零基础学区块链

全面解密区块链技术原理

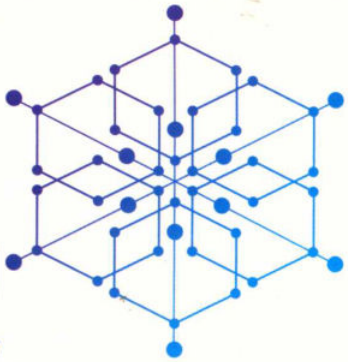
区块链快速入门的必备读物

黄芸芸 蒲军 编著

BLOCKCHAIN PRIMER FOR BEGINNERS

通过生活示例
趣味插图

生动讲解区块链
基础知识



区块链知名技术专家

黄步添 刘振广 陈建海

国内外知名教育学者

张在琛 李易 凌子昂 李超

倾情推荐

清華大學出版社

零基础学区块链

黄芸芸 蒲军 编著

BLOCKCHAIN PRIMER FOR BEGINNERS

清華大學出版社
北京

内 容 简 介

区块链是融合计算机学、密码学、经济学、政治学、博弈论等多学科理论的跨学科技术。本书作为区块链技术的入门科普读物，尽可能涵盖区块链基础知识的各个方面。全书共 9 章，第 1 章通过介绍数字货币的发展历程回顾区块链技术诞生的背景；第 2～7 章是本书的重点，内容涉及区块链核心技术，包括密码学、去中心化及共识机制、分布式网络架构、匿名性，以及基于区块链技术的比特币交易流程、比特币钱包等；第 8 章对中本聪发表的比特币白皮书作了翻译和解读，该白皮书是区块链技术的精华所在；第 9 章分析区块链技术在各个行业的应用前景，同时介绍两个具体的应用案例，旨在抛砖引玉，启发读者思路；最后的附录部分对当前区块链的热门问题作了详细的解答。

图书在版编目(CIP)数据

零基础学区块链/黄芸芸，蒲军编著. —北京：清华大学出版社，2020.1
ISBN 978-7-302-53750-2

Ⅰ. ①零… Ⅱ. ①黄… ②蒲… Ⅲ. ①电子商务－支付方式－基本知识 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字(2019)第 195753 号

责任编辑：文　怡
封面设计：王昭红
责任校对：梁　毅
责任印制：李红英

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
课件下载：http://www.tup.com.cn，010-83470236

印 装 者：三河市君旺印务有限公司
经　　销：全国新华书店
开　　本：186mm×240mm　　**印　　张**：18.75　　**字　　数**：429 千字
版　　次：2020 年 1 月第 1 版　　**印　　次**：2020 年 1 月第1 次印刷
定　　价：69.00 元

产品编号：082558-01

序言
PREFACE

近年来，随着5G应用的推广，物联网、人工智能、虚拟现实/增强现实、自动驾驶等技术实现快速融合发展，我们即将迎来一个智能连接的世界。与此同时，区块链已经全面渗透到各类金融场景，成为金融科技领域的热门话题。区块链与5G的应用看似没有明显的交叉关联，实际上，它将在数据隐私、数据安全以及信任构建等方面发挥重要的作用。

区块链作为一种分布式数据存储、点对点传输、共识机制、加密算法等技术的新型集成应用，具有去中心化、开放透明、防篡改、可追溯和匿名性等特点，而区块链最引人入胜的就是去中心化的信任构建。有了信任，数据可以安全地交换，包括价值。互联网实现了信息的交换，却无法实现价值的点对点直接交换。信息的无限复制破坏了价值的交换，而互联网上泛滥的虚假信息也更加印证了它并非一个可信的网络。价值即货币，所以价值交换一定要建立在信任的基础上，信任意味着共识的达成。在传统模式下，共识的达成需要有中心平台的协助和信用背书，而中心平台固有的弊端促使人们思考是否可以从技术层面实现去中心化来达成共识。计算机领域一直都在致力于研究去中心化的分布式系统，核心就是去中心化共识的问题。虽然应运而生了各类算法，但是在一个复杂的分布式网络系统中，由于存在网络时延、网络信道变化、网络节点性能差异以及行为的不确定性，节点之间达成共识仍然相当困难。直到中本聪提出让网络各个节点按照既定的运算规则来计算哈希值，由获胜节点主张上链数据，其他节点对主张的数据进行投票，同时巧妙地把经济激励应用到共识上，节点为了获得经济奖励而遵守规则，自此，分布式网络才得以自发对数据达成共识。这就是区块链所采用的一种全新的共识机制，它完全不依赖于中心平台。

当经济行为融入到网络共识中，人们惊喜地发现区块链就是一种价值在互联网传播的方法，它使得价值互联网的实现成为可能。价值互联网不是对现有信息互联网的替代，而是一种高阶的互联网形式，是在信息互联网的基础之上，实现数字化资产的互联互通，这样的价值传递就像信息传递一样快捷方便、安全可靠且成本低。可以预见，未来将逐渐形成一个集信息传递和价值传递为一体的新型互联网模式。

区块链将推动数字经济的更大范围发展，使得数据成为关键的生产要素，同时会改变资产的存储和交易形式。特别是产业区块链时代已经来临，行业机构间将走向更加开放的发展模式，协同合作将更加紧密，也必将进一步推动信息互联网走向真正的价值互联网。

本书围绕比特币系统的运行机制，深入浅出地解读区块链基础知识。比特币作为区块

链技术诞生的载体，是区块链技术的起源和具体表现形态，后续区块链技术的发展和演进都是基于以比特币为代表的区块链技术进行的。因此，要全面了解区块链技术，就要从比特币的区块链技术开始。

最后，衷心地祝愿本书能引领更多的读者走进区块链世界！

黄步添

云象区块链创始人，中国区块链技术早期推动者

2019 年 11 月

前言
FOREWORD

区块链，对于大众是一个新鲜而又陌生的词语，但其第一个应用载体——比特币，在投资领域可谓家喻户晓。十年前，比特币横空出世，其价值从诞生时的一文不值一路上涨，到最高峰时每枚接近两万美元，而后开始“跌跌不休”，最低谷时甚至跌破 4000 美元，直到 2019 年 6 月才重回一万美元大关。这期间的过程犹如过山车，时而一飞冲天，时而俯冲直下，不断地刺激着投资者的神经。随着比特币被越来越多的人所认识和接受，其底层技术——区块链，渐渐浮出了水面。

在区块链被国内大众所认识的这几年，很多企业打着区块链的旗号四处融资，甚至在没有具体产品形态的情况下就进行 ICO（Initial Coin Offering，首次币发行，是一种为加密数字货币或区块链项目集措资金的方式），最后由于没有相关的落地应用而被市场抛弃，投资者的钱打了水漂，导致很多人认为区块链行业就是一个骗局。历史证明，真正的金子都是被风浪冲刷出来的。随着时间的推移，不好的东西必定会被剔除，而好的东西终将闪耀于世。大浪淘沙终有尽，我们不能因为曾经有很多人或机构利用区块链的噱头来坑蒙拐骗，就推测区块链技术一无是处，笃定从事区块链行业的人都是骗子。大破之后必有大立，真正好的技术必定有它的应用需求。

当前区块链已经上升至国家战略高度。2018 年 5 月 28 日，习近平总书记在两院院士大会上作了重要讲话，提到“以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”，这是“区块链”第一次出现在国家最高领导人的讲话中，肯定了区块链技术是新一代信息技术的代表之一，为区块链在中国的发展指明了方向。2019 年 10 月 30 日，国家发展和改革委员会修订发布了《产生结构调整指导目录（2019 年本）》，在鼓励类“信息产业”中增加了“大数据、云计算、信息技术服务及国家允许范围内的区块链信息服务”。由此可见，国家对区块链持积极和开放的态度，鼓励社会各界对区块链的商业应用进行探索。目前各地政府、科研机构和企业已投入大量的人力物力开展落地研究，由此催生出了无数的商业想法和应用，涉及金融、制造业、运输业、农业和医疗等各个领域。

这本书讲了什么

本书作为初学者学习区块链技术的入门读物，尽可能用通俗易懂的语言，从小白的角度围绕其第一个成功应用——比特币展开讨论，在内容上尽量涵盖区块链技术基础知识的各个方面。

本书主要回答了五个方面的问题：

第一，为什么出现区块链技术？本书从货币的发展历程来探讨区块链技术如何满足金融领域的现实需求，进而全面阐述区块链技术的重要性。

第二，比特币中的区块链技术是什么？本书全面介绍了区块链的核心技术，包括密码学、去中心化及共识机制、分布式网络架构等。

第三，基于区块链技术的数字货币交易流程是什么？本书介绍了比特币的交易流程、交易结构、交易脚本等。

第四，区块链技术诞生时的形态是怎样的？本书对中本聪发表的比特币白皮书进行了翻译和详细的解读，让读者了解区块链技术的起源和精华。

第五，区块链技术未来的发展趋势是什么？本书结合区块链技术在各行各业的应用前景，详细分析了区块链技术发展趋势和落地实施的方向。

本书第 1 章、第 3 章、第 4 章、第 6 章和第 8 章由黄芸芸编写，第 2 章、第 5 章、第 7 章、第 9 章和附录由蒲军编写。书中未详细讲解当今前沿的区块链技术，比如以太坊和 EOS (Enterprise Operation System，为商用分布式应用设计的一种区块链操作系统)，感兴趣的读者可以在了解区块链原理的基础上自行阅读相关书籍和资料。

如何阅读本书

区块链涉及的学科众多，包含但不限于密码学、经济学、计算机学。本书作为区块链领域的科普读物，更偏重于区块链技术方面的介绍，适合对区块链技术感兴趣的初学者，具有理工科背景的读者更容易理解本书内容。建议读者在通读本书一遍之后，选择感兴趣的章节精读，推荐辅以查阅维基百科。此外，研究中本聪在密码学邮件组与其他人的往来邮件也是一个很好的区块链技术入门辅助途径，帮助读者从本源了解创造者的设计思想，以及比特币从孱弱到健壮的过程。

研究区块链技术就像下棋，需要有严密的逻辑思维。区块链技术本身并没有高深的数学理论，但是它的底层设计极其精密，包括工作量证明机制、数字签名机制、奖励机制、交易模型、防攻击篡改机制等在内的各个模型之间都有关联。希望读者通过阅读本书能够充分领会区块链严谨而巧妙的设计理念。

为什么要写这本书

通往比特币的道路并不是一帆风顺的，比特币的成功得益于其发明者中本聪强大的信念支撑。中本聪作为密码朋克的成员，实现了第一个去中心化的数字货币，颠覆了人们对货币的认知。密码朋克信奉自由主义，认为没有政府干预或者极少干预能让社会变得更好。中本聪从 2007 年开始着手研究去中心化的数字货币，历经一年左右的时间，在密码学邮件组公开发表比特币白皮书，标志着区块链的诞生。对于区块链，一直以来都有一群虔诚的人因热爱和信念而坚守它，并为其技术的成熟和落地而奋斗着。终有一天，区块链将服务于人类社会并改变人们的生活。抱着对区块链这一领域的好奇心，笔者走上了研究区块链的

道路。

目前国内有关区块链技术的书籍多是译著。南京大学周志华教授在《机器学习》一书中提到“中文书当然要国人自己来写”，笔者对这句话很有共鸣。因为译著经过一道翻译的工序，需要译者对其中的知识点尤为理解，对译者的英文水平和专业知识要求都很高，稍有偏差可能会引起读者百思不得其解。笔者查阅了目前市面上介绍区块链的书籍，大多是金融方面以及应用前景的宏观介绍，单纯介绍区块链技术的书籍很少，而这些书中译著又占了很大的比例，这让笔者萌生了写书的想法，帮助初学者迅速掌握区块链核心技术。

写书的感触

笔者入门区块链较晚，但是区块链颠覆性的设计思路引起了笔者浓厚的兴趣。俗话说，种一棵树最好的时间是十年前，其次是现在，于是笔者踏上了研究区块链的征途。从最初接触区块链，到理解其原理，再到用通俗易懂的文字将其呈现在读者面前，这期间，有困惑，有迷茫，特别是有些知识点理解起来很别扭，其核心与跳拉丁舞颇为类似——“拧巴”，这在比特币的交易中尤为明显，但无论如何，重要的是接受这个学习的过程，并迎难而上。研究越深入，越能发现很多细微的问题，而后再去解决它们，就能拨开迷雾看区块链，这个曾经的庞然大物变得越来越清晰，笔者经常感觉到“柳暗花明又一村”；对于不同的知识点，“横看成岭侧成峰，远近高低各不同”；当研究到更深层次时，又是“会当凌绝顶，一览众山小”，最终体会到区块链的博大精深。新世界的游戏规则，只要你参与其中并认识它们，就会发现无穷无尽的乐趣。当你翻山越岭跋山涉水，到达自由的彼岸时，将看到另一番新奇的景象，这是中本聪和众多密码朋克社区的信念坚持者们在很多前人设计数字货币失败的基础上，创造出的一个全新的世界。

区块链的很多思想甚至可以上升到哲学，比如折中妥协。所谓鱼和熊掌不可兼得，如果要把去中心化做到极致，必须牺牲包含处理时延在内的其他性能。区块链正是因为在数字货币的发展史上找到了一个完美的平衡点，才得以蓬勃发展。相信读者学习研究区块链的过程，也是人生进阶的过程。

在本书的编写过程中，笔者本着严谨的治学态度，小到一个词都会反复斟酌，做到精益求精；对于模糊的概念，查看国内外相关文献，力求准确无误。但是，区块链技术是一门融合了很多技术的集大成者，各个知识点内容交织缠绕，它们之间有着千丝万缕的联系，要把每一个独立章节介绍清楚，难免会略显啰嗦。但是笔者认为，宁愿啰嗦一点，也要将其以最清晰的表达方式呈现在读者面前。另外，将复杂深奥的区块链知识用通俗的文字表达出来，需要在严谨和易懂之间找到平衡，这着实是一门学问，用“绞尽脑汁”这个词一点也不夸张。为了不那么晦涩难懂，笔者在书中用了很多的图表和日常生活中的例子，希望助于读者理解。达芬奇说过一句话：“Simplicity is the ultimate form of sophistication(简单就是终极的复杂)”。衷心地希望读者能通过本书进入美妙的区块链世界，将书“越看越薄”，最后达到心中无剑(书)的至高境界。

写书耗费了笔者工作之余大量的闲暇时间，但屡屡听到垂髫犬女蹦出“区块链交易无法篡改”“区块链就是很多区块组成的链条”之类的话语，让笔者在蓦然惊喜的同时，因能为小女提供这样的家庭学习氛围而感到欣慰，也更加有了写作的动力。

勘误和支持

区块链是一门跨学科技术，笔者才疏学浅，加之时间和精力有限，只是利用工作之余的时间研究，自认为不能准确掌握其方方面面，书中错谬之处在所难免，翻译的英文文献也不尽准确，敬请广大读者朋友批评指正。

比特币刚诞生时，与其他新生事物一样不可避免地存在很多缺陷，比如在早期版本中允许支付者发送无效交易，支付者可以在该交易中创建新的比特币，这个重大缺陷直到2010年7月29日才得以解决并修复至版本0.3.6，而问题修复时，已经产生了几百万枚无效比特币，后来全部被清除出区块链。不可否认，比特币的成功得益于中本聪在密码学邮件组中公开了源码，很多人基于此提出了宝贵意见，让比特币变得健壮。笔者衷心期望本书亦能如此，得到读者们的反馈，后续不断进行完善，使之成为一本受欢迎的区块链入门科普书。

致谢

写书期间，周边可求教的专家很少，笔者经历了很多的困惑，花费了大量的精力，可谓举步维艰。此书的成稿得到了很多老师和朋友的帮助，笔者表示由衷的感谢！

感谢笔者的导师、东南大学信息科学与工程学院执行院长张在琛教授，正是张老师推荐的《区块链技术驱动金融——数字货币与智能合约技术》一书，将笔者领入区块链这一全新的技术领域。张老师对区块链的真知灼见让笔者坚信区块链是值得深入研究的技术，写书期间也屡屡得到张老师的指导和鼓励，与张老师的交流经常有“听君一席话，胜读十年书”的感觉，给了笔者很大的信心和动力。

感谢云象区块链创始人黄步添先生在繁忙的工作之余抽出宝贵的时间为本书作序；感谢浙江工商大学计算机与信息工程学院正高研究员刘振广先生和浙江大学计算机学院智能计算 & 系统实验室区块链负责人陈建海先生两位技术专家为本书提出宝贵意见；此外还要感谢美国约翰·霍普金斯大学李易助理教授、浙江大学区块链协会发起人、浙江大学客座讲师凌子昂先生、河海大学李超副教授等专家对本书的编写给予的大力支持。

感谢笔者的高中数学老师余晓地老师，正是余老师当年的教学，让笔者对数学的热爱保持至今，区块链的学习多处用到数学知识，帮助很大。余老师学识渊博，执教三十年，桃李满天下，如今年逾古稀仍对新鲜事物保有好奇心，坚持学习，笔耕不辍，使笔者深受感染。

感谢笔者的父母，正是他们在笔者儿时创造的求知上进的家庭环境，让笔者长大后能够力学不倦，在工作之余研究新兴技术，完成书稿。

感谢清华大学出版社编辑文怡，他的专业和敬业令笔者由衷钦佩。在此也对所有为本书付出心血的清华大学出版社的工作人员表示诚挚的谢意。

在完成本书的过程中笔者参阅了大量的文献，其中包括书籍、学术论文、区块链技术报

告以及国内外的区块链论坛等，特别参考了中本聪的比特币白皮书、东南大学出版社出版的《精通比特币（影印版）》（第2版）、林华先生主译的《区块链——通往资产数字化之路》和《区块链技术驱动金融——数字货币与智能合约技术》以及中央财经大学朱建明教授等编著的《区块链技术与应用》。对于这些研究区块链的先驱者，笔者在这里致以崇高的敬意。书中注明的参考文献仅仅是获得相关资料的文献，没有一一列出所有的参考文献，部分引用和举例已经很难查证原始出处，在此对原作者表示衷心的歉意和谢意。

写在最后

生活在南京，每次路过南京大屠杀纪念馆，看到来自全国各地的青少年接受爱国主义教育时，不禁想起日本右翼分子试图歪曲历史，美化其侵略战争。如果区块链技术早一百年出现，那么这段侵略历史就能被永久地记录在区块链里且无法篡改，否认历史将成为全人类最大的笑话！

黄芸芸

2019年11月，南京

目录

CONTENTS

数字货币概述

比特币、以太币、莱特币等数字货币，是当今世界货币领域最热门的话题，也是“币圈”[①]众多人士研究和投资的对象。随着比特币的兴起，区块链技术公之于众。纵观数字货币的发展历程，基于区块链技术的数字货币的成功是必然的而非偶然的。区块链作为其底层技术，它的发展和其他任何新生事物一样，经历过很多失败的尝试，最终走到了今天。本章从介绍货币金融体系的发展开始，带大家了解数字货币的起源，以及比特币应运而生的背景和趋势，最后介绍数字货币的技术基础——区块链的基础架构及技术现状。

1.1 货币金融体系的发展

众所周知，货币是商品交换的媒介，用于物品交换。在原始社会，人们的生活通常能自给自足，包括狩猎、摘果子充饥等，没有太多从别人那里获取物品的需求。但我们可不能小瞧原始人，他们的很多技能是现代人类所不具备的，比如原始人的耳朵非常灵敏，当危险动物靠近时能及时察觉并逃生，这些技能随着人类的进化而逐渐退化了。原始人练就了一身本领，自身或者群体能满足最基本的生活需求。那时人的欲望也很低，面对各种危险，能生存下来就是最大的幸运，不会像现代人有太多的欲望，还有逛街购物、看电影、旅游、娱乐消遣等。所以，对于实物，基本是你有的我也有，大家自得其乐，即使偶尔有几个零星的交易，比如用我的羊去换你的牛，也可以直接通过物物交换来满足双方需求，如图 1-1 所示。

随着人类社会的发展，产生了社会分工，有的群体专门狩猎，有的群体专门织布，物物交换的弊端日渐凸显：交易双方必须在同一时间完成交易，交易的物品都是对方所需要的，并且交易物品的价值要大致相当。假如张三需要一匹布，想拿自己的一头牛和李四换布，但李四想要的是羊而不是牛，于是李四不愿意和张三交换；或者张三觉得自己的一头牛可以换两只羊，但是李四觉得一头牛只能换自己的一只羊，于是物物交换已经不能满足

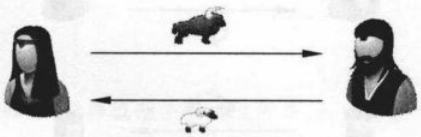


图 1-1 物物交换

① 币圈：由数字货币玩家自然形成的圈子，玩家通过投资数字货币来获利。

人们多样化的需求，如图 1-2 所示。

图 1-2　物物交换的弊端

鉴于此，人们逐渐想出用某种具体的交换双方都能接受的特殊物品作为中介，先用自己富余的物品兑换一定数量的特殊物品，当自己缺少某些物品时，再使用该特殊物品换取所需的物品。这种作为中介的特殊物品就是我们所说的货币。

几千年前人类开始使用货币。货币的形式有很多种，最开始的货币是实物，通过实物货币完成所需物品交换，比如我国夏商时代的天然海贝，是我国最早出现的货币，那时大家都拿自己的物品换天然海贝作为保存财富的手段，或者拿天然海贝换物品，当时的天然海贝就相当于我们今天的纸币，如图 1-3 所示。

随着交易范围的日渐扩大，人们对货币的要求不再局限于交换，还需要方便储存和携带、价值稳定、易于分割、不易消耗磨损等。试想，夏商时代的富豪们都要用一个大仓库储存海贝，出门时备着几车海贝消费，那得多麻烦。人类是聪明的，随着经济的不断发展，各种形式的实物货币逐渐被金属货币所代替，比如金、银、铜。相较于形形色色的实物货币，金属货币有很多优势，比如贵金属产量少、价值稳定，同时易于分割，便于保存。现在我们在博物馆看到的古人使用的黄金、白银、铜钱等，都是金属货币在发展过程中逐渐演变而来的，如图 1-4 所示。

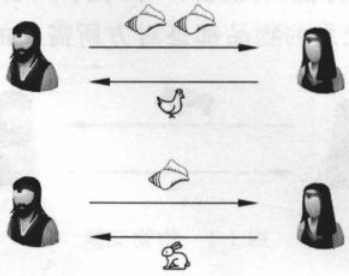


图 1-3　海贝充当货币

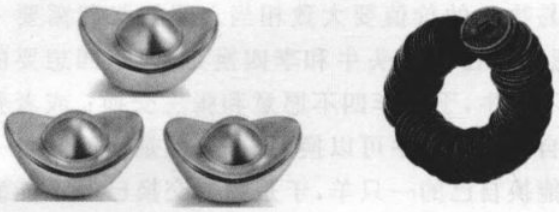


图 1-4　金属货币(金元宝和铜钱)

虽然金属货币有诸多优势，但它的缺点也很明显，例如携带不便且容易磨损。古代进京赶考的学子们，特别是来自巴蜀或闽粤的学子，一般都要提前动身赶赴京城，这一路的跋涉和车马劳顿，总得要带够盘缠[①]，万一这一期科举不中，也许还要留在京城住个三年五载等待下一期的科举，所以需要随身携带够三五年花销的银两。这些银两不但不便于携带，搞不好无意中露财还容易被劫匪打劫。渐渐地，纸币出现了。中国最早出现的纸币叫“交子”，发行于北宋仁宗天圣元年，它作为官方法定货币在四川境内流通了近 80 年，被认为是世界上最早使用的纸币，如图 1-5 所示。

图 1-5　交子

纸币可以理解为一种价值符号[②]，由国家政府委托本国央行设计、印制和发行，由国家权威信用背书，如图 1-6 所示。纸币和不足值铸币[③]的发行、流通和回笼，都属于传统货币金融体系。私自印制的纸币是无法流通的，因为它与国家发行的纸币相比，不具有同等的货币购买力。各国一般根据经济发展的需要决定纸币发行量，并对其实行严格的管理，称为“有管理的通货制度”。

图 1-6　国家央行管理纸币

随着互联网的发展，人们逐渐习惯于使用 POS 机刷卡消费来代替现金支付。银联卡、信用卡等各种卡片在市场上占据了重要的位置，如图 1-7 所示。这些卡片本身并不是传统货币，但从刷卡消费行为我们可以看到，卡片是货币的载体，我们真正关心的是卡片所关联的银行账户里的资金总额。《纽约时报》网络版曾报道瑞典这个国家正迅速迈入“无现金

① 古代人们出远门要带上笨重的成串铜钱，把铜钱盘起来缠绕在腰间，这样既便于携带又安全，所以将这又“盘”又“缠”的路费称为“盘缠”。

② 价值符号又称货币符号，它可以代替金属货币发挥流通手段职能。最早的价值符号是不足值的铸币。

③ 不足值铸币：国家铸造的具有一定形状、重量、成色和面值的金属货币，被视为铸币。铸币最初具有十足的价值，但由于在流通中会有磨损，导致实际重量与名义重量不一致，所以就逐渐发展为不足值铸币，即使重量减轻仍能按名义价值使用。

社会”[①]，无论是街头商贩还是商店餐厅，都觉得现金已经过时，政府允许它们拒收现金，鼓励通过手机支付软件、信用卡等电子支付方式完成交易，很多银行也不再提供现金服务。截至2015年12月，瑞典现金使用比例仅占2%，而美国是7.7%，欧元区是10%。这种以卡片为代表的电子货币有很多优势，比如我们不用担心卡片损坏，如果损坏只需携带身份证去银行重新办一张，卡片所关联账户里的钱不会损失；万一不小心弄丢了卡片或者卡片不慎被盗，也不用担心，只要之前设置了支付密码，对方不知道密码的前提下，无法盗用里面的钱，但现金一旦丢失或被盗，就很难再找回了；如果你出国旅游，也可以使用卡片消费，银行之间会自动根据实时汇率进行结算，而不必提前去银行兑换大量的外币。从这几点来看，卡片比现金更受大家的青睐。

随着移动互联网的兴起，以支付宝和微信支付为代表的第三方[②]支付方式方兴未艾，如图1-8所示。现在人们出门只需要携带手机，通过第三方支付方式进行交易，连卡片都不需要了。这种支付方式逐渐替代纸币和卡片，推动中国的无现金化发展。同时，网络购物的兴起也得益于第三方支付方式的发展壮大。第三方支付方式意味着买家和卖家之间通过中介渠道进行交易支付，双方在第三方公司开设账户，交易支付就可以通过第三方公司完成。支付宝最早从淘宝网推出，近几年已逐渐发展为网络支付的主要手段之一。截至2018年9月30日，支付宝国内年度活跃用户已超过7亿，日均交易量超过5亿笔，其在全国移动支付市场上占据的份额高达53%，目前通过支付宝付款的方式已经遍及国内各大城市的公交车、地铁、医院、商场等。

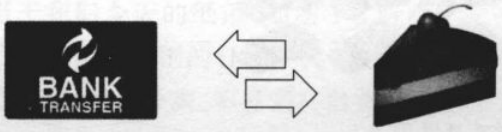


图1-7　刷卡消费

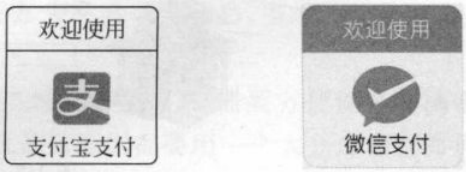


图1-8　支付宝和微信支付

这种第三方支付方式虽然给人们的生活带来了便捷，但弊端也很明显。2017年年底，某第三方支付平台年度账单侵犯用户隐私事件曾一度引起热议，如图1-9所示。当时的微信朋友圈被“2017年年度账单”和“2018年关键词预测”刷爆屏，该支付平台在账单总结分类的基础上，多了很多个性化的标签，如“才华”“颜值正义”等，很是吸引人们眼球，也非常符合大众晒朋友圈的心理。在文字渲染的最下方有一行不起眼的小字，默认勾选同意《服务协议》，大部分人没有注意到，即使注意了也没有深究这份协议的内容。实际上，这份协议与查

① “无现金社会”是指以非现金支付方式取代现金支付，使得刷卡支付、移动支付等“无现金”支付方式成为主流支付方式的社会。

② 第三方可以是发行银行卡或信用卡的银行本身，也可以是除银行以外的具有良好信誉和技术能力的机构。这里的第三方特指后一种。