们打开新的市场。”Talib Kweli 还说：“做喜欢的音乐并把它带到喜欢它的人面前是一件非常好的事情，不管你在哪里或者你是谁。”

ZapChain 还推出了新的数字社区创新工具微打赏，进一步尝试内容货币化实验。现在，你会发现 ZapChain 平台上的提问和评论旁有一个绿色的“打赏按钮”。如果你觉得某个用户提出的问题或者提供的答案很好，你就可以通过点击此按钮，向其打赏相应数量的比特币，比如价值一个苹果、一杯咖啡、一个比萨饼的比特币。打赏的数额都是平台预先设定好的，用户可以选择但不可以自由设置。

ZapChain 表示，他们并不追求通过该工具获得盈利，他们只希望将该产品推广至其他平台。在 Zapchain 的努力下，Zapchain 终将成为公认的顶级比

特币媒体平台。

### 2.3.5 资金最充裕的比特币挖矿公司——BitFury

2011 年，瓦列里 • 瓦维洛夫（Valery Vavilov）和瓦列里 • 讷班斯尼（Valery Nebesny）共同创建了 BitFury 比特币挖矿公司。由于比特币挖矿的利润不断下降，BitFury 已经将核心角色转变为行业的交易处理器。BitFury 网站上称：“整个比特币生态系统都是我们的客户。”

BitFury 堪称资金最充裕的比特币挖矿公司。2014 年 5 月 30 日，Bitfury 正式宣布他们获得 2 000 万美元融资。该融资也是比特币领域最大的融资之一。参与此轮融资的投资者包括 Binary Financial、Crypto Currency Partners、Georgian Co-Investment Fund （GCF）、Queensbridge Venture Partners 和 ZAD 投资公司。

BitFury 的创始人兼 CEO 瓦列里 • 瓦维洛夫说：“这一轮融资的成功表明我们的战略是正确的，让我们有机会向目标迈进——成为世界上第一家公开上市的比特币公司。投资将会大大加速我们的成长，会进一步巩固我们的产品和服务在行业内的领先地位。”

2014 年 10 月 10 日，BitFury 宣布获得新一轮融资，融资金额为 2 000 万美元。此轮融资距离上一轮融资还不到五个月。

2015 年 7 月 10 日，BitFury 宣布完成第三轮 2 000 万美元融资。至此，BitFury 的融资总额达到 6 000 万美元，是竞争对手 KnCMiner 2 900 万美元融资总额的两倍，并占据比特币挖矿行业 1.165 亿美元投资总额的一半以上。

在拿到第三轮融资后，瓦列里 • 瓦维洛夫（Valery Vavilov）表示：“新一轮融资的成功，证明了我们的业务战略，并且令我们更接近我们的宏伟目标。”

第三轮融资的投资方包括格鲁吉亚联合投资基金（The Georgian Co-Investment Fund）、DRW Venture Capital 以及 iTech Capital 等。

DRW Venture Capital 的创始人唐 • 威尔逊（Don Wilson）对 BitFury 表示了赞赏，他说：“我们投资 BitFury，是因为瓦列里 • 瓦维洛夫的工作令人印象深刻，而且，他们的团队已经成为确保区块链安全业务的行业领导者。”

作为资金最充裕的比特币挖掘公司，BitFury 在 2015 年 12 月 16 日宣布它将在 2016 年第一季度在市场上推出新的 ASIC 芯片。

拿到第三轮融资后，BitFury 宣布将投资 1 亿美元在格鲁吉亚建立一个 100 兆瓦的比特币挖矿数据中心，并推出了 28 纳米比特币挖矿芯片。这是继哥里的第一个 20 兆瓦的数据中心之后 BitFury 在欧亚国家建立的第二个比特币挖矿数据中心。据悉，该数据中心将建在格鲁吉亚首都第比利斯，这里将创建一个特殊的技术区，以吸引国际技术公司。

BitFury 在格鲁吉亚的官方代表 Eprem Urumashvili 表示：“格鲁吉亚的受益点表现在三个方面，一是一笔高达 1 亿美元的投资；二是将现代信息技术带入该国；三是格鲁吉亚将因此加入创新技术世界地图。”

值得一提的是，专注于投资格鲁吉亚地区的战略投资基金公司格鲁吉亚联合投资基金连续参与了 BitFury 的三轮 2 000 万美元融资。

2016 年 6 月，BitFury 联合加拿大 NDI 科技公司推出了区块链试行应用——区块链信任加速器（Blockchain Trust Accelerator）。这一应用的意义在于可以连接政府、科技人员和资源来改善治理问题。对于民主制度来说，身份信息、选票以及社会服务等资产都可以被区块链安全且永久地保存。

区块链对加强民主问责制的重大意义已经引起世界各国的关注和重视。比如，区块链信任加速器项目的试行已经于 2016 年 4 月在格鲁吉亚共和国推出。而且，格鲁吉亚共和国政府正在和 BitFury 集团合作创建一种基于区块链的土地所有权数据库。

2016 年 5 月，中国领先的综合互联网金融服务供应商中国信贷控股有限公司宣布与 BitFury 签订协议，用 3 000 万美元购买 BitFury 约 6.38% 的股权。投资完成后，中国信贷将会与 BitFury 在中国成立合营公司销售 BitFury 集团的比特币采矿设备。此次合作对于推广区块链技术，发展以区块链为基础的互联网金融业务有重大意义。

Block chain

# 第3章
# 区块链四大核心技术

区块链之所以为大家带来了一个突破传统、颠覆性创新的机会，主要依赖于四大核心技术创新，分别是分布式账本、非对称加密和授权技术、共识机制和智能合约。下面我们分别讲解这四大核心技术。

practice

## 3.1
# 分布式账本

区块链使用的记账方式与传统的记账方式不同，具有去中心化创新、数据高度透明、无须依赖信任以及信息可回溯性四大特征。在区块链交易记账操作过程中，分布在不同地方的众多网络节点共同负责记录完整的账本，每一个节点都参与并监督交易的合法性，同时共同为其他用户作证。这种分布式账本的记账方式避免了传统单一记账人因不可控因素而记假账的可能性，保证了账目数据的真实性和安全性。

### 3.1.1 去中心化创新

区块链的分布式账本是一个去中心化的、没有更高权威的、分布在众多人计算机中的系统。从区块链的本质来说，区块链提供了一种分布式手段来担保和核实交易，从而为最终甩开中心控制者提供了机会。

在传统的交易支付流程中，存在一个中心机构，所有的节点要参与交易必须通过中心机构来达成交易。这里的中心机构既扮演了维护者的身份，维护交易账目正常达成交且真实可靠的，又扮演了特权参与者的身份，发行货币资产的权利。

在区块链的交易流程中，分布式账本的节点 A 直接将交易发给节点 B，所有节点一起确认并且验证交易的真实性。更新了公共总账以后，所有人再同步一下最新的总账。在这里，维护者的身份下放至每一个参与者手中。分布式账本无须对账，大家只需要维护一条总账就可以，这里的总账指的是每个人都可以看到公共账簿。

分布式账本去中心化的特点为区块链未来发展奠定了应用基础，下面以区块链技术在跨境电商领域的应用为例，介绍这一特征。

跨境电商是从 2016 年火起来的。随着国家政策层面的扶持加强，跨境电商成为新的行业风口。根据行业预测，2017 年中国跨境电商交易额将达到 8 万亿元，年均增速超过 30%。

当前，我国跨境电商存在一些问题。首先是外贸渠道的缺失和信任问题。外贸大环境非常复杂，对商家的要求也非常高，而国内品牌商的外贸之路因为外贸渠道缺失和信任问题而显得迷雾重重。

其次是手续费高昂和转账周期长的问题。以传统跨境汇款方式电汇为例，汇款周期一般长达 3 ～ 5 个工作日，这期间除了中间银行会收取一定手续费，环球银行金融电信协会（SWIFT）也会对通过其系统进行的电文交换收取较高的电信费。在我国通过中国银行进行跨境汇款时，单笔汇款的电信费为 150 元。

订单碎片化也是跨境电商面临的一大挑战。在全球金融危机后，中国外贸发生显著变化，短期订单、中小订单逐渐代替长期订单、大订单。可以说，市场体量庞大，订单碎片化已成为外贸新常态。

在线贸易的刚性需求及交易频次提高的同时利润下降，这是跨境电商面临的另一个挑战。在这种情况下，外贸制造商必须全面转型，从简单的生产制造商进化为贸易综合服务商，以适应全球市场的竞争。

支付不仅是供应链系统的引擎，也是跨境电商的重要环节，其支付模式直接决定跨境电商的生命线。我国国内的第三方支付系统比较发达，但是在国外就不一样了。为了解决跨境电商发展中的难题，关于区块链支付的讨论应运而生。可以说，区块链支付为跨境电商提供了近乎完美的支付解决方案。

区块链分布式账本的去中心化创新使用户在跨境汇款中以更低的费用和更快的速度完成跨境转账，市场空间非常大。

传统的跨境支付方式具有清算时间长、手续费高、容易出现支付诈骗行为的劣势，跨境资金风险较大。区块链打造的 P2P 支付具有去中心化的特征，不但可以全天候支付、瞬间到账，还能降低隐形成本，有利于降低跨境电商资金风险及满足跨境电商对支付清算服务的便捷性需求。

下面我们一起看一下区块链支付为跨境电商提供的解决方案。区块链分布

式账本构成一个去中心的全球结汇系统。这个系统的核心机制包括两方面内容。

一是引入网关系统，解决陌生人之间转账汇款的信任问题。一般来说，银行、第三方机构等具有公信力的主体都可以担任网关。用户与网关之间的关系在整个系统中反映为一种债权债务关系，即如果用户 A 需要通过区块链钱包汇款给用户 B，则其间的网关就与 A 生成了债务，与 B 生成了债权，通过将该网关对 B 的债权转为 A 对 B 的债权并进行清算，继而反映在双方余额变化上就完成了交易。

A 与 B 之间的债权债务关系利用区块链的分布式账本储存在若干个服务器上，而服务器之间以 P2P 的方式进行通信，以避免中心化服务器所带来的各种风险。

二是根据共识选择用于结算的数字货币，如比特币、莱特币等。数字货币的作用是维护系统正常运行，防止恶意攻击者大量制造垃圾账目蓄意破坏。因此区块链钱包要求每个网关都必须持有一定限额的数字货币量，并且每进行一次交易，都需要提供一定量的数字货币，就像传统的每次交易都要交手续费一样。

在区块链打造的跨境结算方式中，银行也可以参与进来。银行不需要提供技术支持和底层协议，只要指定特定的数字货币履行这一职责就可以了。这种模式将会代替传统成本高昂的 SWIFT 技术，从而帮助传统银行以更低的成本、更快的速度来进行跨境清算和汇款。当然银行还可以选择覆盖更多的支付场景和数字币种，就像淘宝和京东为用户提供多样的结算方式一样。

基于分布式账本技术，区块链将会帮助跨境支付解决现存问题，增强跨境电商参与方的体验。

### 3.1.2 数据高度透明

2016 年 7 月 30 日，支付宝爱心捐赠平台上线了一个新项目，名为“听障儿童重获新声”。该项目将会筹集 19.84 万元善款，用于听障儿童一年的听力语言康复、聋健融合教育和人工耳蜗调机费用。这一项目与往常的爱心项目有什么不同呢？细心的捐赠人可以发现，在反馈页面查看善款去向时增加了“爱心传递记录”。

这表明该项目的资金募集及使用将受到公众全程监督，善款在何时流向哪个账户是一目了然的。用户首次可以亲眼见证自己的捐款从支付宝平台划拨到项目执行方账号，最终进入受助人指定账号。这一改变不仅是视觉和用户体验上的升级，更是蚂蚁金服首次尝试将区块链技术应用于公益场景。

对于规模较小、实力薄弱的公益机构来说，提升透明度、打造公信力是非常困难的。举例来说，捐款人捐 5 元后索要免税发票，而项目方邮寄发票就需要 15 元，而且这还没有计算项目方投入的时间和精力成本。在这种情况下，将区块链用于公益显得非常有价值。

蚂蚁金服首席技术官程立称：“在支付宝爱心捐赠平台上，经常有用户捐出几元到几百元不等的善款，但捐款离开公益项目的支付宝账户后，就很难再被用户追踪。而区块链公益平台就像一家专门邮寄善款的互联网邮局。每笔善款都是一个包裹，在投递过程中，经过每个邮寄节点都会被盖上邮戳，每个邮戳都可以被公开查询。”

中华社会救助基金会秘书长胡广华认为，区块链的分布式账本数据高度透明的属性将打造一种不需要第三方背书的新信任机制。他说：“区块链技术让支付宝平台、公益机构支付宝账户、受助人支付宝账户无缝链接起来，成为一个可追溯的闭环，这是低成本高效率，专业公益、有效公益的重要尝试，对提升公益透明度和信任度是一次革命性的助推。”

蚂蚁金服表示，他们将会在合法合规、保证用户信息和资金安全的前提下，与更多的公益组织和审计机构展开合作，让区块链技术助力中国公益信任环境的改善。

将区块链用于公益主要借助了分布式账本数据高度透明，从而达到提升公众信任度的作用。区块链分布式账本向所有的参与者公开数据，让大家共享一个账簿，并通过去中心化的管理达到人人平等，这些创意是前所未有的，并且因此受到广泛关注。

区块链分布式账本的数据对所有的人公开，所有的参与者都能在互联网上共享这些数据，保证了账本的公正性。而且比特币、以太坊超级账簿以及大部分的竞争币系统都具有这种特征。它们对所有人都公开，表明人人都能通过一台联网计算机进入。

以比特币为例，所有的参与者 ID 都是匿名的，但是上面的数据默认对所有人都公开。这种开放性带来了巨大的优势，比如抵抗专制制度资本管控以及抵抗攻击的能力。比特币在保证对所有人公开的同时还具有安全的特征。我们甚至无法想象，只要我们愿意，就能够获知每一个参与者的账户余额以及交易记录。

直到现在，人们依然惊奇于比特币保障安全的方法是如此的新颖，而且在它存在的近 10 年历史中，竟然从来没有人切实可行地打破过这种安全。与之相对，如果用最传统的方法保护用户权利和安全，那么风险是非常高的。这种模式的雏形开始于世界第一把锁的发明。一把锁一般只有几把钥匙，这会让所有者觉得安心。然而，很多例子都证明这种模式失败的可能性很大，钥匙可以被设计得很聪明，但总有聪明的盗窃者不用钥匙就可以打开这把锁。

如果一位用户在计算机的数据库里保存着一些公司的绝密数据，那么一场黑客竞赛也就开始了，胜利者将会以很小的成本获得这些数据，威胁公司的安全。但区块链就不一样了，比特币经过众多考验之后依然保证安全则说明了这一点。显而易见的是，黑客对于比特币在网络中每天潜在交割的 67 亿美元的价值毫无下手的机会。

有人说，区块链比特币可以用于贩卖毒品以及其他违禁类产品和服务。这是事实，但用 1 万美元也能做这些事情，任何纸币都可以。如果说，人们可以接受纸币的匿名性，那为什么要抗拒区块链比特币呢？

事实上，区块链比特币虽然具有匿名性，但是比特币区块链上发生的交易很容易就能进行追踪，任何人都可以查询，而纸币的使用则无迹可寻。业内人士曾经尝试过根据序列号追踪纸币使用踪迹的研究，但是几年后被证明是不可行的。下面是比特币对比纸币的三大优势，如图 3-1 所示。

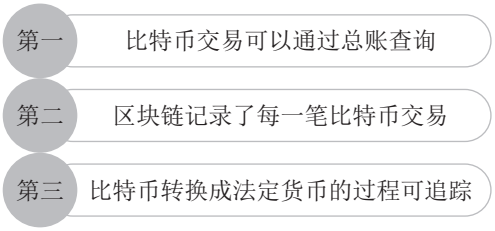


图 3-1　比特币对比纸币的三大优势

第一，比特币交易可以通过总账查询。如今，纸币的追踪依赖于实物检查的方式，而区块链比特币的优势则更明显。区块链比特币的本质是一个庞大的分布式账本，每一笔网络交易都由节点记录在系统中，尽管交易双方钱包的所有者是匿名的，但总账是公开的。包括执法机关、税务当局在内的所有机构和个人都可以访问总账。

第二，区块链记录了每一笔比特币交易。区块链记录了系统中发生的每一笔交易，因此我们可以在总账中查询到所有的交易历史。每一笔比特币交易都可以查询，无法隐藏、改变或者篡改，远远好于纸币消失又出现，交易或转移的情况无迹可寻。如果没有记录，纸币交易各方的情况是无法查询的，而比特币交易则会显示在总账里，除了比特币钱包所有者的身份信息。

第三，比特币转换成法定货币的过程可追踪。另外，比特币对法定货币的转换过程也是可以被追踪的，因为用户要想将持有的比特币转换为法定货币，必须与交易所或提供类似服务的机构进行联系。所有提供相关服务的交易所以及机构都处于相关部门的监管下，以帮助执法机构对犯罪行为进行追踪。

相比之下，纸币可以无限循环使用，无须转换成其他形态。对于罪犯来说，使用比特币的犯罪行为更容易被执法机构追踪到，所以他们更愿意选择真正匿名的纸币。

### 3.1.3　无须依赖信任的哈希算法

哈希算法也被称为“散列”，是区块链的四大核心技术之一。由于一段数据只有一个哈希值，所以哈希算法可以用于检验数据的完整性。在快速查找和加密算法的应用方面，哈希算法的使用非常普遍。

在互联网时代，尽管人与人之间的距离更近了，但是信任问题却更严重了。现存的第三方中介组织的技术架构都是私密而且中心化的，这种模式永远都无法从根本上解决互信以及价值转移的问题。因此，区块链技术将会利用去中心化的数据库架构完成数据交互信任背书，实现全球互信的一大跨步。在这一过程中，哈希算法发挥了重要作用。

可以说，以比特币为首的数字货币并非区块链最重要的价值体现，在信息

不对称、环境未知的情况下建立一个满足人们经济活动需求的信任生态体系才是区块链更重要的意义。

下面我们一起看一下区块链是如何通过哈希算法解决信任问题的。在此之前，我们需要解释一下什么是“拜占庭将军问题”。

“拜占庭将军问题”是由著名计算机科学家莱斯利•兰伯特（Leslie Lamport）提出的点对点通信中的基本问题，也可称为“两军问题”或者“拜占庭容错”。

在 5 ～ 15 世纪，拜占庭就是当时的东罗马帝国，也就是现在土耳其的伊斯坦布尔。可以想象，拜占庭军队有许多分支，驻守在敌人城外随时准备进攻，每一个分支都有各自的将军。当时的环境决定了骑马传递信息是将军之间通信和协调统计进攻时间的唯一途径。

由于敌人的防御比较强大，任何一个军队分支的单独入侵行动都会失败，而且入侵的分支还会被歼灭。因此，只有一半以上的分支同时进攻才能成功占领敌人的城池。

在观察了敌情以后，将军们需要制订出一个统一的进攻计划，即确定出在哪一天的哪一时刻进攻。然而将军中存在一个叛徒，他的任务就是破坏忠诚将军们的进攻计划，使他们的进攻不能达成一致。这样只要进攻时的军队分支少于一半，敌人就会胜利，叛徒的目的就达到了。这是一个由互不信任的各方构成的网络，但是他们需要完成一个共同使命（除叛徒以外）。

由于各个将军之间互相不信任，认为只有在自己的城堡以及军队范围内才能保障自己的生命安全，所以将军们不会聚集到一起开会。在这种情况下，他们在任意时间以任意频率派出任意数量的信使到任意对方，内容如下：“我将在第 × 天的第 × 点进攻，你同意吗？”

如果收到信息的将军同意该做法，他就会在原信上附上一份盖章验证的回信，然后把合并之后的信息拷贝再次发送给其余的将军们，要求他们也这样做。他们的目标就是通过原始信息的积累使最后的信息链盖上他们所有将军的图章，在时间上达成共识。

问题出现在这里，假设有 10 个将军，每个将军向其他 9 个将军派出一名信使，那么就是 10 个将军每人派出了 9 名信使，而在任意时间内有总计 90 次

的传输，并且每个将军分别收到 9 个信息，可能每一封信的进攻时间都不同。另外，叛变的将军还会同意超过一个以上将军的攻击时间，然后重新广播超过一条的信息链。于是，这个系统迅速演变成一个信息虚假和攻击时间相互矛盾的纠结体。

拜占庭将军问题是一个在分布式系统中进行数据交互时面临的难题，也就是说当整个网络中的分布式节点之间都没有信任度，如何操作才能保证信息交互的安全性而且不用担心数据被篡改。区块链利用哈希算法完成了这一挑战，使系统中所有节点在无须信任的条件下自动安全地交换数据。

区块链是这样做的：它为信息发送加入了成本，降低了信息传递的速率，而且加入了一个随机元素使在一段时间内只有一个将军可以广播信息。这里所说的成本就是区块链系统中基于随机哈希算法的“工作量证明”。哈希算法所做的事情就是计算获得的输入数据，得到遗传 64 位的随机数字和字母的字符串。

区块链系统计算的输入数据是指节点发送的当前时间点的整个总账。当前计算机的算力使其可以实时计算出单个哈希值，但是比特币区块链系统只接受前 13 个字符是 0 的哈希值结果作为“工作量证明”。而前 13 个字符是 0 的哈希值是非常罕见的，需要整个比特币网络花费 10 分钟的时间才在数以亿计的数据中找到一个。在一个有效的哈希值被计算出来之前，网络中已经生产了无数个无效值，这就是降低信息传递速率，并使整个系统成功运行的“工作量证明”。

在拜占庭将军问题中，第一个广播信息的将军就是第一个发现有效哈希值的计算机，只要其他将军接收到并验证通过了这个有效哈希值和附着在上面的信息，他们就只能使用新的信息更新他们的总账拷贝，然后重新计算哈希值。下一个计算出有效哈希值的将军就可以将自己再次更新的信息附着在有效哈希值上广播给大家。然后哈希计算竞赛从一个新的开始点重新开始。由于网络信息的持续同步，所有网络上的计算机都使用着同一版本的总账。

比特币区块链系统找到有效哈希值的时间间隔为 10 分钟，这是算法设置好的。算法难度每隔两周调整一次的目的就是保证这 10 分钟的间隔，不能多也不能少。每隔 10 分钟，总账的信息就会在区块链更新并在全网同步一次，因此分散的交易记录是在所有网络上的计算机之间进行对账和同步的。

当用户在区块链系统发起一笔交易的时候，他们会使用私钥和公钥为这笔

交易签名，而内嵌在区块链系统的标准公钥则承担了加密工具的角色，对应在拜占庭将军问题中，加密工具就是用于签名和验证消息的印章。

因此，哈希算法对信息传递速率的限制加上加密工具使区块链构成了一个无须信任的数据交互系统。在区块链上，一系列的交易、时间约定、域名记录、政治投票系统或者任何其他需要建立分布式协议的地方，参与者都可以达成一致。

区块链通过哈希算法解决了拜占庭将军问题，而且这一方案可以推广开来。那些在分布式网络上无法解决信任问题的领域都可以通过区块链得到解决。比如，互联网领域的专家们正在试图为互联网创造一个分布式的域名系统；基于区块链技术的互联网选举投票系统也正在研发中。如果说，互联网云分享搅动了一池春水，那么区块链构建的不依赖信任的交易系统则打开了洪水闸门。

### 3.1.4 银行也抵抗不了的信息可回溯性

2011 年的郭美美炫富事件直接导致公众对红十字会的信任度下降；2016 年震惊全国的雷洋事件始终真相不清；魏则西事件让我们看到了信息不对称社会下的个体悲剧……

如果有了区块链，一切就不一样了。比如，建立区块链公益，记录每一笔捐款的收入和支出，使信息完全对公众公开。区块链分布式账本的可回溯性使“郭美美”们将无法隐藏；如果规定警方出警的时候必须通过指定的多台设备实时上传到区块链视频云上，那么真相将水落石出；如果建立一个区块链平台记录医院信用以及治疗方法，就可以规避由于被不对称信息和不实广告所蒙蔽而产生的悲剧。

总之，这一切改变基于区块链分布式账本的信息可回溯性。下面以区块链在互联网金融领域的应用为例看信息可回溯性的重要性。

2016 年 6 月，中国互联网金融（青岛）高峰论坛在青岛召开。安存科技旗下公司北京安金网络科技有限公司副总裁马成龙在论坛上做出发言：“互联网金融领域之所以有这么多乱象发生，根源在于在互联网这个虚拟空间里，记录主体行为的载体变成了电子数据，很难追溯。”

关于马成龙口中的电子数据，我国最高法院发布的《关于适用〈中华人民共和国民事诉讼法〉的解释》是这样规定的：“电子数据是指形成于或者存储于电子介质里的信息数据。”在互联网行业，电子数据主要指的是电子协议、电子合同以及电子支付凭证等。

电子数据常常与用户的权益挂钩，因为用户的投资项目、投资时间、投资金额、投资的收益回报等信息都可能是通过电子数据记录的。当用户的权益受损时，这些电子数据将成为用户证明自己权利的最核心资料。

然而，实际操作中会出现很多问题。尽管法律承认电子数据可以充当证据，但是电子数据通常都是由平台单方面保管的。用户与平台方发生利益纠纷的时候，平台方很有可能会将电子数据摧毁或者进行篡改。在这种情况下，用户根本无法使用真正具有效力的电子数据进行维权。

下面看一个 P2P 理财的例子：一家理财平台曾经将本应向投资者还款的时间全部延迟一年之久。当投资者想要使用电子合同维权时，发现该平台已经私自在网站内修改双方的合同协议内容，并且私自添加了还款协议；另外，各种网贷 P2P 平台跑路事件也闹得沸沸扬扬。每当平台跑路后，投资人会发现他们的网站、APP 已经无法打开，所有的电子数据都消失殆尽。在这种情况下，执法机关调查取证困难，投资人的维权之路非常艰难。

对于这种现象，马成龙表示：“这些鲜明的例子都在警惕互联网金融消费者，提高电子数据保全意识，用法律的武器保护自己是维护自身权益的根本之道。”

近几年来，政府工作报告都提到了互联网金融。2014 年的表述是“互联网金融异军突起”，2015 年的表述是“促进互联网金融健康发展”，而 2016 年对互联网金融的表述为“规范发展互联网金融”。由此可见，政府已经把互联网规范放在了第一位。在规范互联网金融发展的过程中，区块链具有非常大的价值。

比如在 P2P 网贷行业，2015 年倒闭跑路的 917 家 P2P 网贷平台中，90% 以上的平台都设立了资金池，由于内幕操作无法兑付而选择了跑路。由于信息的不对称性，投资者根本无法知道平台是否设立了资金池、资产是真是假以及资金用途，而且更做不到一一考证。因此，只有用上永久存储以及无法篡改数

据的区块链技术，才能保证 P2P 平台仅仅充当信息中介，不触碰资金。毕竟信息的可回溯性让 P2P 平台难以在众人的监督下做出违法勾当。

再比如票据业务领域，2016 年 1 月 22 日，中国农业银行北京分行保险柜中票据换报纸的新闻震惊了全国。当天，中国农业银行正式发布公告称：“农行北京分行票据买入返售业务发生重大风险事件，经核查，涉及风险金额为 39.15 亿。本应存放在银行保险柜里的票据，却被某票据中介提前取出，与另外一家银行进行了回购贴现交易，但资金并未回到农行北京分行的账上，而是非法进入股市，又由于近期 A 股下跌，导致巨额资金缺口无法兑付。”

票据业务领域的乱象非常多，除了一票多卖等票据违规交易问题，还包括克隆票、假票、变造票等违规操作问题。在这种情况下，市场急需一种更安全、完善的票据交易模式，而区块链为这种模式提供了可能。

作为一种永久存储，信息不可篡改的分布式账本，区块链由数以亿计的大量计算机节点共同维护。复杂的校验机制使得保存在区块链上的数据具有连续性和一致性，就算某些计算机造假篡改了数据也无法改变整个区块链的完整性。私钥签名和公钥验证交易内容全部正确后，数字货币就会在对应的账户地址间转移，而且保证准确无误。

因此，将区块链技术应用到 P2P 网贷领域以及票据业务领域的电子数据存储上，将会彻底解决许多违法违规的问题。一个投资项目的发起到资金筹集，再到后期的偿还以及一张票据从申请到发行，从交易到承兑，整个流程的关键信息都会记录在区块链上，谁都无法篡改。

基于区块链上信息的可回溯性，监管部门的查询将变得非常容易。另外，数字货币的转移路径明确，这就使 P2P 平台只能将投资者的资金用于规定的用途，最后回到投资者手里。而中国农业银行北京分行的票据即使被暗箱提取贴现交易，资金也只能回到中国农业银行北京分行的账上，第三方无法插手。作为全球最热门的金融科技，我国的互联网金融也需要依靠区块链技术崛起。

客观上信息不对称以及主观上受到利益驱使加大了中心节点产生欺骗和伪造信用的风险。区块链技术的加入可以在时间维度上保证连续性，在空间纬度上保证开放性。总而言之，区块链上信息的可回溯性将会影响众多领域，而这种可回溯性是银行业也难以抗拒的。

# 3.2 非对称加密和授权技术

区块链中每一个数据块中包含了一次网络交易的信息，产生相关联数据块所使用的技术就是非对称加密技术。非对称加密技术的作用是验证信息的有效性和生成下一个区块。另外，区块链上网络交易的信息是公开透明的，但是用户的身份信息是被高度加密的。只有经过用户授权，区块链才能得到该身份信息，从而保证了数据的安全性和个人信息的隐私性。

## 3.2.1　私钥掌握在用户手里

由于私钥是非对称加密技术涉及的概念，所以我们首先探讨对称加密技术以及非对称加密技术。对称加密技术的特点是数据加密和解密使用的密钥（意思是秘密的钥匙，在密码学中，密钥是在明文转换为密文或将密文转换为明文的算法中输入的参数）相同。也就是说，加密密钥也被用作解密密钥。这种加密技术在密码学中叫作对称加密技术。

对称加密技术的优势是使用方便，密钥简洁而且破译难度高。DES、3DES、Blowfish、IDEA、RC4、RC5、RC6 和 AES 是较为常见的对称加密技术。

在电子商务交易中，对称加密技术主要存在四个问题，内容如图 3-2 所示。

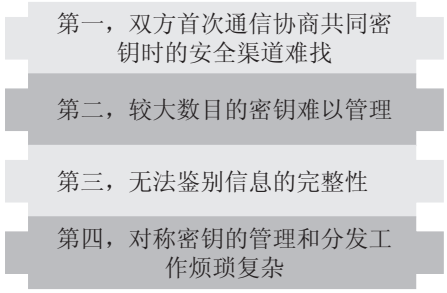


图 3-2　对称加密技术的四个问题

第一，双方首次通信协商共同密钥时的安全渠道难找。直接的面对面协商

是协商共同密钥最安全的方式，但这是不现实而且难以实施的。因此双方很可能会选择其他相对不够安全的渠道进行协商，包括使用 QQ、微信、发送邮件或者通电话等。

第二，较大数目的密钥难以管理。对于一方来说，对于每一个合作者使用的密钥都不相同。在开放的社会环境中存在大量的信息交流，而数目较大的密钥与社会发展环境是难以适应的。

第三，无法鉴别信息的完整性。对称加密技术不具有鉴别信息完整性的功能，因此发送者和接受者的身份也是无法验证的。

第四，对称密钥的管理和分发工作烦琐复杂。采用对称加密技术的贸易双方必须使用相同的密钥，保证密钥的安全可靠。另外，双方还需要设置防止密钥泄密和更改密钥的程序。

如果两个用户使用对称加密技术交换数据，那么涉及的密钥为 2 个。如果企业有 $n$ 个用户，那这个企业共需要密钥的个数为 $n\times(n-1)$ 个。如此看来，企业信息部门需要在密钥生成和分发工作上付出很大一部分精力。

为解决信息公开传送和密钥管理问题，公开密钥系统应运而生。相对于对称加密技术，这种方法也叫作非对称加密算法。非对称加密技术允许通信双方在不安全的媒体上交换信息，安全地达成一致的密钥。RSA、ECC（用于移动设备）、Diffie-Hellman、El Gamal、DSA（用于数字签名）是比较常见的非对称加密技术。

非对称加密技术中存在两个密钥，一个是公开密钥（以下简称公钥），另一个是私有密钥（以下简称私钥）。公钥与私钥是一对，在加密时，如果用公钥对数据加密，那么只有用私钥才能解密；如果用私钥对数据加密，那么只有用公钥才能解密。

非对称加密技术实现信息交换的过程为：A 生成一对密钥，并将公钥公开。B 得到公钥后用其对机密信息进行加密然后发送给 A。A 再用自己保存的私钥对加密后的信息进行解密。

非对称加密技术的优势是保密性好，双方无须交换密钥，缺点是加密和解密花费的时间长、速度慢。

如果企业中有 $n$ 个用户，那么企业需要生成的密钥数目为 $n$ 对，并将 $n$ 个

公钥公开，*n* 个私钥由用户自己保存。由于用户掌握的私钥是唯一的，其他用户可以通过公钥来验证信息发送者的来源是否真实可靠，而信息发送者也无法否认发送过该信息。

作为区块链的核心技术之一，非对称加密技术可以用于用户的身份验证。由于用户掌握的私钥是唯一的，所以身份验证显得非常容易。下面一起来看中本聪通过比特币的创世块证明自己身份的原理。

比特币的创世块有 50 个比特币，而且代码是确定、唯一的，这就使这 50 个比特币不能使用。中本聪的创世块地址为“1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa”，很多比特币爱好者还向中本聪的地址捐币，使其余额超过了 50 比特币。对中本聪来说，他拥有这笔比特币的所有权，但是没有使用权。

比如说，一个比特币的狂热爱好者在网上发言，并称自己就是中本聪本人。如果中本聪自己觉得有必要澄清，就可以使用创世块的私钥签名，并注明该发言并非由自己本人发出，全世界的人们就知道真相了。

那么我们每个人以及企业机构等如何使用区块链来标识自己的身份呢？首先，我们需要使用比特币 QT 钱包（比特币本地钱包）生成一个收款地址，该收款地址可以是空地址，不需要有任何余额。其次，我们需要用 QT 钱包对生成的空地址进行签名。签名一般都是使用特定消息，然后就可以得到签名结果。然后，我们需要向全世界公布自己的比特币地址，包括特定消息和签名结果。这时，全世界都知道了这个地址是我们的。

如果在一些情景下，你需要向对方证明你的身份，那么对方给出一个特定消息，你只需要签名，对方进行验证即可证明你的身份。

用区块链验证身份的唯一风险就是私钥被盗，所以只要用户妥善保管好自己的私钥，别人就无法伪造你的身份。

截至 2017 年年初，区块链数据已经超过了 25G，如果我们仅仅使用 QT 钱包进行身份验证，就不需要同步庞大的区块链数据，否则启动和关闭 QT 钱包都无比慢。

一个企业机构也可以使用这种方法验证自己的身份真假。与个人一样，企业需要使用一个地址进行签名声明自己是该私钥的唯一拥有者。很多时候，企业的身份都是由多人共同确认的，遇到这种情况，企业可以预先将私钥分成多

份，让几个人共同保管。比如私钥分成三份，只有两人以及两人以上共同签名才能确认企业的身份。在这种情况下，企业遇到任何伪造机构身份的行为，都可被轻易验证。

区块链让人类第一次不需要依靠任何第三方中心机构就可以完成身份验证，也是人类第一次在互联网上创造了一个不能复制、不可伪造的数据库。

从比特币创世块开始，世界已经发生改变。也许到 2026 年，你可能会看到以下场景成为事实。一个英国海关官员对某个中国游客说：“先生，请对这一消息‘welcome to England’，在您的比特币地址‘×××’上签名。”该先生拿出手机，点了点，官员也在他的桌面设备上点了点，然后说：“welcome to England，×××。”

基于非对称加密技术，区块链将如何改变我们的生活呢？只有时间才可以验证。

### 3.2.2 匿名，这里可以实现

区块链的授权技术保证了未经用户授权，任何人都无法获知用户的身份信息。下面以比特币为例，看用户如何实现合理的匿名性。

试想一下，发送和接受比特币就好比作者用笔名发表作品。如果作者的笔名与自己的身份无关，那么谁都无法得知作品背后的作家的真实身份。在区块链上，用户接收比特币的地址是公开的，凡是与该地址有关的交易信息都会被永久保存在区块链上。如果用户的地址与真实身份没有任何关系，那么用户便实现了合理的匿名性。

要实现匿名，用户需要保证比特币钱包地址与自己的身份信息没有关联。也就是说，用户需要匿名购买比特币。下面是三种匿名购买比特币的方法，内容如图 3-3 所示。

| | |
|---|---|
| 第一 | 用现金购买 |
| 第二 | 在VirWox网站上购买 |
| 第三 | 通过匿名贷款获得比特币 |

图 3-3　三种匿名购买比特币的方法

用现金购买是匿名购买比特币最好的选择。大多数比特币在线交易的过程是类似的，即需要用户上传身份证。而用现金购买可以避免在线交易，不用上传身份证用户，可以亲自接见比特币卖方，支付现金即可获得比特币。只要用户愿意，用现金购买比特币有很多可以使用的方法来避免卖方知道自己的身份信息。

在 VirWox 网站上购买比特币也可以实现一定的匿名性。当然，在 VirWox 上购买比特币无法实现完全匿名，因为该网站仍然要求用户透露一些信息。不过，相比于其他一些比特币在线交易要求用户提供银行账户和个人证件信息，通过 VirWox 网站购买比特币可以实现更好的匿名性。

在 VirWox 网站上，用户需要一个免费账户来购买林登币（第二人生 3D 网络游戏里的虚拟游戏币）。用户可以使用的支付方式有 PayPal、Skrill 等。为了实现更好的匿名性，用户可以选择使用 paysafecard 支付。有了 paysafecard，即便没有身份证、银行账户或者信用卡，用户也可以购买林登币，还可以在无须验证的情况下将林登币兑换成比特币。

通过匿名贷款获得比特币也是一种可行方式。根据以往经验，用信用卡购买比特币是很难实现匿名的。但是，比特币贷款就不一样了。比如，Reddit 就免除了小额贷款项目中复杂的身份认证过程。

事实上，以区块链作为底层技术支持的数字货币都可以实现匿名，下面我们看看新兴数字货币 ZCash 如何实现匿名的。

ZCash 与比特币一样，都建立在区块链之上。不同的是，ZCash 实现了完全的匿名。ZCash 有一个非常特别的功能，即用户可以自由选择隐私级别，自主决定公开哪些数据。比如，一个大学生接受了父母给其发送的一笔 ZCash，然后这个大学生将隐私级别设置为只有父母可以看到这笔钱的交易信息。

ZCash 的发明者以及公司 CEO Zooko Wilcox 称：“这款新型货币使用者的身份将在真正意义上难以识别，使其管理具有更强的保密性。”尽管比特币等数字货币都具有匿名性，但在现实生活中我们可以通过区块链的记录与追踪交易获知比特币的发送地点，从而定位到发送者。

然而 ZCash 通过密码计算，即零知识证明（密码学术语，意思是在不让对方知道任何信息的条件下证明一件事）保证了用户在不泄露身份信息以及执行金额的情况下进行交易，给了用户更多的控制权。

对此，ZCash 官网有如下说明：“不同于比特币，ZCash 的交易完全对发送者、接受者以及交易链中的其他信息保密。只有那些有权限者才能够了解交易细节。使用者有完全的控制权自行决定是否赋予他人了解交易细节的权限。”

ZCash 的设想最早出现在 2014 年 Zooko Wilcox 的一篇学术论文中。按照计划，ZCash 的开发工作非常顺利，并且取得了初步进展。当然，在形成完整的开放系统之前，Zooko Wilcox 还需要做很多工作。

为了进一步调试 ZCash 的开发和设计，ZCash 团队于 2016 年 7 月推出了 Zcash 测试版。同时，人们可以通过 ZCash 网站上“testnet”系统参与测试版的体验，提前使用这种当前没有价值但未来将有很大升值空间的货币。

2016 年 10 月 28 日，ZCash 正式推出同名数字货币—— ZCash。Zooko Wilcox 说：“我们非常兴奋，因为 ZCash 数字货币的诞生意味着区块链属性和加密功能首次结合在了一起。”

比如说，如果用户使用 ZCash 完成了一笔交易，区块链上留下的信息就是交易发生了，而具体花费了几个 ZCash 货币，购买了什么，只有用户自己才知道。

Zooko Wilcox 还说：“ZCash 通过给每笔交易加密，解决了用户的隐私问题。我们使用的加密算法是标准的、现代的、高科技的，如同保护网站、电子邮件和互联网上一切内容的加密方式一样。”

ZCash 的投资人 Roger Ver 说：“经济学规律和物理学规律一样都是一成不变的。优秀的货币应当是每一个单位都与其他任何单位都一样。对于数字货币来说，将其设为私有是最好的方法。”

如果有足够多的人关心数字货币交易的匿名性问题，那么这种货币将会大获成功。其实，早在 1998 年，DigiCash 由于日常消费者对金融隐私不够重视而宣告破产，但随着人们对隐私的重视度增强，DigiCash 的历史应当不会重演。

Zooko Wilcox 对 ZCash 的未来也非常有信心，他说：“我认为隐私具有重要的个人和社会价值，它可以保护个人和社会的隐私，让个人和社会的价值升值。每当有关 ZCash 项目的文章出现的时候，网友或者身边的朋友们就会告诉我他们也感受到了这一点。他们对此非常开心，并且很高兴看到我们为之努力，他们希望我们能够成功。”

无论是比特币还是 ZCash 都说明了一点，区块链可以帮助人们实现匿名，这不仅仅是梦想。

## 3.3 共识机制

区块链的共识机制用于验证每一次记录的有效性，从而防止任意节点篡改数据。区块链上的共识机制有很多种，不同的应用场景根据效率和安全性的考量选择不同的共识机制。共识机制主要包括工作量证明（Proof of Work，PoW）、权益证明（Proof of Stake，PoS）、股份授权证明（Delegate Proof of Stake，DPoS），其简介如表 3-1 所示。

表 3-1　区块链三种共识机制的简介

| 共识机制 | 工作原理 | 优点 | 缺点 | 使用项目 |
| --- | --- | --- | --- | --- |
| 工作量证明 | 利用机器进行数学运算来竞争记账权；与其他共识机制相比，资源消耗高、可监管性弱；每次达成共识需要全网共同参与运算，性能效率比较低；容错性方面允许全网 50% 节点出错 | 完全去中心化，节点自由进出 | 比特币已经吸引全球大部分的算力，其他再用工作量证明机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长 | 比特币；以太坊前三个阶段：即 Frontier（前沿）、Homestead（家园）、Metropolis（大都会） |
| 权益证明 | 节点记账权的获得难度与节点持有的权益成反比；比工作量证明机制的资源消耗少，性能有所提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱；容错性方面允许全网 50% 节点出错；权益证明是工作量证明的升级版本，根据每个节点所占代币的比例和时间等比例的降低挖矿难度，从而加快找随机数的速度 | 在一定程度上缩短了共识达成的时间；不再需要大量消耗能源挖矿 | 本质上依然是挖矿，没有解决商业应用的痛点；这种确认是一种概率上的表达，不能保证是一个确定性的事情，理论上有可能存在其他攻击影响。例如，以太坊的 The DAO 攻击事件造成以太坊硬分叉，而 ETC 由此事件出现，事实上证明了此次硬分叉的失败 | 以太坊第四个阶段，即 Serenity（宁静） |

续表

| 共识机制 | 工作原理 | 优点 | 缺点 | 使用项目 |
| --- | --- | --- | --- | --- |
| 股权授权证明 | 与权益证明的主要区别在于节点选举若干代理人，由代理人验证和记账；其合规监管、性能、资源消耗和容错性与权益证明相似。类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账 | 大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证 | 整个共识机制依然依赖于代币，而很多商业应用是不需要代币存在的 | 点点币（Peercoin）和未来币（NXT） |

### 3.3.1 工作量证明机制

由于比特币是区块链的第一个产物，所以，我们以比特币为例讲述区块链的共识机制——工作量证明。

本书 1.1.3 小节中讲道，比特币区块链是以每个节点的算力来竞争记账权的一个系统。在区块链系统中，算力竞赛每十分钟进行一次，而竞赛的胜利者就获得一次记账的权力，即向区块链这个总账本写入记录的权力。这就导致在一段时间内只有竞争的胜利者才能完成一轮记账并向其他节点同步增加新的账本信息、产生新的区块。

作为一个记账系统，区块链不仅可以记录以比特币为代表的数字形式的货币，还可以记录能用数字定义的其他任何资产。这意味着区块链可以定义更为复杂的交易逻辑，比如股权、产权、债权、版权、合约、公证、投票等可以用数字形式进行价值存储或转移的任何东西。但是，当区块链应用于不同场景时，使用的共识机制就不一定是工作量证明机制了，还有可能是上文提到的权益证明机制、股权授权证明机制或者其他共识机制。

### 3.3.2 中心维护到参与者共同维护

在区块链共识机制发挥作用的过程中，所有当前参与的节点共同维护着交

易及数据库，它使交易基于密码学原理而不基于信任，使任何达成一致的双方，能够直接进行支付交易，无须第三方参与。

作为记录交易的数据结构，区块链由众多已经达成交易的区块连接在一起形成，所有参与计算的节点都记录了主链或主链的一部分。在区块链上，每一个节点都有一份完整的已有区块链备份记录，而这些都是通过进行数据验证算法解密的矿工网络自动完成的。区块链上保留着所有关于每个节点和节点上比特币余额的信息，这些信息也被记录在完整的区块链上。

公共式区块链账本完全对外公开，这意味着区块链信息可以通过特定地址在区块链浏览器上进行查询。因此，我们才敢肯定地说，区块链通过均等的节点权利和义务保证了绝对公正。

大家可以想象一下以下这个场景：这里有两个银行和两个用户——银行甲和银行乙以及用户 A 和用户 B，用户 A 还使用一款第三方支付软件丙。银行甲、银行乙以及第三方支付丙都分别用自己的信息系统为用户记录账户余额，这基本上就是当今金融世界里的样子。

在银行甲的系统中有如下记录：“银行乙欠自己 100 万美元；用户 A 透支了 20 万元人民币；用户 B 有存款 5 万元人民币。”

在银行乙的系统中有如下记录：“自己欠银行甲 100 万美元；用户 A 有存款 12 万元人民币；用户 B 有存款 4 万元人民币；自己在第三方支付丙上有 200 万元人民币。”

而用户 A 在银行甲透支了 20 万元人民币，在银行乙有存款 12 万元人民币，在第三方支付丙上还有 2 万元人民币的余额。因此，只有通过两个银行和一个第三方支付的三个系统才能计算出用户 A 真正拥有的财产。

我们可以看到，银行甲与银行乙之间 100 万美元的借款被记录了两次。事实上，每个银行都必须花费大量的时间与金钱去开发和维护系统用来记录信息。更麻烦的是它们需要花费更多的时间和金钱在各银行之间互相检查对账，银行业的数据还需要使用多个不同的系统去记录。而且银行需要在对账方面付出高昂的成本，以确保各方信息的准确性。

下面用一张图表来记录上面例子中的所有数据，如表 3-2 所示。

表 3-2　银行、用户以及第三方支付之间的所有数据

| 甲方 | 乙方 | 数额 | 货币类型 |
|---|---|---|---|
| 银行甲 | 银行乙 | 100 万 | 美元 |
| 银行甲 | 用户 A | 20 万 | 人民币 |
| 银行乙 | 第三方支付丙 | 200 万 | 人民币 |
| 用户 A | 银行乙 | 12 万 | 人民币 |
| 用户 A | 第三方支付丙 | 2 万 | 人民币 |
| 用户 B | 银行甲 | 5 万 | 人民币 |
| 用户 B | 银行乙 | 4 万 | 人民币 |

表 3-2 和之前银行各自记录的内容是一样的，但是这种记录方式使得银行与用户之间不用维护自己的系统，而且最关键的是完全省去了银行之间对账的流程。这时可能有人就会有疑问，为什么不用一个统一账本记账呢？区块链就是这样做的。

区块链是一个共享网络，所有银行和用户都在这个网络当中，没有一个中心系统会维护账本，取而代之的是网络中的所有银行和用户都有这个账本的最新内容，账本由网络中的所有参与者共同维护。这样就防止了中心系统故障引起的账本丢失，而且每个参与者都对账本的安全与稳定起到了重要作用。

## 3.4 智能合约

智能合约指的是基于区块链中不可被随意篡改的数据自动化执行一些预先设定好的规则和条款，比如基于用户真实的信息数据进行自动理赔的医疗保险。区块链使智能合约有机会用于现实生活中。

### 3.4.1　以数字形式定义的承诺

智能合约（smart contract）的概念可以追溯到 1995 年，由密码学家和数

字货币研究者尼克 • 萨博（Nick Szabo）提出。尼克 • 萨博对智能合约的定义如下：“智能合约是一套以数字形式定义的承诺（promises），合约参与方可以在上面执行这些承诺的协议。”

在该定义中，“一套承诺”指的是合约双方共同制定的权利和义务，合约的本质和目的都将通过这些承诺体现出来。以一个买卖合约为例，一套承诺指的是卖家承诺发送货物，买家承诺支付合理的货款。

“数字形式”指的是合约将会以可读代码的形式写入计算机。因为智能合约建立的权利和义务是通过计算机网络执行的，所以参与方达成协定后必须完成这一步操作。

“协议”指的是合约承诺被实现的技术，合约履行期间被交易资产的本质决定了协议的选择。还是以买卖合约为例，假设买卖双方都同意使用比特币作为支付方式。在这种情况下，双方选择的实现合约承诺的技术就是比特币协议，智能合约将会在比特币协议上实现。在这里，用比特币脚本语言的数字形式定义合约承诺。

智能合约的诞生扩大了区块链的应用范围，更多的指令将会通过区块链智能合约来执行。由于智能合约完全是代码定义和执行的，所以实现了完全自动而且人工无法干预的模式。智能合约的操作方式是由其自治、自足、去中心化的三大特征决定的。

自治指的是智能合约一旦启动就会自动执行整个过程，包括发起人在内的任何人都没有能力进行干预；自足指的是智能合约通过加强服务或者发行资产的方式来获取资金；去中心化指的是智能合约的运行系统是分布式的，没有中心化的服务器，而且通过网络节点自动运行。

尼克 • 萨博认为，智能合约最简单的形式就是自动售卖机。两者的道理是一样的，用自动售卖机买东西，只要放入钱，选择商品，商品就会自动掉出。操作相同，结果相同。而智能合约只要有预先设定好的代码，就会一直按照代码来执行，代码相同，执行结果相同。

在商业领域，很多问题的执行依赖于信任，这使执行变得非常复杂，而智能合约帮助大家解决了这一难题。当高效的全自动执行系统替代了低效的人工判断机制，智能合约在最小化信任的基础上让事情变得更加便捷。

下面以智能遗嘱为例，看智能合约的应用。假设“如果父亲去世，儿子在结婚后才可以获得其财产”是一个智能遗嘱。这个交易事件需要到未来某个事件发生或者未来某个时间点被触发才能执行合同。第一个条件是父亲去世，系统首先会扫描一份在线死亡数据库证明父亲已经去世；第二个条件是儿子结婚，当智能合约确认了死亡信息后，程序会设定一个交易日期，一旦通过婚姻信息在线数据库扫描到儿子登记结婚，就会自动发送财产到儿子名下。

区块链智能合约在遗嘱执行方面的应用已经被某些公司关注，比如Blockchain Apparatus。Blockchain Apparatus 是美国 Blockchain Technologies Corp 集团启动的众多创业公司之一。该公司致力于研究基于区块链技术的新应用，目前从事一些法律领域方面的研究，这为法律服务行业提供新发展。

截至 2016 年 7 月，Blockchain Apparatus 已经开发了一些区块链投票创新应用，并且开始研究执行医嘱的区块链智能合约。将遗嘱管理交给软件来运行，无须人为控制，这在历史上第一次有可能实现，而且这一创新应用必将在未来改变人们管理自己财产的方式。

Blockchain Technologies Corp 的法律顾问成员艾瑞克·迪克逊（Eric Dixon）认为：“智能遗嘱或者更广泛的智能合约文件击中了大部分家庭和法院诉讼代理人的心。它在一个可定义且固定的时间内为立遗嘱人的真实意愿提供了更有力的证据。”

当前，因为无法保证遗嘱的真实性而导致的遗嘱诉讼案件非常多，遗嘱的表述模棱两可或者无法处理而造成解读分歧，这也是发生遗嘱诉讼案件的原因之一。

艾瑞克·迪克逊强调说：“区块链智能遗嘱可以保证遗嘱的真实性、排除伪造的可能性、使遗嘱的维护变得更容易、使法院获得事实的速度加快。”

区块链技术允许遗嘱修改，每次修改存储在其原始状态，而不需要经过繁杂的法律程序。艾瑞克·迪克逊解释说：“区块链将文件创作和提交到区块链的信息全部记录下来，很容易就能证明遗嘱的存在。这样一来，猜测一份遗嘱签订的时间将是一件愚蠢的事情，因为区块链给出了最好的答案。”

智能遗嘱只是一个开始，智能合约还将会改变政府、企业以及个人管理文件的方式。总而言之，智能合约有着广泛的应用领域，但产业化之路还需要大

家共同探索。

### 3.4.2　全面解析智能期权合约

期权与股票一样是一种金融工具，是买方向卖方支付一定的权利金后拥有的在未来某一时间段内或特定日期以事先约定价格向卖方购买或出售特定商品的权力，分为看涨期权和看跌期权。

看涨期权指的是在合约规定的有效时间内，期权持有者按照规定价格和数量购进相应标的物的权力。期权持有者之所以购买这种期权，是因为他对标的物的价格看涨，可以在未来获利。与之对应的，看跌期权指的是在合约规定的有效时间内，期权持有者按照规定价格和数量出售相应标的物的权力。

下面我们以看涨期权为例，讲解期权的运作过程。购买看涨期权后，如果标的物的市价高于合约规定的价格与期权费用之和时（不包括佣金），期权持有者就可以按照合约规定的价格和数量购买标的物，然后按照市价出售或者转让买进的期权，获取利润；如果标的物的市价高于合约规定的价格，但是低于合约规定的价格与期权费用之和，那么期权持有者将会损失一部分期权费用；如果标的物市价低于合约规定的价格时，那么期权持有者将会损失全部的期权费用，而且没有行权权力。综上，期权持有者购买期权的最大损失为期权费用加佣金。

比如，一个石油提炼商根据形势判断原油的价格会上涨，于是想到购买原油看涨期权。他以每桶 0.5 美元权利金的价格买入了执行价格为 54 美元 / 桶的 100 手合约（每一手合约代表 1 000 桶原油）。在到期时，该石油提炼商的收益损失如表 3-3 所示。

**表 3-3　石油提炼商的收益损失**

| 市场价格（美元 / 桶） | 结果 |
| --- | --- |
| 大于 54.5 | 收益 =（市场价格 − 54.5）×1 000×100 |
| 54.5 | 损益平衡点 |
| 54 ～ 54.5 | 损失 =（54.5 − 市场价格）×1 000×100 |
| 小于 54 | 损失 =0.5×1 000×100（全部权力金） |

了解了期权的运作过程后，我们接着看智能合约在期权领域的应用。以一个简单的智能期权合约为例，甲从乙处购买了智能股票期权合约，这个合约就使乙可以用每股 10 元的价格购买甲在 A 公司的 2 000 股股票。这个合约规定了期限，如果乙超过期限未行权，期权合约将自动作废。

智能股票期权合约定义的相关条款包括合约相关资产、合约方身份、行使价、合同有效期等。合约到期以前，智能期权合约的“exercise”功能将会自动执行持有人以行使价购买股份的行为。首先，“exercise”功能会检查发起交易者是否是合约股票的持有人，然后检查当前是否依旧是合约有效期。如果两者检查均通过，合同会立即执行，系统户根据合约条款将现金从持有人一方转移到卖家一方，而将股票资产转移给持有人。

截至 2017 年，智能合约还仅仅作为理论存在着。智能合约应用到现实世界里有两大难题。

第一个难题是智能合约难以把控实物资产保证合约的有效执行。以售货机为例，售货机通过将商品保存在内部硬件中严控财产所有权，但是代码应当怎么做呢？在智能期权合约中，“exercise”功能需要在合约双方之间转移现金和股份资产，但是计算机程序要怎么控制现实世界的现金、股份等资产呢？

第二个难题是智能合约难以获得合约双方的信任。对于合约代码以及解释和执行代码的计算机，合约双方需要有一个共享的标准，可以验证计算机是否有问题。

当前，区块链技术的发展应用还处于探索阶段，但是没有人怀疑区块链将会解决智能合约面临的两大难题。

首先，区块链使得计算机代码控制现实资产，保证智能合约的有效执行。区块链数字货币可以使现实资产转化为计算机代码，从而控制现实中的资产。在区块链上，资产的控制不需要控制实物，而是控制资产对应的密钥。因此，在上述案例中，期权智能合约就可以控制合约相关资产，而不需要代管机构。一旦启动“exercise”功能，代码执行就可以完成资产转移，无须人力参与。

其次，区块链解决了信任难题。区块链的功能不仅限于数据库，还可以记录资产所有权以及执行代码的分布式计算机。期权持有者可以将购买的期权上传并存储在区块链中，并根据指令执行。区块链这一优势同样适用于执行智能合约。一旦区块链记录了合约代码，合约方就可以确定合约不会被更改。

区块链智能合约离我们的生活并不遥远。证券交易所、银行以及其他金融机构都在积极研究开发区块链相关应用，希望可以实现利用区块链技术记录和交易现实资产的功能。

目前，通过区块链技术将智能合约的应用真正落地还处于研究探索期，但是区块链是人类发现的首个可以实现智能合约商业用途的技术。

### 3.4.3　票据理财的守护神——数字化契约

“收益不需要太高，只要安全；模式新不新不重要，只要能够正常运营”这体现了投资人对理财风险的无奈表态。在股市、基金、P2P、股权众筹纷纷不乐观的情况下，一直以“安全”著称的票据理财也出现了诸多意外。

2016 年 1 月 22 日，中国农业银行北京分行买入返售业务发生重大风险事件，这一新闻震惊了全国。

当天，中国农业银行正式发布公告称：“农行北京分行票据买入返售业务发生重大风险事件，经核查，涉及风险金额为 39.15 亿元。本应存放在银行保险柜里的票据，却被某票据中介提前取出，与另外一家银行进行了回购贴现交易，但资金并未回到农行北京分行的账上，而是非法进入了股市，又由于近期 A 股下跌，导致巨额资金缺口无法兑付。”

在之后不到一周的时间里，2016 年 1 月 28 日，中信银行兰州分行也爆出 9 亿～ 10 亿元的票据诈骗事件。

本书在 3.1.4 小节中已经指出，票据业务领域的乱象非常多，除了一票多卖等票据违规交易问题，还包括克隆票、假票、变造票等违规操作问题。票据识别、担保信息不透明、风险高、票据质量差等问题已经成为票据理财的威胁者。中汇在线、农业银行北京分行以及中信银行，都是这些威胁者的牺牲品。随着区块链智能合约的兴起，更多人将票据理财安全的重担寄希望于它的身上。

在票据理财业务中，银行的承兑汇票是安全的基本保障，而最大的风险来自于票据的真假和交易信息的不对称。而区块链智能合约将会保证参与者有能力查看区块链上的各项操作信息。

金银猫运营总监葛雷称：“一旦区块链技术运用到票据理财中，将彻底杜

绝票据理财交易中的票据作假、一票多卖等现象，同时可追踪票据兑付时间及主体，以保证各方的利益。”

当区块链智能合约被运用到票据理财交易中，票据从申请、发行、交易到承兑，整个过程中的所有环节都将被完整记录下来，并且无法篡改。监管部门可以很方便地查询，如果票据被非法占有，区块链智能合约上将显示出票据的转移路径，有利于将其找回。

然而，要实现以上设想，前提是由数字化契约形成数据票据池。票据的发行方、流通方等必须按照区块链智能合约的规则将票据进行登记和数据备份。

从表面上看，区块链智能合约将会解决票据理财的风险敞口，但事实并非如此。区块链本质上只是一种互联网技术，其作用是将票据信用转化为数字信用，并没有改变票据的金融属性。利用区块链智能合约可以降低票据理财的风险，但依然离不开风控。

盈灿咨询数据组组长杨凌驰表示：“目前区块链技术只是一项新的金融工程，我们可以把它想象成是一个公共账簿，拥有为系统数据提供可靠架构、为互联网金融建立信任关系等特点。这样可以在比较大的程度上改善信用问题，但是其依然不能代替风控，至少目前是无法实现的，未来的路依然漫长。”

票据宝 CEO 李华军的观点更加明确，称：“当前的区块链根本不可能运用到票据理财交易中，因为区块链技术在国内金融体系内还没有任何应用，国内当前仍然以纸质商业汇票为主，电子商业汇票只在人民银行大额支付清算系统中流转，数据对外完全是封闭的。”

我们无法否认李华军的观点，但是探索区块链智能合约在票据理财领域的应用依然显得很有必要。对于区块链智能合约应用在票据理财领域后的未来，我们表示期待。

Block chain

# 第4章
# 区块链与数字货币

区块链诞生于比特币，而以比特币为首的数字货币是区块链当前最主要的应用。自从2009年比特币诞生以来，基于区块链技术底层技术的数字货币在全球兴起热潮，并以颠覆世界的姿态冲击着人们对以传统货币为主体的现代金融体系的认知。本章一起了解区块链与数字货币的知识。

practice

## 4.1
# 货币的终极形态——数字货币

对很多中国人来说，手机支付已经成为日常生活不可或缺的一部分。即便是二三四线城市，依靠一部手机也可以完成衣食住行，包括吃饭、打车、看电影、订酒店等。在手机支付过程中，人们使用的货币形态是电子货币。货币就像一种活的生物体，在不同的时代环境下进化和演变出不同的生命形态，从贝壳到黄金白银，再到纸币，再到电子货币，最后到数字货币。尽管当下我们对电子货币已经习以为常，但是纵观整个人类货币体系，我们很有可能已经迎来了货币的终极形态——数字货币。

### 4.1.1 货币自身形态进化论

自人类诞生以来就出现了价值交换，这也是货币自身形态进化的基础。人类历史发生了翻天覆地的变化，除了科技的巨大驱动以外，货币形态的进化也起到了巨大作用。下面一起看货币自身形态进化史。

在原始社会，人们主要以打猎为生，于是产生了最原始的价值交换方式——物物交换。这种交易方式难以满足人们对公平的需求，比如一个人试图用自己饲养的一只羊换另一个人饲养的一头牛。

当人们意识到物物交换烦琐而复杂的时候，作为交易媒介的实物货币开始出现。实物货币诞生的时间是原始社会末期。一般来说，游牧民族以牲畜、兽皮类来实现货币职能，而农业民族以五谷、布帛、农具、陶器、海贝、珠玉等充当最早的实物货币。据考古发掘，新石器晚期遗址陕西西安半坡出土大量陶罐作为殉葬物；大汶口文化遗址殉葬大量猪头和下颌骨。这些殉葬物表明在原始社会后期猪和陶器曾起过货币的职能。

然而，最早充当货币功能的实物流通范围较小，而随后出现的贝壳是流通最为广泛的古代实物货币。因为牛、羊、猪等牲畜充当实物货币不能分割，而五谷的保质期较短，而珠玉又比较稀少，刀铲等农具较为笨重，因此最后的实物货币集中为贝壳。漂亮的贝壳可以用作颈饰，体积小，便于携带与计数，而且还非常坚固耐用，因此在长期商品价值交换中被选为主要货币。作为实物货币，贝壳一直沿用到春秋时期。因此，很多与价值、财富有关的中国汉字都与“贝”字有关，比如财、资、贵、贫、贪、购等。

春秋战国时期的商品经济急速发展，贝壳因为数量有限已经无法满足人们在日常商品价值交换中的使用，于是，金属称量货币开始出现。金属称量货币在流通中需要分割和鉴定成色，使用起来比较麻烦，因此金属铸币逐渐取代了金属称量货币。

政治统一要求经济统一，于是秦统一六国后，秦始皇顺应历史发展趋势，在统一文字、度量衡的同时，也统一了货币。秦始皇规定以“黄金”为上币，以镒（相当于 20 两）为单位，以圆形方孔铜钱为下币，以半两为单位。钱文“半两”的实重为半两，这种圆形方孔的铜钱从此成为中国货币的主要形式，一直沿用两千多年。秦朝的圆形方孔铜钱是世界上最早由政府法定的货币。

金属货币也存在一些问题。动辄好几十斤的金属货币在运输时会耗费很多的时间和精力，于是北宋时出现了纸币。在货币史上，纸币的出现是一个重要转折点，也是人类历史上的一大进步。纸币出现在北宋具有一定的必然性，因为它是社会政治经济高速发展的必然产物。

众所周知，宋代的商品经济空前繁荣，商品的价值交换也异常频繁。频繁的商品交易活动需要用到更多的货币，而当时铜钱短缺，已经远远无法满足流通用量。当时的四川地区通行铁钱，铁钱量重值低，使用起来非常不方便。当时的一个铜钱相当于十个铁钱，一千个铁钱的重量为大钱 25 斤，小钱 13 斤。当时的人如果想要到集市上买一匹布，大概需要铁钱两万，重量为 500 斤，如果没有车根本过不去。

作为宋代的经济重地，成都通往外界的道路异常崎岖难行，客观上需要更为轻便的货币，这就是纸币最早出现在四川的主要原因。另外，尽管北宋是一个高度集权的封建专制国家，但是没有统一的全国货币，而是由几个货币区各自为政，互不通用。当时，4 路专用铁钱（宋代的行政单位），13 路专用铜钱，

陕西、山西则是铜钱、铁钱兼用。而各个货币区都严禁货币外流，纸币的出现正好可以防止铜钱、铁钱外流。

此外，宋朝政府与夏、辽、金的关系紧张，经常受到这三个国家的侵略，于是需要用到大量的军费和赔款开支，这也要求宋朝政府发行纸币来弥补财政赤字。总之，种种原因促成了纸币的产生，而纸币在当时被称作“交子”。一般来说，人们通过钱庄兑换交子。

1688 年，英国发生光荣革命，从此进入君主立宪制。到 1717 年，英国政府建立了事实上的标准化金本位英镑，货币的标准化影响了全球各个国家，也是人类货币史上的重大进步，直接促进了工业革命的发展，使英国成为当时的世界霸主，人称“日不落帝国”。

信息革命爆发后，电子货币出现了。Digicash 公司发明匿名数字货币的技术宣告电子货币诞生。1995 年 10 月，第一家网络银行在美国成立，随后推出各种电子货币。

电子货币的产生和流通使实体货币与观念货币发生分离，解决了经济全球化背景下降低信息成本和交易费用的问题。电子货币突破了空间限制，使信息流、资金流可以通过网络迅速、便捷地传输。总之，电子货币的出现加快了经济全球化，使人们可以更快、更省地处理经济事务。

2008 年，全球经济危机爆发，中本聪在网上发表《比特币：P2P 电子货币系统》论文，描述了比特币的模式，并搭建起比特币体系。之后陆续出现的莱特币、约克币等数字货币的相继出现标志着人类历史进入数字货币时代。

数字货币是货币自身形态进化史的一部分，是数字科技革命的结晶，其诞生具有必然性。回顾人类历史，任何一种新事物从诞生到发展成熟，都会经历质疑乃至排斥。

与传统货币一样，数字货币也将不断发展完善，最终走向成熟，以更适应社会生产力并为人类服务。目前来看，数字货币应当是人类货币的终极形态。

### 4.1.2 数字货币的零通道费用

2014 年 12 月 14 日，“三亚 • 财经国际论坛”在海南省三亚市召开。火币

网创始人兼 CEO 李林作为数字货币的一个从业者，向大家介绍了数字货币近几年的发展状况以及大家对于这个行业的未来预期。

李林称：“人民币和美元本身在国际上两大货币，中国跟美国也是两大经济体，而在数字货币领域，中国和美国依然是两个领头市场。中国目前的主要产业集中在生产环节和货币兑换环节，美国集中在流通以及存储的环节。再看全球范围内主要的经济体，英国美国日本实际上基本政策差不多。美国考虑更多的是如果将其当作商品怎样进行征税，英国更开放一点，认为这个是私人金钱或者私人货币，但日本目前没有这个法规。”

纵观全球，数字货币与 20 世纪 90 年代初互联网行业的发展情况非常像，任何新技术的发展也都会经历这一历程。从新技术的发展曲线来看，数字货币还处于一个很早期的阶段。

那么，数字货币对现有的金融体系会带来什么挑战呢？与法定货币 7% ～ 8% 的通道费用相比，数字货币的通道费用几乎为零。作为一个去中心的低成本通道，数字货币挑战了当前的跨境支付体系。

关于当前的跨境支付体系，本书在 3.1.1 小节中有具体讲述，这里不再赘述。

### 4.1.3　顺应经济全球化趋势的全球流通特性

经济全球化趋势的逐渐加强要求一种具有全球流通特性的货币去进行全球贸易，同时，如果由一个国家发行这种全球流通货币，结果就是极大地增加不同国家之间的交易成本。

假设 A 国的货币充当全球货币，那么，B 国和 C 国进行贸易的时候都必须先向 A 国出口他们所能出口的东西，拿到 A 国货币，然后 B 国和 C 国才能用 A 国货币进行贸易。也就是说，凡是 A 国之外的其他国家进行贸易，都必须先对 A 国进行出口换取货币。在这个假设中，只有 A 国全体国民享受了隐形的货币收益。如果 A 国又发生了通货膨胀，那么 B 国和 C 国付出的成本将更多。

一旦 A 国从全球贸易中获取的收益难以支撑货币成本，那么随着货币使用范围的收缩，全球贸易体系将面临崩溃。更致命的打击是，一旦 A 国之外的另一个国家 D 建立了一个足够齐全的工业门类和巨大规模的工业生产，那