比特币入门

为什么比特币对你的自由、财务和未来至关重要

蒂米·阿吉博伊 | 路易斯·布埃纳文图拉
亚历克斯·格拉德斯坦 | 刘莉莉
亚历山大·劳埃德 | 亚历杭德罗·马查多
吉米·宋 | 艾琳娜·弗拉诺娃
著

熊越 | 万卉
译

前言

我们是社会活动家、教育家、创业者、企业高管、投资者和研究者。我们来自非洲、亚洲、欧洲、北美和南美。我们在许多方面有所不同，但都痴迷于比特币的一切. 我们相信它将对我们的世界和我们的生活产生至关重要的影响。

在 2019 年 3 月，吉米与我们中的一些人讨论了做一次写书冲刺的想法，我们将在一个与世隔绝的地方待上几天，写一本关于比特币及其对社会的重要性的书。两个月后，在奥斯陆自由论坛上，我们聚在挪威的一个屋顶上，周围是来自各大洲的人权活动家和记者们激动的嘈杂。谈话不可避免地转向了比特币及其改变世界的可能性。亚历克斯鼓励大家写一本书来解释比特币为什么重要，而不使用在此类书籍中常见的技术黑话。我们想帮助感兴趣的人理解我们这个时代最深刻的创新之一和它对人们的影响。几个月后，我们八个人在加利福尼亚的一所房子里相遇，使这个想法成为现实。

你现在拿着的是这我们四天集中努力的结果。本书的目的是帮助你理解为什么今天的货币体系存在问题，为什么有人发明了比特币来提供一种替代选项，它将如何改变政治和社会，以及它对未来意味着什么。

我们真诚地希望，当你阅读本书时，你将会像我们一样对比特币的力量感到震惊。

2019 年 8 月 8 日

加州红木城

关于作者

蒂米·阿吉博伊（Timi Ajiboye）是位于尼日利亚拉各斯的软件开发者和企业家。他共同创立并运营 BuyCoins（buycoins.africa），这是一种让非洲人可以用当地货币轻松买卖比特币的交易所。推特：@timigod

路易斯·布埃纳文图拉（Luis Buenaventura）是 BloomX（bloom.solutions）的联合创始人，BloomX 是菲律宾的一家初创公司，为新兴世界带来安全的加密货币交易。作为一位多产的演讲者和作家，他也是 Cryptopop.net 的创始人，这是一项使主流社会更容易理解加密货币的艺术计划。推特：@helloluis

亚历克斯·格拉德斯坦（Alex Gladstein）是人权基金会（hrf.org）的首席战略官，该基金会是一个促进公民自由并挑战全世界威权主义的非营利组织。他也为奇点大学（Singularity University）讲授比特币和治理，并在《时代周刊》（TIME）、美国有线电视新闻网（CNN）和《比特币杂志》（Bitcoin Magazine）等媒体渠道上撰写技术与自由的交叉。推特：@gladstein

刘莉莉（Lily Liu）是一位投资者和企业家。最近，她是 Earn.com 的联合创始人兼首席财务官，这是一个允许你在空闲时间赚取比特币的平台，该平台于 2018 年被出售给 Coinbase。在此之前，她在中国建立了一家医院，在 KKR 和麦肯锡工作，并在斯坦福和哈佛大学学习。推特：@calilyliu

亚历山大·劳埃德（Alexander Lloyd）自 1998 年以来一直投资于早期创业公司，2008 年他创立了加速器风投（Accelerator Ventures）。他的第一份工作是高盛（Goldman Sachs）的货币交易。2016 年，他加入了人权基金会董事会，专注于朝鲜。推特：@alex01

亚历杭德罗•马查多 （ Alejandro Machado）是开放货币计划（openmoneyinitiative.org）的创始人，该计划是一项研究人们如何在封闭经济体和瘫痪货币体系中使用货币的非盈利组织。他专注于改善委内瑞拉人获得数字货币的机会。推特：@alegw

吉米•宋（Jimmy Song）是比特币的开发者、教育家和企业家。他是 O'Reilly 出版的《编码比特币》（Programming Bitcoin）（programmingbitcoin.com）的作者 。他专注于为世界带来健全货币。吉米的牛仔帽颜色表明了他计划友善一点还是刻薄一点。他的 PGP 指纹是 C1D7 97BE 7D10 5291 228C D70C FAA6 17E3 2679 E455。推特：@jimmysong

艾琳娜•弗拉诺娃（Alena Vranova）自 2003 年以来，建立了成功的金融服务业务。在过去的 7 年里，她一直在帮助个人和小企业用非托管产品和服务保护他们的比特币。2013 年，她推出了第一款比特币硬件钱包 Trezor，她目前负责 Casa（keys.casa）的战略，让每个人都能获得个人比特币安全和金融主权。推特：@AlenaSatoshi

作者们在第 3 天的写书冲刺。

第一章
今天的货币出了什么问题？

这一年是 1981 年。

在马尼拉，在十年来第一次正式取消军事管制几个月后，一对年轻的菲律宾夫妇欢迎他们的第一个孩子进入这个世界。独裁者费迪南德·马科斯将继续执政几年，但就目前而言，路易斯的父母只关心他们年轻家庭的幸福。他们有一个小额的储蓄账户，并且已经开始认真地第一次存入资金，为未来动荡的岁月做好准备。汇率是 7 菲律宾比索兑 1 美元。

这一年是 1993 年。

在拉各斯，尼日利亚将军萨尼·阿巴查（Sani Abacha）夺取政权并将 1 美元固定在 22 尼日利亚奈拉（naira）。这是一个激进的举动，试图通过阻止奈拉进一步贬值来稳定经济。固定汇率让地下经济蓬勃发展，在这里奈拉的交易价值低得多。在阿巴查于 1998 年去世时，美元在黑市上的交易价格高达 88 奈拉，是官方汇率的四倍。数百万人受苦，因为拿着固定政府工资的他们再也无力承担不断上涨的食品价格。

这一年是 2018 年。

在委内瑞拉千疮百孔的边界，许多委内瑞拉公民在这里尝试进入邻国哥伦比亚和巴西，以此来逃离该国破纪录的 400000％恶性通胀。超过 300 万人已经通过这个方式摆脱了毁灭性的饥饿和社会崩溃。

48 岁的面包师罗蕾娜做出了逃进哥伦比亚的艰难决定。在边境，警卫搜查她的财物，试图没收她的贵重物品。他们一无所获。他们并不知道罗蕾娜事先花了几个小时小心翼翼地将美元钞票绕在发夹上

并将它们隐藏在精心编织的辫子中。她走进了一个新的国家，高昂着头。

在马尼拉，路易斯的父母运气非常糟糕。汇率现在是 50 菲律宾比索兑 1 美元，他们多年来的耐心储蓄结果是他们的财富总体损失超过 80%。随着退休迫在眉睫，他们别无选择，只能为了一个无情的、不可预测的未来继续工作和储蓄。

在拉各斯，奈拉在短短几年内在兑美元汇率再次下跌 50%之后处于相对稳定的短暂时期。当地商品价格再次飙升。没有人相信政府可以阻止另一场经济危机，甚至连政府官员自己都不会相信。

这一年是 2019 年。

在奥克兰，亚历克斯走进一家宠物商店购买狗粮。他找到了他在找的东西，以及一个有趣的新产品，一个有望让他的狗身上味道更好闻的产品。他刷了摩根大通的 Visa 卡来买单并走出商店。几分钟之后，他查看了推特，一个和他刚买的狗护理产品一样的广告弹了出来。他发现摩根正在在分享他和第三方公司日常付款的交易信息。

亚历克斯意识到，他的个人生活细节正在被移交给广告商，智能手机一代对这种令人不安的感觉再熟悉不过了。即使在美国，金融隐私也在消失。

这些都是我们现在用的 “钱” 出了什么问题的故事。

路易斯的父母以及菲律宾和尼日利亚中产阶级的数百万人都眼看着他们的储蓄在一代人中慢慢消失。罗蕾娜需要一种方法将她微薄的积蓄带到哥伦比亚的新家而不被没收，所以她在她的发型上花了一番功夫。

这些案例并非个案。

自 2000 年以来，几乎所有通货都对美元汇率损失惨重。许多通货，如南非兰特、阿根廷比索、土耳其里拉和捷克克朗，已经损失了近 50％。像乌克兰格里夫纳和多米尼加比索这样的不幸少数通货失去了多达 70％。在那个时候，即使是美元和欧元也损失了 33％的购买力。

在世界各地，有 2.5 亿移民和难民努力将他们的钱汇回家或带着它到新的边境。大约 20 亿人无法获得银行账户或缺少获得银行账户所需的官方身份证明。在一个日益全球化的世界中，资金仍然顽固地保留这地方的局限性。

与此同时，在上海和旧金山这样的超级城市里，被人监控和密切关注的不安之感是显而易见的。一方面，老大哥在看着你。另一方面，监控资本主义（surveillance capitalism）会跟踪每一次购买行为，并在未经购买者许可的情况下将数据出售给数十家公司。隐私现在是一种奢侈品，其价格似乎越来越高。

什么是货币？

归根到底，货币是一种社会协议。

货币要求人们相信他们钱包里的账单，他们银行账户里的数字以及他们礼品卡里的余额都可以在未来兑换成他们想要或需要的东西. 卖方需要同意买方的钱是有价值的。

纵观历史，社会已经尝试了各种方式来执行这项协议，使用了从贝壳、盐和黄金，到今天在用的复杂的央行系统。某些货币比其他货币更健全，这意味着随着时间的推移，它们更好地保留了自己的价值。

每个人都知道货币很重要，他们希望拥有尽可能最健全的货币。因为大多数人都在用他们的劳动力交换货币，它代表了一个人的时间和努力。货币是劳动力在当前和未来转化为商品和服务的媒介。从这个意义上说，获得健全的货币是最持久，强大的个体能力之一。

货币对政府来说也很重要。因为今天的经济是由国家来组织的，政府拥有控制货币的权力。然而，对货币的控制可能是一种会被滥用的诱人之物。官员经常操纵这种权力来满足他们的利益。只有保护个人权利、权力分立和法治的最民主的政府，才能有效防范货币滥用，如失控的通胀、任意没收以及腐败。

现代货币如何运作？

今天流通的所有国家货币都被称为法定货币（fiat，拉丁语“法令”）。这些货币的价值由发布和接受它们的国家来规定。由于政府可以用很低的成本创造更多的法定货币，因此，可以在任何时候无限地印出新的货币单位。

美联储前主席艾伦·格林斯潘（Alan Greenspan）曾说，美国可以“偿还任何债务，因为我们总是可以通过印钞来实现这一目标。”即使在世界上最稳定的经济体中，这种做法也会引发问题。最古老的国家货币是英国的英镑，在过去的 300 年里，它已经失去了 99.5％的购买力。在上个世纪，美元已经失去了 90％的购买力。1925 年的牛排价格为 0.36 美元，在 20 世纪 90 年代为 3 美元，今天的价格为 12 美元。这些是迄今为止最稳定的法定货币。普通法定货币的寿命仅为 27 年。

低而稳定的通胀是现代央行的目标，并且根据国家的不同而取得了几个不同的成功时期。然而，大多数货币长期遭受高通胀，这可能对储蓄造成破坏性影响。对于那些无力承担硬性资产（如房地产或蓝筹股，其价值随着通胀而上升）的人来说尤其如此。高通胀可能使除了富人之外的所有人都难以为未来储蓄。

对于生活在专制政权下的数十亿人来说，由于未经选举的政府官员的决定，他们的储蓄价值会减少。只有精英才能获得美元、黄金或房地产来保值。与此同时，富裕民主国家的公民享有一些重要的保护。他们可以轻松获得相对稳定的货币，如美元或欧元。他们的经济往往表现良好，因此他们更有可能找到一份随时间推移而报酬更丰厚的工作。他们还可以获得一系列投资产品，以抵消或超过通胀。

精英不成比例地受益于新印的钱，这种影响是如此的普遍，以至于有一个术语来描述它：坎蒂隆效应。它以 18 世纪经济学家理查德·坎蒂隆（Richard Cantillon）的名字命名，作为一位在英国的银

行家，他在工作期间注意到了这种影响。急剧的或大规模的通胀可能是一种不公平的财富分配方式，因为它不可避免地以牺牲穷人的利益为代价来造福已有的财富。虽然它对英美普通人的影响可能并不明显，但在经济不那么稳定的国家，数十亿公民痛苦地感受到这种影响。

法定货币体系也是现代长期战争的推动者。政府可以为战争印更多的钱，通过通胀把成本分摊在后代身上。这意味着更长、更昂贵的战争。第一次世界大战是一个悲剧性的例子，因为主要行动者用通胀为战争的后期阶段提供了资金。俄罗斯和德国均暂停了*金本位*，在金本位下法定货币可兑换为固定数量的黄金。相反，他们暂停了兑换并印出没有黄金支撑的钱来继续战斗。结果，战争最终持续的时间比任何人想象的都要长。德国战败后，他们能够支付巨额赔款的唯一方法就是印更多的钱。到 1923 年，德国马克贬值到其战前价值的万亿分之一，为第二次世界大战奠定了基础。

近期也有类似的政府挥霍性支出。无论人们如何看待美国军事介入阿富汗和伊拉克，这些入侵的成本都超过了 5.9 万亿美元。如果要求美国纳税人直接为战争提供资金，那么每个家庭将承担超过 46000 美元。

现代货币体系的另一个问题是，在全世界不同国家之间转移资金是极其困难的。中国、俄罗斯、阿根廷和印度尼西亚等国政府都在积极限制其公民可以兑换、转移或带出国外的金额。这主要是通过控制每个人兑换美元等外币的能力来完成的。例如，中国人平均每年只被允许兑换 5 万美元的人民币。

在世界其他地方，即使是在当地获得本地法币的能力也会严重受限。在 2015 年金融危机之后，希腊公民被限制每天从他们的银行账户中提取超过 60 欧元，这清楚地告知他们无法控制本该属于自己的钱。

即使人们可以向国外汇款，也很麻烦且成本高昂。2018 年，移民工人和难民向境外汇出了近 7000 亿美元来支持亲人。汇率和关税消耗了 450 亿美元的资金，这对那些没有多余的钱的人来说是一笔巨款。

全球单点故障

所有央行都是其国民经济的一个重大单节点故障。在某种程度上，美联储是所有世界银行的央行。对于美国人来说，这种安排似乎运转良好。任何地方都接受美元，大多数人很容易开设银行账户，获得信贷额度，并支付商品和服务费用。大多数美国人并没有明显受到通胀的影响。

充满活力的美国经济有助于巩固和推动当今的全球经济体系。其核心是*美元本位*，这是一种全球货币霸权，始于一起鲜为人知的事件，它发生在 1994 年新罕布什尔州的一家酒店，被称为“布雷顿森林协定”。

随着第二次世界大战即将结束，全球大国在布雷顿森林举办了一场聚会来建立统一的货币秩序。在三周的时间里，来自 44 个国家的 700 多名代表就未来金融体系的结构进行了辩论和谈判。一些代表建议建立一种名为*班科*（bancor）的新国际储备货币。最后，代表们同意他们的货币将与美元挂钩。因此，今天的国际贸易主要以美元结算，每个国家都试图维持他们的美元储备。

美元对全球经济体系的核心性质体现在资金在各国之间流动的方式上。例如，从韩国汇款到菲律宾。韩元通常不可能被直接兑换成菲律宾比索，因为这两个国家手上没有足够的对方货币。相反，他们依靠美元和一系列交易。首先，韩元在首尔被卖成美元。这些美元通过美国银行从韩国银行转移到菲律宾银行。最后，马尼拉的银行将美元兑换成菲律宾比索。这需要至少几天时间，并且会产生外汇和交易费用，从流行路线的百分之几到不太流行的路线的低两位数百分比。即使对于小额汇款来说，这种跨境支付的全球平均成本仍然超过 7%。

虽然世界在许多方面从美元本位中获益，但它也导致了一种脆弱性，即每个经济体都在某种程度上依赖美元，并且很容易受其崩溃

的影响．结果就是美国的少数银行倒闭，可能导致全球性的经济灾难。

财务隐私的终结

过去二十年的货币数字化导致个人隐私水平不断下降，每笔交易现在都被用于政治控制和可能的商业利益挖掘。电子货币已存在很长时间，但直到最近才出现让有效进行大规模监视成为可能所需的大数据分析。无论是线上购买还是实体购买都不安全，因为政府和广告商在越来越多地挖掘每个人的偏好、购买决策和社会关系画像。这些用户画像就像个人隐私数据的足迹和指纹，每个人都独一无二，每次新购买都会使其变得更加精致和易于识别．这会让我们生活在这样的一个世界里：在谷歌搜索一次产品可以导致几分钟后出现同一产品的 Facebook 和 Instagram 广告。

公众对企业和政府追踪公民的消费行为有着不同的反应。有些人觉得它令人不安，其他人认为这是对隐私的重大侵犯，而大多数人似乎并不关心。无论哪种方式，事实是，除了控制货币供应和资金可以被发送到哪里之外，当局现在几乎可以了解买家和卖家的一切。世界上越来越多的数字支付系统可能会导致个人隐私的消亡。

存在另一种方式吗？

四种全球现象——个人财富的贬值、价值转移的限制、金融中心化和隐私的丧失——代表了个人在 21 世纪货币体系中的主要风险。随着各国努力维持现状，世界各地的人们都感受到了压力。

如果出现一个新系统，其中政府没有能力随意贬值货币，不露面的公司无法冻结用户资金或拒绝处理交易，会怎么样？如果货币完全是数字的，可以被世界上任何地方的互联网访问者使用，而无需征得当局的许可，会怎么样？

在 2008 年金融危机之后，有人决定建立这样一个系统，为下一次重大的金融革命奠定基础。

第二章
什么是比特币？

2008 年 9 月 15 日，著名投资银行雷曼兄弟（Lehman Brothers）申请了美国历史上最大的破产案。成立于 1850 年的雷曼兄弟的倒下，是全球借贷狂潮的高潮。该公司的风险远高于该公司抵押担保证券（包括许多高风险次级抵押贷款）的总价值。当房主停止支付抵押贷款时，该公司变得无力偿还债务，无法恢复。

突然间，各家银行在雷曼兄弟和彼此之间建立起来的信任蒸发了。在这种信贷危机中，企业发现很难借出贷款来为他们的活动提供资金。由于没有资金购买库存、投资新设备或支付工资，许多行业的公司看起来都无法继续经营。恶性循环似乎迫在眉睫。

美国财政部和美联储迅速采取措施，通过借钱给银行来维持金融体系的运转，从而避免经济危机。2008 年 10 月 3 日，国会通过 2008 年紧急经济稳定法案来救助了几家陷入困境的银行。政府花费了数千亿美元来支撑崩溃的金融部门。

走进比特币

2008 年 10 月 31 日，在美国政府授权 7000 亿美元救助银行的几周后，化名中本聪（Satoshi Nakamoto）的一位（或一群）匿名人士发布了一份技术*白皮书*，概述了一种名为比特币（Bitcoin）的新电子支付系统。中本聪把这份白皮书提交给了一个名为赛博朋克（cypherpunks）的密码学研究者电子邮件列表——他们是一群隐私活动家，创造了挑战监控和滥用国家权力的工具。

白皮书有两个重要的吸引点。首先，作者选择使用假名。中本聪的身份至今仍然是人们关注的一个谜。其次，该论文引入了以前从未存在过的东西：不依赖于一个中央权威的数字货币。之前很少有人认为这种突破甚至是可能的。

几个月后，中本聪推出了比特币网络，并留下了一行文字说明用意，这行文字被嵌在比特币账本的第一个条目里：

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

（泰晤士报 2009 年 1 月 3 日 总理即将面临银行第二轮救助计划）

这是 2009 年 1 月 3 日出现在英国著名报纸《泰晤士报》上的一个标题。中本聪向全世界传达的信息是，以牺牲人民为代价救助银行的现有体系破产了。比特币的去中心化金融技术是一条出路。

要理解比特币背后的科学创新，首先要理解稀缺性。

两种稀缺性

在物理领域，有两种形式的稀缺性。第一种是人造的（以及在此意义上，人为的）：比如限量版香奈儿手提包、迈克·乔丹篮球卡、罕见年份的葡萄酒或特定艺术家的编号艺术品这样的收藏品。这也称为*中心化*稀缺。请注意，这些物品往往存在假冒问题。

第二种稀缺是自然的。这个类别包括盐（salt，“工资/salary”一词的来源）、来自加纳的玻璃珠、来自美洲原住民文化的贝壳、来自中国的白银，当然还有世界各地的黄金。这些是*去中心化*稀缺的例子，往往更难以伪造。

盐和黄金等去中心化、稀缺的商品被用作货币并非巧合。首先，使用没有个人或团体控制的商品是公平的。其次，这些商品更难以伪造。最后，稀缺性有助于保持经济交易容易进行，因为没有必要携带不合理数量的货币来买东西。

两种不同形式的稀缺性的区别在于能否被控制。中心化稀缺是由一个公司或个人创造的——无论它是中国人民银行、美联储、一位艺术家还是一个大型跨国公司。该实体或*中央权威*通过创建、发行、回购和没收来完全控制商品的稀缺性。

去中心化稀缺商品是由自然创造的，这意味着没有中央权威来制造商品。没有制作，相反，这个过程更类似于收集或收获。为了开采一种天然稀缺的商品，如黄金或石油，矿工要从地下开采已经存在的东西。

在黄金的情况下，其积累在历史上不需要矿主之外的任何人的许可。换句话说，没有一个中心是所有黄金都诞生于此，也没有全球权威有权限制挖矿或增加供应。

这是中心化和去中心化稀缺商品，特别是那些被用作货币的商品，之间的关键区别。

为什么去中心化对货币来说是件好事

正如前面提到的，中心化货币一个不可避免的特征是创造者可以任意地膨胀供给量，随心所欲地印更多钱。虽然相比民主政权，这种做法在专制政权中更为常见并且更大程度上发生，但这种情况在所有社会中都会发生。

在影片《巴格西》（Bugsy）中，主角一次又一次地向投资者出售 Pink Flamingo 赌场的股份。对每个人，他都以 10000 美元的价格出售赌场的 20%。他把股份卖给了十几位投资者，歪曲了他们购买赌场的数量。每个投资者都假设自己现在拥有赌场的 20%，但实际上他们拥有的要少得多。然而，巴格西却受益匪浅，因为他拿到了更多的钱。

每个中心化商品都面临同样的激励问题。中央权威可以创造更多的这种商品，稀释所有其他所有者的价值。印出更多货币的央行通常会为这种行为制定积极有益的社会目标，如建设社会基础设施，支持社会福利计划或稳定经济危机。但是，回想一下第 1 章的坎蒂隆效应：即使合理使用这种权力，也会牺牲穷人和无权者，为富人和当权者带来好处。印钱的能力造成了一种道德风险。

当然，稀释也可能发生在去中心化的货币上。新技术可以使收集一种罕见的天然商品更便宜，因此市场可能充斥着新的供应。一旦一种商品失去其稀缺性，它就会变弱和健全。这就是为什么盐、贝壳和玻璃珠不再被用于货币。它们在过去很难去大规模采集，但由于技术创新，采集它们现在变得简单和便宜。

黄金是为数不多的例外之一，即使经过数千年的开采，黄金仍然保持着非常好的价值。虽然黄金具有一些工业和装饰用途，但其历史挖矿难度意味着一种相对稳健的货币，其稳定的购买力使其成为非常好的价值储存。即便在今天，黄金首饰在一些国家仍被当成对冲经济危机的一种方式。黄金的主要缺点是其物理性和重量，因为存储、安全和转移都可能具有挑战性。

许多比特币支持者认为，比特币最终可能会取代黄金作为长期储蓄的首选价值储存。正如本章所示，它是去中心化的，比黄金更稀缺，并且也更易于运输和安全存储。

去中心化的数字稀缺性

随着互联网的出现，信息终于可以被数字化并大规模分发。复制一份数字文件比在物理世界中复制某物品更容易，也更便宜。

货币的数字化是电子商务的必要创新，消除了物理转移的需要。一切都可以以电子邮件或网页加载的速度发送，从而减少摩擦并使贸易真正全球化。数字版本的法定货币由银行创建，然后由信用卡网络（Visa、万事达卡），零售公司（阿里巴巴、亚马逊、苹果），甚至互联网本地支付处理商（微信、PayPal、Square）处理。

由于他们货币使用的唯一仲裁者，所有这些公司都可以审查交易。他们可以没收资金并关闭账户，而且经常在没有客户同意的情况下这样做。更重要的是，由于它们是中心化结构，这些公司往往是政府压力或甚至黑客攻击的目标，这可能导致客户资金或数据的损失。在比特币之前，这是数字货币不可避免的取舍：它必须是人为稀缺的，或者说由中央权威控制的。似乎没有办法在数字领域创造稀缺性。

中本聪在 2008 年 10 月 31 日发布了一项突破，提出了比特币这种新的数字货币，其稀缺性源于数字领域中存在稀缺物品的事实：稀有数字。

一些最稀有的数字是素数。素数（如 2、3 或 5）只能被 1 和它自己整除。

随着数字越来越大，素数越来越少。例如，在 1 和 100 之间，有 25 个素数。你可能会期望在 1 到 1000 之间有 250 个素数，但只有 168 个。在 1000 亿之后，素数变得非常稀缺，以至于对于最大素数的全球数学搜索仍在继续进行之中。

在比特币网络中，新比特币是通过全球竞争来生产的，比特币挖矿的参与者需要找到稀有数字，就像素数一样。这使得数字领域的去中心化稀缺成为可能。这就是中本聪的发明如此深刻的原因。在比特币之前的每一项资产，要么完全中心化（《魔兽世界》里的黄金），要么是实物的 （白银），要么无限丰富（MP3）。比特币之前根本不存在去中心化的、数字的和稀缺的资产。

比特币挖矿：去中心化支付处理

比特币的去中性化本质基于这样一个事实：它是一种稀缺的天然商品（类似黄金）并且很难找到。就像挖黄金一样，挖比特币是在更为常见的情况下寻找非常罕见的东西。一旦比特币矿工找到合适的稀有数字，就可以便宜且容易地被其他人验证，就像黄金可以相对容易地与愚人金区分开来。

比特币矿工使用功能强大的计算机来搜索特定的稀有数字，而不是使用镐和挖掘机来搜寻黄金。一旦找到，每个稀有数字都被称为一次*工作量证明*（proof-of-work），因为它向每个人*证明*，寻找它花了很多工作量。

与黄金一样，挖矿不需要来自一个中央权威的许可：任何人都可以下载挖矿软件来开始搜索符合标准的稀有数字。

甚至比挖黄金更好，不需要特殊类型的土地，只需要计算机设备和负担得起的电源。因此，世界各地的矿工在竞争中独立搜索，以找到符合比特币网络要求的标准的工作量证明。

因此，比特币在没有单点故障的情况下运行。与中心化系统形成对比。如果 Visa 网络出现故障，没有人可以使用 Visa 卡支付任何费用。Paypal 或亚马逊同样如此，如果它们各自的网络出现故障。与这些公司不同，比特币没有中央权威或单点故障。没有人可以选择审查特定交易。比特币的矿工网络提供了一种关键的核心服务：在没有一个中央权威的(以及其带来的缺陷)情况下永不停歇的处理交易。

比特币交易如何运作

那么比特币交易是如何运作的？

要理解这一点，请想想你可能更为熟悉的事情：银行的账本系统。在有人写一张支票来为一件商品或一次服务买单后，接收人去他的银行存入支票。假设两个客户在该银行都有一个账户，银行只需借记发送人的账户并记入接收人的账户。整个过程只需要在银行的会计账本中添加两个条目。银行官员不会进入保险库，从发送人存放的硬币和账单中拿出确切的金额，然后将其存入接收人存放的硬币和账单。使用账本进行会计处理是一项重要的历史发明，使货币的流转好不费力。在比特币里，相当于一张银行支票的是一笔*交易*（transaction）。

比特币运营着一种被称为*区块链*（blockchain）的特殊账本。成千上万运行着比特币验证软件的人，而非中央权威，在不断检查区块链。运行该软件的每个人都会保留整个账本的副本并验证新条目。这被称为运行一个*全节点*（full node）。每个全节点不断检查账本以强制执行相同的比特币规则，这样，任何中央权威都不能随意编辑记录来窃取比特币或花费他们没有的比特币。比特币的区块链被称为*公链*（public blockchain）， 因为任何人都可以查看交易记录。

比特币所有者以与编写支票相同的方式进行交易。他们指定金额，然后签署支票。但是，比特币所有者不是在一张易于伪造的纸上乱写他们的名字，而是通过密码学用*数字签名*（digital signature）签署他们的交易 。

这个数字签名是使用一个只有比特币所有者知道的秘密来创建的。这个秘密被称为*私钥*（private key）。使用私钥，发送人可以制作数字签名，向接收人证明发送人拥有比特币。

用户将他们的比特币存储在*钱包*（wallet）里，钱包是在计算机、电话或专用硬件上运行的软件。每一秒，新的比特币交易都是从世界

各地的钱包开始的，但没有中央支付处理商。相反，来自世界各地的矿工竞相将交易记录到账本中。他们运行他们的计算设备，并试图找到一个特殊的稀有数字。每隔 10 分钟左右，世界某处的比特币矿工就会找到工作量证明，并将其与一组等待处理的交易组合成一个*区块*（block）。然后矿工将此区块提交给比特币网络进行验证。

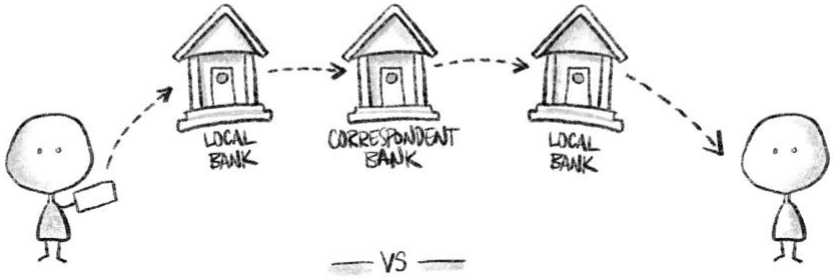
每个区块都像比特币全球账本中的新的一页，网络上的全节点验证其中包含的交易是否有效。任何人都可以运行全节点，因此成千上万的用户不断验证每个新区块的有效性。如果网络确认矿工的建议区块有效，那么矿工将获得 12.5 个新比特币的奖励，并且该区块及其中包含的所有交易成为比特币历史的永久部分。在撰写本文时，典型的比特币链上交易需要不到一个小时才能在区块链上完成。

比特币区块链的名称源于它是历史账本中所有区块（或所有页面）的集合。换句话说，区块链是比特币网络上自 2009 年 1 月创建以来所有交易的完整、不可变的账本。

组成比特币网络的有数千个全节点。每个全节点独立地验证来自矿工新建议的区块。相当适中的硬件要求意味着大多数现代笔记本电脑都可以运行比特币全节点。由于运行全节点仍然相对便宜且多数人负担得起，因此网络仍然是去中心化的。

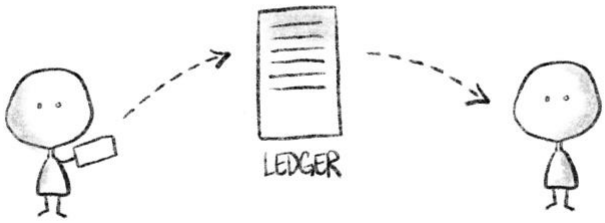
HOW TO SEND MONEY ACROSS THE WORLD

THE OLD WAY



— VS —

THE BITCOIN WAY



比特币的货币政策

与目前的央行体系不同，比特币的货币政策是透明和一成不变的。

如何发行新比特币？如上所述，找到有效的工作量证明并将其与一组有效交易配对——制作一个有效的新区块——的矿工有权获得所谓的区块奖励。在撰写本文时，区块奖励是 12.5 比特币并每四年减半一次，这意味着奖励将是 2020 年的 6.25 比特币，2024 年的 3.125 比特币，等等。

如果矿工试图欺骗并要求超过预定区块奖励的奖励，则该区块被验证该区块的所有全节点拒绝。全节点检查所有建议的区块，任何不遵守规则的区块都不会被放入其区块链中。这类似于银行拒绝发送帐户透支的支票。结果，没有人可以伪造假比特币。尝试花费不存在的比特币的任何欺诈性交易，以及包含此类交易的任何区块都将被全节点拒绝。

一个无效区块对矿工来说是昂贵的，因为它被拒绝了，而他们运行自己的计算设备来找到工作量证明所花费的大量电力被浪费了。这让欺诈变得非常昂贵，并保护了比特币网络。但是，如果比特币网络上只有少数全节点，那么矿工可能会通过贿赂那些少量的全节点来让一个欺诈性区块进入区块链。由于网络上有数千个全节点，并且由于它们在地理上分散且彼此不未知，因此这种策略几乎肯定会失败。

中本聪从一开始就设定了所有比特币的总供应量为 2100 万。今天，超过 85％的比特币已经被挖出来了，这意味着现在有超过 1700 万比特币在流通。其余的将按照一份众所周知的时间表，以越来越小的量奖励给矿工们。

区块链技术：仍在等待

许多人试图复制中本聪发明的成功。一种流行的策略是采用比特币的区块链账本系统并将其应用于其他用例。自 2014 年以来，许多知名公司都试图在各个行业中使用区块链，投入了数百万美元。这引起了围绕*区块链技术*（blockchain technology）的大量炒作和媒体关注。

不幸的是，到目前为止，大多数这些尝试都相当于开叉车去杂货店购物。该车辆在其原始环境中完美运行（存储去中心化数字货币的账本），但对于其现代应用来说似乎太慢且有不必要地浪费，（譬如区块链上的医疗保健记录、在区块链上追踪农产品来源、把天气数据放上区块链等）。

比特币是四个重要组成部分的组合产物，区块链只是其中之一。首先，比特币是一种稀缺的数字资产。第二是比特币是一个有大量全节点的点对点网络，无法被关闭或被审查。第三是挖比特币需要找到有效的工作量证明数字，这让欺诈成本非常高，并且保证了随意性和稀缺性。第四是比特币有一个完全可公开审核的区块链。这四种技术紧密结合，当一部分被移除时，结果就没那么有用了。

对于比特币这样的纯数字资产，使用区块链作为公共记录是有效的。它的创造和它的转移的每个实例都是完美记录和绝对可靠的。但对于咖啡豆或医疗保健数据等现实世界的对象，无法保证信息是绝对可靠的，因为出于疏忽或甚至是彻头彻尾的欺诈，在数据源和每个数据输入期间总是存在错误的可能性。因此，必须有一个中央权威来保证所有信息，这从一开始就消除了对区块链的需求。

尽管如此，为了寻找去中心化货币之外的用例，人们已经投入了大量资金到区块链技术里。在撰写本文时，暂时没有人能够用区块链来创造一种大规模的记录存储系统，使其可以与传统系统优势相当或者有显著改善。

其他加密货币怎么样？

人们不只是试图复制比特币的区块链；他们还尝试创建其他加密货币，因为这些新数字货币的发送人使用数字签名来签署交易，就像比特币一样。这些项目通常被称为山寨币或代币，它们不是去中心化的，而且许多都是彻头彻尾的诈骗。Bitconnect 是加密货币欺诈的一个著名例子。

少数加密货币可能具有正当的用例。这些包括门罗币（Monero，XMR）和大零币（Zcash，ZEC），它们旨在让用户以比比特币或以太坊（Ethereum，ETH）——用于尝试和构建区块链应用平台——更私密的方式进行交易。大公司也在试验加密货币。Facebook 宣布了 Libra 数字货币，由于数十亿人使用 Facebook 的服务，它有可能变得非常流行。然而，Libra 本质上是中心化的，不会有比特币的抗审查和稀缺性。

有几个团体试图以特别厚颜无耻的方式复制中本聪的成功，并创造出了几种名称中包含比特币一词的加密货币。因此，对于哪种加密货币是真正的比特币，人们经常搞混。要区分它们，请在交易所和钱包里查找代码 BTC。比特币的变种就像是愚人金；它们可能看起来相似，但更中心化，价格更低。这些包括*比特币现金*（Bitcoin Cash，BCH），*比特币黄金*（Bitcoin Gold，BTG）和*比特币中本聪愿景*（Bitcoin Satoshi’s Vision，BSV）。

总结

比特币是一项深刻的系统工程突破，为现有的金融系统提供了新的替代方案。

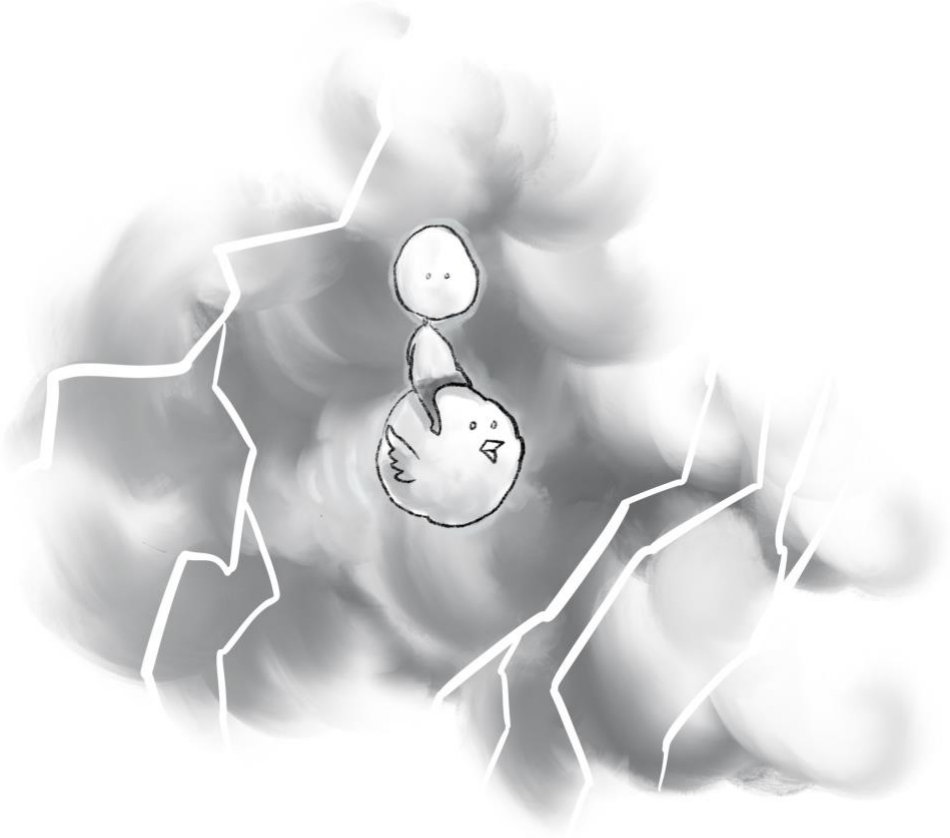
比特币是一种数字货币，在全球范围内易于交易，因为它可以在几分钟而不是几天内结算。

比特币是一种稀缺资产，可以抵御肆意通胀的威胁。

比特币是去中心化的，可以抵抗任何人审查。

比特币是当今世界上唯一的去中心化、数字化稀缺的货币。

比特币有可能颠覆当前的货币秩序。



第三章
比特币的价格和波动性

免责声明：本书作者不是投资专业人士。本章提出比特币价格变动和整体波动的可能原因，并不包含投资建议。

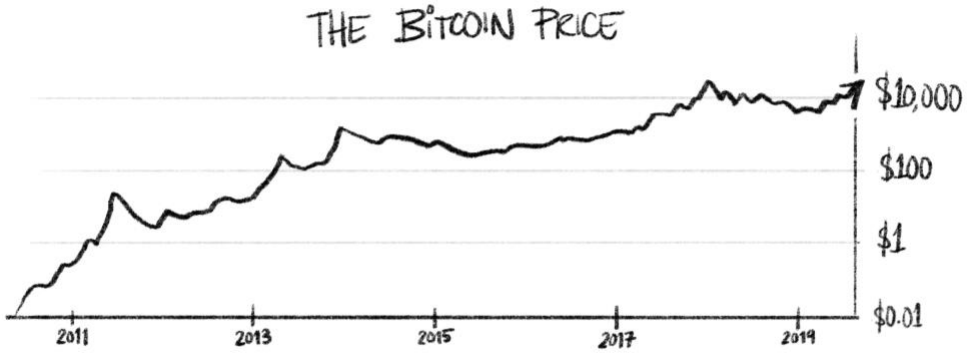
每个人都想知道：为什么比特币有价值？为什么价格涨得这么多？为什么如此波动？如果和美元不同，比特币不是靠一个经济体背书（或者更愤世嫉俗地说，靠罚款和监牢的威胁背书），为什么比特币会有价值？

当买卖双方存在不平衡时，资产的价格就会发生变化。对比特币来说，这些不平衡是由一些因长期、中期和短期视角而不同的因素驱动的。

长期视角

在过去的十年中，比特币的价格从几分之一美分上升到近两万美元的高位。截至 2019 年 8 月的价格接近 11000 美元。

从开始到现在的比特币价格（对数坐标）



比特币是稀缺的。如第 2 章所述，供应量被设定为 2100 万个币。

比特币的固定供应和透明的发行时间表对买家来说很有吸引力，因为替代品——法定货币——普遍会被稀释，从而导致通胀，这意味着同样多的钱每年只能买更少的东西。从长远来看，更多人可能会发现比特币具有吸引力，因为政府无法印更多的币或审查交易，因为它很难被没收。

挖出来的所有比特币的总价值仍然只有 2000 亿美元。相比之下，挖出来的所有黄金价值估计约为 9 万亿美元。比特币的市值很小，只有 2%的黄金价值，因此对价格波动更敏感。每日交易量也相对较小：每天约 100 亿美元，而黄金为每天约 3000 亿美元。由于*流动性*（liquidity）——即在特定时期内可以方便地买卖的资产数量——较低，即使是小买家或卖家也会对价格产生很大影响。随着比特币接受度的增加以及比特币作为全球资产类别的增长，其波动性将会下降。这可能需要几十年的时间。

中期视角

在几个月和几年的时间框架内看比特币，价格变化的最大驱动因素是挖矿成本、大型机构买家的需求和减半事件。

挖矿有成本：设备、数据中心运营、电力。这些费用必须使用法定货币支付。因此，大多数矿工会定期出售他们挖出的部分或全部比特币支付运营成本，这笔费用大约相当于每月 2.5 亿至 3 亿美元，或者是撰写本文时每月开采比特币价值的 40-50％。

对这种规模的比特币的需求，通常来自机构买家、富有的个人、家族办公室以及希望接触加密货币（通常从比特币开始）的捐赠基金。

影响中期价格的另一个重要因素是*减半*（halving）。如第 2 章所说，挖矿奖励每四年减少一半。到目前为止，比特币在 2012 年和 2016 年已经有两次减半。两次减半都创造出了一个让波动性剧增的供应断崖。

不断上涨的比特币价格往往吸引更多的投机者，从寻求购买价值 100 美元价值比特币的零售投资者，到购买价值数百万美元的机构投资者。反过来，这会推高比特币的价格，因为媒体的关注以及对错过机会的的恐惧会加剧这种心态。这种动态创造出大量的价格泡沫，最终价格可能崩溃 80％或更多。这些价格周期很有可能在未来减半的前后继续下去。

短期视角

没有中央权威有一个重要的副作用：波动性。

交易比特币的场所为短期波动的原因提供了至关重要的背景。有很多地方可以交易，例如*法币交易所*（fiat-to-crypto exchanges），允许将法币直接交易成比特币，*点对点交易所*（peer-to-peer exchanges），这需要亲自会面，以及*币币交易所*（crypto-to-crypto exchanges），这只允许加密货币之间的交换。因为交易者寻求从波动中获利，所以有*杠杆交易所*（leveraged exchanges），交易金额可达到存款金额的 100 倍。

加密货币交易所主要存在于互联网上。因此，它们在一年中的每一分钟都在运营，并且可以直接服务散户投资者。相比之下，传统市场通常位于伦敦、纽约或香港等大型金融中心，仅在周一至周五的约 7.5 小时里开放实时交易，主要用于经纪人，而不是散户投资者。

因为任何人都可以通过计算机和互联网连接来收发比特币，所以企业家建立一家基本交易所相对容易。由于比特币不被视为证券，因此交易比特币的交易所所用的监管标准可能没有传统市场严格。此外，币币交易所可以设在马耳他、塞舌尔或菲律宾等友好的管辖区，因为它们不需要法币银行账户，团队可以远程操作。存入交易所意味着信任该交易所可以保证资金安全。不幸的是，许多交易所管理不善。有充分记录的渎职或无能的事件导致大规模盗窃，包括 Mt. Gox，Bitfinex 和 Quadriga 共同失去了数以万计的比特币（价值数十亿美元）。

警告读者：许多交易所曾遭到黑客入侵或丢失客户的比特币。读者在使用交易所时应该谨慎行事，并且应该只用自己能够承受的比特币数量来冒险。

比特币适合散户在线交易有助于其短期波动。尽管央行通常会寻求将波动性降至最低，但交易者更倾向于波动，因为它有利可图。

在从一个月到一分钟的时间范围内，比特币的价格波动可能是极端的。在 2019 年 1 月 1 日，一个比特币价值 3500 美元。截至 2019 年 8 月，它价值接近 11000 美元。每日波动高达 20％并非异常。这对投资者来说是可怕的，但却是寻求从价格走势中获利的投机者的天堂。

不同于传统的股票或债务市场，比特币没有决定价格共识的业务基本面。比特币没有员工，没有产品性能，也没有现金流。缺乏此类近期业绩指标意味着强调交易的技术要素，这通常是零和。对于这样的投机者来说，交易加密货币是另一种形式的在线扑克，需要长时间的微弱优势，在舒适的客厅和方便的时候玩。

与传统市场一样，比特币的价格对重大新闻也会有所反应——但它并不总是随着利好消息上涨或者随着利空消息下跌。例如，在 2013 年，黑客袭击了当时最大的交易所 Mt.Gox，随后价格大幅下跌。然而，在 2018 年，如今最大的交易所 Binance 被盗了大约 4000 万美元，而比特币的价格实际上上涨了。

随着比特币变得更有价值和更具流动性，波动性可能会减少。这类似于著名股票与较不知名股票的价格波动。例如，对于个体交易者来说，影响苹果公司的价格比低价股的价格要难得多。

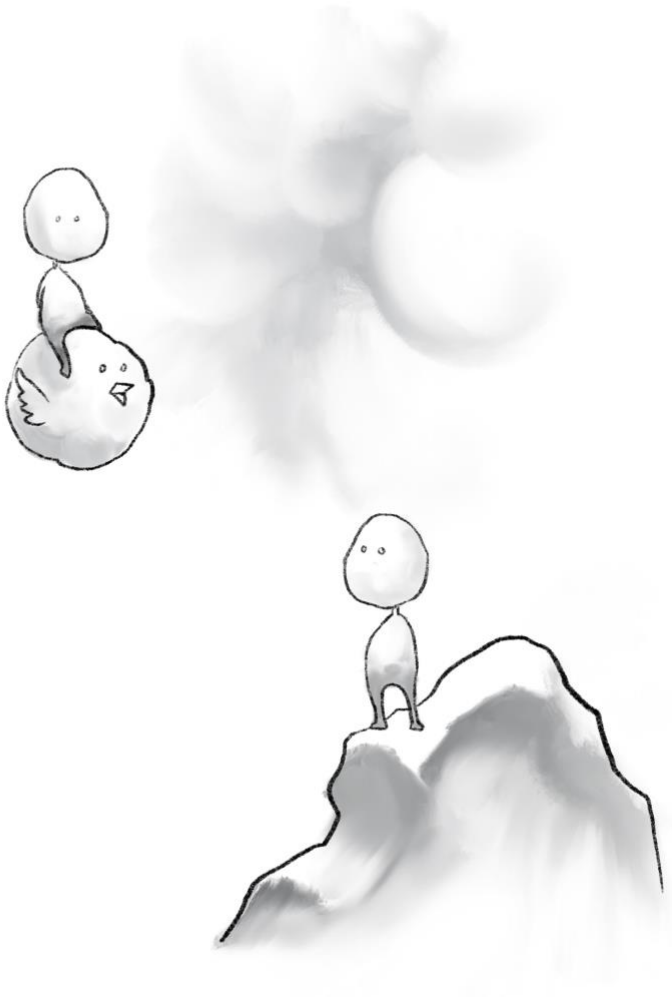
对于交易者来说，比特币是一种独特且风险极高的工具。比特币对交易者的吸引力，加上其缺乏流动性和杠杆交易的可用性，增加了其价格的短期波动性。

总结

自诞生以来，比特币的价格随着其固定供应和不断增长的需求而总体向上和向右移动。在短期内，价格受到投机、市场操纵和大规模波动的影响。

归根到底，是比特币的固定供应和去中心化性质赋予了它价值和波动性。

如果比特币进化到超越了价值储存并且开始代表数字经济的规模（就像法定货币对今天的实体经济所做的那样），比特币将成为一种支付方式和一种记账单位。此时，由于比特币固定在价值交换而非投机活动上，波动性可能会下降。在此期间，它将继续受制于本章中期和短期部分所描述的市场力量，并继续大幅波动。



第四章
为什么比特币对人权至关重要

随着比特币的发明，个人现在能够整合他们的辛勤工作的产出，并将他们的财富存储为数字信息。这有助于防止政权或公司任意控制他们储蓄或随意转移他们的财富。世界各地——尤其是独裁国家，但即便是自由民主国家也包含在内——已经感受到这场金融革命对人权的影响，并将继续加剧。

第 1 章介绍了从尼日利亚到委内瑞拉的个人的故事，他们一直在努力应对高通胀、金融监管、难以获取的银行业务和破败的经济基础设施。

这些不是孤立的故事。根据人权基金会的数据，世界上大约一半的人口生活在威权主义之下。从古巴到白俄罗斯，从沙特阿拉伯到越南的大约 40 亿人正受到政府的严重压迫。其中许多人是经济难民或政治犯。这些人不享有法治或和平推动改革的能力。甚至美国和欧洲政府也经常通过不断增加的监督和通胀来压制其公民。对银行家的救助，对外部军事干预，加强边境安全和补贴福利只是印更多钱所带来可疑行为的一部分。

当一个人权组织的银行账户被一个独裁者冻结，或者因为一个未经选举的统治者犯下的罪行却要制裁一整个国家的人民时，比特币可以是一条出路。

中本聪的发明可以极大地帮助没有银行账户或正式身份证件的数亿人拥有和使用货币。只需电话和互联网连接，地球上那些最脆弱的人就可以快速廉价地从任何人那里获得比特币而不会被审查或扣押。

因此，比特币正在改变跨境支付和汇款的游戏，并有可能改善社会的许多其他方面。比特币创造了一个真正的全球商品和服务市场，可以为更公平的竞争环境铺平道路。

成为自己的银行

在巴林、俄罗斯和津巴布韦这样的地方，政府对银行系统施加独裁控制，导致高度贪污和腐败。比特币为一个政权和公司控制较少、个人拥有更多自由和个人选择的世界奠定了基础。

比特币是一种不记名票据，意味着人们可以完全控制他们拥有的比特币。此外，在发送比特币时，没有中间人可以审查交易或泄露发送人的个人信息。这可以防范窃贼、恶意公司和间谍政府。没有其他货币或支付公司可以夸耀这种安全性。

在床垫下藏现金长期以来一直是那些破败的经济体里的人存钱的方式。明显的缺点是现金很难保证安全并且传输不方便。如果当局找上门，他们可以拿走他们找到的任何现金。相比之下，比特币易于存储和保护，因为私钥或密码可以存储在纸张、计算机、U 盘上，甚至可以被记下来。比特币所有权的合理可否认性是可能的，当局没有简单的方法来实际扣押比特币。

逃避高通胀

伊朗到索马里兰的公民生活在肆无忌惮地印钱的政权之下，从而耗尽了他们省下的来之不易的储蓄。

当然，通胀是所有央行都参与的事情。他们通常认为把在经济体中发行更多货币是可取的，因为这会使市场保持运转。民主国家可能表现出一些克制，但正如我们所看到的，通胀可能很快失控。

根据消费者价格指数，从 2018 年到 2019 年，德国的价格上涨 1.7%，美国的价格上涨 1.9%。在许多国家，消费品价格上涨幅度更大：巴西为 3.75%，印度为 5%，尼日利亚为 11%，土耳其为 20%，阿根廷为 47%。价格涨幅超过 10%的国家的人们注意到他们的收入和储蓄突然贬值。

一个极端的例子是委内瑞拉。由于毫不留情的印钞、系统性的腐败和普遍的经济管理不善，2018 年价格上涨了 2300000%——恶性通胀如此严重，使得储蓄无法实现。货币到达银行账户后数小时开始蒸发。这迫使委内瑞拉人只能勉强维持生计，一旦赚到钱，就把钱换成必需品上。委内瑞拉人生活在专制政权之下，无法参加自由和公正的选举，而通过这种方式他们可能才会选出可靠的政府。在过去几年中，超过 400 万公民（占该国人口的 10%以上）已逃往邻国，如巴西和哥伦比亚，这已成为世界上最严峻的难民危机之一。

除了摧毁国内经济外，委内瑞拉政权近二十年来一直实行严格的资本管制。将钱汇入或带出国家非常困难。汇款的主要方式是通过可在两个国家获得账户的中间人：一个人可以把哥伦比亚比索交给一个在委内瑞拉拥有账户的中介人，该账户将等量的委内瑞拉玻利瓦尔转移到最终目的地。由于银行在政府的压力下正在标记那些在国外使用委内瑞拉账户的人，因此即使这种解决方法现在也已经停止。回想一下第 1 章：政权不希望其民众能够获得比委瑞内拉玻利瓦尔更好、更健全的货币。

另一种选择是，让生活在美国的朋友或家人把美元发送到哥伦比亚边境城市的西联办公室。接收人必须逃离委内瑞拉，冒着极大的风险前往该市，从西联取回美元，衣服里藏好现金潜回委内瑞拉。不用说，这是耗时且危险的，因为陆地边界和机场充斥着想要没收现金的腐败官员。

解决方案：使用比特币跨境转移价值。委内瑞拉人可以通过短信向国外的朋友或家人索要比特币，并在付一小笔手续费后收到币。此交易无法进行审查，也不易追查。对于生活在稳定经济体中的人来说，比特币可能看起来很不稳定，但对于委内瑞拉人来说，即使比特币价格突然上涨 20%，与最近玻利瓦尔 2300000%的贬值幅度相比，仍然是温和的。

一旦他们通过手机或电脑收到比特币，他们就可以在 LocalBitcoins.com 轻松将其变成当地货币，这是一个 eBay 风格的网站，连接着 100 多个国家的交易员。他们可以在网站上出售新收到的比特币。他们可以在 15 分钟内卖掉比特币并在银行账户中获得玻利瓦尔。该系统每天用于让数百万美元进出委内瑞拉。截至 2019 年中期，对于委内瑞拉这种完全破碎的经济体系里人们来说，比特币已经成为最后的平行经济体。

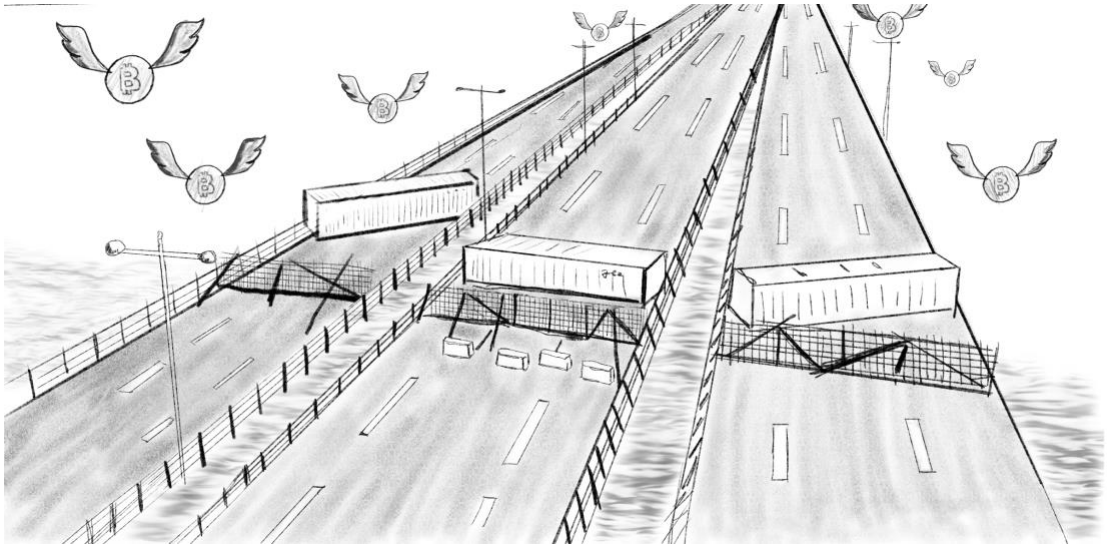
普遍获得货币

一个稳定的民主国家的受过教育公民很容易开设一个银行账户。但对于全世界数十亿人来说，情况并非如此。在阿富汗和沙特阿拉伯，妇女的男性亲属禁止她们开设自己的银行账户。她们实际上被剥夺了金融自由。

对她们来说，比特币可以提供一条新的生命之路。2014 年，一位名叫罗娅·马哈布博（Roya Mahboob）的阿富汗科技企业家面临了一项重大挑战：她无法付钱给她的女性雇员。如果她给她们现金，她们的家人会把钱拿走。男性亲属不会让她们开银行账户。PayPal 等软件在她们的国家/地区不可用。一位朋友提到了使用比特币的可能性，她开始用它来付钱给她的员工。比特币给了她们金融自我主权。

其中一名年轻女性因为生命受到威胁而不得不逃离阿富汗。但她带上了她存在手机里的比特币。她穿越伊朗和土耳其，最终到达德国。在那里，她把她的比特币——幸运的是在她的旅程中已价格大涨——换成了欧元来开始新的生活。在没有其他选择的时候，比特币可以帮助被压迫和没有银行账户的人。

随着比特币的基础设施和当地的人对人交易在未来几年内不断增长，它将对外援和人道主义援助产生重大影响。也许关于援助业出现问题的最生动的画面是出自 2019 年 2 月委内瑞拉边境的一张照片，当时马杜罗政权通过用拖拉机拖车将边境桥架起来阻止外援进入该国。在照片中看不到的是，数百万美元的比特币在政府控制之外来回移动。



今天的外援系统存在明显的漏洞。无论是向另一个政府提供援助的政府，向非政府组织捐赠的慈善组织，还是在医疗紧急情况下向家庭汇款的个人，钱只有在通过第三方之后才能到达目的地。

即使在最基本的情况下，也至少有三个中间方：发送方银行，央行和接收方银行。通常有更多的中间方，有时多达 7 个。每一方都可以放慢流程、冻结交易，甚至窃取资金。前联合国秘书长潘基文在 2012 年的一次讲话中宣称，去年腐败“使得所有发展援助的 30％无法到达其最终目的地”。

根据 GiveDirectly 和世界银行等组织的研究，直接现金转移是提供援助的最有效方式。比特币可以在几分钟内完成对地球上任何人的无限制转移。接收人不需要银行帐户或官方身份证明，只需要上网。

皮尤最近的一项研究发现，新兴经济体中有 45％的人已经拥有智能手机，这一数字还在不断增加。要了解比特币在这一领域的潜在影响，请考虑在像菲律宾这样的国家，只有 20％的成年人拥有银行账户。

要用作支付轨道，比特币接收方必须能够将其交换为当地货币。除非可以将比特币用于商品或服务结算，否则比特币目前不具备捐助的作用。但根据马特·艾尔博格（Matt Ahlborg）对比特币市场数据

的详细分析，从东亚到西非的新兴经济体的个人越来越容易将比特币兑换成当地货币。

更重要的是，当传统银行歇业时，比特币网络继续运转。随着其全球基础设施改善全球人们的流动性和获取渠道，比特币作为受援助者生命希望的能力将急剧增加。

已经存在网状网络、卫星系统和基于无线电的技术，这些技术允许人们在不访问互联网的情况下收发比特币。工程师们正致力于创新，使政府越来越难以阻止公民获取比特币，这是一种他们无法通胀或轻易没收的货币。

无现金社会

无现金社会的想法通常被描述为非常方便。但从人权角度来看，它为政府和银行提供了前所未有的权力，同时也带来了新的危险。

现金是保护个人隐私的最佳方式之一。当用纸币支付某些东西时，只有买方和卖方知道交易，并且政府难以跟踪购买行为。当纸币被放入慈善捐款箱时，可以用现金进行匿名付款。

不幸的是，现金正在世界各地消失。在像委内瑞拉或索马里兰这样的恶性通胀的社会中，纸币是如此毫无价值，以至于它们需要按公斤的重量进行称重。与此同时，在斯德哥尔摩和上海等先进城市地区，居民几乎只使用数字支付。据估计，全球所有交易中只有 8% 仍然使用硬币或纸币进行。到 2030 年，能够在日常生活中有意义地使用现金的人数将接近于零。

在爱沙尼亚，政府正在免费提供公交服务。这听起来不错，但有一个问题：乘客只能通过使用他们的公民卡来获得免费乘车，从而使得政府能够跟踪他们的活动。虽然爱沙尼亚人可能不必担心，但俄罗斯或白俄罗斯等附近威权政府的公民有理由担心。类似的，即使在西方民主国家也开始出现不那么令人痛苦的趋势，信用卡公司和商家把交易活动卖给广告商来获利。

比特币与老大哥

人们在买什么比他们在说什么透露出更多信息。交易披露了大量信息，关于人是谁和他们做什么，他们何时去何地，或者他们喜欢或不喜欢什么。跟踪的支出越广泛，个人面临奥威尔式结果的可能性就越大。

在民主社会中，出现了一场关于像 Facebook 这样的公司发行自己的货币的争论。Facebook 正在提出通过 WhatsApp、Instagram 或 Messenger 上现有的社交媒体账户向数亿人引入 Libra。虽然像 Libra 这样的项目可以很好地为大量目前没有银行账户的人提供金融服务，但许多人担心 Facebook 会记录用户的支付活动，影响选择，或者取消个人资格，并冻结他们为表达特定政治观点付款的能力。

为了阻止老大哥，每个人都必须减少不断扩大的数据踪迹。在公司和政府之间传播和共享与身份相关的信息越少，就越难以被监视、操纵和控制。

无现金社会是一个个人金融行为被监视社会。无论是政府控制的线上交易还是企业控制的 Libra，公司都可以追踪所有经济活动来获利、压迫人们的日常金融行为。

如果未来可以有所不同会怎么样？如果现金可以以数字形式存在会怎么样？虽然目前比特币交易只是使用的，但开发者社区正在做很多工作来为比特币网络及其用户带来更多隐私。在不久的将来，当在线购物、购买公交或地铁票，或订阅政治杂志或播客的时候，个人在付款时不需要透露他们的身份。

用闪电网络让比特币变得私密

消费者越来越失去财务隐私。闪电网络（一种目前正在比特币上构建的支付网络）中可能存在一种解决方案。

现有的支付系统创建了各种隐私蜜罐，因为每个金融中介都是潜在的安全漏洞。比特币的不同之处在于没有中介，因此至少在原则上，这个漏洞可以被消除。不幸的是，比特币交易的关键细节记录在区块链中，任何人都可以看到。研究人员已经探索了是否有办法隐藏或模糊交易的具体细节，并仍使用比特币支付，这可以通过闪电网络来实现。

闪电网络不会直接将每笔交易的详细信息记录到比特币区块链中。闪电网络的目标是提高比特币可以处理的交易速度和数量。隐私恰好是实现该目标的副作用。

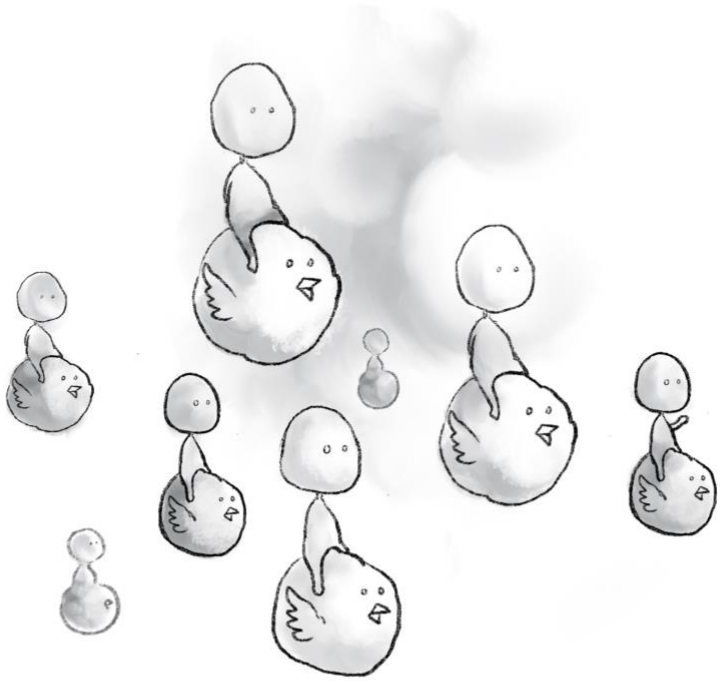
这项技术突破很像比特币，因为它是开源的，无需许可的，并且可供任何人使用，无论其位置、年龄、收入、性别或公民身份如何。比特币闪电可以帮助防止反乌托邦的未来，在这种未来里隐私是昂贵的，只有富有的个人才能实现。

即使在无现金社会，也很快就可以在手机上使用闪电网络应用来匿名购买公交票来参加一场示威游行或在线购买政治书籍。地铁票务机或亚马逊不会对购买者有任何了解，也无法泄露数据或与政府分享信息。

也就是说，闪电网络不是一种隐私灵丹妙药。匿名支付信息只是确保完全隐私的一步，因为还需要废除诸如电话后门、地理定位跟踪和监控摄像头等隐私缺陷。

《黑天鹅》作家纳西姆·塔勒布（Nassim Taleb）写道，比特币是“针对奥威尔式未来的保险政策”。随着世界范围内不断增长的监控和现金消失的趋势继续存在，未来似乎迫在眉睫。

技术并不总能改善全世界的自由。相反，人工智能和大数据分析正在系统性地剥夺个人的自由。历史学家和《人类简史》（*Sapien*）的作者尤瓦尔·诺阿·赫拉利（Yuval Noah Harari）警告说，现代信息技术倾向于支持暴政，但技术也可以支持自由——在为此目的而故意设计和部署时。比特币，特别是当它被赋予像闪电网络这样的新发展时，可以成为全球人权斗争的重要工具。



第五章
两种未来的故事

这一年是 2039 年。

过去 20 年来，全球性战争显著增加。各国都在力争摆脱美元和人民币的主导地位。有时，这种经济动荡会引发暴力冲突。富裕国家遭受政治衰落和棘手的经济衰退之苦，而贫穷国家则徘徊在几乎全面崩溃的边缘，因为连续的经济危机将财富和权力进一步巩固到核心的中央与财团的手中。

阿里巴巴、腾讯、Facebook、谷歌和亚马逊等全球性科技公司控制着国际互联网市场，经过几轮政府施压、反托拉斯诉讼与和解，它们均同意交出用户数据以换取市场保护。巨头公司与世界各国政府全面分享各种用户信息，了解每个人购买记录，视听记录，每个人在社交网络上发布的内容以及每个人的实时地理位置。科技公司已成为国家政权的“雷达卫星”。个人隐私不复存在。

这使政府能够对其公民进行前所未有的控制。随着坎蒂隆效应的加剧，与政权核心有裙带关系的人获得了极高比例的财富，贫富差距继续扩大。数字监控是一种常态，而对专制政府的批评逐渐消失。政府和大型企业对货币的控制，意味着他们可以审查言论，异议内容创作者无法获得报酬以支持他们的工作。

思想的多样性如今变成了异教徒的产物。世界各地的警察使用物联网、医疗植入数据、电话跟踪、交易历史和搜索查询来定位和惩罚持不同政见者。反对意见基本上是不可能的，因为现金已经消失，所有购买行为(包括可能隐藏一个人身份的地铁票、报纸和面具等物品）都是数字化和被监控的。国家和跨国科技公司比以往任何时候都更强大。

这一年是 2039 年。

充满活力的全球经济继续蓬勃发展。世界各地的人们正在积累财富，能够负担得起住房，并开展新的业务。来自曾被称为第三世界国家的企业家正在推动全球经济的创新。换个地方生活比以往更容易。政府之间不得不相互竞争，因为公民可以选择他们想要居住、工作和纳税的地方。个人所得税降低，而市政基础设施、服务和学校的质量因全球之间的政府竞争而得到提高。

许多小企业提供的多种新兴商品和服务的激增，带来了比想象中更多的创新。曾经占据市场主导地位的许多跨国公司已经被来自全球各地的小型企业所淘汰。任何人都可以使用无需许可的、私人的支付手段来支付任何费用。

随着公民越来越擅长绕开严苛的资本管制，并为自己保留财富而不是将其交给精英阶层，许多独裁政权已被推翻或削弱。

政府被迫从控制转向竞争；个人比以往任何时候都更自由。

基于比特币的世界是什么样的？

预测未来始终是一个冒险的立场。鉴于世界目前的轨迹，以上是两个可能的不同愿景。也许两种极端都不可能实现，但个人可以控制他们的社会未来的方向。

货币体系处于十字路口的中间。比特币有可能将货币和国家分割。值得一提的是，比特币如果在全球范围内被广泛采纳和使用，将如何改变社会？

无边界经济兴起

自 20 世纪以来，国家就基本上控制了经济。向数字货币的过渡一开始会允许政府通过轻易增加货币供应来支付各种财政计划，从而以一种前所未有的方式来控制经济。

但随着数字时代的发展，经济开始超越国家的控制。在 21 世纪初，当消费者购买世界各地生产的商品时，这是显而易见的。公司可以聘请菲律宾到尼日利亚的自由职业者作为软件开发人员、虚拟助理甚至远程放射科医生。贸易伙伴可以在数千英里以外。所有通信都是数字的、即时的、无缝衔接的。然而，跨境支付仍然是缓慢且昂贵的。支付在线商品仍然依赖于传统渠道，而金融机构间的美元结算仍需要几天的时间。货币体系尚未适应日益互联的数字世界。

比特币的出现是推动下一波金融发展浪潮的火花。

社交媒体内容、视频游戏等数字原生的商品将占据世界经济的更大份额。比特币将越来越多地用作跨境交易的支付方式，因为法币结算在很长一段时间都会非常繁琐笨重。比特币的微交易，快速结算以及不断增长的比特币用户群将迫使商家以比特币的价格结算。

今天这些经济体规模很小——就像 20 世纪 90 年代在美国在线聊天的社区一样——但随着它们的成长，它们将进一步侵蚀各国政府的经济控制。由于更多的财富来自无国界网络，并以个人拥有的无国界货币计价，财富将变得更容易流转与移动，并将从任何一个民族国家的实体经济中解放出来。

政府面对真正的战争价格

当比特币无处不在时，国家简单地印更多钞票来资助战争的能力将会受到更多限制。战争将不再像过去一百年那样容易获取资金。如果战争确实发生，将会是更有限和更短暂的。

俄罗斯对叙利亚和乌克兰的干涉，或美国对伊拉克和阿富汗的占领等长期冲突可能已成为过去，因为此类行动将越来越难以融资。国家之间的战争更加成为最终且最差的选择，因为政府更愿意找到解决分歧的更便宜的方法。

威权主义变得过于昂贵

威权国家将难以在他们无法控制的全球环境中竞争。随着世界各地的公民可以全权控制他们的个人资产的转移，任何具有高生产力与核心竞争力的人才就会*带着其财富*离开，去一个与他之前生活地竞争的城邦或者国家生活。为了留住这些人才，政府必须实施严格的边境管制，或让这些公民在政治治理中有他们的声音。

独裁政权不会悄然消失，但他们将被迫做出选择：面对大规模资本外逃，还是允许更多的自由。感谢互联网，自由文学和电影作品现在可以出现在生活在厄立特里亚和朝鲜等最暴虐政权之下的家庭中。随着可以与信息一样通过互联网无缝安全传输的货币的出现，这种现象将会被大大加速。

资产可以被正确定价

比特币都为每个人都提供了一种有效的价值存储，无论其身份、种族或所在地。作为对法币通胀的一种对冲，目前大多数人都选择将其部分财富储存在房地产、股票和贵金属中，它们都更为中心化并因此比比特币更难获取。在一个用比特币来储存财富的世界里，这些资产的投机泡沫将不再那么普遍。

例如，通胀引发的房地产泡沫的案例将会减少，因为更少的外国人会在一个城市大量购买住房而不打算住在那里。有了比特币这种更好的选择，在国外购买稳定的资产将不具吸引力。房价不会飙升，更多的人将能够在自己的城市买得起房子。

去中心化金融到来

随着各国能够以比特币（一种真正的全球储备货币）而非区域性的美元、欧元或人民币结算贸易，美国、欧洲和中国的统治地位将逐渐消失。劳动力将可以在世界范围内自由行动，对劳动力的竞争将更加激烈，这让工人可以得到他们生产的更多价值。

美国、欧洲和中国的银行将失去其压倒性的影响力，因为每个人都可以成为自己的银行，从而随时间推移实现真正的储蓄。财富将在出口劳动力的国家积累，使国内企业如雨后春笋般涌现，并建设基础设施和服务。

大银行的力量被削弱

银行由于与政府的特殊关系以及对人民的财富控制而变得庞大，它们要么破产要么变得更小。“太大而不能**倒闭**”将不再是常态，银行和大公司在出现错误时将不再能够依赖 2008 年金融危机那样的政府救助. 如果没有这些优势，银行和跨国公司将需要专注于为客户提供服务，而不是向政府提供服务。由于比特币的无边界性质，较小的公司和银行将能够为全球客户提供灵活服务，并将取代过去僵化的巨头。

老大哥的衰落与监控资本主义

今天，数字支付信息被公司用于谋取利润和政府监控。由于互联网已发展成为一个默认的开放市场，因此隐私标准在保护越来越多的在线个人信息和重要信息方面一直很缓慢。结果，大量个人数据在不知情或没有明确许可的情况下，被不断地重新打包、分析和利用。

随着以比特币为基础的闪电网络的出现和采用，大多数日常小额购买都将与身份隔离。

在在线购物，订阅政治杂志，捐赠民间社会组织或支付医疗费用的时候，除了消费者以外，没有任何人会知道交易的全部细节。从中间位置泄漏信息的支付处理商将不复存在，因为交易是点对点的，商家只能看到付款。在这种环境中没有身份识别信息，监控系统更难以跟踪消费者的行为并预测他们的行动。

自我主权的开始

比特币这种现象所具有的潜在影响与民主政体和互联网类似：这些技术各自推翻了政治权力的暴政和巨头公司对知识的控制。通过民主，公民集体控制着政府和独裁者的权力，通过互联网，普通公民获得了更强大的声音和更自由的知识获取渠道。

同样，比特币将打破各个国家与大公司所享有的货币垄断权。一个世纪以后，人们将回顾 2019 年，回想起一个少数特权阶层控制经济成为过去的时代，就像今天有人回顾君主制封建制或国家宣传机器的观念成为过去的时代。随着比特币发展成世界货币，这种演变将分三个阶段进行。

阶段 1：价值存储

比特币采用的第一步将是作为一种价值存储。在这个阶段，全世界的储蓄者保护自己免于地方政府的通货膨胀。今天，这种情况不仅发生在委内瑞拉和津巴布韦这种恶性通胀的经济体中，还发生在美国和欧洲这样的地方：在过去的几年中，比特币的表现超过当地的法币。在价值存储阶段的后期，养老基金和主流金融机构将开始在其投资组合中添加比特币，再后来，政府将开始在其央行储备金中添加比特币。

在这个阶段，接受度将随着人们意识到它的好处而缓慢而有机地增长。

阶段 2：付款方式

当足够的商家意识到比特币以外的货币实际上是一种劣质的价值存储时，他们会希望人们用比特币支付他们。这类似于委内瑞拉的黑市商人拒绝玻利瓦尔而索要美元。随着越来越多的商人、企业家和

雇员开始喜欢比特币，对比特币的需求将会增加，就像引入布雷顿森林体系的黄金可兑换体系后，对美元的需求飙升一样。

这种情况最初不会发生在像美国这样的发达经济体中，而是发生在通胀和腐败的破败经济体里。这些社会可能会受到压迫性政权的统治，这些政权会削弱容易被没收的价值储备（如美钞和黄金）的可用性。这些地方的人们将使用比特币来规避对其财富的没收，并在必要时完全逃脱。

在这个阶段，精心设计的软件，更快的结算技术，改进的基础架构和隐私创新将成为最前沿。比特币用户将能够实时而私密地进行交易，使监管变得更加困难。

阶段 3：账户单位

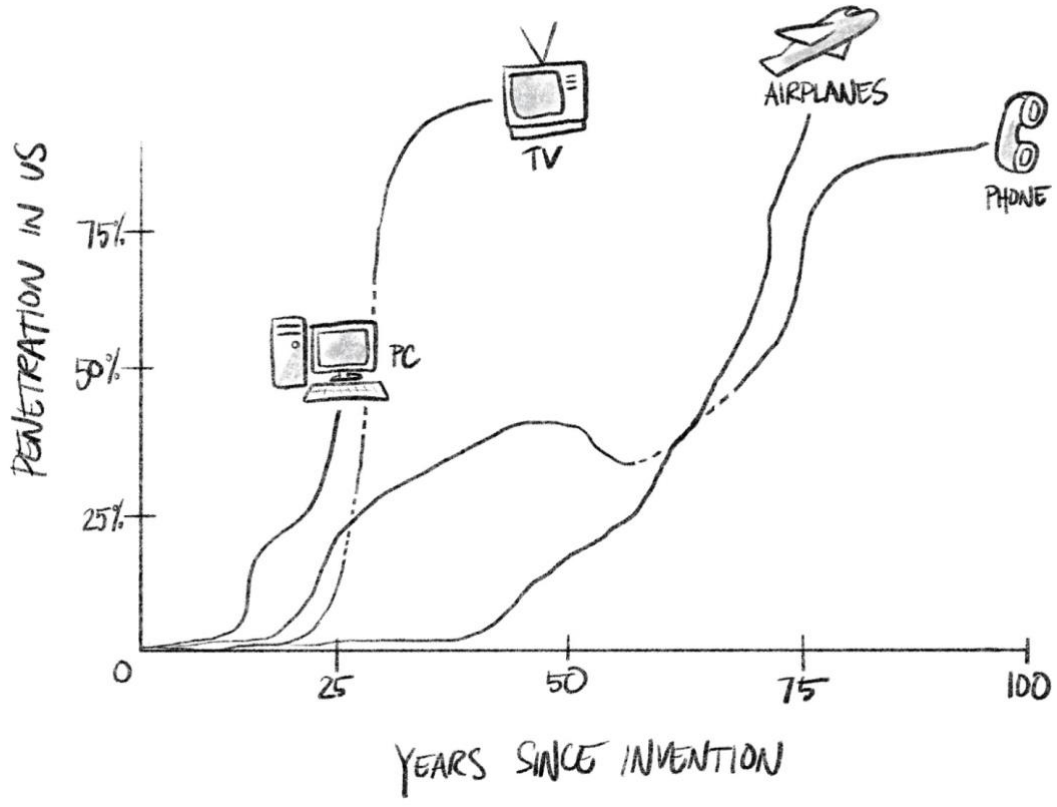
随着越来越多的人持有和赚取比特币而不是当地法币，商品和服务将开始以其绝对比特币价格而不是当地法币或美元定价。在这一点上，将有利润丰厚的套利机会：借入快速贬值的货币并将其转换为比特币将变得有利可图。

这将是超比特币化（hyperbitcoinization）的开始，美元和人民币将失去其特权地位，比特币将成为世界结算货币。反过来，这将导致大多数其他货币的恶性通胀，因为贷款将非常昂贵，以防止套利。由于比特币将是最值得存储价值的地方，因此这种正反馈循环将导致许多其他货币大幅贬值。

现在还很早

大多数改变世界的技术最初都被人群所忽视。想想电力，它最初被认为非常危险；电话，当初没有人想买它；汽车，肯定不能在鹅卵石路上跑；飞机，可能不太安全；微波，据说会破坏食物里所有营养价值；手机，据说会导致癌症；或者互联网，注定要失败。请记住《纽约时报》专栏作家保罗·克鲁格曼的话，他在 1998 年写道：“到 2005 年，互联网对经济的影响将不会超过传真机。”

任何基础技术，从冰箱到信用卡，都遵循接受曲线（adoption curve），并在一开始就有很多怀疑论者。最终，曲线指数上升，呈现为一个 S 形，技术传播开来。我们很难想象一个比这一事实更公平或民主的想法了：今天的任何人——无论他们的所在地点、性别、语言、年龄、教育水平或财富——都可以充分参与到比特币（一种仍在其接受 S 曲线底部的快速增长的技术）里面来。



就可用性、容量、公众意识和商业利益而言，比特币目前远未达到所需的水平。没有足够的公司建立在比特币上；没有足够的学者专注于它；没有足够的教师传授它；没有足够的商家接受它；没有足够的非盈利基金会支持其发展；并没有足够的公众领袖认真地用其能力去帮助实现金融隐私。在这方面我们需要更多的关注度、参与度和批判性思考。

世界上只有不到1%的人口拥有过比特币。如果投入适当的时间和资源来开发用户友好的钱包、交易所和教育材料，比特币有可能为全球数十亿人带来真正的改变。比特币可以帮助任何人获得更多的财务自由，但它可能首先会帮助那些最需要它的人。

尼日利亚、土耳其、菲律宾、委内瑞拉、伊朗、中国、俄罗斯或巴勒斯坦的人民在他们的金融体系中没有与西方国家一样的自由、人权和信任。对他们来说，比特币是一种出路。

选择退出、沉默和离开是抗议的新形式。为了实现变革，个人无需与成千上万志同道合的人进行协调，就可以每天或每周一次地淹没街道。这些人可以像发送电子邮件一样轻松地转走他们的财富。现在，一次一个人就能发起抗议。最初的接受度将是涓涓细流，然后汇聚成溪，最终成为滔天洪水。

未来在你的手中

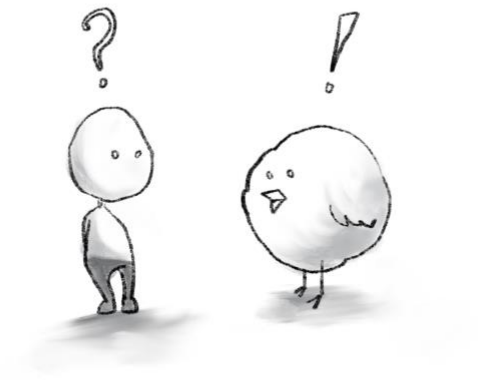
比特币是一项意义深远的发明，为当前货币体系和经济体系的许多问题提供了新的替代方案。不平等、垄断的跨国巨头和威权主义，在某种程度上是由于国家对货币的控制来驱动的。随着世界了解到比特币以及它如何通过技术手段实现自我主权，权力将在全世界以显著的方式变得去中心化。相比威权体制，更多政府会尊重人的尊严、价值与才能。相比与客户脱节的跨国企业，将会有较小的公司为客户服务。虽然结果平等是不可能的，但比特币将通过使人类能获得并持有他们创造的价值，从而创造公平竞争的环境。

只需一部便宜的智能手机和互联网就能参与下一次金融革命，有什么比这个想法更加公平呢？没有银行，没有政府监管机构，无需许可就能成为这个未来的一部分。

通过从掌权者的突发奇想那里夺回对财富的控制，每个人都可以更自由地创造他们自己的命运。

比特币以一种在 21 世纪初从未想到的方式实现了人类自由。

请接过这棒火炬，传阅这本手册，让更多人知道比特币。



比特币问答

在过去的几年里，新手和怀疑论者提出了很多关于比特币的问题。本节试图回答重要和常被问到的问题，解决关于比特币的一些神话、挑战、缺点和常见困惑。本节旨在提供足够的基本信息，让对比特币好奇的人们有一个正确的认识开端，但绝不是详尽无遗的。

谁是中本聪？

中本聪是比特币的匿名创造者。

在比特币历史的前两年里，中本聪是该社区的积极成员。中本聪经常在线发布有关比特币技术及其社会影响的想法，同时为软件开发做出贡献。2010 年末，中本聪失踪了。

中本聪拥有价值数亿美元的比特币，任何人都可以在区块链上看到它们。这些比特币从未动过，可能是永久性的遗失了。在撰写本文时，中本聪的身份尚未揭晓，这使其成为 21 世纪最大的谜团之一。

谁控制比特币？

没有中央权威在负责比特币。没有 CEO，没有董事会，也没有控股公司。比特币最强大的特性之一，是它的创造者不再参与其中。

全世界有成千上万的验证者来验证比特币区块链的正确性，并存储比特币交易的完整历史。这些验证者被称为*全节点*。

如第 2 章所述，世界各地的矿工的都在竞争生产区块。这些区块由全节点验证。用于运行这些全节点的软件由比特币开发者编写。当然，这些区块里的交易大部分时候是由用户从他们的交易所、钱包或支付处理商发起的。所有这些参与者对比特币的运作都至关重要，但他们都没办法*控制*比特币。

如果开发人员决定创建截然不同的全节点软件，那么几乎没有人会去运行该软件。如果矿工试图把不符合验证要求的新交易区块偷偷放到链上，全节点会拒绝该区块。如果矿工试图发起政变，在网络上施加新功能，他们也会失败，因为他们无法强迫其他全节点用户运行他们不想运行的软件。

因此，比特币的任何变化都需要达成共识。从这个意义上讲，比特币治理模式类似于具有制衡机制的民主系统。矿工就像政府的行政部门，处理日常事务运营和执行规则；开发者就像立法部门，制定和通过新法律；（全节点客户端的）用户是司法部门，确保其他两个部门不做任何违宪的事情。

比特币是不是波动太大了？

自 2009 年诞生以来，比特币经历了巨大的波动。从更长的时间尺度来看，比特币自成立以来已经大幅升值，在撰写本文时，从不到 0.001 美元到超过 11000 美元。正如第 3 章所解释的那样，有几个因素推动了其长期的价格上涨，并且有可能会继续上涨。

中本聪在一开始就设定了比特币的货币政策。任何个人或团体都无法决定创造更多比特币或更改其供应时间表，因为全节点将拒绝这种改变。

结果，由于没有央行的校正机制，比特币将更容易受到市场操纵。央行可以印新钱或回购更多自己的货币来维持价格的稳定。作为一种去中心化的货币，没有纠正的监管机构，比特币将继续经历波动，因为它被世界各地采用。

经济现实是这样的：货币必须在通过中心化的短期价格稳定和通过去中心化的长期升值之间做出选择。中本聪选择了去中心化。

最重要的是，比特币的波动并没有阻止它拥有巨大的现实价值——作为一种供身陷破碎金融系统之中的人们使用的金融工具。比特币的用例，包括逃避制裁、恶性通胀、资本管制和监控。现在，日常波动是持币者们一直愿意付出的一种妥协。

究竟是什么在支撑比特币的价值？

这个简短的回答是：人民支撑着比特币（people back Bitcoin）。有足够的投资者购买它，所以它有价值。有关比特币历史价格上涨的详细解释，请参阅第 3 章。比特币作为一种资产是稀缺的，有实用性的，并且作为一种技术能做到其他金融工具无法做到的事，对它的需求是全球性的。

怎么能相信比特币？

现代世界充满了复杂系统与设备，它们没有被充分理解，却受到了信任：医疗保健被提供给了不是医生的人，天气预报发布给了不是气象学家的人。笔记本电脑由不是电气工程师的人使用。旅行者不必理解空气动力学就可以乘坐飞机旅行。

信任新货币体系的标准应该更严格，因为这种信任经常被滥用，本书中已经有了诸多记录。但最终，使用和信任比特币并不需要学科知识专长。最终，收发比特币就像收发电子邮件一样简单。目前，对比特币感兴趣的人肯定会自己研究。本书的“其他资源”部分列出了许多优秀的信息来源，包括比特币核心源代码、其他书籍、网站和播客。

比特币有多可靠？

如果使用得当，比特币比任何中心化支付处理商都更安全、更强大、更私密。例如，万事达和维萨会时不时地中断。自 2009 年 1 月上线以来，比特币在其历史中有 99.98%的时间是完全可用的。信用卡公司也经常出售客户信息并被黑客入侵。比特币无法出售任何有关其用户的信息，因为没有人可以控制比特币或者获得其背后的用户信息。与支付处理商和银行不同，自从 2010 年价格上涨至 0.10 美元以上以来，比特币从未遭到过重大的黑客攻击。没有任何人的币在网络层面被盗。这是一个了不起的记录。

为什么有这么多交易所被黑客入侵过？

加密货币交易所非常受欢迎，它既是投资者首次购买比特币的地方，也是投机者把比特币兑换成法币或其他加密货币的地方。结果，交易所代表其客户持有大量比特币和法币，这使它们成为黑客和窃贼的诱人目标。托管服务还存储其客户的个人身份证、护照和家庭住址的副本等等，作为其 KYC（“了解你的客户”）程序的一部分。

攻击可以在内部和外部发生。内部攻击可能来自有权访问交易所系统并使用该系统窃取客户资金的员工。外部攻击是由利用软件漏洞，安全性较差的操作系统，或者是社会工程学来窃取比特币的黑客进行的。

许多交易所都受到过内部和外部的攻击。案例包括日本的 Mt.Gox，香港的 Bitfinex，欧盟的 Bitstamp，以及最近加拿大的 Quadriga。每一次都导致数百万美元的比特币丢失。这些黑客行为向允许他人托管其比特币的用户发出了强烈的警告。在交易所进行交易的客户可以定期将比特币提取到个人钱包中，以避免任何潜在的由于黑客导致的损失。

犯罪分子会用比特币来洗钱吗？

是的。犯罪分子把比特币用于洗钱和非法活动，并且他们会继续这么做。最著名的案例是丝绸之路，这是一个暗网市场，在这里比特币被用来买卖在美国被认为非法的药品。

因为比特币是一种无需许可的技术，任何人都可以使用它，就像手机或互联网一样。很少有人会质疑今天这些普遍存在的技术的合法性，或者因为不良行为者使用它们而要求禁止它们。但许多人会对刚出现的技术持怀疑态度。

无论如何，当今世界上绝大多数的金融犯罪都是通过受监管的银行和汇款人，利用现有的金融系统来进行的。大多数欺诈是由政府和跨国公司实施的，而不是由顽劣的个人。民主政府已经制定了反洗钱规则（AML）来迫使银行停止某些交易，但每年仍有超过 1 万亿美元的资金通过银行系统进行洗钱。举个例子，最近的报道披露，丹麦丹斯克银行（Danske Bank）的一个办事处就洗了惊人的 2300 亿美元，这超过了撰写本文时所有流通的比特币的市值。

因此，尽管犯罪分子使用了比特币，但犯罪分子更喜欢法币体系。

比特币是庞氏骗局吗？

庞氏骗局承诺为投资者在风险很小的情况下带来巨大的利润。庞氏骗局通过把向后期投资者收取的钱支付给早期投资者，从而让早期投资者获得承诺的回报。除了试图让尽可能多的新投资者偿还以前的投资者之外，并没有真正的盈利机制。当没有新投资者进入这个骗局的时候，这个计划就会崩溃。

比特币不是庞氏骗局。比特币背后没有一群人试图吸引新买家来偿还老买家的本金。然而，策划庞氏骗局的人可以像对待所有其他形式的货币一样接受投机者的比特币。

比特币是泡沫吗？

当投机性投资者以远远超出其基本价值的合理价格购买某种金融资产时，就会出现泡沫。一旦对资产的信心丧失，泡沫总会破灭，没有其他投资者愿意以要价购买。历史的例子包括 16 世纪的荷兰郁金香，18 世纪的南海公司和 21 世纪初的互联网股票。

第 3 章描述了比特币价格波动的一些主要驱动因素。由于资产具有刚性货币政策的自然波动性，定期供应冲击，以及其他加密货币的不稳定性和崩溃，市场操纵以及比特币交易的杠杆性质，出现了几次价格飙升，随之而来的是重大崩溃。这种趋势可能会持续下去。

在考虑比特币的长期价值，价格驱动因素以及比特币的持仓分散性，随着更多人使用比特币，其价值自然会增加。与郁金香或互联网股票不同，随着全球越来越多的人获得比特币，比特币的价格在每次重大市场崩盘后都会反复回升并呈上升趋势。

什么是泰达币以及它如何影响比特币？

泰达币（USDT）是一种理应与美元挂钩的数字货币。为实现这一目标，泰达币背后的公司打算用公司银行账户中的每一美元支持流通中的每个泰达币。这让考虑数字货币变得更容易，因为大多数人仍然在用法币本位思考，因此将 USDT 作为美元的代理货币使得所有人都可以在币币交易所中进行美元本位的数字货币交易。

然而，在 2019 年 4 月，泰达币的总法律顾问透露，他们的美元只能支持流通中 74％的泰达币。如果泰达币与美元脱钩，其价格崩溃可能会导致短期比特币波动。但是泰达币的许多竞争对手已经准备好代替它的位置。

政府可以禁止或关闭比特币吗？

因为没有公司，没有中央协调的服务器组，也没有哪个团队在运营比特币，所以没有切实可行的方法来关闭网络。

比特币是开源软件，这意味着源代码可以在互联网上公开获得。由于人们无时无刻都在看着这些开源的信息，因此破坏或更改该软件非常困难。任何人都可以下载、使用、复制和运行比特币软件并验证账本。这被称为运行全节点。网络上的节点越多，比特币就越有对抗破坏的韧性。

即使是一个庞大而富有的警察国家也无法阻止其公民使用比特币。由于网络没有单点故障，政府无法关闭比特币网络。

威权政府可以禁止人们拥有比特币，但执行起来将非常困难。由于其数字特性，隐藏比特币相对容易。可以将比特币存储在手机里、USB 设备里、甚至是一个人的头脑里，这将难以被发现和惩处。相比之下，政府寻找和没收黄金、房地产、股票和银行账户中的法币都相对容易。

比特币合法吗？

大多数情况下，是的。截至 2019 年 8 月，除纳米比亚、阿尔及利亚、玻利维亚、伊拉克、摩洛哥、尼泊尔、巴基斯坦、阿联酋和越南外，所有国家都允许公民持有比特币。从监管的角度来看，比特币已经走过了漫长的道路：在过去 10 年中，比特币已经从被视为网络罪犯的钱转变为被国际货币基金组织、美国国会议员和华尔街承认的资产。

在中国，政府已经对加密货币交易和 ICO 进行了监管，但比特币在法律上被认为是数字财产。即使在伊朗，比特币挖矿现在也是一个合法化的行业。

在非洲大陆，大多数国家的政府都没有公开立场。在尼日利亚和肯尼亚这样的地方，公职人员警告不要使用它，但没有具体的规定。南非是目前唯一正式接受和监管比特币的非洲国家。

在加拿大、美国和欧盟，拥有和使用比特币是合法的。

一些国家为希望经营加密货币交易的公司创建了一个特定的许可框架。其中包括日本、马耳他、菲律宾和泰国。

税收影响更复杂，取决于每个政府对比特币进行分类的方式。如果税务机关考虑比特币为财产，那么个人将会根据其购买、清算、升值和贬值被征税，类似于房地产。

展望未来，如果政府想密谋禁止比特币，他们不太可能达成协议。即使一些国家成功地制定了禁令，其他国家会跳出来欢迎比特币矿工、企业家和交易者。人才和财富会向那些友好的司法管辖区迁移，使得限制性政府重新考虑他们的政策。

挖比特币是否浪费能源或者对环境不利？

截至 2019 年 6 月，比特币网络消耗约 73 太瓦时的电力。这比奥地利（69 太瓦时）略高，但远低于中国（6100 太瓦时）和美国（3900 太瓦时）这两个最大的能源消费国。

批评者很快指出，这是巨大的能源浪费。虽然这在数字上是正确的，但它没有解答比特币是否浪费能源或对环境不利这一问题。比特币矿工通常使用的能源类型和比特币提供的价值可以为这一问题提供一些背景。

比特币挖矿预防能源浪费

比特币挖矿可以帮助过剩能源产能找到一个好用途。挖矿是一项需要四处流转的业务，也是低利润业务。因此，矿业公司有特别大的动力来寻找最便宜的电力。通常，最便宜的能源来自处于未被使用的电力产能，或者是在偏远难以无法进入地方的产生的电能。

大多数比特币挖矿发生在中国，在那里发电厂在任何特定时间共同产生 200 太瓦时的剩余。由于无法存储这么大的电力（世界上最大的电池农场只能容纳约 0.5％的电量）——并且由于不可能有效地将电力传输到偏远地区。发电厂可以购买比特币挖矿设备并将多余的能量转化为新的比特币，而不是浪费这种潜在的能源。在能源产生过多的任何地方都是如此。

比特币矿业对可再生能源的依赖

今天的大多数比特币挖矿都采用可再生能源，对环境的成本最低。根据最新估计，目前大约 75％的比特币挖矿都采用水力、太阳能，风能和地热能所产生的电。大约 50％的可再生能源比特币挖矿在中国的一个地区完成，由水力发电大坝提供动力。

水力发电厂具有巨大的能源生产能力，但往往未得到充分利用。由于挖矿作业可以放置在水力发电厂旁边，比特币挖矿在现场就可以使用过剩的产能，从而消除了传输成本。产生的收入使水力发电的生产和研究更有利可图。通过这种方式，比特币挖矿补贴了水力发电。

挖矿还可以激励更多的太阳能、风能和地热能的产量开发。

比特币挖矿让安全、可获取的货币成为可能

比特币矿工为网络提供安全保障。正如第 2 章所讨论的那样，矿工为了竞争有效块区块而进行的工作量证明所需的电力使得欺诈成本非常高。比特币挖的越多，攻击网络就越困难。用于保护账本的能源可以与创建和维护保护 2000 亿美元资产的高安全性保险库的成本进行比较。

比特币可能只是生活在第一世界的人的众多金融选择之一，但在世界其他地方，Venmo 或 ApplePay 等支付服务不可用。将比特币挖矿视为浪费能源其实是弱化了比特币给技术底层金融阶级带来的实际效用。这种能源的一部分用于处理没有银行账户或身份证的人的交易，或者不希望政府严格监督他们的金融活动的人。银行和信用卡在美国这样的地方可能会超过比特币的效用，但对于迪拜的无银行账户的移民工人或生活在联合国制裁下的伊朗人来说，他们什么都做不了。

能源利用与技术创新

比特币是一项重大的技术创新，它在本书中概述的许多内容是当前货币体系所无法做到的。从历史上看，新技术比它们取代的旧系统需要使用更多的能量。例如，考虑汽车对马的破坏; 现代医院的野外帐篷; 用洗衣机洗手;冰箱冰箱;和电灯的油灯。技术创新的电力成本被其提供的改善的生活质量所抵消。随着文明的进步，每个人消耗更多的能量。创新让社会变得更好，但是创新从来都伴随着权衡之后的选择。比特币的权衡后的选择是用电力使用，以换取公平方便和安全的货币体系。比特币耗费了大量能源，但它推动可再生能源

的创新。比特币提供了巨大的价值，特别是对穷人和受压迫者而言，取代了使用更多能源的有缺陷的旧系统。

如果有人用超级计算机或量子计算机攻击比特币网络会怎样？

从理论上讲，具有足够计算能力的攻击者可以破坏比特币网络。在实践中，这很难做到。

使用当前的硬件，攻击者必须以超过 10 亿美元的成本资助、建造和运营挖矿设施，然后找到一个输出相当于 8 个胡佛水坝的能源供应商。诚实地用于挖矿的相同资源将是一个非常有利可图的企业。因此，这种攻击在经济上是不合理的。

在撰写本文时，这些都适用于量子计算：

1. 与传统计算机相比，量子计算机的速度非常慢，达到了很多个数量级。
2. 量子计算机的构建成本非常高，并且在相当长的一段时间内仍然会成本过高。
3. 最著名的量子算法是一个重大的飞跃，但它们仍然需要数十亿计算机运行数十亿年才能破解比特币中使用的加密技术。

即使科学家们发现了可能破坏现代密码学的新量子算法，比特币代码也会采纳抗量子的加密技术。

换句话说，比特币的用户和开发者社区将能够比任何量子攻击者领先一步。虽然比特币社区应该警惕大规模的攻击可能性，但普通比特币用户不必担心。

比特币如何保持去中心化？

比特币最重要的特性之一是，世界上任何人都可以下载整个比特币账本的完整副本——包括在网络上进行的每一笔交易——并自行验证历史记录是否正确。

如第 2 章所述，这种做法称为运行*全节点*。运营一个全节点的便利性对于比特币网络的抗审查能力至关重要。如果比特币网络依靠少数几家公司或一小群富人来运行完整的节点，他们可以串通和篡改记录，或者窃取比特币。每个用户都可以通过运行全节点来验证所有内容，而不必信任其他任何人。如果需要昂贵的服务器设备或快速的互联网连接来运行整个节点，这将迫使较贫穷的人信任其他人。该网络自然会集中在第一世界和高科技企业。

幸运的是，由于运行全节点的要求非常低，不同大洲的成千上万的用户（彼此完全不认识）会持续验证比特币的区块链。此外，市场上越来越多用户友好的硬件全节点可用，非技术用户可以在家中操作全节点。目前，麻省理工学院和斯坦福大学等机构的几位科学家正在帮助设计未来任何人在手机上运行全节点的方法，这将进一步改善比特币网络的去中心化。

比特币会保护隐私吗？

一个流行的误解是比特币是匿名的。比特币是伪匿名的，通过足够的侦探工作和取证分析，可以连接到用户的真实交易和身份。但通过适当的安全操作，精明的比特币用户可以将交易伪装到使监控变得极其困难的程度。然而，如果有足够的时间或资源，国家或公司仍然可以追踪使用比特币的个人。

也就是说，比现有的支付系统，比特币为交易提供了更好的隐私。可以使用比特币进行在线购物，而无需泄露私人数据，如某人的姓名，银行帐户或地址。这是对现有银行系统的改进。当今的政府、公司和商家在每天共享这类系统，销售或泄露个人数据。

比特币在持续进行预期中的改进，如闪电网络、Taproot、Graftroot 和 Schnorr 签名，这些会使私人比特币交易更加便宜和容易。比特币有可能成为一种出色的隐私技术，使得大规模金融监管变得极为困难。

互联网曾经完全开放和公开。随着用户和企业需要更多的私人交易，工程师在原始互联网之上增加了隐私层。现在可以使用自动发送加密消息的应用程序进行私密通信。比特币的开发将会遵循类似的路径。

比特币如何满足 70 亿人的需求？

1989 年，当科学家发明万维网在互联网上运行时，用户有朝一日可以交换照片或者视频的想法，在技术上似乎是不可能的。随着技术的不断完善和发展，互联网已经扩展到适应曾经不可思议的带宽密集型应用，如视频共享和会议。每分钟上传 300 小时的视频到 YouTube，每天观看 50 亿个视频。就像互联网一样，有很多方法可以扩展比特币。

正如第 4 章所讨论的，比特币的容量目前正通过闪电网络得到增强。除了增强交易隐私外，闪电网络还增加了比特币网络的容量。

闪电网络每秒可处理数百万比特币交易。比特币有望按指数级增长，而像维萨这样的传统支付网络通过增加越来越多的服务器来线性扩展。比特币可以彻底改变货币，并使用小额支付全新的产品，一次只有千分之一（1/1000）聪的价格。

通过结合谨慎、缓慢、超安全和抗审查的偶尔的*链上*交易，以及闪电网络里批量、即时和便宜的交易，比特币可以成为一个功能齐全的全球支付系统。这是一个值得追求的愿景，因为它将进一步将金融权力从政府和公司手中夺回并将其交还给人民。

虽然今天很难想象，但比特币满足数十亿人的需求并不是一个古怪的概念，与当年流媒体视频可以在互联网上有数十亿观众的一样。

比特币中存在极端的财富分配不均吗？

在早期阶段参与比特币的人确实有机会积累大量比特币。然而，区块链显示，2009 年至 2012 年的许多早期接受者也在同一时期出售了他们的比特币。许多 2011 年 1 美元的买家在几个月后以 4 美元的价格卖出，在此之后的几个月以 30 美元卖出。

许多早期采用者没有忍受早期的极端波动和不确定性的勇气，或者丢失了他们的私钥，导致他们的比特币永久丢失。那些还在坚持的人们许多在这个生态系统在处在婴儿期就开始持这个新生事物, 并真正相信比特币改变世界的潜力。今天，有几千个地址存储了大部分比特币。有些是非常富有的个人，但大多数是公司地址，用来存储数以万计的客户的财富（比如 Coinbase 和 Binance）。由于地址和用户之间没有一对一的关联，因此很难确切地说出财富的分布是什么样的。

比特币不会解决财富不均问题。任何说比特币可以解决财富分配不均问题的人都在说谎。然而，与当前的货币体系不同，比特币作为一种无法被政府贬值、普遍可获取的价值储存，为储户们提供了一个公平的机会，让他们可以随着年龄的增长保持他们的收入。

如果只有 2100 万比特币，整个世界怎么能用它们呢？

传统的法币单位通常被分为 100 个子单位，称为便士或美分。美元和欧元可分为 100 美分，人民币可分为 10 角或 100 分，捷克克朗可分为 100 个。

另一方面，比特币可以分为 100000000（一亿）个较小的单位。比特币的原子单位被称为聪（satoshi，或简称 sat），以比特币的发明者命名。

因此，比特币的总供应量为 2100000000000000 聪。就上下文而言，这比美元更可分割，截至本文撰写时，其 M2 货币供应量为 1500000000000000 美分。比特币的可分割性与美元相当或更好。

作为一项思考训练，将所有现有的聪分配给 70 亿人，每人可以有 300000 个。如果比特币成为世界的主导资金，那似乎足以满足每个人在经济活动上的可分割性。

我怎么买得起比特币？价格太高了！

比特币是可分割的，因此可以买一小部分比特币——价值 5 美元或 25 美元的比特币目前相当于 0.00044 比特币和 0.0022 比特币。

我如何获得比特币？

获得比特币的主要方法包括：

1. 挖矿
2. 购买
3. 赚取

挖矿

在比特币的历史上，比特币挖矿是一项利润率很低的业务。就像黄金挖矿一样，需要设备、行业关系和专业知识来盈利，这需要多年的经验和数百万美元的资金。因此，挖矿已成为重资源和专业知识的领域，对于没有经验的个人来说，挖掘利润不一定可期。对于新用户来说，通过购买或赚取获的比特币更便宜。

购买

有几种方法可以购买比特币，有些比其他方式更私密。比特币 ATM 和点对点交易快速且相对私密。

投资者可以注册在线交易所，其中许多都列在“其他资源”中。新客户需要提交他们的个人信息，批准过程需要几分钟到几天。这些公司就像银行一样，持有客户的比特币和法定货币。因此，使用它们会放弃一些隐私，但客户可以把购买所得的比特币提取到其个人钱包来确保其比特币的所有权。

赚取

使用比特币或闪电钱包，任何人都可以直接接收比特币作为商品或服务的付款。员工可接受比特币工资来获得以比特币而不是法币来支付的工资。

我如何使用比特币钱包？

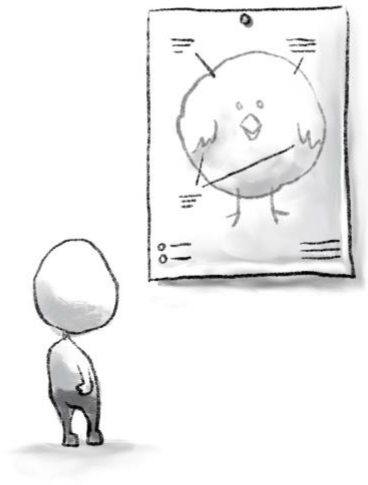
有许多不同类型的比特币钱包，包括硬件钱包、桌面钱包、手机钱包和在线钱包。每种钱包都有不同的安全、便利和隐私之间的权衡，用户们应该学习这些知识。

存储比特币的一种相当安全的方法是通过非托管钱包，这些钱包列在“其他资源”的**硬件钱包**中。同时，最方便的入门方式是下载免费的手机钱包，“其他资源”的**手机钱包**一栏列出了其中一些钱包。

下载后，设置比特币钱包的第一步是创建备份。此备份称为*助记词*（seed phrase），用于在钱包丢失时重新创建钱包。种子短语是通常写在纸上的单词列表。由于种子短语可用于重新创建钱包，因此必须小心保护。把助记词看成金条或钻石。助记词具有重要价值，必须相应地加以保护。随着生态系统的发展，新的钱包专注于降低复杂性，同时提高可用性、安全性和隐私性。

设置钱包后，它可以为每个新付款生成唯一的地址。这与通常的银行支付方式不同，在这种情况下，客户通常只提供一个帐号。比特币通过发布唯一的收付款地址来提供更好的财务隐私，所有这些地址都属于同一个比特币钱包。

正如“为什么有这么多交易所被黑客入侵过？”这部分里面提到过的，使用托管服务的投资者会受制于交易所被入的风险。购买后把资金提现到个人钱包将缓解这种风险。



其他资源

比特币白皮书

中本聪的 *Bitcoin: A Peer-to-Peer Electronic Cash System* 是最初的杰作，它是过去十年金融创新的开端。

源代码

Bitcoin Core 是比特币参考全节点软件的源代码。它最初由中本聪创建，拥有来自全球 500 多名开发者的贡献。

书

Andreas M. Antonopoulos 的 《互联网货币》（第 1 卷和第 2 卷） 用一系列文章和演讲深入探讨了“为什么是比特币”。

吉米·宋的 Programming Bitcoin 是一本来自比特币编程领域领先教学者的实用技术指南，适用于有兴趣使用该技术并为该技术做出贡献的开发人员。

Saifedean Ammous 的 The Bitcoin Standard 提供了货币的经济历史，并解释了比特币如何成为央行的替代品。

Yan Pritzker 撰写的 Inventing Bitcoin 逐步说明了比特币如何运作，只需要高中水平的数学背景。

Kalle Rosenbaum 的 Grokking Bitcoin 是比特币如何运作的完整图解指南。

Bitcoin Money: A Tale of Bitville Discovering Good Money 是一本儿童用书，上面有丰富多彩的人物，帮助孩子们了解比特币。

Mastering Bitcoin: Programming the Open Blockchain 是 Andreas M. Antonopoulos 写的比特币编程和综合指南。

网站和出版物

Bitcoin.org 包含有关如何入门的有用信息，以及文档和其他资源的链接。但我们不推荐使用 Bitcoin.com，因为该网站故意将其他数字货币与比特币混为一谈，试图让用户购买这些其他类型的数字货币。

Bitcoin.page 是由 Jameson Lopp 维护的的有关比特币的教育资源和信息的宝库。

比特币 Wiki 是比特币用户、开发者、企业以及任何对比特币感兴趣的人的社区公共资源。

Coin Center 是一家总部位于美国的非盈利组织，专注于比特币和其他加密货币所面临的政策问题。他们不断发布各种有深入洞见的文章。

Bitcoinmining.com 拥有比特币挖矿的资源, 它是如何工作的，入门以及硬件比较列表。

Global Coin Research 专注于美国和亚洲之间的加密货币趋势。

播客

Tales from the Crypt 是由 Marty Bent 主持的一个播客，与有趣的人讨论比特币。

What Bitcoin Did is 是每周两次的节目，彼得·麦科马克在比特币社区采访领导者和影响者。

The Stephan Livera Podcast 是一个播客，专注于教育访谈和有关比特币经济和技术的讨论。

Noded 是由 Michael Goldstein 和 Pierre Rochard 主持的播客，重点关注比特币的新技术发展。

Off the Chain 是 Anthony Pompliano 的播客，探讨新老金融体系的投资者如何考虑像比特币这样的数字资产。

Unchained 和 Unconfirmed 是每周播客，主持人 Laura Shin 采访加密货币中的著名人物。

Let's Talk Bitcoin 通过主持人的一系列访谈和对话，介绍加密货币所涉及的想法和人员。

The Bitcoin Knowledge Podcast 中 Trace Mayer 采访了比特币行业中的杰出贡献者，以帮助听众更好地理解该技术。

在线交流

免责声明：虽然本节提到了比特币生态系统中的特定网站，应用程序或服务，但这不应被视为代言或投资建议。与本书的其他部分一样，我们鼓励读者进行自己的研究。

法币交易所

Bitfinex - 始于 2014 年的香港交易所

CashApp - iOS 和 Android 上的 Square 应用程序，用于用借记卡购买比特币

Kraken - 始于 2014 年的美国和欧盟交易所

币币交易所

Binance - 始于 2017 年的马耳他的交易所
BitMex – 始于 2014 年的塞舌尔交易所
Bittrex - 始于 2016 年的美国交易所

点对点交易市场

LocalBitcoins - 始于 2012 年的芬兰比特币市场
Paxful - 始于 2015 年的美国比特币市场
Bisq - 始于 2014 年的主打隐私的市场

钱包

托管钱包（客户不控制他们的私钥）

Blockchain.info
CashApp
Coinbase

非托管（客户控制他们的私钥）

BreadWallet - iOS 钱包
Bitcoin Core - 桌面钱包
Casa Keymaster - 支持硬件钱包的 Android 和 iOS 多重签名应用
Samourai - Android 钱包
Wasabi - 桌面钱包

硬件钱包（客户控制他们的私钥）

ColdCard
Ledger

Trezor

全节点解决方案

Casa Node - 即插即用闪电网络和比特币全节点
Nodl - 比特币和闪电网络全节点

词汇表

地址 - 与银行帐号类似，比特币地址是接收比特币的地方。每个地址都有一个相应的私钥，允许所有者通过创建数字签名来使用比特币。

bancor - 1944 年在布雷顿森林会议上提出的全球货币单位。

Bitcoin - 由中本聪创建的去中心化、数字化、稀缺的货币系统。

bitcoin - 比特币网络上的价值单位。每个比特币都是 100000000 聪。

区块 - 一组比特币交易与一个稀有的工作量证明号码相结合。一个区块相当于比特币会计账本中的单独一页。大约每 10 分钟创建一个新区块。

区块链 - 由比特币开创的去中心化账本系统。在比特币中，区块链追踪每个地址中有多少比特币。区块链的组成部分是区块。

区块链技术 - 旨在以某种能力利用比特币区块链创新的系统。除了比特币和少数其他加密货币之外，没有任何一个被广泛采用。

BTC - 用于在交易所、商家和钱包上代表比特币的符号/代码。XBT 也是一种流行的符号。

中央权威 - 为特定系统做出决策的机构或组织。

中心化 - 具有单点故障的系统。例如，这可以是一个由个人、基金会、公司或政府运营的系统。

币币交易所 - 一种只允许在加密货币之间进行交易的交易所

去中心化 - 没有单点故障的系统。

数字签名 - 用户或签名者知道一个给定地址的私钥的证明。这在概念上类似于签署银行支票以确认给定的人是帐户持有人，但具有实际上不需要透露该人笔迹的额外优点。发送比特币时，发送人签署交易，证明比特币的所有权，而不泄露私钥。

美元本位 - 在全球贸易中由美元占货币主导地位的制度。始于 1944 年布雷顿森林之后，并于 1971 年通过石油美元延续。

法定货币 - 由央行发行的货币。

法币交易所 - 允许用法币直接交易加密货币的交易所。

FOMO - “害怕错过某种机会”，这个术语通常用于描述从众心理和不合理的购买决策。

全节点 - 用于验证交易和区块链完整性的软件。

金本位 - 一种占主导地位的世界货币体系，其中一个国家的法定货币的价值受到政府储蓄黄金数量的支撑。

减半 - 比特币网络上每四年发生一次事件，一个区块内的挖矿奖励减少一半。

KYC - “了解你的客户”，这是政府强制执行的一种做法，银行需要收集大量有关某人的个人信息，以便为他们提供金融服务。然后通过诸如美国银行保密法（US Bank Secrecy Act）等法律向政府提供此信息。

杠杆交易所 - 交易所允许交易金额高达存款金额的 100 倍

闪电网络 - 一种系统，用于将比特币的容量扩展到每秒数百万次交易。这项创新还为比特币交易增加了重要的隐私。

流动性 - 在特定时期内可以用于买卖的资产数量。

矿工 - 使用专用计算机通过工作量证明来创建新区块的个人或团体（被称为“矿池”）。

挖矿奖励/矿工费用 - 矿工收到的用于处理交易和保护比特币网络的比特币。

链下交易 - 一种未记录在比特币区块链中的交易，与闪电网络交易的情况一样。

链上交易 - 直接在比特币区块链中处理和记录的交易。

点对点交换所 - 一种需要亲自见面来执行交易的交易所

私钥 - 类似于银行帐户的密码，私钥解锁了从给定钱包转移比特币的能力。因此，私钥的所有权与拥有比特币相同。

工作量证明 - 矿工证明他们已经花费能量来提议可以把新的有效区块添加到区块链的过程。

公链 - 任何人都可以下载、访问和浏览的区块链。

sat / satoshi 聪 - 比特币的最小单位。100000000 聪是 1 比特币。

中本聪 - 比特币的创造者。

钱包 - 允许用户收发比特币的应用程序或硬件设备。

白皮书 - 一份权威的（通常是学术性的）报告，旨在向读者充分告知一个特定主题。描述比特币及其技术细节的原始文件于 2008 年 10 月由中本聪以此格式呈现。

致谢

作者们要感谢以下人员为这本书付出的时间和专业知识，如果不是他们，这本书的编写将会是一份更加艰难的挑战性工作：

Leigh Cuen
Sam Corcos
Nick Foley
Irl Nathan
Jane Song Lee
June Park
Rodrigo Linares
Nick Neuman
Tomiwa Lasebikan

我们还要感谢以下个人在我们的冲刺期间对我们的支持：

Bill Barhydt
Daniel Buchner
Cryptograffiti
Jill Carlson
Juan Gutiérrez
Han Hua
Ben Richman
Bill Tai
Mike Youssefmir
Sebastien Lhuilieri

这些年来，以下人士既为我们提供了信息，又给我们带来了启发：

Nick Szabo
Andreas Antonopoulos
Jameson Lopp
Elizabeth Stark
Marek Palatinus
Pavol Rusnak
Michelle La

我们还要感谢以下组织鼓励我们编写此书：

Blockchain Capital
BloomX
Casa
Human Rights Foundation
BuyCoins Africa
Open Money Initiative
University of Texas

最后我们非常感谢 Tim Chang 让我们用他漂亮的房子，以及最重要的，感谢我们的家人和爱人们为我们加油助威。