
The
Internet
of
Money
A COLLECTION OF TALKS BY
Andreas M. Antonopoulos
VOLUME ONE

互联网货币

翻译：节奏大师

作品鉴赏

我一直在想如果从一开始就实现通过浏览器进行一键支付，世界会发生什么变化。比特币让我们最终了解到《互联网货币》这本书，但这本书不只称颂了比特币，还赞许了开放协议、人与人之间的在线沟通带来的变化以及网上创新的能力。

——网景和 Andreessen Horowitz 联合创始人 马克·安德森（Marc Andreessen）

Andreas M. Antonopoulos 撰写的《精通比特币》一书是最好的数字货币技术性书籍之一。与之相媲美的则是他撰写的《互联网货币》一书，该书是最好的比特币书籍之一，为广大读者编制了作者的演讲内容。强烈推荐！

——21.co 首席执行官 Balaji Srinavasan

三年来，人们对比特币颠覆性变革潜力的认知迅速增长，作为比特币底层技术的区块链也迅猛发展。因此，人们不仅要掌握此非正统技术的操作方法，还需领悟其对社会的深远影响。为帮助人们实现该目标，Andreas Antonopoulos 比任何人付出的都多。读懂他会让你变得更智慧。

——《加密货币时代：比特币和数字货币如何挑战全球经济秩序》的合著者 Michael J. Casey

序

—Don Tapscott

2014 年初，我和我的儿子亚历克斯开始撰写《区块链革命》一书。此前，我一直致力于撰写《数字经济》一书的 20 周年纪念版。随着对过去二十年的变化和未来发展的思考，我已经对比特币和加密货币着迷了。期间，亚力克斯是投资银行 Canaccord Genuity 的高管。2013 年，他就注意到初创时期的公司对比特币和区块链的热情日益高涨，随后便带领他的公司进入此领域。2014 年初，我们父子俩在蒙特朗布朗（Mt. Tremblant）滑雪之旅期间共进晚餐时，集中讨论了我们在该领域的合作方式，简言之，我们决定写一本书。

我们得知 Andreas M. Antonopoulos 的作品后，迅速把工作重心放在 YouTube 上大量收集他的演讲作品。我记得，我们一遍又一遍观看他的演讲视频，每次长达数小时，并在观看过程中做大量的笔记。他渊博的知识、对复杂概念流利地解说和清晰的思想令我们惊叹不已。我们看到在每一次演讲过程中，他都充满着激情、具有深远的见解；他使用强大的类推法，用简单的术语来介绍最难理解的主题内容。记得我当时还在想“这个人怎么能对这么新颖的事物有如此深刻的了解呢？”

2013 年，YouTube 的一段视频中 Andreas M. Antonopoulos 与其他人围桌而坐进行会谈——当时数万人在场观看这场会谈。另外一段视频则显示了他在面对逆境时的超然洒脱，最令人难忘的就是他做过一场关于“比特币中立性”的杰出演讲。当时他在一个大型会场做演讲，但台下只有两位观众。当镜头拉近时，从他演讲的状态和表现力来推断，你可能认为台下座无虚席。

Andreas M. Antonopoulos 的坚持不懈是件好事。幸而，他的这些演讲和其他的讲话都被拍摄下来了，现如今，我们都能从中获益。《互联网货币》一书对他的演讲内容进行了严格的编辑，包括我在内的许多人必定对该书的出版心怀感激。他的每一场演讲都各具特色（而非预录的）、即兴而且是令人信服的。很少有人具备对挑战性主题进行即兴演讲的能力，更

别说互联网货币的主题了。

大多数技术革命在早期阶段都受控于创建者，这通常就造成了概念性匮乏和解释不明的问题。终于，继 Arpanet——互联网的前身创建后，大思想家们花费数十年的时间深挖第一代数字革命对我们的生命可能隐含的蕴意。互联网的第二个时代——数字货币革命随之来临。比特币在最初的几年中受控于开发者，而后受控于投机者——某种意义上讲，受控于两者。比特币的早期拥护者提出如何使它人们摆脱政府监管的理论，但要想让全世界都了解加密货币的重要性，仅仅宣传它的思想理论是不够的，还需有人来解释它是如何操作的。

简言之，Andreas 对其做了解释。事实上，我相信他对比特币的定义和对比特币起到的重要作用，历史上无人能比。当我们要为自己的书深入采访某位思想领袖时，不用说，我们几乎都想首先采访 Andreas。

通过阅读这份演讲集，我们了解到 Andreas 在几乎没人听说过比特币的时候就一直进行着丰富又深刻的演讲，这真是让人难以置信。不过，不要因为它是历史记录就带着异样的心态去阅读，而是要理解它那丰富的见解，这些见解纵使不具高度相关性，但同样有关联。

Andreas 早期就在做一些重要的事情，亚力克斯和我都认为一种新型互联网正在形成。过去几十载里，我们已经看过了《信息互联网》，而如今我们亲眼目睹了《互联网价值》或被 Andreas 称为《互联网货币》的诞生。各位亲爱的读者需了解这次革命的影响肯定比第一代技术有过之而如不及。

请允许我插入说明一下，作为一名加拿大人，我是 Andreas 的隐秘思想的直接受益人。2014 年 3 月份，加拿大参议院授权参议院银行、贸易及商业常务委员会研究数字货币，特别是研究它的潜在风险、威胁和优势。最初，受媒体关于比特币被用来洗钱和实施犯罪的报道的影响，参议院否定了数字货币。Andreas 在委员会面前作证，而关于他出庭所做的区块链演讲，现在看来有几分传奇色彩，因为一位参议员曾告诉我“Andreas 冲击了我们的思想”（对于汇聚在这个朴实无华的加拿大议会厅里冷静的绅士们来说，这是一件非常艰难的事情）。

最后，参议院发表了一篇优异的报告，强调要积极把握机遇，强烈反对过早对区块链进行监管和干涉。非常感谢 Andreas，很喜欢这本书。如果你刚步入这个行业，准备加入冷静的加拿大参议员行列，也让你的思想饱受冲击吧；如果你觉得你已了解这个行业，请保持谦卑心态并自我激励吧。我非常感谢 Andreas 花时间将这些视频内容译成文字，这本书将为我们确保新型互联网实现其巨大潜力做出重要贡献。

Don Tapscott，加拿大安大略湖湾（Lake of Bays），2016 年 8 月 20 日。

*Don Tapscott 撰写了 15 本关于社会新科技的书籍，包括**《模式转移》**（Paradigm Shift）、**《数字化成长》**、**《数字经济》**、**《维基经济》**以及最近他和儿子亚力克斯合著的**《区块链革命：比特币背后的技术如何改变货币、商业和世界》**。他是 Tapscott 集团智囊团的首席执行官、多伦多大学罗特曼管理学院副教授、哈佛大学伯克曼克莱恩互联网及社会研究中心助理。*

前言

—*Andreas M. Antonopoulos*

当开始我的比特币之旅时，我从未想过会是这样。这本书就像是我探索比特币的短篇日记，它在一些演讲中发表，从 2013 年开始一直持续到 2016 年年初。

在过去的三年里，我已面向全球观众做了 150 多场演讲，录制了 200 多个播客节目，回答了数百个问题，接受了 150 多个电台、出版社和电视采访，在 8 部纪录片中露面，并撰写了《精通比特币》。这部作品的大多数内容都是可以在线免费获取的。本书包含的演讲仅仅是一小部分范例，由编辑团队挑选，让我们了解比特币、比特币的用途以及比特币对未来的影响。

每场演讲都是面向现场观众的，没有幻灯片或任何可视资料，而且大多是即兴演讲。演讲之前，我的脑海里都会有一个主题，但我的很多灵感都来源于与每一位观众的互动。每场演讲中，我都会尝试新想法，我的演讲话题也随之改变，先看看观众的反应，然后进一步展开。最后，一些以单个句子开头的想法会通过几场演讲演变为一个完整的主题。

当然，这个探索过程并不完美。我的演讲中可能会有一些小错误，我列举了日期、事件、数字和技术细节，并经常搞错这些信息。本书中，编辑们已校正了我的即兴错误、错误用词和口头错误，剩下的就是每场演讲的精髓——这正是我所希望的，而不是演讲时的文字整理稿。但是，通过这种校正，产生另一个代价：观众的反馈和能量、我说话时的语气和场内的观众自发的咯咯笑声消失了。对于所有的这些，您都可以在本书“视频链接”中的视频内看到。

这本书和我过去三年里的工作不仅仅是与比特币相关，它们反映了我的世界观、政治理念和希望，以及我对技术的痴迷和我无所畏惧的极客精神。它们总结了我对这项技术的热情以及我设想的令人惊叹的未来。这个愿景起源于比特币，一个风格奇特的密码朋克实验，它引发了创新的波澜，创造了“互联网货币”并彻底改变了社会。

编者注

几乎整个比特币社区都知道 Andreas 对比特币的贡献。除了他的书籍和视频作品外，他还是一位备受欢迎的演讲者，因其不断发表创新的、发人深省的、吸引人的演讲而备受赞誉。本书仅仅陈述了过去三年内比特币和区块链行业 Andreas 作品的一小部分节选。内容很多，仅仅决定选取哪些内容就是一项艰巨的任务。我们选择这些演讲是因为它们符合本书的标准，我们已经将十几个演讲涵盖在本书中了。这本书是第一册，我们希望能很快再出版一本。

基于这样的愿景，我们开始了这本书的编撰：为什么比特币如此重要，为什么我们许多人对比特币感到如此兴奋，我们进行了易于读者阅读、带有简短故事风格的概括。我们希望它能与家人、朋友和同事分享。它需要有吸引力，使科技便于理解；它需要能鼓舞人心，展现新的技术对人类产生积极影响；它需要诚实，承认我们目前的系统和技术本身的缺点。

尽管我们已经尽了最大的努力，但我们仍相信本书有可以改进和提高的地方：这是第一版。为了便于阅读，我们在某些地方进行了大量编辑，同时努力保持演讲的精髓。我们相信它已经取得了良好的平衡，并且我们对整本书很满意。希望你们也是。

为了让您的阅读体验更好，我们温馨提示：每场演讲都是独立的。*您会注意到一些重复的主题和类比，例如红旗法案或父母和孩子关于金钱的谈话。虽然这些例子偶尔会重复出现，但它们通常用来说明每场演讲中的不同观点。*

第 1 章 什么是比特币？

破坏，启动，扩展：希腊雅典：2013 年 11 月

视频链接：https://www.youtube.com/watch?v=LA9A1RyXv9s

致读者：我于 2013 年底做了这场演讲，比特币交易不再免费，但收费极低。当时，无论交易的货币价值多少，每笔交易费大约为 10 美分。

雅典的朋友，下午好！非常荣幸受到各位的邀请来这里做演讲。你想要破坏吗？我已经经历了破坏的阶段，彻底接受了革命的洗礼。今天，我们会讨论过去 20 年来在计算机科学领域最令人兴奋、最有趣、也许是最重要的技术发明——比特币。

比特币是一种数字货币，但它同时又是有别于数字货币的存在。说比特币是数字货币，就像是说互联网只是一部新奇的电话，或者互联网只跟电子邮件有关那样肤浅。货币功能只是比特币应用的第一步。比特币是一项技术，是一种货币，是一个完全去中心化的跨境支付和交易网络。它不需要依赖银行，更不需要依赖政府。

“说比特币是数字货币，就像是说互联网只是一种新奇的电话一样。”

在人类历史上，我们从未做到过这样的事情。这项发明确实是具有革命性意义的。当我们回顾过去时，我们会发现这是计算机科学发展史上一个历史性的时刻，它同样也是一场正在兴起的社会和政治革命。

所以，让我们开始吧。

1.1 发明比特币

比特币是一种数字货币，就像欧元或美元一样，只是它不属于政府。你可以实时安全的将其从世界任何地点发送到其他地方，交易费极低甚至不收费。两天前，我们看到了比特币网络上有史以来最大的一笔交易，有人一秒钟内在两个比特币账户之间交易了 1.5 亿美元，而且是零交易费。正因为如此，你才会了解这项技术将会对国际支付系统有多大的破坏性。但这仅仅是个开始。

比特币是一种数字货币。2008 年，一名化名为中本聪（Satoshi Nakamoto）的人提出了这一概念。他发表了一篇研究报告，假设已经找到了创建去中心化网络的方法，可以在没有任何中心控制机构的情况下达成共识、一致。如果你学过计算机科学或分布式系统，都会知道拜占庭将军问题。这一概念于 1982 年首次提出，截止到 2008 年，仍是个悬而未决的问题。然后，中本聪说，“我已经解决了这个问题。”猜猜接下来发生了什么？每个人都笑了，忽视他，甚至否定他。他发表了一份白皮书，三个月后，他发布了能让人们创建比特币网络系统的软件。

比特币不是一家公司，也不是一个组织。它是一个标准或协议，就像 TCP/IP 或互联网一样，不属于任何人。它能在简单的数学规则下运行，这些规则需要得到每个参与网络的人同意。通过这个简单的机制，通过中本聪的这项发明，比特币能够允许一个完全去中心化的计算机网络系统就网络上发生的交易达成一致，本质上就是确认目前谁拥有这笔钱。

所以，在这个点对点的完全去中心化的网络上，如果我从我的账户将钱汇入到其他人的账户中，就像发送电子邮件一样，中间没有任何人参与。每隔十分钟，在没有任何中心机构的情况下，整个网络就可以通过简单电子投票的方式对发生的交易达成一致。

这个特别的解决方案，也就是这项发明，远比货币重要的多。货币功能只是比特币应用的第一步——只是你可以在分布式共识系统中创建的第一个应用程序。其他应用程序包括分布式公平投票、股权、资产登记、公证以及我们以前从未想过的许多其他应用程序。

“这个特别的解决方案，也就是这项发明，远比货币重要的多。货币功能只是比特币应用的第一步。”

我在 2011 年第一次发现比特币，这是自互联网以来，我第一次被某种事物将创造的种种可能性所震惊。1991 年还是互联网的黎明时代，那时还是商业化的前期，我就看到互联网将会改变整个世界，但那时没有人相信我，我对比特币有完全相同的感觉。

今天，你们中的一些人也许听说过比特币，作为一种货币，某天它的价格非常高，未来某一天价格又非常低。在这里，我告诉你要忽略价格，忽略比特币作为货币本身，而要了解这项技术、这项发明以及它所创建的网络系统。如果我们搞砸了这个货币，我们会重新启用另一种货币。比特币这项发明，使其成为可能的这项技术，是不可能消失的。它在一个前所未有的范围内实现了创造去中心化组织的可能性。

1.2 人类的货币

目前大概有 10 亿人可以享受到银行服务、信贷服务和国际金融服务——主要是上层阶级，也就是西方国家。这个世界上有 65 亿人与国际金融没有任何联系，他们的金融体系在现金基础上运作，很少获得国际金融资源。他们不需要银行。但是这部分人中有 20 亿人已经有互联网连接了，通过下载简单的应用程序，他们可以立即成为国际经济体中的参与者，可以使用能够在任何地方流通的国际货币，没有任何的交易费用，也不需要受政府控制，他们可以完全点对点的与国际金融世界连接。比特币是人类的货币。它的核心是每个人都认同

并且没有人为控制的简单数学规则。把这 65 亿人与世界上其他人联系起来确实是具有革命性意义的。

“比特币是人类的货币。”

支付服务提供商将受到影响，这些大型公司收取高额交易费用将钱汇入贫穷的国家，这是一种剥削和腐败的局面。这些组织通过比特币可以免费实现的功能（跨国转账）获得了巨大的利润。正如一句互联网谚语所说“我只用 100 行 Python 代码就可以替代整个行业。”这正是我们用比特币所做的事情。

1.3 货币、商业与国际支付

现如今，你是怎么使用比特币的？简单来说，比特币可以作为一种货币。你可以认为是购买外汇：通过网络与交易所连接，电汇欧元，并使用这些欧元以当前的汇率购买比特币。然而，这不是最佳的方式。我们是创新者，对吧？我们想要破坏。最好的办法就是找到你可以提供的产品或服务，如果有比特币的人想要购买这个产品或服务，你就能赚取比特币。

1.3.1 支付问题的解决

如果你想在当前国际化环境中创办企业，那么成为全球化的企业有两个主要的障碍：第一个障碍是很难跨境运输产品和服务。有了互联网，我们就可以解决这个难题。现在我们可以创建虚拟的产品和服务，在世界上任何地方销售。因此，我们可以交付产品，但是我们仍有一个大难题：如何接收付款？比特币解决了这个难题，它使我们能够实时从世界任何地方接收付款。比特币网络可以使任何人发送小至十亿分之一个比特币，以当前的情况来讲，这是一笔非常小额的交易，当今的货币和支付系统是无法做到这一点的。信用卡是在 20 世纪

50 年代诞生的，它们当然不是为了互联网时代诞生的，而比特币却是为了互联网时代诞生。

因此，如果你可以发送支付百分之一或千分之一个欧元，你就可以出售内容，你可以做小额交易，你可以从百万人手上接收非常小额的付款。总的来说，你让货币变得有价值了。在可以发送千分之一或百万分之一欧元的同一网络上，你可以发送十亿甚至万亿欧元，而交易费用是一样的，因为费用取决于交易字节的大小，而不是金额。

1.4 中立性，犯罪分子与比特币

让我们回头看看互联网，我们可以从互联网的这堂课中学到比特币为什么如此重要。中立是互联网最重要的原则，互联网不区分机构的大小，它也不知道 CNN 和埃及博客作者之间的区别，但 CNN 和埃及博客作者在互联网上有着相同的话语权。

比特币不区分发送人、接收人和交易金额。这意味着，它能使每个公民、每个比特币用户在金融工具、支付系统和银行业务方面做出创新，你可以像花旗银行一样处理金融业务。这确实是具有革命性意义。

比特币改变了过去国际金融体系那种阶级式的结构。一直到今天，银行这种阶级式的金融系统仍通过限制访问来确保安全性，因为这是银行系统确保安全的主要方法——除非接受审查，否则无法进入该系统。比特币创建了完全平等和去中心化的网络，每个节点都是平等的，协议对交易来讲是中立的，它使用网络将创新推向了顶峰。我们曾经在互联网上见到的完全相同的景象：无需审批的创新——你的应用程序可以自由在互联网上发布，而无需任何人许可。你无需征求任何人的许可就可以用你的信息技术创造一个新行业。就比特币而言，你无需征求任何人同意就可以发明新的金融工具、新的支付系统和新的服务。你可以编写新

的应用，使它成为国际金融网络的一部分，并且与数百万的消费者进行联系。

现在比特币仍处于早期阶段，我们还没有友好的操作界面，使用比特币对我们来说是很困难的。它被犯罪分子使用从事犯罪活动，它也被世界上许多其它组织使用，并且要确切知道是谁在使用比特币并不容易。对于这些事情，我以前就听过。在 1991 年的互联网初期，互联网受到小偷、色情文学作家、海盗和犯罪分子的青睐。但是，无论那时还是现在，这都已经无关紧要了。因为犯罪分子能用这项强大的技术从事犯罪活动，我们其他人同样也可以用它去做那些积极正面的事情，并且在我们所有人中犯罪分子只是少数。

比特币创造了一个成熟的创新环境，因为它不仅仅是一种货币，同样也是一项技术、一种网络系统。我可以这样说：比特币今天的价格大幅上涨，我很高兴，因为我拥有一些比特币。但是，我不在乎价格。如果明早比特币崩盘，这项技术仍然是具有革命性意义的。就好比一个网站或一个应用程序崩溃，互联网也不会消失一样。

1.5 比特币机制

当你认识到比特币是一项技术而不仅仅是一种货币，你才会真正掌握它蕴含的重要意义。再次强调，这不仅仅是关于我们，而是关于另外的六十五亿人，这是关于将全球金融融合提升到一个前所未见层次的能力。从我们在特权世界的角度来看，这是一项伟大的技术，我们可以进行一些破坏性创新，我们可以制作一些有趣的应用。但如果你是一名肯尼亚农民，为了购买种子而筹集资金，现在就可以申请去中心化点对点的贷款了，你可以接触到来自世界各地的贷款人，这就不仅仅是一项技术了——这是真正改变人类生活。

世界上的绝大多数人都生活在压制和腐败政权之下，中央银行每月都要将恶性通货膨胀

强加在 30%。相对而言，了解比特币如何影响这些人尤为重要。使用互联网的人有 20 亿，其中拥有银行账户的人却只有 10 亿。我们可以改变这一局面。对于我们来讲，这并不容易。当你在这个世界上最强大的组织（银行）中引入这项破坏性技术时，他们是不会高兴的。目前，我们仍处于早期阶段，用那句老生常谈的话“首先他们忽视我们，然后嘲笑我们，对抗我们，最后我们就赢了。”我们仍处于被嘲笑的阶段，这很好，因为当他们与我们对抗时，他们就已经输了。当来自中国的投资者买进了 25 亿美元的比特币，从而使比特币可以跟美元的国际储备货币地位相抗衡时，这项技术就进入了全球化阶段。

1.5.1 竞争币：每个人的货币

世界上大约有两百种货币，但是却只有一种国际性货币。近两百种货币是由中央银行和政府控制的，但是却只有一种数学货币，那就是比特币。

“加密货币将会成为金融界的主流货币，你得尝试这种技术，你得往前看。”

我们将创建更多的货币。加密货币将会成为金融界的主流货币，它们将成为这个世界未来的一部分，因为它们已经诞生了，就这么简单，你不可能让这种技术消失，你得尝试这种技，你得向前看。我们在这个领域已经有超过 100 种竞争币，这表明创新的速度有多快，甚至超越了比特币。这里有很多种竞争币—— 使用同样的去中心化资产分类账技术，使用与中本聪相同的算法共识技术，其中一些币是通货膨胀的，一些是通货紧缩的，一些使用了滞留或负利率技术，一些是慈善性的并将一部分收入重新分配给了慈善组织。

我们可以不停地发明货币，并创造新的货币和金融工具。

1.6 可编程货币

总的来说，比特币是一种可编程货币。当你拥有这种货币时，就有了无限可能性。我们可以使用当前系统中依赖算法合约的许多基本概念，转换为可以在比特币网络上强制执行的数字交易。正如我所说的，没有第三方，没有对手方。如果我从网络的一端向另一端发送交易，那么这笔交易就是点对点的，中间没有任何人参与。如果我发明了一种新的货币形式，那么我就可以将它部署到全世界，并邀请所有人加入。

比特币不仅仅是互联网的货币，它更像是一种完美的货币，它的特点是实时、安全和免费，货币功能只是比特币应用的第一步。如果你了解这点，你看的就不仅仅是比特币的价格、波动或一时的跟风。从其核心来讲，比特币是一项革命性技术，并将永远的改变世界。

谢谢。

第 2 章 点对点的货币

货币的重新改造，伊拉斯姆斯大学，鹿特丹，荷兰，2015 年 9 月

视频链接：https://www.youtube.com/watch?v=n-EpKQ6xIJs

有很多人希望我谈一下关于比特币的最新讯息，但是我真正想谈的是货币的发展历史。我希望通过货币发展的历史背景来说明比特币的重要性。

2.1 货币出现的历史有多古老？

首先，对我们的听众有一个小问题：如果你觉得货币是一种技术，那么作为人类文明创造的一种技术系统，它诞生有多长时间？*现场观众此时给出许多千奇百怪的答案。*

对于这些回答我感到很惊奇，有说 400 年的，1000 年的或是 2000 年的。事实上，我们并不知道货币的出现有多古老了。部分原因是我们研究过某种古老的文明，但是它并没有货币出现。

另外一件让人们惊叹的事实是货币的出现甚至比文字更古老，考古学家通过对古人类文字的研究发现了象形文字和契形文字。当我们对这些古老文字进行研究时，我们惊奇的发现这些文字记载的内容竟然是货币！最古老的人类文字，记录的内容是账目。迄今为止我们发现的所有古文字，都是以分类账的形式记录的，所以货币的出现比文字更古老。

那么货币的出现是否比轮子更古老呢？我并没有答案。但是我们知道轮子也是古人类货币的一种，或许人类历史上的第一个轮子当时被出售用于兑换货币，甚至轮子本身也是货币的一种。石器时代的古文明遗址发现贝壳，羽毛甚至珠子都被用来充当货币。

我们甚至可以训练灵长类动物使用货币。有部分研究是关于训练黑猩猩使用货币，研究人员训练这些黑猩猩使用某种特别种类的石头来交换香蕉。如果你殴打某只猩猩，并且抢走它手中的石头，那么你就可以用这个石头交换它们手中的香蕉。接下来，其他猩猩很快就学会这种抢劫行为。出人意料的是，这些猩猩自我发明的另一种交换行为是性，通过交换这些石头，可以跟异性猩猩换取性欢悦。通过这些事实，你了解货币的本质了吗？

我认为洞悉货币的本质关键在于认识到它是交流的一种形式。在最基本的层面，货币并不具有价值。货币只是展示了一种抽象的价值，它是连接价值的一种的方式，甚至可以说它是一种语言，它是一种古老的、价值传递的语言，在许多种方面，货币的特征构建了完备的语言体系。

“我们使用货币来传递价值，来定义某个产品，某种服务，某个指令的价值。”

使用货币是一种基础的社交行为，货币创造了某种社会关系纽带，因此，从古代开始，它就是一种重要的社会建筑。具有讽刺意味的是，它是至少要从历史和科技角度加以研究的一门学科。我们今天来看比特币，它代表了一种创新，它展示了货币的一种全新的形式。

2.2 货币的技术演变

货币的技术革新有多频繁？货币有多少种不同的形式？从最基本的层面来讲，价值交换的关键在于我们认为交换双方具有同等价值。“这是一只山羊，为换取我这只山羊，我需要收取 20 个香蕉。”在这个例子里，并没有真正的货币出现，这是物物交换。

2.2.1 从物物交换到贵金属

然后，我们来观察货币的抽象形式。交易形式最早的技术变革在于出现了某种媒介，它不能食用—— 一个羽毛，一颗珠子，一串带有结的绳子，或者是五颜六色的具有美观性的某些东西，这就是最早的货币形式。货币最早的技术变革就是从某种可直接消耗的，具有内在价值的东西演变为只具有抽象价值的东西。

贵金属是当时最流行的，只具有抽象价值的货币形式。它具有货币的几种重要特征：很难被找到（稀缺性），方便携带（相对于大块的石头或者整桶的羽毛来说），容易分割（可以把金币切成小块甚至更小），和通用的美观价值。人类历史上耗费了成百上千年才有了贵金属的出现。从历史学的角度来讲，我们把贵金属的出现视为农业文明的开端。历史上，贵金属货币在中东，巴比伦，埃及和希腊地区均有发展。

2.2.2 从贵金属到纸币

两个重要的技术变革之后数千年都没有变化，然后某个人想出了一个绝顶聪明的主意：如果我把金子押在某个可以信任的人手里，他们就可以给我一张纸注明我有等价金子，然后我就可以用这张纸而不是黄金做交易，这样更方便携带。只要人们信任这种模式，那么我就有了一种新的货币形式。

货币的每次技术进化都会有怀疑论者，但是我相信这一次的争议是人类文明史上最大的一次。那时对于很多人来说，货币演变为纸质的形式具有很大争议。你觉得现在人们被比特币吓坏了？想象一下，当时你告诉人们我们现在不用金子，而是用纸做交易，那时对于很多人来说这是不敢想象的。我的意思是，不管怎样，纸并不具有任何价值。纸币大概花费了400年时间才被人们广泛接受。这是一个巨大的畸变。

2.2.3 从纸币到银行卡

然后，大概 60 年前，我们看到了货币演化成一张塑料卡片的形式。事实上，第一张银行卡仍然是纸质而非塑料制成的。在美国，Diners Club 是第一家创造信用卡的公司，最初的信用卡是一种旅行支票的形式。然后，人们拿在手里说，“这不是钱，你为什么不给我些旧的，质量上乘的纸币呢？”这就是货币形式的另一次重大变革。

2.2.4 从银行卡到比特币

现在，我们有了比特币。比特币在我看来是一种很激进的变革，就像货币从贵金属演化成纸币那样，甚至更为激进。所以什么是比特币？根本关键在于描述比特币时是基于我们过往的认知，人类几千年的认知都认为货币是一种物理存在的形式。现在，我们尝试着去解释有一种货币的形式是非常抽象的，“它是一种在网络上被接受的代币，是一种以网络为中心的货币。”但是这种解释完全没说明白比特币到底是什么。

有一种广泛的误解，当我尝试去描述比特币的时候，人们会把它简单的看成是一种支付类的系统，或者一种数字化的货币。有人认为我们已经有了数字货币了，所以比特币并没有什么用。的确，在比特币出现之前，我们就在使用数字货币了。我们有银行账户，账户里面有数字账簿，我们用银行账户往世界各地进行电子转账，这些都是数字货币。

“比特币是货币技术的一次基础性转变。”

比特币不仅仅是数字货币而已，比特币是货币技术的一次根本性转变。它很难描述是因为它与我们所知的一切都太不一样了。所以，我会从多个不同方面来解释，首先，我们来看一下网络的构架。

2.3 进入以网络为中心，以协议为基础的时代

比特币并不是凭空诞生的。它产生于一个历史性的时期，在这个时期我们见证了许多社会组织的的转变，这个转变就是伟大的互联网时代。

很多世纪以来，社会组织都是按等级划分的：社会事业机构，民主政治，银行，教育机构，所有的这些都呈现出官僚主义的形式。但是自从互联网诞生以来某些东西正在被悄悄的改变，我们看到越来越多的机构从系统上做出改变，从原来封闭的、不透明的、复杂的等级式结构改变为平台式结构，这些官僚机构开始有了互动页面（网站），他们提供 API 可供访问，信息开始从机构内部流出。

然后，我们审视此次变革更为重要的部分，就是从平台的模式进入协议的模式。有趣的是，当人们有了协议之后却并没有一个集中的诉求。TCP/IP 协议并不需要服务器供应商才能工作，TCP/IP 协议在世界范围内都能使用而不需要一个特定的环境，你并不需要登陆某个账户才能使用 TCP/IP 协议。

比特币是首个以网络为中心，以协议为基础的货币形式。这意味着它的存在并不需要涉及到任何的组织或者平台。后面我会提到，这是非常重要的一点。

2.3.1 点对点结构

我们说比特币是一种点对点的货币，意义在于，它涉及到通过计算机技术、互联网和分布式系统来描述参与者和系统之间的关系。比特币结构是点对点的，因为系统里的每一个参与者在使用比特币协议时都是完全平等的，这里面并不存在一个特殊的节点，所有的节点都

完全相同。点对点的意思是当你在网络上发起某笔交易时，所有的节点对此次交易的处理都完全一致。

点对点的系统不同于互联网上的其他系统，它没有内在环境，它的有趣之处在于它的环境和状态。然而，假如你拥有并登陆一个脸书账号，你并没有使用到任何协议，所有的状态和数据都被脸书公司所控制，你拥有的只是一个登录框而已，我们称之为客户端服务器结构。比特币之所以不同因为它是点对点的，就像电子邮件或 TCP/IP 协议一样。

2.3.2 客户端——服务器结构

我们平时不愿意谈论钱。有个令人感到震惊的事实，在大多数国家，钱并不在他们的教育体系之内。一个 5 岁儿童都能提出关于钱的很多问题，而大部分家长都将难于回答“妈妈，什么是钱？钱是怎么运作的？为什么我们家没有更多的钱？为什么每一个人不能拥有更多的钱？”你总不能说，“回你房间去，好好学学通货膨胀，学不会别出来。”

有个有趣的事实——我们的社会交往活动中几乎方方面面都会用到钱，但是钱仍然是个禁忌话题。我们所有人都在假装我们并不在乎钱，至少本质上不在乎，因为我们有更高尚的目标和抱负。我们每天都在用，但是却没有认真讨论过它，这是一个“肮脏”的话题。

我认为这个问题跟货币的结构有关，在比特币之前，贵金属作为货币的媒介并且抵押在某个有名望的人手中时，它的替代品——纸币此时呈现的是债务的模式。这是一个非常重要的概念，它可以用来帮助我们理解后面的讨论。

你们中有多少人在银行里面有钱？答案是一个人都没有。你把纸币存放在银行里面的保险箱了吗？如果是，那么你可以说你在银行里面有钱。其余的人只是把你们的钱贷给银行了

而已。作为把你们的钱贷给银行的好处，你们每年会获取 0.00001%的利息。你们的银行会拿着你们的钱，转手，贷给其他的人每年收取 24.99%的利息。

“这就是客户端——服务器结构，因为货币只是记在账本里面以负债的形式表现，账本数据又储存在银行服务器里面，你仅仅是一个用户而已。事实上，你对你的资金没有任何权限，对于你存在银行里的资金，你甚至连一个连接银行服务器的相互交流的页面都没有，这就是客户端——服务器结构要干的事情。

2.3.3 主人——奴隶结构

在分布式系统里面我们有另外一个术语用来描述客户端——服务器结构，那就是主人——奴隶结构。这时就要提出一个令人不那么舒服的问题了：谁才是奴隶？因为整个系统是以债务的形式表达的，所以债务的双方必定有一方是奴隶。

对于你来说，你只是一个顾客，你并不是服务器，甚至连银行的服务器也并没有真正的对你服务，他们只服务于他们自己，因为他们才是主人。这就是我们当代的货币结构，这是一个我们自己无法控制的结构，这是一个货币被借贷之外的第三方完全掌握的结构。

今天，如果你去自动提款机取钱，银行可能会把你的钱付给你。但是有一天，当塞浦路斯，希腊，委内瑞拉，阿根廷，玻利维亚，巴西，甚至除此之外的很多国家的人们去取钱，却发现银行并不愿意把钱付给他们，这是因为银行并没有义务支付。这就是主人——奴隶结构的精华所在。

“比特币跟以往出现的货币有本质的不同，因为在比特币的世界里，你并不欠任何人任何东西；同样的，别人也不欠你任何东西，这不是一个基于负债的系统。”

比特币是一个基于所有权的系统，完全的所有权。在美国我们有这样一种说法“在所有权争执中，物品占有者往往会在判决中占据上风。”对比特币来说，谁拥有私钥谁就拥有了比特币，如果你没有私钥，那么比特币就不是你的。没有比特币，就意味着重新回到主人——奴隶的货币系统。

2.4 比特币，货币的根本性转变

比特币代表着传统货币模式的根本性转变，在人类文明史中它是对货币这种最古老技术的一种创新，它对以往货币体系中不平等规则造成了强烈的破坏，在这里，你的钱永远都是你的，通过私钥签名你对你的资金拥有绝对的控制权，在这里没有任何人审核你的交易或冻结你的资金，也没有人对该如何使用你的资金指手画脚。

这是一个实时同步的系统，无国界的系统和自由转账的系统。在人类历史上，我们从未有过任何一个类似的系统。这是一个资金以光速转账的系统，是这个世界上任何一个角落任何一个人只要拥有一部智能手机就能参与的系统。

这次的技术革新如此猛烈以至于吓坏了很多人，他们可能会告诉你他们真的非常担忧，担心这个技术被某些犯罪分子所使用，但是事实是假如世界上所有人都使用了这项技术，他们会更加害怕。

谢谢。

第 3 章 隐私性，身份认证，监管和货币

巴塞罗那 Fablab 比特币集会，西班牙，2016 年 3 月

视频链接：https://www.youtube.com/watch?v=Vcvl5piGlYg

今天，我要谈论的是中立性，去中心化和隐私的概念，正是因为这些特性才使比特币如此特别。前面你已经听我讲过比特币了，当我提到比特币这个词汇，我说的并不只是货币的其中一种，而是一个更为广义概念：完全的去中心化，以互联网为基础，平等的网络条件提供给可信任的应用程序。假如你刚巧具备这样的条件，那么从逻辑上讲，第一个产生的应用必然会是货币，但是货币仅仅只是其中的第一个应用而已。

3.1 银行：从解放者到束缚者

我们的社会正在通过各式各样新的组织机构来重新构架。传统上讲，我们的社会机构是等级式的，18 世纪，在工业社会有一种新兴的思潮，那就是允许人们在更大的规模上组织和联系起来，这对打破君主制非常有效，现在它的历史使命已经完成了。

有人问我的政治观点，这很难解释，但是有一句话可以概括：我是一个秩序打破者。历史上，每过 30 或 40 年，原有的秩序就会被打破一次。但是每当一种新秩序建立起来，权利就会增长，然后就会变得中心化，中心化的权利必然导致腐败。这并不是一个新的概念。我是希腊籍移民，我的祖先早就发现腐败产自于权利，绝对的权利导致绝对的腐败。在金钱的权利面前没有任何一种权利更强大。

我们目前生活在一个银行是一个伟大解放者的时代，把财富从封建君主手中转移到普通民众中是一个巨大的进步，这个系统解放了万亿计的民众。然后这个系统变得中心化了，它

开始要求权利，然后导致了腐败。现在留给我们的不再是一个解放性的系统了，是时候打破它了。比特币是一种能彻底摧毁权利中心化的东西，为什么这么说？

3.2 负面的结果并不是人为产生的，而是系统设计的

作为一名分布式系统领域里的计算机科学家，让我感到有趣的一点就是系统的结构，对于我们这个城市来说，结构是一个伟大的话题，体系的结构会决定最终产生的结果。

我曾经和许多银行从业人员共事过，他们都是不错的人，他们只是为了供养他们的家庭，偿还他们的房贷，保障一份稳定的工作。但是在他们中间，有一些是具有反社会性格的人，这部分人最终坐到了最高的权利位置，因为在我们的等级制度中，反社会性格是一种优势。传统上讲，金钱的权利引发的大部分问题都与人性的善恶无关。事实上，这些金融机构因为自身的结构导致了很多不平等、不受约束的结果，它们开始呈现出本土主义，国家社会主义，部落性，社会等级，所有的这些都让我们的世界变得更狭窄。

3.3 通讯行业快速扩张，银行业务逐步降低

事实上，过去的 15 年中，我们见证了互联网成为通讯行业去中心化的一股重要的解放性的力量，但是如果你了解经济的包容性以及银行业是怎么运作的，会发现我们机遇并没有增加。事实上，在金融领域，我们机遇正在减少，经济的包容性正在减少。

原因在于金融业孤立性的结构，他们做了很多限制：国家的界限，等级结构，以及不同地位的人的资金和商业活动遭受到不公平的对待。我们生活在一个越来越全球化的世界，通过互联网甚至出现了全球性的文化，然而我们的金融系统仍然是狭隘的，孤立的和分隔的。

从系统的角度来看，金融业务分为小额交易和大额交易，日常开销属于小额交易，商业活动属于大额交易。所有的这些金融业务都受到法律条款，国家界限的限制。这意味着，对于我们普通人来说，我们于世界上其他国家的人做交易受到的限制越来越多。地缘政治严重影响到了金融业务，国家和货币的结合造成了更多的有害后果。

我们将会打破这现有的一切。

3.4 新的结构，新的通道

比特币带给我们的是重新规划这个世界的一种全新模式，就像平等的互联网连接对传统通讯行业造成的改变那样。假如我有一个 IP 地址，互联网对我的数据包的处理和对其他任何人数据包的处理都一样。就绝大部分而言，互联网给予每一个人发表他们观点的渠道，它授予了任何一个人在全球范围内发布刊物的权利。比特币将会在金融领域内赋予每一个人同样的权利。

把它想象成一个桌面银行系统。假如全世界所有的大型银行把权利分配到单个个体手中，这会对现有金融体系带来毁灭性打击。

想象这样一个世界：每一个人不单有执行转账的权利，还有制作一个全新复杂金融体系、金融工具的权利而不需要任何人的许可。这里甚至简单到只要连上网，任何人都可以创建一个新的应用程序，而中心化的系统可做不到这些。

在一个中心化的系统里面，你离得越远，受到的束缚就越小。你离系统的中心越近，等级越高，受到的限制就越多。但是比特币的系统却不同，所有的节点都享受同等的金融服务。在中心化的系统里面，如果你想要创建某项新的业务，首先需要获得许可，然后被批准的唯一可能性就是你的这项业务有广泛的客户群体并且是可盈利的。

而在互联网或者区块链的世界里，创建一个新的应用所需的仅仅是两个人，两个节点或两台电脑。两个人就可以开始通讯，建造他们自己的协议，创建他们自己的系统，并且只有两个人的应用将会和网络上所有的其他应用一样有效。

3.5 绝对的中立和无歧视性

当我们审视互联网的时候，一个根本性的误解是很多人认为互联网的核心在于快速的传递信息，然而网络真正的力量来自于它的中立性。绝对的中立是这样一种概念：互联网并不会因为资源，目的或者内容而做出差别对待。

比特币是第一个展现出中立性的金融类网络。进行比特币转账时，网络并不在乎资金来源，收款地址，金额大小或者资金用途。唯一的问题就是当你使用比特币网络资源时，你是否对系统付出了相应的贡献（交易手续费），如果是，那么你这次交易就是有价值的。

3.5.1 比特币系统里面没有垃圾交易

目前，关于比特币，人们有一个很有趣的争论，那就是“垃圾交易”。什么是垃圾交易？某笔交易是否属于垃圾性质应该如何确定？我觉得这个条款是没有意义的，因为要判断哪些交易属于垃圾交易而哪些交易不是，你就会做出一个上下颠倒论断，你就会强制性的，在结

构层面上选择哪些交易是合理的，接着带来的问题就是判定哪些终端用户是合理的，这简直是荒谬。其实没有任何一笔交易属于垃圾交易，原因很简单，如果一笔交易附带了一定量的交易费，这就说明发送人觉得相对这笔转账来说手续费已经足够了，因此，这是一笔合理的交易。通过简单的市场机制来判定什么是对什么是错，什么是合理的什么是不合理的，什么是有价值的交易什么是没有价值的交易，这是控制欲的另一种概念。只要你发起的交易附带了少量的、必须的手续费，那么你这笔交易就不是垃圾交易。

3.6 以网络为中心的货币

从上世纪 70 年代起，我们看到世界开始逐步适应数字化形式的货币，当人们把比特币称之为数字货币，他们弄错了关键的一点。欧元是数字货币，美元也是数字货币，世界范围内，只有不到 8%的货币仍然采用纸币的形式，其余的都是账簿上的数字。不同之处在于，这些所谓的数字货币都是由中心化的机构所控制的，而比特币是一个去中心化的、开放式的网络。

比特币不是数字货币，它是加密货币，它是一种基于网络的货币。我尤其喜欢货币网络化的这个概念，它把人们以往对机构的信任、对阶级的信任替换成了对网络的信任。网络就像一个把真理广泛传播的布道者，在这里一切金融业务和安全性的问题都可以得到解决，并且不受任何人管控。

3.7 集权主义者对掌控一切金融业务的梦想

上世纪 70 年代，我们的货币开始演变成为数字的形式，这就给了当权者一个梦想，一个把世界上每一个人类个体的每一次金融活动都置于权利体系监控之下的梦想，在这里，将再也不会有隐私。我们自己给自己早就了这么一个全球性金融监管体系。

这个体系要求身份认证、信用审核及有限的金融服务，这个体系需要对逐渐降低的经济包容性负责，这个体系需要对世界上 25 亿人完全享受不到任何银行服务负责。这个数据仅仅统计的是一个家庭的主要收入者，还不包括其余家庭成员。这个数据还不包括那些仅仅能享受有限的银行服务，以及只能使用本国货币的人。

3.7.1 金融交易的审查制度

作为发达国家精英特权阶层中的一员，我有 24 小时随时开通经纪账户的权利，我可以随时在东京证券市场用日元做交易，我可以在世界任何地方方便的收款和转账而几乎没有任何限制，为此我需要付出的是牺牲我个人的隐私和自由。

当权力机构非常强大的时候，有些事情是我不能做的，我指的并不是购买毒品，我对那些不感兴趣。我说的是一些简单的小事，比如向维基解密之类的组织捐款。几年前，维基解密被世界金融体系完全封锁，世界上几家主流支付服务提供商受到了法律之外的压力，其中包括 Visa, MasterCard, PayPal 以及所有银行的转账系统，没有审判也没有走任何法律程序。或许，我本人认为他们除了揭露犯罪事实之外本身并没有触犯任何法律，维基解密被世界金融体系完全隔离了。此类事情不仅发生在激进组织身上，几乎世界上所有国家都有发生。

国家政权的这个梦想，建造一个极权的金融体系，在 2009 年 1 月 3 号破灭了，比特币诞生了。

3.7.2 基于网络的货币是反金融审查制度的

比特币是反金融审查制度的，你可能听说过，比特币转账不受任何控制，它与身份认证和地理位置无关。在比特币的世界，监控每一个人是不可能做到的。比特币通过其平等的网络连接，中立的，无国界的特性来对抗现有的金融审查制度。资源，目的，交易价值的多寡对于比特币的结构来说没有任何意义。

3.8 监管和反监管

隐私权的意义非常重要，但是目前这个词汇却被赋予了非常深刻的政治含义。但我想把隐私权和另外一个概念并列比较：保密权。两者之间的区别是什么？其最终演变为在我们今天的字典里面，隐私权是我们几千万个体民众不受监控的权利，而保密权是指极少数人逃脱了这种被监管的责任从而拥有的绝对隐私。

我们生活在这样一个世界：我们每个人的每一笔交易都会被金融系统归类、分析，然后转移到情报部门手中，全球的情报部门都会相互合作。我们尚不知道政府是如何处理货币的，强大的金融体系是完全不透明的，我们所有人的交易在这个体系监管之下一览无遗。这个世界已经上下颠倒了，而比特币将会纠正这一切。

隐私权是基本人权，而保密权是人权赋予我们的特权。我们需要生活在这样一个世界：人类拥有完全的、彻底的、强烈的隐私权。因为这是基本人权，因为这是自由发表言论，自由集会，自由发布政治观点的基石。我们需要生活在这样一个世界：保密权可以随意获取，而权利将至于监督之下。我们需要快速纠正现在这个系统。

我最喜欢的一个词汇是一个法语单词：反监管，刚好与监管相反。监管是自上而下的监督，而反监管是自下而上的。在国家政权的设想里面，他们希望在将来可以控制我们所有人的金融交易，但是他们犯了一个致命的错误。你可以设想一下，是几百上千个人监管全世界75亿人容易还是全世界的人监管他们容易？当这个环形的监狱翻转过来，当我们的金融系统，通讯系统属于每一个人，当保密权不再是一个难以为继的幻境，当以国家和巨头公司的名义犯下的罪行容易受到黑客、告密者和泄密者的攻击时，当一切的真相浮出水面时，我们那时将拥有巨大的优势。新的系统平衡点在于每个人都将会拥有隐私权，而当权者的保密权将会被剥夺。而比特币将是做到这一切的第一步。

3.9 每一个人都将拥有的银行

拥有跨国界交易的能力意味着我们现在可以向数亿计无法享受银行服务的人提供金融服务，而不一定需要复杂的技术。我曾经和不同地区那些并不担心比特币的银行家们谈过，他们告诉我大约有80%的人离最近的银行网点尚有上百英里远，银行无法为这些人提供服务。其中的一个例子是，有一个地区的居民需要乘坐独木舟划行几百英里才能到达最近的银行网点。但是，即便是地球上最偏远的地区，现在也有了信号塔。即便是世界上最贫穷的地区，我们也可以经常看到一些民房上面装有太阳能电池板可供诺基亚1000，这种制造史上产量最多的手机充电。我们可以把所有的这些手机都变成不仅是一个银行账户，而是整个银行。

“我口袋里拥有的不仅是一个瑞士银行账户，而是整个瑞士银行。”

两周前，奥巴马总统在西南地区做了一场关于隐私权的演讲，他说，“如果我们政府不能解锁手机，那么就意味着你们每个人的口袋里都有一个瑞士银行账户。”这句话并不完全

正确。在我口袋里的并不只是一个瑞银账户，我拥有的是整个银行。只要有一颗种子我就可以产出 20 亿个账户地址，我可以每笔交易都使用不同的地址。这个银行是完全加密的，所以即便你解锁了我的手机，我仍然可以和我的银行建立连接。这件事代表着对于隐私权，人权主义者和极权主义者有着不同的认知。但是如果你觉得我们将来可以不通过抗争而轻而易举的获取这一切，那么你就大错特错了。

3.10 比特币，货币中的僵尸

如果你以往对比特币有所了解，那么你就会知道他们对于比特币的评价和在 90 年代初期对互联网的评价完全一样，这是恋童癖者、恐怖分子、毒贩和犯罪者的天堂。你们中有多少人拥有比特币？然后你们中间又有多少人是恐怖分子，毒贩和犯罪分子？

其实你们认识的比特币是他们口中的比特币，不时的，某些从来不了解比特币的人会注意到两件事情。第一个是比特币还没有死亡，这真是令人惊叹，因为每过两三个月媒体上就会有文章发表来说比特币快要完了，这简直是一个伟大的市场推广，因为每次有人听到比特币快完了，但过了两三个月人们又听到比特币还没完，他们就会想“老天，比特币这个东西生命力真强。”我说比特币是互联网货币，或许应该改一下说成“货币里的僵尸”，因为这是一种永远都死不了的货币。

现在的问题是，我们正在创建一个威胁着世界上最大产业系统的新体系，这就是金融体系。他们必然会否决，他们必然会逼迫我们后退，他们必然会使用一个非常有效并且常用的情感武器来对付我们——那就是恐惧，他们会像对一个傻瓜那样说服你，说比特币是一种让人感到恐惧的东西。人们得知了这个讯息，然而当他们第二天出门和某个拥有比特币的牙医、建筑师或者某个曾经使用比特币往自己老家转过钱的出租车司机，又或者任何一个曾经使用

比特币赋予自己金融自由的人交谈的时候，这个谣言都会不攻自破。目前来看，比特币仍然发展的挺好。

3.11 货币的进化

在目前这个以网络为中心的世界，货币占据着进化的有利位置，与任何物种都一样，周围的环境会不断的刺激它们成长。比特币是一个动态的系统，随着软件的更新它会不断变化。问题是，比特币将来的发展方向是什么？哪一种环境更适合它的存在？当权者的举措会对它造成什么样的影响？如果受到攻击，它会进化到可以自我防御吗？

答案是，如果他们攻击比特币的匿名性，比特币的匿名性将会变得更强，如果他们攻击比特币网络的自我恢复能力，比特币就会变得愈加去中心化。最终，不管有多少类似于“比特币让人们感到恐惧”的谣言，比特币终将进化成货币领域里永远打不死的参天大树。

有人问我，“你觉得政府会禁止比特币吗？你觉得他们会规范比特币的发展吗？你觉得他们会杜绝和比特币相关的任何服务吗？”答案很简单，在一个以网络中心的系统里，系统是动态的和自动调整的，系统展现出来抗脆弱性——攻击导致系统自我调整，自我进化，具备抗体，变得越来越具有抵抗性。

3.11.1 攻击将导致抵抗

自 1989 年以来我一直在使用互联网，我记得非常清楚，早期很多专家评论说互联网的功能不够强，不能兼容语音文件，不安全。我记得在那时拒绝服务攻击可以在数小时内摧毁雅虎，AltaVista，甚至谷歌。到目前为止发生了什么？过去 5 年中你见过多少次谷歌停止服务？人们停止对谷歌的攻击了吗？截然相反，谷歌现在可以抵抗千兆位的拒绝服务攻击并且

动态的变更线程。其他的互联网应用也是如此，攻击从未停止，而系统却变得免疫。这和人体的免疫系统一样，如果你暴露在某种病毒中而病毒却没有杀死你的话，你就会产生抗体。下次你再接触这种病毒，什么问题都不会有。

政府会禁用比特币吗？会限制比特币吗？会攻击比特币吗？他们已经这么做了。从比特币诞生的第一天起他们一直都在这么做，但是比特币系统却变得更加强大。这是一个由始以来一直暴露在拒绝服务攻击中的系统，不同的人群对它的攻击从未停止，黑客、情报部门或是其他的系统，一天二十四小时从未停歇。

关于安全性，我们有一个搞笑的词："蜂蜜罐"。蜂蜜罐是一个设计用来吸引黑客的系统，你能找到一个比价值 60 亿美元的金融网络更大的蜂蜜罐吗？如果你能黑掉比特币网络，那么就会获得价值 60 亿美元的奖赏。目前还没人能获得这笔奖赏，不是因为没人去尝试，而是因为比特币系统强大的恢复性。

3.12 欢迎来到未来货币

请记住我们正在做的并不只是关于货币，而是重构这个令人失望的社会组织体系。这个自 18 世纪以来就已存在的等级式体系已经不再合适目前这种全球化的趋势了，过往相互连接的世界模式正在被以网络为中心，平等的结构体系所替代——不管是互联网，抑或是运行在上面的其他程序，还是比特币自身。货币只是其中的第一个应用。只要你有网络它就可以提供给你不带任何偏见的信任，你可以在上面创建无数的应用程序，而无需任何人的批准。

比特币比货币的含义更广泛，当我说比特币是"互联网货币"强调是互联网而不是货币。欢迎来到未来世界的货币。

谢谢。

第 4 章 创新、颠覆与比特币

Maker Faire（美国 Make 杂志社举办的全世界最大的 DIY 聚会）：密歇根州底特律亨利福特汽车博物馆；2014 年 7 月

视频链接：https://www.youtube.com/watch?v=LeclUjKm408

在演讲开始之前，出席者观看了由博物馆放映的关于汽车历史的视频。在演讲中，会提到这段视频。

早上好！这段视频很有趣，是吗？大约一个月前，我为了买比特币把车卖了。那是一次有趣的经历，开启了一个全新的世界。

4.1 对创新的认识

比特币是互联网货币，但远不止于此。我想从那些与现实格格不入的、古怪和荒诞的人的角度谈一谈比特币，他们拒绝像普通人那样思考，当他们看到某项不成熟但却优雅的技术，他们并不在意技术的成熟度，而是技术的优雅性。他们意识到了创新，不仅仅是比其他人早几个月或几年意识到创新，有些时候甚至会比普通人早上十年，他们会来到 Maker Faire（美国 Make 杂志社举办的全世界最大的 DIY 聚会）。所以，在这里谈论比特币，再好不过了。

比特币很让人意外，比特币并不是我们所知的那种普通货币，它本不应该出现，也很难成功，但实际上却发挥作用了，就像维基百科、Linux 操作系统和互联网一样，就像那些留有马尾辫和络腮胡的人经常会冒出的一些新奇想法一样，怪人通常是很难被信任的。

比特币取得了成功是因为它确实发挥了作用，这的确是一项优雅的技术，但我想谈谈那些与现实格格不入的人的精神：他们在某个行业的董事会上发言“你们知道吗？我们将会改

变一切。”然后他们会被一阵嘲笑声赶出会议室，但他们初衷却从未动摇，一直到他们真正改变一切。这在技术领域是常有的事，只是被我们所忽略、遗忘，并且用优美的言辞改写了这段历史。

4.2 汽车、电力和比特币带来的危险

我们刚刚看完关于汽车早期的视频，你知道当时的媒体对于早期的汽车是如何评价的吗？在他们看来，汽车相当可笑。当时，汽车跑的比马慢，还总是出故障。汽车需要消耗昂贵的汽油，但那时没有地方能供应汽油。它们需要大量的基础设施才能启动。媒体唯一关注的是能使报纸销量上升的新闻报道：例如车祸，被车辆撞伤的行人等等。自第一辆汽车问世的 20 年后，新闻报道都是关于那些如地狱般的、令人厌恶、肮脏、嘈杂的机器，它们远不如马匹，哪儿也去不了，只有怪人才会去开车，而且很多时候，乘客和任何靠近它们的人都会深受其害。

受到这种狂热情绪的感染，在 1896 年，英国通过了一项《红旗法案》，其中规定：每一辆行驶在道路上的机动车，都必须由 3 个机组人员操作：司机、工程师和旗手。司机负责开车，工程师负责监督（想一想火车的运行模式），旗手在车前面 100 码做引导，还要用红旗不断摇动为机动车开道，提醒行人那些地狱般的死亡机器即将到来并会把他们撞倒。

你猜英国那时发生了什么？他们在汽车产业竞争中输了，虽然他们发明了这项技术，但没有看到它的潜力，他们对汽车的第一反应是恐惧。他们营造了这样一种环境，以至于汽车做不到它本应能做到的事情。如果你让汽车跑的像被红旗指引的行人一样慢，那么就失去了汽车所有的优势。如果一辆汽车需要 3 个人操作，那么就失去了汽车的所有优势。他们试图从铁路和马匹的角度去了解汽车，他们失败了。

这段视频中你没能看到的是，在那个时刻之前他们一直都是胜利者。第一批真正实用的汽车是在英国制造的，他们已经通过蒸汽引擎在工业革命中取得了胜利。当时，英国是工业创新的强国，在他们决定将这个肮脏的机器限定在一个有限的空间和一套规则之前，他们一直都是胜利者。但他们将鹅杀死了，也就再也得不到金蛋了。

这很富有启发意义，因为在技术领域的情况通常如此。当电力首次用于家庭照明时，你以为媒体会发表报道“真是太棒了！爱迪生是个天才！这将会改变整个世界!”？不！他们说的是，这是一项危险的技术，会烧毁人们的房屋。他们会不断报道人们触电身亡、房屋烧毁的新闻。

当电力首次用于家庭照明，你以为媒体会发表报道“真是太棒了！爱迪生是个天才！这将会改变整个世界!”？不！他们说的是，这是一项危险的技术，会烧毁人们的房屋。”

当然，真正实现家庭用电并不容易，因为这要求房屋彻底翻修。首先你必须安装电线，这些电线可能会烧毁你的房屋。在房屋被烧毁之前，还必须购买专门的设备与这些电线连接，只有富人才能负担得起这样的开销。显然，这项技术是为了富人装腔作势而存在的，这仅仅是一种消遣，没有任何实用价值。

在 1900 年世界博览会上，巴黎市长表示，“展会结束后，电力这股风潮会像灯灭一样迅速被人们淡忘。”在技术领域，那些著名的从未实现的预言常常如此，回想起来会很可笑。就像 IBM 的创立者曾经说过，“我认为全世界大概只需要五台计算机就够了。”

“在技术领域，那些著名的未曾实现的预言常常如此，回想起来会很可笑。”

你能猜到人们对比特币的评价吗？他们告诉你，这是一项奇怪而又复杂的技术，这项技术是为了迎合那些与现实格格不入的人、毒品贩子、堕落的人、色情文学作家、恐怖分子、

小偷和骗子。在这个展厅，我没有见到这样的人，但是我们要多加小心防范。

当然，他们错了，比特币其实不是那么回事，它只是一项技术，犯罪分子可能会率先使用这项技术。汽车最初被用作逃亡，电话最初被用作策划阴谋，电报最初被用作实施长途邮件骗局和庞氏骗局，电力最初被用作实施医疗诈骗。随着新技术的诞生，经常会有这样的情况出现，比特币也是一样。

你觉得犯罪分子为什么会青睐于新技术？我们可以站在道德的高度了解一下实际原因。犯罪分子会使用最尖端的技术，是因为他们被高利润和高风险的环境所驱动，在那样的环境中，竞争非常激烈。如果你已经承担了巨大的风险，那么使用最新的技术并不是什么大不了的事情。如果你赢了，会给你带来很多好处。纵观历史，最了不起的技术通常都是由犯罪分子率先使用的。我认为这不一定就是我们想要放在比特币营销计划上面的事情，但是看看犯罪分子从事的犯罪活动以及 10 年后这项技术如何成为主流技术，很有意思。一定有某种力量在推动事情的发展。

比特币已经不再处于早期阶段了，并且已不再受犯罪分子所青睐。事实上，无论媒体如何报道，它都不是犯罪分子的首选。现在，比特币已经成为主流，并且发展非常迅速。

“比特币作为一项技术，引发了一些令人兴奋的事情。我们的金融和银行体系将会被动摇，就好像汽车替代了马匹，石油动摇了捕鲸业，电力动摇了木材火炉行业一样。”

今天我会谈谈比特币的技术，因为发生了一些令人兴奋的事情。我们的金融和银行体系将会被动摇，就好像汽车替代了马匹，石油动摇了捕鲸业，电力动摇了木材火炉行业一样，银行业要被搅乱了。事实上，当他们意识到这种破坏有多么严重时，这场游戏就已经结束了。

4.3 人们对创新的反应

当现有的行业第一次遇到某项破坏性技术时，这项技术往往会被忽视，因为它不可能构成威胁。从现有的利益来看，从已处于垄断地位的企业来看，这些威胁看起来像是孩子们在玩耍。对于摩根大通来说，比特币就像是试图取代沃尔玛的柠檬水摊位。如果这项技术继续存在，他们会开始嘲笑这项技术。当这项技术已经随处可见了，他们会拿这项技术做成各种各样的笑话。所以，就像随着汽车的问世，第一个买车的人会被嘲笑那样：一些人总是随身携带扳手试图修复再次发生故障的机器——这就是早期购买汽车的人在人们心中的形象。

他们嘲笑比特币的同时，这项技术仍在不断地发展。每过一段时间，你会发现一些新的变化。最终，这些行业内专家会说“嘿，也许我们需要实验这项技术，或许我们需要正视这项技术。”人们闻讯后蜂拥而至，因为他们突然意识到这将永远改变我们的行业。

到那时，已经太晚了。到那时，那些所谓的大公司就会成为下一个“柯达”。柯达曾经是业内的龙头企业，但是三年内，价值 120 亿美元的产业被一家他们从未听闻的小公司夺走了，这家公司甚至从来没有生产过相机。你知道谁击败了柯达吗？一家芬兰公司，名叫诺基亚。经过三年的时间，他们制造出 5 亿台手机并且摧毁了传统相机、胶卷产业。Tower Records 曾经在音乐产业占据着主导地位，但是他们在四年的时间就销声匿迹了。这是为什么？因为 MP3 让人们有了更多的选择。

IBM 曾是计算机行业最坚不可摧的企业，这个品牌曾经是品质的保证。在那时，购买 IBM 之外的任何计算机产品都代表你是一个失败者。然后 Linux 操作系统出现了，它从根本上动摇了 IBM 的地位，因为它推翻了一个基本认知，那就是：为了保证工程的质量，为了给银行业、工程业和政府部门交付最好的计算机，你需要 IBM。你需要由 IBM 博士级别的工程师创建的那个封闭式的、严格受控的、精心打造的操作系统。

1992 年，Linus Torvalds 说“我会在宿舍创建一个新的操作系统，因为我负担不起现有操作系统的费用。”这个想法荒唐透顶。因为操作系统是一个非常复杂、庞大的系统，它需要成千上万的工程师一起创建。Linus Torvalds 开始把操作系统做的简单化，6 年后，Linux 已经在计算行业占据领先地位，Sun Microsystems 开始经历切肤之痛。8 年后，Sun Microsystems 走向破产，被惠普收购，他们的计算机部门关闭。同年，IBM 逐步退出个人计算机市场。

现在，全球 80％的手机都在运行安卓操作系统 ——对了，就是 Linux。手机连接的服务器运行的是 Linux，银行运行的是 Linux，我们使用的娱乐系统运行的是 Linux，我们开的汽车运行的是 Linux。你总能辨别出这些系统是否停止运行了 Linux：蓝色的小屏幕上会提示*“抱歉。系统崩溃了，操作系统选择错误。”*你登上一架飞机，启动娱乐系统，它运行的是 Linux。如果你在 15 年前对一名 IBM 工程师说，“你们将会被一个由芬兰学生在宿舍里创建的操作系统打败。”他们肯定会笑话你。

如果你在 15 年前对一名 IBM 工程师说，“你们将会被一个由芬兰学生在宿舍里创建的操作系统打败。”他们肯定会笑话你。

这就是我们目前的情况，比特币正在承担整个银行系统的作用，这可是世界上最具权势的行业。猜猜接下来会怎样？比特币会由于一个非常简单的原因取得胜利。它不仅仅会获胜，还会发展的更好。因为银行系统是由那些恶棍、骗子和徒有其表的人管理的，因为银行系统用了五十年的时间只为用户做了两项创新——自动提款机和信用卡，然后用余下的时间进行敲诈，比特币因其开放性必将成为最后的赢家。在这个充满思想者、实验者和创造者的世界里，开放性必将获胜，因为它能将创新推向繁荣！

4.4 开放式创新和选择性系统

让我对上面的陈述做出解释：世界上每一个独立的金融系统都会有一个安全和信任模式，这要求排除不良行为者。我无法连接 Visa 网络并对其重新进行编程，因为这样做会危及 Visa 网络的安全。我无法连接 SWIFT 网络（全球跨行电汇网络），因为这样做会危及该网络的安全。所有这些网络都是封闭的，因为它们主要依赖访问限制来保障网络安全。网络会非常仔细地审查有权限访问，或者可以接触到代码的每一个人，它会非常仔细地审查在该系统上运行的所有程序，如果他们允许任何一个不良行为者进入系统核心，那么整个系统的安全性就会丧失，那个人就会控制整个系统并做任何他想做的事情。当然，在 2008 年，我们发现那些恶意行为者掌握了银行系统，由于他们的贪婪，毁掉了全世界数百万房屋所有者、退休人员和储户（讽刺 2008 年银行家人为造成美国次贷危机）。

“比特币是不一样的，是因为它不依赖访问限制来确保网络安全，它依赖可获取奖励的简单数学公式。”

比特币是不一样的，不是因为我们突然间发现了世界上最诚实的人，不是因为比特币网络中没有蹊跷的事情发生，也不是因为网络没有受到攻击。比特币是不一样的，是因为比特币网络中也有很多骗子——网络也一直受到攻击——但它不依赖访问控制来确保网络安全，它依靠可获取奖励的简单数学公式。你可以作为矿工加入比特币网络并确保其安全，同时必须使用大量计算能力并耗费大量电力。如果在挖矿的竞争中获胜，作为回报，你会得到比特币作为奖励。这个简单的等式创造了一个激励体系，在这个体系中遵守规则要比违反规则要好得多。这就是博弈论。

如果你作为一个计算机科学家或者一个银行家来看待这件事，可能会说：“这不可能奏效。每个人都在相互竞争是什么意思？这不是一个安全系统的基础，这会引发混乱。”这就像说“这是百科全书，如果任何人都可以编辑将会引发混乱。”

比特币是一个完全开放式的网络，任何人都可以与之连接。你可以编写应用程序，连接到比特币网络，并用它做新的事情。你可以编写新的金融服务工具，当你这样做时，不必通过网络验证你的身份，不必征求任何人的许可，不必接受审查，不必做担保。网络并不畏惧你，因为它并不是靠让恶意行为者出局来确保其安全的。实际上，在系统的核心有很多恶意行为者，但是比特币仍然可以正常工作，这是因为这里并没有所谓系统核心，这是一个完全去中心化的系统。当你创建一个开放式的金融服务系统时，当人类历史上第一次，任何人都可以连接这个系统并且编写新的应用程序时，将会造成多么巨大的影响！

比特币不只是货币，这是我们需要认识的一件非常重要的事情。比特币是一个网络系统，货币是第一种在比特币网络上运行的应用程序。今天，有上千家公司编写比特币系统里的应用程序。作为过去二十年最具活力的行业之一，这些公司招聘了数万人。2014 年，比特币初创公司获得了超过 2.5 亿美元的投资。值得注意的是，这比 1995 年互联网的投资速度还要快。我们抢占了先机。比特币的增长速度比推特前三年的增长速度还要快，甚至比脸书前几年的增长速度更快。其原因是来自世界各地的每一个与现实格格不入的人、古怪、荒诞的人都可以自由连接比特币网络，采用新奇的想法并创建新的金融服务程序、新的银行应用程序、新的购物应用程序和新的在线托管交易程序。这正是人们现在做的事情，他们正在创造新颖、新奇、出色的事物，这在之前的银行业中从未见过。

当你处于两种环境：一种是传统银行的环境，在这里什么事情都需要许可（当然多半不会授予许可）；另一个是完全开放、自由的系统，在这里创新可能随时发生——你猜谁会赢？你猜所有令人兴奋的事情会在哪儿发生？

“比特币是一个具有选择性的系统，你可以选择性的使用它，你可以选择上面的应用程序，你可以选择进行互动的人，你可以选择互动的游戏规则。这就是为什么比特币会赢的原因。它提供的创新是消费者需要和想要的。”

没人研究那种可以比大型银行快上四微秒或者多出三微美分的高频交易算法，也没人研究那些可以取消你银行账户透支状态的方法。2007 年某家大银行做了一项创新，他们认识到，如果你的账户接近透支限额，他们可以调换交易顺序，优先处理你账户里的多笔小额交易，而后才是大额交易，这样他们银行就可以从每笔交易中收取 25 美元的手续费。这就是银行关注的那种创新！

对于比特币来说，没有人做那种创新。因为在比特币的世界，你不能强迫别人使用你的应用程序。如果你办理银行业务，就需要使用他们的网络，遵守他们的政策。如果你使用他们的银行卡，就得遵守他们的规则。如果你对这家银行不满意，去到其他地方却发现所有银行的模式都是一样的。然而比特币是一个可供选择的系统，你可以选择性的使用它，你可以选择里面的应用程序，你可以选择进行互动的人，你可以选择互动的游戏规则。如果你不喜欢一个应用程序，你可以不下载。如果你喜欢一个应用程序，你可以下载并转发你身边的朋友。这就是为什么比特币会赢的原因，它提供的创新是消费者想要和需要的。

4.5 全球经济中包含的另外 65 亿人

比特币会赢还有另外一个原因：这里存在一个巨大的不平衡。今天现场的每一个人都可以自由使用银行账户而不受外汇管制。通过这个银行账户，他们可以自由买卖任何一种货币；通过这个银行账户，他们可以往世界任何地方汇款；通过这个银行账户，他们在东京证券交易所或德国证券交易所做交易；通过这个银行账户，他们可以享受银行信贷服务，包括汽车贷款和房屋按揭等等。银行账户功能是如此强大，这个世界上大约有 10 亿人受惠于此，这些人可以享受成熟、国际化、高流动性的银行服务。

世界上没有银行账户的人大约有 20 亿，另外 40 亿人仅能享受有限的金融服务：没有外汇服务，没有国际市场的银行服务，没有流动性的银行服务。比特币不是与这 10 亿人相关的，而是关于另外的 65 亿人，他们被切断了与国际银行系统之间的联系。

当那些位于尼日利亚偏僻地区只具备发送短信功能的手机可以接入银行系统终端时，你认为会发生什么事情？它们将会演变成一个新的西联汇款系统，一个新的国际贷款系统，一个新的股票市场！

当手机技术部署在非洲时，它的发展比任何其他技术都要快。随着这项技术的发展，我们已经看到了变化。我们看到一些小村庄，那里没有自来水，仍在用木柴烧火，也没有国家电网——但每家的泥屋顶上都安装了一个小型太阳能电池板，这个太阳能电池板的功能不是为了照明，而是为了给 Nokia 1000——这种过时的功能手机充电。有了手机，他们就可以了解天气预报，当地市场的粮食价格，并且与世界其他地方建立连接。当手机可以成为银行时，又会发生什么呢？

4.6 电汇对全世界的影响

比特币不只是货币，作为一项技术，它可以使全球数十亿人全面参与经济活动。我会举一个具体应用的例子来说明它将在未来五到十年彻底改变数十亿人的生活。

在美国，每天都会有移民在某个地方排着长队等候兑现工资支票，他们将一半的工资汇回他们的国家，供养他们的家人。在我们这个国家，有六千万人没有银行账户，但这部分人仍需要将工资支票兑现并汇往国外。在全球，每年有 5500 亿美元的汇款从第一世界国家汇出，大部分被汇往墨西哥、印度、菲律宾、印尼和中国这五个国家。在某些地区，汇款占当

地经济收入的 40%。在这个 5500 亿美元流动资金食物链的顶端是西联汇款这样的公司，就平均而言，每笔交易他们会从世界上最贫穷国家的人民那里收取 9%的交易费。

想象一下，当某个移民发现他们可以用比特币做到同样的事情时，会发生什么——在这里汇款费用不再是 15%，不是 10%，也不是 5%，而是 5 美分。交易费不是按百分比计算的，而是一笔固定的费用。有一家比特币初创公司业务是处理美国与菲律宾之间的汇款，他们目前的营业额只有几百万美元，但发展迅速。如果你是一名移民，当你不再需要支付 9%的交易费就可以把钱汇给家人，当你每个月可以寄 100 美元而不是 91 美元回家，想象一下会发生什么。

4.7 比特币将会改变世界

总而言之，比特币是我见过的最令人兴奋的技术。1989 年，当我还是个孩子的时候就已经接触到了互联网，早在大多数人明白互联网是怎么一回事之前，我就已经知道它将改变世界。我告诉身边的每一个人“我们将会在互联网上购物，我们将会在互联网上处理银行交易。”人们的反应是可以预见的“噢，是吗？Andreas，去做你的功课，打扫你的房间吧。”当我第一次看到 Linux 时，我说“老兄，这将永远改变操作系统，IBM 正在走向衰落。”每个人都嘲笑我。当我看到第一个网站时，我说“美国的每家公司都会在 10 年内建立自己的网站。”每个人都嘲笑我。那么，让我来告诉你，我不知道接下来比特币会发生什么，但我确实知道这项发明——无需银行，无需政府，没有中心机构控制，任何人都可以自由使用的数字货币系统——将会改变世界。

谢谢。

第 5 章 哑网络、创新和公地狂欢

O'Reilly Radar 峰会；加利福尼亚州旧金山；2015 年 1 月

视频链接：https://www.youtube.com/watch?v=x8FCRZ0BUCw

今天，关于哑网络(仅提供最基本服务的网络系统)、智能网络、开放源代码在金融领域的意义以及公地狂欢（所有人都可以占用公用资源而不会导致资源枯竭）等概念，我来谈谈我的看法。

比特币是一种货币，一种网络，同时也是一种技术，你不能将这些概念完全区分开来。没有货币，建立在以货币为基础的共识网络就是行不通的；没有货币，区块链是行不通的；没有网络，货币也无法起作用。但比特币两者兼具，它是参与型的共识网络和全球性的货币的一种融合。今天，我想谈一谈比特币网络，并重点关注在互联网初期曾经出现过的一个相似概念。

5.1 智能网络与哑网络

比特币不是智能网络，而是一个哑网络。它仅有交易处理和验证简单脚本语言的功能。它不提供全面的金融服务和产品，也没有内置令人惊奇的自动化功能。

比特币是一个哑网络，这是它最显著也是最重要的特点之一。当你设计网络、建造网络系统时，最重要的一个选择就是：是创建一个支持智能设备的哑网络，还是支持哑设备的智能网络？

5.1.1 智能网络——电话

电话网络是一个非常智能的网络，而网络末端的电话是一个哑设备。如果你有一部脉冲拨号电话，那里面可能只有四个电子元件。它有一个开关，开关线的一头连接着扬声器，你可以快速按键来拨打电话。

电话是一个哑设备，一点也不智能。电话所能实现的一切功能都在网络中，来电显示是一种网络功能，呼叫等待也是一种网络功能。如果想要更好的体验，你只需升级网络，而不必升级设备。这是一个关键的设计决策。因为在那时，人们觉得智能网络体验更好，因为只需要升级网络你就可以为每个人提供超乎预期的服务。

智能网络有一个瑕疵：需要由内而外的升级网络。也就是说，创新只会在系统核心出现，并且需要获得许可。由于智能网络的设计，当所有网络用户都需要一项新的功能时，不得不破坏整个网络系统来进行升级，这样创新才会产生。

5.1.2 哑网络——互联网

互联网是一种哑网络，就像石头一样毫无生气。它所能做的只是将数据从 A 点移动到 B 点，它甚至不知道移动的是什么数据。它无法分辨 Skype 通话和网页之间的区别，它不能识别网络那一端的设备是台式电脑、手机、吸尘器、冰箱、还是汽车，它也不了解这个设备是否能提供强大的功能。它不知道所有这些，也根本不在意。

在哑网络中增加一个新的应用或创新只需在终端进行添加即可。因为哑网络完全能够支撑得起智能设备，你不需要对网络作出任何改进。一个需要五个用户就能执行的应用，要求的仅是这五个用户升级一下他们的终端设备即可，哑网络仍会传输他们的数据，因为网络不

知道也不在意新旧应用之间的区别。

5.1.3 比特币的哑网络

比特币是一个支持智能设备的哑网络，这是一个非常强大的概念，因为比特币将智能网络边缘化。

它不在意也不知道比特币地址是属于一个百万富翁、中央银行、智能合约、设备、或是一个普通人。它不在意成交金额的大小，也不在意比特币地址是位于吉隆坡还是纽约市中心。它对这些毫不知情，也根本不在意。

基于一个简单的脚本，它可以将资金从一个地址转移到另一个地址。也就是说，如果你想在比特币领域构建一个新的应用，你只需要升级终端设备即可。编写应用，在你的终端设备上发布，网络就会自动传播，因为它是一个哑网络。

这就是互联网创新的力量。这项创新不必申请许可，不需要权威批准，也不需要广泛的网络升级。这意味着，比特币不是一个特定的金融网络，它不是一个进行特定大型交易或小型交易、快速交易或慢速交易的金融网络。根据在需要的操作，你可以随意使用它。

将其与现有的银行系统进行比较。银行系统是根据非常智能的网络建立的，通过绝对控制的系统，向终端用户提供非常具体的应用。即便是结构最复杂的网上银行，你所能做的也只是访问超文本链接标记语言（HTML），这些超文本链接标记语言提供了银行能给你的服务，你不会获得应用程序编程接口（API），无法运行其他应用，无法升级、创新或更改任何内容。除非银行为了支持新应用，而改变整个网络。现有银行的系统支持大额支付、小额支付或快速支付，但这并非全部。比特币包含所有的这些功能，并且它不对交易做任何区别

对待，它是中立的哑网络。

无需系统核心做决策将会导致智能网络边缘化，并且将创新的权利交还到终端用户手中，使这些终端用户可以自由的、有针对性的创建仅有少数人需要的应用。

5.2 公地悲剧

另外，比特币还有一个独一无二的特点。这也是它能在过往中心化的、封闭式的网络中获胜，并且继续生存的一个重要原因：比特币是开源的、公开标准的和开放式的网络。

有一个关键的经济学概念是公地悲剧。当有一项无限制消耗的公共资源，所有参与者都倾向过度使用这些资源，这会导致资源枯竭，系统崩溃。这就称为“公地悲剧”。其中最常见的例子就是古英国大草地区域的公地。假设你有一块土地，每个人都可以在这里放牧，但如果每个人都不顾一切地恣意放牧，不久以后，这里将会变成一个大泥坑，牲畜也不会再来了。因为每个人都过度放牧，导致资源耗尽了。

5.3 公地狂欢

比特币和大部分金融网络不同，不会受困于公地悲剧。我们不可能在其他的金融网络中进行创新。VISA 的创新改革赢家只有自己；万事达卡的创新改革也是如此；SWIFT 部署的新功能，消费者是无法感受到的；如果美国银行推出创新方案，他们肯定会优先保证自己的竞争力，确保其它银行不会盗用他们的方案。

比特币是一项公共资源，资源的频繁使用反而会提高其价值，并且比特币不具有排他性。

如果一家公司在开源的基础上推出可用于比特币的新功能，那么该功能就可供这个生态系统中的每个人使用。这意味着创新会使每一个比特用户都变得更富有。如果一家公司投资研发比特币应用或是比特币协议，他们会从中受益，而其他人也是如此。当人们拥有比特币时，他们会从其他人在比特币技术上的投资中受益，有时，这种收益率会翻几倍，这就是一种奇妙的协同效应。在新技术上投资的每家公司都会使其余的人获得收益，这种现象就是公地狂欢。比特币只会因为频繁的使用和部署新的应用而发展得越来越好。

5.3.1 公地狂欢 2012-2014

让我们来看看其中的几个例子。2014 年是比特币情况最糟糕的一年，如果你只是关注比特币价格，那么情况确实如此。但是在 2014 年我们见证了两种新技术的部署，第一项技术是多重签名技术（multisig），核心协议需要进行微小的改动，但我们可以由此创建大量新的服务和产品。第二项技术是分层确定性钱包（hierarchical deterministic wallets，简称为 HD 钱包），它不需要对核心内容进行任何改动，但会让我们在钱包方面获得不可思议的新体验。那些公司从 2012 年就开始研究的技术使我们现在从中获得了可观的收益，目前整个生态系统都是从这两项发明中建立起来的。这些公司两年前的投资价值获得了爆炸式增长，并且由此催生了一个新产业的全系列产品。

2014 年是比特币最糟糕的一年。但是，在这一年里，500 家初创公司获得了 5 亿美元的投资，创造了数万个就业岗位，但是这些创新目前都没有产生效益，因为他们才刚刚起步。我们在 2014 年见证的所有令人难以置信的技术进步都是源于 2012 年的发明。现在，你觉得这 500 家公司和 1 万名开发人员会给我们带来什么？给我们两年时间，你将会在比特币的领域中看到一些非常神奇的事情。这就是公地狂欢的优势。

5.4 加速创新

当那些记者再次发布比特币的讣告时，我看到的却是一个开放性的生态系统，我看到了一个几乎死亡的经济体创造出了大量的就业机会，我看到在这个生态系统中，最聪明的人推出了最惊人的创新方案。最令人惊讶的是，我们都从中受益。真正意义上讲，我们并不是在相互竞争，我们是在参加公地狂欢，并且我们看到创新的速度正在加快，它正以惊人的速度飞速发展。

加入这个开放式的、去中心化的生态系统的公地狂欢。开源的、公开的标准的开放式网络能使用户自己掌握需要的创新，以及具体投入时间、金钱和精力。与封闭式的系统相比，在那里你需要获得许可才能进行创新，并且你的创新会被那些大公司之间的竞争排除在外。我们将会摧毁这种局面。

人们问我“如果高盛集团创造了高盛币，会发生什么？”我说，随他们去吧。如果它真的是开放的、去中心化的，那么正好证明我们这种开放式的系统是对的，我们就可以宣告胜利，回家庆祝了。如果它是封闭的，并且不允许创新，那么它就会在短短几个月内停滞不前，而我们将继续加速前行，越来越多的创新将由此诞生。

没人能阻挡这一趋势，这就是为什么我如此兴奋加入比特币这个行业的原因。比特币是一个哑网络，它将创新的权利置于每个人的手中。欢迎加入公地狂欢！

谢谢。

第六章 基础设施倒置

苏黎世比特币爱好者大会上的演讲，瑞士，2016 年 3 月

视频链接：https://www.youtube.com/watch?v=5ca70mCCf2M

今天，我想要介绍一个“基础设施倒置”的概念。当一项新的技术应用到旧系统时事态会如何变化，它将会如何制造矛盾冲突、压力，以及最终引起的基础设施倒置。

6.1 应用在旧设施之上的新科技

比特币是一项新的，与众不同的东西。当我使用“比特币”这个词的时候，我指的是更为广义的概念——去中心化的，以网络为中心的平台。一个可以被货币、支付方式以及所有其他可信任应用程序所使用的平台，这个平台可以是比特币也可以是其他东西。在这里，我用“比特币”这个词汇来涵盖所有加密货币。这是一项新的东西，在某种程度上，我们把它强加在现有的银行体系之上，结局必然是混乱的。

不只是目前这种混乱的局面，这同样也给了那些支持传统银行系统的人指责的借口“看，这个东西不好用。这个东西很慢。”这样的事情并不新鲜，每一次当有一种新的颠覆性技术诞生时都会发生这种情况。在新技术被采用的最初几年，它仍需要以现有的技术框架为依托。

让我们以历史的眼光来观察此类事情将会如何变化。当你见到一个可以颠覆未来 20、30、40 年的新科技，感觉它的发展非常平滑。这明显是因为人们的后见之明。比如说，汽车是一项伟大的发明，但是最开始人们第一次认识汽车的时候，他们不会说“太棒了！我们以后再也用不着马匹了。”对不对？事实上，他们说的是“这太疯狂了，这个嘈杂的机器会害死我们，它们永远也派不用场，除开那些人傻钱多的人。我们已经有了一架完美的马车，

为什么还要这么一个恐怖的，制造巨大噪音的玩意？”

贯穿历史，每当一项新的颠覆性技术问世，这种现象屡屡发生，抵触是人们的第一反应。最终成功的人是那些能坚持下去的人——即便社会上其他人都认为他们太疯狂了——追逐那些疯狂的想法，比如手机，电气化，互联网，比特币。这些疯狂的人，被其他人所嘲笑的人，最终都坚持到了所有人都认可他们的那一天。

6.1.1 马匹的基础设施

纵观历史，一件有趣的事情是，一项具有颠覆性的新技术往往诞生在并不合适它的旧世界中。人类发明的第一辆汽车当时是行驶在供马匹通行的马路上面的，那时道路的基础设施都是为了马车建造的，没有信号灯，没有交通规则，甚至没有水泥路面。

“生活在马车的世界里却开着四个轮子的汽车是多么疯狂。”

有些东西是马匹具备而汽车没有的，最早的汽车是前轮驱动，相对于马，它缺少了很多灵活性。此外，在没有平整水泥路面，只有鹅卵石、马粪的泥泞街道上行驶，马的平稳性更好。这就是人类第一辆汽车问世时所面临的生存环境。它诞生之时人们并没有说“太棒了！我们发明了汽车，让我们展示一下它在高速公路上的性能把。”相反的，正是那些人傻钱多的人在布满马车车辙的泥泞道路上测试车的性能，而且当时只有前轮驱动的汽车往往会被卡住。

这时那些批评人士就会说，“看吧，我们早说了这东西没用。看看你自己，甚至不能从泥里爬出来。另外，你到哪去加油？这只有一个加油站。如果到那之前没油了怎么办？我们的马匹即便饿了还能再往前跑个几英里，你的车呢？没油就完了。这是行不通的。”

6.1.2 从马匹到汽车

一项新技术诞生时必须要使用旧技术的基础设施。正如汽车最开始需要使用为马车设计的马路，然后，人们才开始修筑水泥道路。有意思的是，当人们修筑了水泥道路并且适合汽车通行的时候，旧的技术（马匹）也可以使用它们。假如你想在马背来一个休闲的苏黎世观光，我确定马匹不会对现在的道路有任何不适。

平坦的、坚固的路面不只是方便汽车、马匹的使用，它同样为未来的新科技打开了一扇大门。赛格威两轮平衡车、踏板车、滑板、旱冰鞋、婴儿手推车以及其他的种种新生事物都可以在现在的道路上使用。

这就是一个基础设施倒置的例子。你在现有的旧基础设施上开发一种新科技，然后情况颠倒过来，你建造了新的基础设施，旧的事物仍然可以用。

6.1.3 天然气的基础设施

历史上最具讽刺意味的事情之一是，某些自信满满的“预言家”因为他们的荒谬被人们嘲笑了许多年。当电首次在巴黎世博会上向人们展示时，巴黎市长说，“电只是一种时尚，一旦我们结束了世博会并拆除了埃菲尔铁塔，电这种东西就会从历史中消失。”他说的两点都错了，埃菲尔铁塔依然矗立，电也没有消失。

但是想象一下电刚从实验室里被发明出来的那个时期：没有任何基础设施。所以怎样把电接入家里？首先，把电接到家里的唯一原因就是你属于那种“人傻钱多”的人，和最早的那批把汽车买回家的人属于同一类人。把电接回家事实上需要把电线埋在墙里，这当然是一个疯狂的想法并且有可能把你的房子烧掉。在当时报纸上也确实是这么写的，他们报道了每一个把电接回家并且把房子烧毁了的“疯子”。

当时电的基础设施有哪些？在那时，大部分的设施都是天然气传送管道。在大城市中，天然气照明已经很普遍了。天然气管道在那时不只是用来给路灯和家用照明，同样也支持供暖。但这些设施不支持居民供电。

最初，电力的唯一用途就是工厂，这是人们能找到的关于电的最大用途。那时每家工厂都会有一个大型的天然气发动机，然后通过带子和滑轮把动能输送到工厂的各种设备上面。然而电力可以通过电线直接带动各个设备。

很显然，工厂可以从电力直接获益，但是为什么要把电带回家？为什么在已经有了天然气可供照明和取暖的情况下还需要用电？这里甚至没有电力的基础设施，如果需要用电的话，还必须建造新的设施。

那些投资了天然气管道的人会说，“这里没有足够大的配电网络来吸引用户，并且也没有足够多的用户需求来创建一个新的配电网络。这是行不通的。”正如他们之前对汽车所说的那样，“这里没有足够多的加油站给你们的汽车加油，也没有足够多的用户需求来建造新的加油站。这是行不通的。”

6.1.4 从天然气到电力

接着，电气化发生了，人们发现一旦你建好了电力的基础设施，不仅可以用电去做更多的事情，那些旧的功能仍旧可以实现。通过新的电力网络，你仍旧可以照明和取暖，甚至效率更高。通过电，你可以吹电风扇也可以吹空调，你可以带动发动机也可以带动搅拌机，你还可以使用吹风筒，更重要的是，房子并不会因为电力的频繁使用而烧毁。

再一次的，我们见证了基础设施倒置。在最初的几年，你必须要在旧设施上使用新技术。这几乎是不可能实现的。理论上你可以在家里安装一个天然气发动机，通过输入天然气来产

生电力，这样效率非常低。但是，你可以为了这种新的技术重建基础设施，旧的功能在新设施上实现的仍然很好——照明、取暖。并且这为新的应用打开了一扇大门，世界就是因为如此才改变的。

6.1.5 语音传输的基础设施

我的第三个例子更具专业性，通过这个例子可以区分出 35 岁以上和以下的观众。

Andreas 此时模仿拨号式调制解调器拨号上网时发出的嘟嘟声。

35 岁以下的观众完全不理解这是什么东西，超过 35 岁的观众会说，“这是一只“猫”，我以前就是用这个上网的。”请原谅我把大家带入这么古老的历史，猫就是调制解调器，这是一个通过电话线来传输网络数据的设备。问题就在这里：试想一下，电话线就像是以前的泥泞道路，而你试着把汽车开在这条道路上。

电话线是设计来传输语音的系统。在我小的时候，电话线仍然是模拟的，我们那时用的是脉冲拨号系统。我们过去有时会试着通过电话给朋友播放音乐，如果你也这么做过，你会发现这行不通，原因是电话线的频率非常窄。

现在你明白了，电话网络的设计只能用来做一件事情。它的专业性很强，就像天然气管道一样，它只能传输天然气，像水、电、油之类的其他东西都不行。电话系统的设计使它只能传递声音，尤其是人类的声音。我们声音的主频率是 1 千赫，大多数人都在这个频率的上下波动，少数人可以略微超出这个频率，有些孩子的尖声尖叫甚至能把我的耳膜刺穿。基于声音的特性和远距离传输声音的困难，工程师们把接收频率设定在了一个很窄的范围。假如是一个完整的接收频率，你可以听到对方讲话，但是静电噪音会很大。在高频，往往伴随着大量的电流干扰。在低频，会有嗡嗡响的噪音，同样有大量的电流干扰。如果你的电话有

静电和嗡嗡响的噪音应该怎么办？你可以加装一个过滤器滤掉低频噪音，另外安装一个过滤器滤掉高频噪音。现在，连接就会更清晰了，但是人发出的声音却会变得很古怪，因为它被压缩了。

当你传输互联网数据时，在这种被压缩之后的电话网络上很难使用，因为你需要把大量的数据输入一个非常狭窄的带宽。拨号上网时你听到的尖锐口哨声其实是两只调制解调器在不同频率测试可用的频段，就像一个说“你能听见我吗？”另一个回答“我听见你了，你能听见我吗？”这样一来一往一直到建立可用的频段。

用这种方法来传输数据简直是疯狂的。你基本上是把两部设备在一个非常狭窄的通道上相互连接，设法把尽可能多的数据塞进一个狭窄的管子里面。然后，我们升级了这个系统，人们把这件事情做的更好。

电话公司讨厌这样，“这不是我们设计这个网络的目的，这是一个原始的，依据当前的技术水平打造的语音通讯系统，你们这帮人在做什么？”事实上，在我长大的那个国家，希腊，如果你想用猫打一个长途，你首先听到的是调制解调器连接的声音，然后是一个突兀的咔哒声。发生了什么？这是因为电话公司检测到猫的时候他们切断了线路。为什么？因为这是在跟电话公司竞争。就像现在银行关停了某些比特币公司的账户一样。

那时电话公司说，“我们可以部署互联网数据连接网络——光纤、同轴电缆、宽带、或是在一个很高的带宽上建立直接的数据连接。但是首先，没人需要一个很高的带宽，你觉得这些用户能干什么？传输语音？我们已经有了电话网络了，并且运行的非常好。我们不需要这些新的东西。其次，我们没有足够多的用户基数来部署同轴电缆，也没有足够大的同轴电缆网络来吸引新的用户。这行不通。”这与之前马路和天然气管道的情形完全一样。

6.1.6 从语音到数据

然后，我们见证到了有史以来最为壮观的一次基础设施倒置。首先，互联网被电话网络不情愿的支持，然后那些支持互联网的电话公司逐渐转型成了互联网服务供应商，再然后他们的主营业务变成了面向数据的服务，后来他们的网络系统变成了数字网络，最后他们整个网络系统，包括所有的电话网络全部都在互联网上运行。今天，在世界任何一个角落拨打的任何一通电话都是在互联网上进行的，这就是一个完全的基础设施倒置。

事实证明，数据通过狭窄的电话网络进行传输会异常困难，但是你把这个等式翻转过来，在互联网上传送语音就非常容易。区别在哪？一个是非常专业性的设计，它已经为你选择好了应用，这个应用就是语音，数据传输是你强行挤进去的。另一个是通用的设计，数据意味着所有的东西，语音只是其中之一。

对于这些电话公司来说，最具讽刺意味的是，他们制造了一款名为“舒适噪音”的产品。如果你是一个电话工程师，你就会明白我说的是什么。我这一代人在年复一年的使用电话的过程中，经常伴随着静电噪音。而当我们有了蜂窝电话和数字网络之后，情况变得非常完美，它们完全是无噪音的。当电话的另一头停止说话的时候，你听到的是完全的安静。所以，你会觉得，“好吧，他把电话挂了。”但是对方并没有挂电话，他还在，只是完全没有静电噪音而已。

然而在那时，名字叫“舒适噪音”的这项产品是这样一个设备，它安装在你的电话听筒上面，监测你拨打的电话是否仍处于通话中，如果是，它就把静电噪音转换成你的耳朵刚刚能承受的程度，它实际上是一个产生高频噪音的设备，通过这个高频噪音你就能判断对面是否挂断了电话。

就是发明了“舒适噪音”的这家公司说，“我们永远也不能在互联网上做出高品质通话，我们不希望互联网部署到我们的电话网络上。”然而当我们现在可以在互联网上远距离传输 CD 甚至更高品质声音时，这家公司也加入了互联网行业。完全的基础设施倒置。

6.2 从银行到比特币

现在，我们有了比特币，我们有了一个去中心化的可信任平台，我们可以在全球范围内结算交易而勿需任何中介。但是我们仍生活在旧系统中。今天，我们做交易仍需要传统银行账户，IBAN（国际银行账号）码，或者信用卡。今天，比特币这部超级汽车，金融领域的 F1，仍然行驶在自 1970 年就已形成的银行体系这条泥泞道路之上。这条道路注定是崎岖不平的。

银行说，“这样行不通，看，你需要遵守我们也在遵守的这些规章制度，你需要进行跟我们一样的身份认证，你需要把进展速度慢下来跟我们的速度保持一致，这永远都行不通。不只是这样，你还没有足够的用户基数来建设新的基础设施，你也没有足够的基础设施来吸引新的用户。所以，事情很清楚了，这永远都行不通。”

但是我们拥有的是什么？正如汽车、电和互联网一样，这是一项新的技术，通过它我们可以创造出令人们意想不到的成千上万种新应用。

我预计，在接下来的 15 到 20 年，我们将见到金融领域基础设施的巨大倒置。最初，银行会进行抵制。然后，银行会采用这项技术，银行会把他们的系统运行在区块链和比特币系统之上，最后所有的传统银行业务都会变成运行在去中心化可信任分类账之上的一个应用。因为，创建一个新的去中心化可信任分类账系统来连接所有旧的银行体系是非常难的，但是在比特币这个公开的、全球性的区块链系统上处理旧的银行业务非常简单。你要做只是把银

行所有的功能都汇总起来，然后把处理事情的节凑放慢。比如，我可以做一个处理你交易的比特币应用，处理每笔交易只需 3 到 5 个工作日和 5 美元的手续费。其实，我这样做只是在模仿传统银行的工作方式，就像以前的“舒适噪音”产品那样。

我们中间那些适应了目前银行工作状态的人会说，“我不喜欢这种快速的金融方式，这让我感觉很不舒服，我喜欢每个星期天早晨坐在餐桌旁慢慢核对我的账户余额，确保我开出的每一笔支票都不会跳票。我不喜欢这种全球性的电子实时转账，这让我感到害怕。”为了照顾这类人，我们可以让系统慢下来。

基础设施倒置可以使传统银行系统舒服的运作在全球性的分布式账本之上—— 一种像比特币那样的开放式区块链系统，一种同时为更多种应用打开大门的区块链系统。那些新的应用或许会跟传统银行完全不同，就像赛格威两轮平衡车、滑板与马车的差别那样巨大，就像电灯与维多利亚时代那些老房子里的煤油灯的差别那样巨大。

在遗留的旧系统上保障未来是非常困难的，当你尝试的时候，每个人都会说，“看吧，这行不通。”但是一旦基础设施倒置过来，在未来的系统上实现过去的功能会变得非常容易。

当我们展望未来的货币，我们目前所处的阶段仍是一个非常初期的阶段，这是伟大的基础设施倒置的第一阶段。

谢谢。

第 7 章 货币是一种语言

2014 年比特币博览会：加拿大安大略省多伦多：2014 年 4 月

视频链接：https://www.youtube.com/watch?v=jw28y81s7Wo

接下来会有一些关于加密货币的未来在哲学上的思考，以及我在这次博览会上的收获。这次展会应该被称作“2014 年比特币和以太坊博览会”，我不知道你留意到没有，以太坊在这次展会上曝光率很高。由此产生了一个有趣的问题，实际上也有不少人问我：“以太坊是否会威胁比特币的未来？是否窃取了比特币的闪电网络？”我有好几次都听见过类似的问题，并且人们提及此事是为了试图了解竞争币——想知道竞争币是否会从根本上威胁比特币的主导地位，竞争币是否会超越比特币，竞争币是否会分散加密货币的价值。

7.1 人们无法选择货币

很长一段时间，我都在思考一个问题。我认为，从根本上讲，这是一个能够引起人们对货币的旧范式进行思考问题。我们都是在这样一个世界中长大的：货币以垄断的形式强加在我们身上，按其出现的地域被严格定义，并且货币的选择权不在你的手上。这是一个不可避免的意外，就像在我们生活中发生的许多其他事情一样。我出生在希腊的一个中上层阶级家庭，一生过着优越的生活，这就是一场意外。我出生就需要使用德拉克马（希腊货币），但这并不是我的选择，同样我没有选择成为白人，没有选择出生在一个可以接受良好教育的家庭。但是，这些事情就是这样发生了。

据我们所知，货币是国家的产物，它将某些限制强加在我们身上，我们不能选择货币，是货币选择了我们。在日常生活中，我们不得不使用本国货币，我们没有其他的选择——直到 2008 年。现在，我们的世界与以往不同了，但是我们的思维还停留在过去。

我们生活在这样一个世界，在这里，货币是受地域限制的国家垄断产物，这是一种零和博弈（指参与博弈的各方，在严格的竞争中，一方收益必然意味着另一方的损失）。货币就是国旗，它是国家的象征，它是国家经济价值的体现。它定义了在地缘政治中，全球各国争夺主导地位的活动。这与个人的选择无关。

7.2 货币是财富的一种表达方式

现在，我们生活在一个新世界，一个可以自由选择货币的世界。作为人类个体，现在我们不仅可以自由选择货币，还可以把货币用作表达财富的一种方式，我们中的任何人都可以使用简单的网页表格创建货币。

当我看到竞争币的演变时，我意识到我们以前提出了一个错误的问题。以后会有多少种货币？会有多少种竞争币？在不久的将来，竞争币如何在加密货币的世界中保持竞争力？以后会有数百种竞争币吗？如果有数百种，那么每种竞争币的价值意味着什么？它们如何竞争？——这是错误的思考方式。我最初把货币看成是一种零和博弈，就像在我以往的世界观里认为货币必定是国家政权的产物一样。然后，我认识到货币是一种应用。最后，我开始明白货币是财富的一种表达方式。

从本质上讲，货币是一种语言，是用于向对方表达价值。当我给你一张一美元的钞票时，我其实是在表达我想把有同等价值的东西交给你。我表达了与你交换价值的意愿，因为我很感激你为我所做的某些事情，或者作为交换你可以给我一些等值的东西。我正在把货币作为语言使用。

7.2.1 创造货币

无论你是否拥有正式的货币，这类事情在人类社会中都会发生。如果没有国家发行的那

种货币，你可以自己创造。令我着迷的一件事是：如果你在幼儿园观察那些孩子，那么你会发现孩子们是没有货币的，他们也不了解货币。但是他们能创造货币，他们会使用橡皮筋、口袋妖怪卡片、电子宠物、爱情符号、受欢迎的代币等东西进行交易。人们创造货币是为了表达他们的意愿和个性。你想，当一个五岁的孩子可以使用网站创建 Joey 币（以名字命名的货币），在他们学校的人气游戏里与另一种 Maria 币竞争时，会发生什么？

然后我才明白“以后会有多少种货币？”这个问题就相当于“互联网上以后会有多少个博客？”答案其实很简单：我们所有人。

现在，货币是财富的一种表达方式。但是，如果每个人都可以创造货币，它是如何产生价值的，每种货币又意味着什么？*现在，Andreas 指向大厅外，外面正在举办一场加拿大青少年偶像大赛。其中一名参赛选手 Amir，他的粉丝团阵容非常强大。*也许他想创造 Amir 币，这样他的粉丝们想看他更多舞蹈的愿望就可以实现了。为什么不呢？人们都在谈论我会创造一种 Andreas 币，我觉得这有点傻。但是，为什么不呢？我认为在将来某一时刻我们会见到这样的事情发生。

将来我们不会有数百种竞争币，也不是数千种竞争币，而是几十万甚至几百万种竞争币。再往后，为了表达某种风潮或者某种互联网流行文化，每天都会有上千种竞争币诞生。

7.3 根据产量决定权威

在这么多竞争币中，你要怎么分辨哪个币有价值、哪个币没有价值呢？为了解答这种类型的问题，我经常用互联网，这个我人生中出现的首个去中心化系统来寻找答案。在理解信息、信息的稀缺性、信息的权威性方面，互联网是怎么做的？随着互联网走向全球舞台，它作为一种社会体系又给我们带来了什么？

在过去，如果你想了解权威的观点，可以从《纽约时报》这样赫赫有名的传统媒体那里购买报纸。他们有着宏伟的总部大楼，他们的报纸产量如此之高，以至于需要成桶的购买墨水。但是这就是权威了吗？我们把权威赋予这些机构，由他们决定哪些观点重要，哪些观点不重要。我们让他们作为权威的“守门人”，在理解信息方面，对我们进行指导。

互联网的出现摧毁了这一切，突然间，任何人都可以印刷，任何人都可以出版了。

7.4 根据价值决定权威

在以前，人们会有这样的疑问，“如果任何人都可以自由发表观点，那么我们如何得知些观点重要呢？”他们认为如果出现这样的情况将会是世界末日。但是，一件有趣的事情发生了。在过往的世界里，权威来自于发行方和出版商，现在，权威却来自事实的真相。纽约时报作出失实的报道，致使整个国家卷入战争，而某个身处“阿拉伯之春”（2010 年席卷阿拉伯世界的一次革命浪潮）战争前线的埃及博客作者披露了事实真相，却无人问津。突然间，这个世界反转过来了，权威不再来自拥有报纸的那个人，事实的真相才真正重要——正如我们在货币领域做的那样。

7.5 通过使用价值决定货币价值

现在，权威不再来自出版商或者某个国家政权，他们以往可以通过垄断和武力的方式来宣布这就是你要使用的货币。但是现在，我们可以自由选择货币，甚至一个五岁的孩子都可以创造货币，哪怕他创造的这个货币并不具备金融价值。我们需要适应这个新的世界，在这里，我们不是通过发行方而是通过用户来衡量货币的价值。确切的讲，我们是通过货币的用户数量和使用用途来衡量它的价值。

让我们想象这样一个世界：一种货币被人们广泛使用，没有人记得是谁创造了这种货币、

为什么会创造这种货币。他们只知道在当地社区内，它具有购买力。假设在一个远离发达地区的小山村，村民使用两种货币进行交易。第一种叫作狗狗币，在货币的正面有 Shiba Inu，这是一种日本本地土狗。我不知道这名字如何发音，并且这也不重要，但是你可以用它买六个鸡蛋。其他的村民用另外一种货币做交易，这种货币上有一个名叫伊丽莎白的白人老太太的头像（英镑）。他们不知道伊丽莎白是谁，也不知道为什么钱币上为何会有她的头像，可能是因为她写了一首好歌，也有可能是她获得了加拿大青少年偶像奖，没有人记得这是怎么一回事，但是你可以用它买六个鸡蛋。

对这些人来说，谁发行了货币并不重要，重要的是它是否具有购买力。货币的价值纯粹基于其金融基础，由于货币广泛被人们所采用，由于它可以被用来做交换，所以才具有价值。这两种货币有着本质上的区别。第一种货币基于可预测的、稳定的算法供应，而第二种货币上除了印有名叫伊丽莎白的白人老太太的头像之外什么都没有。所以事实上，其中的一种货币具有内在的真实价值，因为它消除了货币体系的一些不确定性。而另一种货币就不是这么回事了。

我们要准备好在多种货币共存的世界里生活。

7.5.1 多种货币共存

货币是财富的一种表达方式，更是一种语言交流工具，它不再受发行方主宰。我们每个人都可以作为一个独立的个体通过选择使用哪一种货币，并且在使用的过程中才给予货币价值。令人惊讶的是，以后货币可能会因为一时的风潮，一个笑话、甚至是令人作呕的笑话而产生，并且会在互联网上呈病毒式的爆发，然后被人们广泛使用。

处于这样的世界我们应该怎么做？如果有数百万种货币，货币之间竞争意味着什么？假

如货币的稀缺性仅仅适用于当地，或者仅仅适用于这些货币所处的环境，会怎么样？假如货币的稀缺性不再源于发行方，而是源自货币被人们的接受程度，会怎么样？

我们将会有很多种不同用途的货币，包括具有明确发行规则的比特币，提供智能合约平台的以太坊、以及建设分布式域名系统的域名币等等。将来为了解决蛋白质折叠、寻找外星生命等问题，还会有其他新的币种产生。也许我们将来会有一种更适合小额快速支付的货币，和一种更适合房地产交易等大额支付的货币。如果你认同货币是一种应用，那么你会意识到担忧币种过多并不必要。

在互联网上，电子邮件是最早的应用，与比特币一样，它是一个杀手级应用，它让我们所有人都看到了去中心化通信系统的威力。正是这种去中心化的能力，使它在全球范围内广泛传播，随后就是实时通讯、论坛、公告栏、脸书、推特这些应用。你担心推特会摧毁电子邮件吗？你担心脸书会摧毁实时通讯应用吗？你担心推特的存在会削弱电子邮件的价值吗？我并不担心，因为我知道每个应用的用途都是独一无二的。有些应用能让我们实现实时通讯，而有些应用能让我们进行非对称通讯，比如我可以使用推特向上千观众讲话，这里无需双向同步通讯即可获得实时反馈。有些应用比如电子邮件，可以让我们与其他人进行长期异步通信。

我们需要做的事情就是创建界面，创建抽象概念，创建统一的工具，使我们能在统一的界面上实现所有的这些功能。我们可以向某个人发送短信，进行会话，并且将会话转换成音频会话，如果我们想展示我们的宠物，可以打开摄像头，变为视频会话，结束会话后可以发送一封电子邮件来总结我们已经达成的共识。现在，在一个的统一界面上我们已经进行了五种不同的通信模式。

7.5.2 货币是一种应用

我认为这就是货币以会将发生的事情。我们把货币视为一种应用，因此我们需要统一的操作界面来揉和多种货币体验，比如我们将来的钱包中可能包含 150 多种不同的货币。因为有了这些发明，例如侧链、去中心化交易所、流动性资金系统，以及完全的去垄断化、清除货币锁定、消除货币扣押等，我们就能以非常低的成本把比特币兑换为域名币、狗狗币和以太坊。甚至统一的钱包界面会根据我们希望用货币达成的目的，来帮助我们实现相应的目标。如果我想买房，它会以比特币的形式表达我的交易意愿，因为比特币是最适合的货币。当我想为这套房子所在的区域命名，这就需要把货币转换为域名币，而合同将会以以太坊的形式执行。当我想为早晨的一杯咖啡打赏服务员时，我会用狗狗币。统一的钱包页面会将不同货币的功能综合在一起。

我能预见这样一个世界：我们可以在多种模式下顺畅的兑换货币。此外，假如我们有多模式通讯系统，以后就再也不需要一一查看每种商品、资产、货币的价格和汇率了。

7.5.3 指数货币

有一种非常现实的可能，我们将会有一种指数货币：这是一种本身不可交易的货币，它不像商品那样具有内在用途，但是它可以把我们钱包里的多种货币折算成一种统一的货币单位。比如当你想兑换比特币，你可以知道一枚比特币相对于统一的货币单位的汇率是多少。我们可以用统一的货币单位对所有的东西进行定价，然后根据用途支付狗狗币、域名币或者以太坊。

我们已经在金融市场实现了这一点。实际上，你可以交易标准普尔 500 指数，你买入的不是一只单独的股票，你买入的是股票市场上不同股票的集合，它表达的是市场的总价值。

然后，你可以使用金融工具为交易定价。例如，LIBOR(伦敦银行同业拆借利率)作为一个基准利率，以契约的形式将全球多种利率集合捆绑在一起。你不会说，“无论德意志联邦银行的利率是多少，我都会买这件物品。”而是说，“我会以 LIBOR+2 的利率购买”，然后交易就会有一个稳定的参考点。

我估计数字货币将会发生同样的事情。我们可能会见到一些基准货币，其唯一目的是汇总我们钱包中所有货币的价值，并使我们理解价值是货币独立存在所表达出的抽象概念。

7.6 货币和社区的选择

所以，这是从哲学的角度看待货币和社区之间的关系，这也是以太坊与比特币之间的竞争，或者比特币与莱特币之间的竞争并不重要的原因，它们都是用来表达我们想要在特定时间、特定地点达成某种目的的交易模式。在我们选择货币的过程中，同时也是在选择与社区合作。

选择采用哪种货币包含的并不仅仅是使用货币这种简单的行为，它同时也是将用户与选择同种货币的整个社区联系在一起。当我选择比特币时，说明我相信比特币总量 2100 万的货币政策可以作为一种稳定的价值来源。如果我选择弗雷币，说明我相信这种通货膨胀性的货币，利率作为负数可以刺激消费并减少储蓄。通过货币，我选择了我的政治立场，我将自己与有同样选择的全球社区联系在了一起，这就是通过货币做出的选择。就像我在互联网上选择某种应用进行通信一样，这同样是将自己与相应的社区联系在了一起。我不使用推特仅仅是因为它是一个方便的通讯机制，我使用推特是因为我对选择推特的社区人群的观念和哲学表示赞同。

货币的选择更像是一种强有力的政治选择。通过货币的选择，我们已经进入了一个算法

决定政治，货币决定全球社区政治共识的全新政治领域。你希望通货膨胀？那么可以选择通货膨胀型货币。你是黄金的狂热信徒？那么可以选择通货紧缩型货币。你希望为穷人创造最低的收入保障？那么可以选择表达这种政治立场的货币。你希望减少碳排放？那么可以选择代表环保立场的货币。我们将会看到社区、政治和货币在汇聚在一起，并允许我们做出抉择。就像我支持 Joey 币，就说明我认为在这群五岁孩子中乔伊实际上是最酷的；我支持 Greencoin，是因为我担心全球温室效应；如果我真的非常喜欢红烧肉，那么我可以支持 Meatcoin。甚至是出现关于世界摔跤大赛的货币也没问题，总会有这样的货币出现。

实际上，所有的这些都只是一种表达形式，而这又回到了我们最初的观点：货币实际上是一种语言，我们用它来表达我们对价值的渴望。现在我们可以在如此广泛的范围做到这一点。如果每个人都可以创造货币，那么我们的选择将会至关重要。我们已经经历过了零和博弈的阶段，这不再与国家有关，同样也与是谁最先采用比特币或者是谁最先采用加密货币无关，是互联网这个世界上最大的经济体接纳了加密货币。它是世界上首个跨国性经济体，它需要跨国性货币。

7.7 货币创造主权

总而言之，我们已经反转了货币最根本的等式，2008 年之前的一千年中，货币一直由国家主权定义。国家主权是创造货币的基础，而货币是表达国家主权的方式，对货币的垄断控制则是国家主权的根基。现在，互联网有了货币，它将会通过货币创造自己的主权。

2008 年以后，货币创造主权。当互联网拥有了属于自己的货币，这就意味着互联网拥有了购买力，这就意味着互联网拥有了经济自由，这就意味着互联网可以用后民族主义和忽视国家界限的方式实现经济自由。当埃及的博客作者可以发表关于革命的博客并且用比特币资助革命时，当他们能与来自世界各地的人联系，并且分享自主、自由的观念时，他们是在

表达个人的主权，通过使用货币，他们同样也在是表达整个社区的主权。

这就是我们现在生活的世界，在这里多种货币可以共存，货币及其拥有者可以创造主权。

谢谢。

第八章 比特币设计的基本原理

此次演讲发表在 2015 年 6 月份，波士顿哈佛大学的创新实验室里，它是全球设计和创新实验室(IDEO lab)的一部分。在为期两天的研讨会上，同学们比赛制作基于比特币和区块链上的雏形应用。

视频链接：https://www.youtube.com/watch?v=Ur037LYsb8M

大家早上好。哇，你们这次的作业真难啊。在一个最基本的层面上，你需要理解究竟什么是比特币。我可以用几个字来回答这个问题，比特币是数字货币。但这并不能涵盖比特币的所有特质，它更像是货币的网络系统。实际上这是一个基于区块链技术和工作量证明算法的具有共识性的去中心化的网络，它允许数字令牌作为博弈竞争的系统奖励去分发给那些验证了交易信息的去中心化矿工——“哦，天呐。。。”许多人听到这里都会一头雾水。

即便是花费了几年的时间来探索什么是比特币，你仍会发现你要学的东西还有很多。部分原因是因为比特币仍是一种新技术，一项具有颠覆性的技术，但它仍是现有旧技术的抽象概念，这个旧技术就是货币。货币是一种工具，同样也是一种技术。它实际上与语言结构有共同之处，因此我们把它当成一种语言来在社会中传递价值。

8.1 货币的历史

谁来告诉我货币的历史有多久？观众：“五千年？”好，这是个不错的猜测，实际上货币出现的更早，这个问题的目的是让我们明白货币的历史甚至比历史本身更古老。我们可以去查询一下关于货币最早的书写记录，货币比文字更古老。有些人可能会感到疑惑，“货币比文字更古老？不可能吧。”事实是，如果你观察文字最早的书写形式，你会发现，它们是表格、账本。最早刻在石碑上的东西是由树枝和看起来像是账本的东西构成的，它们代表着

有多少罐油贡献给了法老。如果回到更早的时期，你会在古文明遗迹中发现古货币形式：珠子、羽毛、贝壳、巨型的石头。货币可以是多种形式，它的存在跟语言一样古老，这是一项真正古老的技术。所以，不止五千年，可能有会有五万年那么久。

8.1.1 灵长类动物和货币

事实上，我们看到其它物种也会使用货币。高智商物种比如灵长类动物，某些特别种类的鸟类比如乌鸦，甚至海洋类哺乳动物比如海豚，都有某种形式的代币用来在同类之间传递价值。或者它们可以快速学会货币的机制，比如说你可以训练灵长类动物，当它给你一个鹅卵石，你就给它一个香蕉。接下来你就可以观察，在很短的一个时期，这种交换货币的行为不仅会成为这群灵长类动物的文化，并且会继续传递给它们的下一代，它们就这样开始创造经济活动。

不光是好的经济活动，它们中间强壮的那些会开始抢劫，殴打其它的猴子并夺走它们的鹅卵石，由此来换取香蕉。它们还发明通过性来换取鹅卵石，从而获得香蕉，以及其他的一些最初级的经济活动。

货币是一项古老的产物，同样也是一种古老的技术，我们中间没人能真正理解货币。如果你想要验证这件事，坐下来和一个四岁的孩子聊聊什么是货币，你会发现这个孩子很快就会问出一些让你无法回答的问题。我们可以看到有些父母经历过这种事，非常滑稽：

“妈妈，钱是从哪来的？”“银行制作的。”“他们怎么做的？”“他们印的。”“我们为什么不能多要一些呢？”“去打扫你的房间。。。”

在和一个小孩子进行关于货币的对话的时候，你离“去打扫你的房间”这个回答往往只有四步，因为大人并不真正理解货币的本质。尽管货币这个文化产品在我们人类中已经存在

几百上千年的历史了，但是我们仍不明白它是怎么运作的。

8.2 货币的特征

我们的货币已经经历了几次技术上的迭代。今天我们就从货币最基本的形式开始，这些货币的基本形式都带有某些独特的特征。什么才是好的货币？是那些罕见的东西，贝壳、羽毛等等。你可以使用贝壳当作货币，除非你生活在海边。如果你确实生活在海边，那么贝壳就充当不了货币。其次，你需要方便的传递价值，所以，它必须是轻便携带的。除了极少数特殊的例子外，大部分货币形式都是非常轻便的。假如你买一头牛所需的货币重量甚至比这头牛还重的话，那就不是一种好的货币。这也是我们为什么不常见到金子被用来做大额交易，它太重了。货币的其他特征包括：它需要很难被仿造，它需要很难被超量发行，它需要被一眼就能鉴别真假，它需要是可互相替代的，比如我使用贝壳作货币，那么一只贝壳需要跟另外一只贝壳具有相同价值。又比如我给你一美元钞票，我具体给你的是哪一张纸币都是无所谓的，每一张一美元面额的纸币都能被另一张代替，这就是可相互替代性。

“货币本身就是一个抽象的概念，如果不是，那么它就不是货币——是物物交换。”

这些就是货币的技术，随着时间的推移，我们逐渐创造出了货币的抽象概念。货币本身就是一种抽象的概念，如果不是，那么它就不是货币，是物物交换。如果我给你一些香蕉来换取你的山羊，那么香蕉就不是货币，因为香蕉可以食用，人们不能用香蕉来作更进一步的交换。因此，香蕉换取山羊的例子就是物物交换，这是在使用一件商品来换取另一件。如果是抽象的货币——它本身并不需要具备任何实用价值——它代表的是其他的东西，一些共享的价值。

这就产生关于货币的一个无可避免的结论：货币是一个共享的文化幻觉，它是一个共享

的错觉。我们与其他人联系的基础就是这一张张布满细菌的、用绿色油墨印刷的纸张（美元）。假设你以一个外星人类学家第一次来到地球的角度来观察这件事，你会发现货币交换这件事非常奇怪：通过交换一张张纸片，你就可以建立社会关系，做交易——你就可以养活你自己，给自己建立一个居住的地方，等等。这虽然看起来完全没有道理，但这就是一个共享的幻觉。它基于这样一个假设：如果今天你给我一美元，那么明天我就可以拿这一美元跟另外的人换取其他一些有价值的东西。只要我们仍保有这个信念，那么美元就一直具有价值。价值来源于我们还能使用它的假设。

8.2.1 货币的另一种抽象概念

比特币只是货币抽象概念最新的一次迭代。前面我们已经讲过货币的抽象概念了，但是每一次我们再去讲比特币这种抽象货币的时候，人们都会恐慌，因为他们觉得这种新东西不可能是真的货币。回溯历史看看当硬币和纸币刚出现时发生了什么，当纸币刚开始流通时，没人相信它们真的有价值，这种共享的幻觉还没有出现，那时想说服人们用一张纸来交换他们手中的金币银币非常困难。

当你问人们有关比特币的问题，大多数人说的第一句话都是这不是真的货币，因为它不像美元那样有黄金做支撑——这让我感到很惊诧，美元从 1936 年起就不与黄金挂钩了。但仍然，有很多人觉得在某个地窖里，或者电影里面演的那些守备森严、固若金汤的地方，有一锭锭的金块来一一对应他们口袋里的美元。事实不是这样，没有这样的事。为什么比特币是货币？是因为有些人认为它是货币。你可以写一篇博士论文来论证为什么比特币不是货币，但是我仅仅使用比特币已经生活两年了。因此，你的博士论文上怎么写一点关系都没有。对我来说，这就是货币，对于其他信任比特币的人来说也是一样，这就是真的货币。

8.3 比特币的设计

你们前面的任务是在区块链上制作货币的新概念和新设计，世界上只有很少一部分人才能真正理解它。这是货币最新的，最抽象化的表达，它是全新的东西，它与以前货币的表达方式完全不同，并且它是一种非常复杂的技术。这真的是一项非常难的任务，面对这项任务，你的首选技巧就是使用隐喻，“隐喻”是我们创造期望的工具。比如说，你可以把电脑桌面比喻成真的桌面，然后你可以在这个桌面上创造各式各样的东西。但是如果误用隐喻的话，结局会变得很危险。

8.3.1 比特币钱包不是真的钱包

对比特币来说，每一个单独的术语和隐喻都是错误的和不正确的。让我们过一下比特币术语的这份清单。首先，一个“钱包”，什么是钱包？钱包就是存放钱的一个东西。但是比特币的钱包却不是这样，它的币不是放在钱包里面，而是放在网络上面。它的钱包包含的是私钥。所以，这不是钱包，这是一个钥匙串。为什么说这不是一个钱包？你能复制一个钱包吗？不。但是你可以复制私钥。钥匙串是一个更好的比喻。如果我有一个钥匙串，我就有了一串钥匙，我可以去一家商店把所有的钥匙复制并创建第二个钥匙串。两个私钥对同一个锁（公钥）都可以使用，并且它们之间可以互换。如果你了解钥匙串是做什么的，你就会理解比特币钱包是怎么工作的。你可以复制私钥，如果你给了其他人私钥的副本，他们也可以开这扇门，而不需要任何人的许可。

所以，比特币“钱包”不是一个真正的钱包，它是一个钥匙串。这是一个可怕的错误。你本以为钱包是用来装东西的，它装的东西会是不相关的和没用的。然而这些东西在比特币中都不存在。

8.3.2 比特币里面没有币

让我们从最基础的开始：“比特——币”，币是一个糟糕的词汇，一个糟糕的烙印。币，用了一个我们所创造的最有具体形象的货币形式，然而这个完全去中心化的网络系统里并没有币，但是它却取名叫“比特币”。这让所有人都感到困惑。硬币，是两代货币技术之前的产物，它是有形的，物理形式表达的货币。把比特币这种最抽象化的货币用最有具体形象的硬币来命名，只有工程师们才会这么做。

这里有一个小秘密：比特币里面并没有币。当矿工挖矿的时候，他们并不制造币，他们创建分类账，这些分类账并不列举币的数量。他们有输出——交易输出——这些都是可无限分割和重组的价值块。硬币并不能做到这些。在比特币里面你追踪不到某个币的来源是因为这里并没有币。

所以，你有一个并不包含“币”的“钱包”——因为这些币只是存在于网络上面它们并不是真的硬币，它们是交易输出——并且你真正持有的是一个私钥串。一笔交易并不是由发送方到接收方，比特币地址也并不含有资产负债表。一个比特币地址可以控制输出，如果你把区块链上所有的输出加起来，你可以得到一个名义上的资产负债表。然而这否是属于可花费的输出，具体数量是多少，却很难确定。所以，这里并没有资产负债表，比特币系统中也不包含类似银行账户的东西。

比特币所有的这些术语都是不正确的。问题在于，从设计的角度来看，这些隐喻不但没有表达正确的意思，反而误导了我们，我们原以为它会以某种方式做某件事，然而事实却完全不同。就像 Windows 桌面一样，对我来说 Windows 桌面与现实桌面完全没有一致性，它的比喻完全不对，你本以为它是做这件事的，它却做了一些完全不同和令人混淆的事情。一项好的设计本质是选择恰当的隐喻。

8.3.3 同形设计

下面是关于隐喻和设计的另一个关键问题，这里有一个特定的概念——同形设计“skeuomorphic”，意思是形式的影子。它的意思是当你在设计中创建元素时，给你一些现实事物的参考或暗示。有一个经典的例子，在第一代 IPAD 中，iOS 软件就有很多同形设计。当你在上面玩纸牌游戏的时候，纸牌下方有一种虚幻的感觉，那是因为它通过引入这个设计元素来描绘一个赌场的隐喻。同形设计是一种非常有强大并且危险的工具，如果你不能恰当的使用它，会给人带来错误的判断。

对于比特币来说，有很多同形设计。我最喜欢同时最痛恨的同形设计就是每一篇关于比特币的报道都会有这么一张图片：一堆金币，然后上面有一个大写的字母 B 在上面。通常这种卡修斯式的金币是由麦克卡德维尔设计的，可能其他人渲染了这种设计。他们使用比特币最差的隐喻设计，然后用漂亮的渲染实化它，使它看起来更加真实。这种同形设计使得很多人产生误解，有些人甚至真的到 eBay 上面查询，想去买这种名叫比特币的“金币”。他们想买的是一种镀金的、有一个大写 B 刻在上面的实物金币，这与区块链没有任何关系。“看，我加入了数字货币的革命。”他们说，但是这种有形的复制品并没有任何比特币的价值。就是这样的结果，然后，有人开始写文章，他们看着这种图片然后想“这就是比特币的模样”。然而这并不是真的比特币，我前面已经说过，比特币并不是硬币，这种结果很危险。

8.4 设计创新

为比特币设计一个好的隐喻真的是一项非常难的任务，因为它没有任何类似的参考物。我们以前从未做过类似的事情。我们想从过去的经验中寻找答案，但是失败了。在一种增量技术中，只要把你目前的理解稍微扩展一下，就能了解这种新技术，因为它本质是过往技术的一种延伸。然而，了解传统货币是怎么运作的并不助于你了解比特币，它是过去的一种激进式变革。对比特币理解最少的是货币经济学家，他们很难把思想扭转过来，他们会写出很长的理论来说明为什么比特币不是货币，哪怕事实上我已经用它生活很多年了。

理解颠覆式技术甚至比理解增量式技术更难，因为它并没有任何类似的参考物。你可以这样想，回顾一下 1970 年的《星际迷航》，那时他们对未来的预测有哪些是准确的？影片中有分析仪、移动式通讯和视频电话，这些都是基于 1970 年已有技术的预测。他们那时不可能猜到互联网，也不可能理解信息储存网络化的理念。他们有会说话的电脑，却不能使用电脑访问任何数据，他们更不可能预测到社交媒体这样的东西。更重要的是，如果你认真观察，你会发现一件很奇怪的事情——星际迷航里面没有使用任何货币。为什么？这是因为他们认为未来社会是一种无货币的社会，一个不需要价值传递的社会，也许这就是对现实最离谱的预测。

8.4.1 对未来的预测

当我们尝试预测未来的时候，有些特定的区域是完全黑暗的。这是一个我们以往从未见过的区域，这里有一些我们以前不敢想象的应用。因为为了使它们产生，许多条件都需要具备。为了网络的诞生，你需要普通标准化的传输协议。为了社交媒体的诞生，你需要大量电子邮件的基础和 TCP/IP 连接，并且这些连接必须永远处于在线状态，你需要有连接互联网的高密度计算移动设备。在社交媒体可能实现之前，所有的这些条件都要具备。

当你回顾 1992 年时的互联网，你觉得它有可能代替电话，这是你唯一的经验，互联网将会是一部不错的电话，甚至有可能同时具备电话、传真的功能。所以，当时那些电话公司说“它会是一部不错的电话，我们能做到这个。”幸运的是他们错了，否则的话，每次我拨打 Skype 电话，我的电脑旁边都会有一个硬币投币口，然后每三秒钟都需要往里面投进二十五美分。幸运的是，电话公司并没有制定相关规则。看到互联网，他们不可能预测到将来的发展，因为这不是以往事物循序渐进的发展，它是对过去的一种彻底背离。

让我们回到比特币上面想一下，考虑一下我们前面所讨论的：金融交易、银行业、支付

系统，“这会是一个不错的信用卡”“这是一个支付宝，或者说，全球性的支付宝。”但它并不是这样，这是一个完全不同的东西，我们看不到它将来会如何发展。在比特币上面可能会出现一些有趣的应用，但这些应用只有当你对这种新技术有了足够的洞察和适应之后才会产生。

今天，世界上有三十亿人口没有任何的银行服务，另外三十亿人没有银行账户——没有获得任何信贷或金融服务的机会。我现在就可以在券商网站上开一个美元账户，并且 24 小时都可以在东京证券交易所做交易，这就是特权，世界上只有不到十亿人才能享受这样的待遇。这只是七分之一而已，剩下的六十亿人，勉强有最基本的支票服务，他们中的大部分都生活在现金或者物物交换的社会里。因此，你接下来的问题应该是当一个生活在肯尼亚的农民，他只有一部诺基亚 1000，这种只能发送短信的手机。突然，这部手机具有了一个彭博终端，一个贷款发放终端，一个西联汇款终端，一个证券交易市场或者整个银行的功能，当这些功能提供给世界上余下的六十亿人时，将会发生什么？

比特币的发展不会被阻止的另一部分原因是，人们对于这种技术有一些强烈的需求。在发展中国家，银行很难把他们的服务提供给每一个人。最近，我和某个国家的银行从业人员交谈，他告诉我“他们国家半数的人口离最近的银行网点至少都有 100 英里远，人们甚至要乘坐独木舟才能到达，银行无法为这些人提供服务。”但是即便在亚马逊流域最偏远的村庄也有手机信号塔，太阳能充电板和诺基亚 1000 手机。世界上诺基亚手机的数量比其他任何种类的电子产品都要多，这是人类有史以来生产量最多的设备。世界上几乎五十亿人都有手机，然而有三十亿人有手机却没有安全的饮用水。考虑到这种情况，手机甚至比水源更广泛。当那些人中的每一个都变成银行家时会发生什么？对我来说，我对比特币的愿景不只是为世界上六十亿人提供银行服务，而是让我们所有人都去银行化。我们能做到，银行只是一个手机应用程序！

8.5 空白创新

这只是开始，比特币将会产生的真正趣事是我所说的“空白创新”——创新和空白，这是今天的系统做不到的地方。当技术改变基本的假设条件时，它会产生一些有趣的效果。互联网上发生的一些有影响力的事件不仅仅是因为网络的连通性，而是因为远距离传输信息的边际成本。在互联网产生之前，把信息从 A 点到 B 点传输需要昂贵的成本，而网络现在几乎把这个成本降低为零。结果是，数百万以前无法实现的应用突然间变为可能。为什么你会在线听音乐而不是把唱片买回来本地储存呢？因为它不花什么钱。一旦不花什么钱而你又可以在线听音乐，你突然就会意识到版权费被高估了。一旦整代人都意识到这件事，那么知识版权也就被高估了。所以，再见了，唱片产业。这些影响的产生是因为技术改变了成本。

让我们想想当比特币改变交易成本时会发生什么——远距离转账、价值转移、记录信息、以一种不可篡改的方式记录信息等等，当这些技术都成为可能时会发生什么？

当有这样一个系统，一个无需人为干预就可以评估交易规则，一个不需要信任任何人就可以被信任的系统出现时会发生什么？在比特币中，我们称之为消除对手方风险。当我创建一笔交易并且用私钥签名之后，比特币网络上的任何一个人都可以独立验证这笔交易，他们通过查验区块链信息就能验证这笔 350 个字节大小的交易。这是一种工作量证明系统，一种自我验证系统，一种不受人为影响的系统，它是一种网络拓扑结构系统。

这是什么意思？它对商业、交易有什么作用？我们能理解它对于银行业的作用，我们知道西联汇款业务在过去这十年非常艰难，它对世界上最贫困的人口收取 30%的手续费，由于比特币这种颠覆性的技术它的业务肯定会下滑。去年，西联汇款的 CEO 说，“中期来看，我们并不担心比特币。”我想把这句话记录下，这只不过是他们的一种说辞而已，就像当年诺基亚抢走了柯达的午餐，柯达的老板当时说的那些话一样。柯达曾经是世界上最大的相机

公司，一直到另一家并不属于相机行业的公司（诺基亚）一年生产十亿台手机，并且把这个行业彻底摧毁。他们从来看不到将要发生的事情，现在这种事情将会发生在西联汇款身上。

这只是小事，假如无需第三方对交易规则进行验证会发生什么情况？它会彻底改变我们今天的几个基本社会规则，它改变了所谓的“科斯系数”，这是机构产生的管理费用。当我们想以团队的形式做某件事情的时候，两个人能比一个人做的多，三个人甚至能做的更多。但这有一个上限，一旦这个团队变得过于庞大的时候，其中通讯成本就会大于边际成本。所以，超过限度之后，增加更多的人反而会使事情变得更糟。比特币改变了这种情况，因为它可以在交易、商务、独立验证的基础上，大规模降低机构的科斯系数。我们目前大概有一百万用户，五千台矿机，以极低的成本每十分钟验证一次账本的状态。这种事情在以前从未发生过，它为我们不敢想象的东西打开了一扇大门，比特币是与过去彻底的分离。

让我举一个简单的例子：人格。为了拥有金钱，为了拥有银行账户，为了接受账单，为了支付，你首先必须拥有法律人格。在世界金融网络的任何一个角落，人们都拥有金钱，他们可能会以公司的形式拥有金钱，但公司也只是一群人聚集在一起。比特币并不要求自然人的身份，一个软件代理就可以拥有金钱，一个无需人类干预的软件就可以控制金钱。这在人类历史上是从未出现过的，目前我们也看不到这种趋势将会如何发展。

这里有一个小的思想实验，把比特币、优步和自动驾驶汽车这三种颠覆性的技术混在一起，接下来会发生什么？一部自我拥有所有权的汽车，一部自动支付丰田租约、保险、汽油、自动搭载乘客的汽车，一部不属于任何公司的汽车，一部自身就是一个公司的汽车，一部自身既是公司股东又是所有人的汽车，一部作为独立金融实体而不被任何人拥有的汽车。这种事情以前从未发生过，但这只是开始。

我可以肯定，首个分布式自治公司必将是完全的自治，基于人工智能的勒索病毒会在网

上到处掠夺别人的比特币，用这笔钱进化自己，编写更完美的程序，购买更多的服务器，并且四散扩张。这是关于未来的第一个幻境。另一个关于未来的幻境是数字化自治慈善机构，想象一下这样一个系统，接受别人的捐赠，并且实时监控推特和脸书这样的社交媒体，当达到一个特定的阈值，比如说十万人在讨论某个自然灾害，例如发生在菲律宾的龙卷风，它可以自动整理捐赠并且在当地设立帮助基金，无需经过董事会或者股东批准，100%的善款都直接发给受害人，并且任何人都可以查看这个自治式慈善机构是怎么运作的。我们现在正在逐步接近一些以前从没见过的东西，比特币不仅仅是货币而已。

现在，让我们看看比特币社区是如何处理它不可思议的潜力的，天呐，这简直是一团糟。

8.6 自动提款机的用户体验

举一个简单的例子，你们当中有多少人使用过比特币自动取款机？这个经历怎么样？谁喜欢它？答案是没人！什么是自动取款机？自动取款机已经发明了有将近 25 年了。自动取款机的功能是什么？处理现金用的。当你在自动取款机前操作的时候，你预先已经和银行建立关系了，你预先已经有账户余额了，你主要目的是存入、取出现金。20 秒钟的时间太长了，三次按键太多了。在过去的 25 年中自动取款机最令人难以置信的创新就是快速现金处理，然而他们此后并没有任何改进。现在，我按一下按键就可以拿到现金，15 秒钟，就可以把钱转进转出。为什么这很重要？因为自动取款机的使用高峰是下午一点，在市中心一百个人排成长队聚在四、五个自动取款机面前，等着取 20 美元来为午餐买单。这种情况几乎在世界任何一个地方都能看到。

自动取款机的目的是什么？对银行来说，它可以减少人力成本，并且把顾客与银行之间的互动时间减少到最低。这与比特币有什么共同之处？什么都没有。

8.7 比特币自动提款机的用户体验

现在让我们看一下比特币自动取款机的用户体验。比特币自动取款机的普通用户是那些从未见过比特币的人，是那些不了解比特币的人，是那些与比特币的持有者没有任何联系的人，是那些没有比特币钱包的人，比特币自动提款机对他们来说是对这种货币的最初介绍。他们不懂什么是比特币钱包，更不懂这实际上只是一个私钥串。这是一台由工程师设计，模拟自动提款机的机器。

所以，用户走上前希望通过几次按键就让这台机器吐出比特币。这是建立品牌忠诚度的办法吗？这是建立良好用户体验的办法吗？这是吸引新用户的办法吗？我的意思是，这台机器只会把情况弄的更复杂。“请打开你的手机并展示 QR 码。”用户会说，“什么？什么是 QR 码？等等，让我打开谷歌应用商店查一下，嗯，这里有一个扫码的手机应用，我应该用这个吗？可能我应该用这个而不是那个，天呐，这里面大概有 26 个同类应用，哪一个才是最好的？我不知道，嗯，我想用这个 Coinbase 的，晕，需要事先有 Coinbase 账号，天呐。。。”

终于，用户弄好了钱包并且出示了 QR 码，存进一点钱然后获得了比特币。这时问题来了，用户应该拿他做什么？谁接受比特币？在哪里可以花费比特币？怎么花费？怎么转账？怎么保障币的安全？如果手机丢失了币会不会丢？一点头绪都没有。为什么？因为这该死的机器什么介绍都没有。它只是把币丢给你，15 秒后就退出页面然后接待下一个客户。

如果是我设计比特币自动取款机，首先，我会把它放到酒吧里面，其次，上面不会是英文而是西班牙语，因为我准备推出的是具有汇款功能的机型。第三，在这台机器上首要的功能将会是“把钱转到墨西哥城”，因为我希望人们能够使用比特币去做一些事情。第四，我会在上面设置一个大键钮写着“与人工客服交谈”，我会设置一个电脑屏幕与互联网连接，并且上面有一个摄像头对准前面。客户：“比特币是什么鬼东西？我在哪可以使用它？”客

服：“噢，先生，我看到您在第二十五大道的酒吧里面，这附件有三家商店接受比特币支付，让我为您播放一部简短的介绍影片吧，把所有的孩子都叫到店里来，我们可以跳一支关于比特币的歌曲。接下来请看另一部影片。。。”我不希望客户与 ATM 机的互动只有十五秒钟，我希望是两个小时，我希望把所有的朋友都叫来坐在这部机器前面观看比特币的视频，学习比特币的知识。它应该有漂亮的色彩，它可以告诉我去哪可以花费我的比特币，它可以给出关于比特币钱包的建议，它可以直接把币转到我的手机里面，它可以建立客户忠诚度、品牌和用户体验。这不应该只是一个十五秒的互动，因为这将是很多人使用比特币的首次经历，人们本来有机会可以把它做的更深刻、更有意义、更具教育体验，然而却没有。

8.8 孩子们使用比特币

平均来说，银行开户的最小年纪是 16 岁。当一个 16 岁的孩子去银行开户的时候，我希望他们至少有六年的比特币使用经历了。因为那时，当他们第一次面对银行柜台工作人员时，情况会是“3 到 5 个工作日？什么是工作日？下午 5 点关门又是什么意思？我下班时间才刚到 5 点。存款又要手续费是什么意思？这太荒谬了，你们这些人就没听说过比特币吗？”

这就是我所希望的经历。你知道吗？甚至一个十岁的小孩就能开比特币账户。知道为什么吗？他们可以在网络上下载应用，并且人生中第一次自己掌握金钱。因此，父母大可以进行“先有鸡还是先有蛋”的讨论，同时也需要进行关于私钥的讨论，这可能会是一个巨大的代沟。对很多年轻人来说，比特币将会是他们第一次金融体验。当他们第一次走进银行时，他们早已体验过银行业务了，这会是一个巨大的优势。

8.9 新的技术，旧的名词

所以，比特币应该如何吸新用户？诀窍肯定不是模仿银行，不要做任何和传统银行类似

的事情，那样只会污染他们的思想。我希望新用户可以获得比特币的全新体验，不希望它看起来像一个支票账户。老天保佑你不会用“支票”这个词，现在打开任何一个加密货币交易所——Circle, Coinbase，里面的账户名称是什么？是支票账户。里面显示资金余额和交易明细。他们到底是请谁来做的这个设计？“支票账户”这个名称是什么意思？字面意思是你开具支票的账户。我知道这里是美国但是我们在金融科技上已经落后 25 年了，我可以向你保证，世界上其他国家很少使用支票。什么是支票？支票就是一个老奶奶在超市里面结账同时使二十个人在后面排队抱怨的东西。我每月都用这个东西支付房租，但是我也不知道为什么，我不能用其它的方法来做这件事。现在已经是 2015 年了，可我仍需要在一张纸上签字，然后通过邮局把它寄出去，这简直是神经病。然后我的房东就可以拿着这张支票到银行，把里面的钱存进银行账户。大概 3 到 5 个工作日之后，银行系统才会清算这笔钱，然后房东还要为自己钱付上 5 美元的手续费。

我们用不着强行推销才能让比特币赢过银行，想要比特币赢过银行你需要做的是让某个人用上一个星期的比特币，银行自己就会把后面的事情做完。

8.9.1 国际电汇的趣事

我被邀请去德意志联邦银行做一次演讲，支付预付款的时候出了点问题，我平时都是接受比特币支付，然而他们却不会用比特币，最后我们协商用国际电汇的方式支付。汇款过程需要 16 天。首先，他们问我要银行账号，接下来那天他们说还需要银行国际代码（SWIFT number)，那时我这边的银行已经关门了，所以我拿不到银行国际代码。第二天早上，我拿到代码并发去德国，但是根据欧洲时间他们那边的银行又关门了。等到隔天早上他们用银行国际代码转账时发现这个代码是错的，这是美元账户的代码而不是外汇账户的代码。于是他们发了一封邮件给我说明情况，但这时我这边的银行又关门了。又过去一天，我终于拿到另一个代码并把它发去德国，然而由于时差的原因他们那边的银行又关门了。最终，我收到了

这笔电汇，然而我这边的银行看着电汇单说，“德意志联邦银行？从来没听过，听起来怪怪的，先把这笔汇款冻结 14 天，以防跳票。”这可是世界第三大的中央银行，是德国的国家银行，他们不会跳票！14 天后——最棒的事情来了—— 他们说，“外汇扣留，付你美元。”最后结算外汇，他们付给我 80 美元！为什么才 80 美元？这算什么鬼事情？我能怎么办？让他们全部扣留算了。这是在戏弄我吗？完全说不通。

8.10 使用银行类隐喻

这就是我们需要用比特币解决的问题。如果你是设计师，往市场推广新产品的时候，你会在产品中重新设计哪些隐喻？根据比特币市场，全部都需要！这样你就可以说服人们比特币具有跟银行同样的功能。它不包含传统银行那些好的部分——比如能够轻易的撤回交易，丢失私钥的时候能够得到退款等等，它没有任何这些功能。但它同样也没有传统银行不好的部分，但人们很难注意到这点。所以，我们以前完全没有把比特币的优势展示出来。

8.11 创新、设计和采用

比特币迫切需要重新设计，它以前是由工程师设计的并且很难理解。但我仍抱有希望因为我们以前曾经做到过这点。我第一次上网是在 1989 年，那时在互联网上进行商业活动是非法的。它属于国家科学基金会所有，并且只能用作学术用途。那时，域名系统（DNS）仍属于婴儿期，大多数系统尚未分配有域名，它的结构还不完善，很多有意思的东西只能通过 IP 地址查询，我那时兜里随时揣着一本 IP 地址目录，这样才能接触到那些有趣的网站，使用过程中还必须具备 UNIX 命令行技术。

那时绝对没有办法来忍受我妈妈，有次我妈妈告诉我她的立体声播放器坏了，我试着弄明白出了什么问题，她说，“这机器坏了，上面总是有个 0：00 在闪。”我只花了几分钟时

间就弄明白是她把机器上一个按钮拔了出来并且重置了时钟，所以时钟一直在等待重置并且在 0：00 的时间闪烁。这就是我现在尝试通过互联网联系的一个人，但这很难做到。我用了大概 20 年时间才给她发了第一封电子邮件，为了做到这样事许多条件都必须具备，其中最重要的就是 iPad，她需要用一根手指猛戳屏幕才能使用。因此，在 1989 年，互联网是不可能被主流社会接受的。

8.11.1 用户体验和社会

1994 年早间有一个很棒的电视新闻节目，那时很多记者都挤在一起等待节目播出，他们会讨论即将到来的互联网，并试图得到正确的信息。一个记者问另一个“所以，等等，互联网就是那个带有@符号的东西吗？”“不，这是电子邮件，互联网是那个有 www 的东西。”“哦，我还以为那个是电子邮件。”“不，那就是互联网。”“但你确定那个东西不是网站吗？”全都是这样的讨论，由工程师设计的东西就是这样令人难以理解。随后发生了两件事，第一，我们让技术变得更容易理解，更方便，更精良。第二，社会发生了改变。今天，每一个普通人都知道@和 www 的区别，虽然它是一个很糟糕的设计。社会学会了互联网的语言，因为它非常有价值。

当我们使互联网变得简单的时候，社会也赶了上来，现在人们都能理解互联网中哪怕是最难的那一部分。比特币上也发生了同样的事情，在我参加的某些主流论坛，那里有人从未听说过比特币，我说“听着，不用担心，会有人向你解释比特币的。当他们清理完会议室后，让他们教你就行了。”有些 10 岁的孩子都能理解比特币，我遇见过一个小孩，他能通过网络接口自己制作山寨币。

我经常被问到一个问题“将来会有多少种加密货币？”答案相当于“互联网上会有多少个博客？”我们所有人，他们所有人。将来不只是几百种币，会有几千种，上万种。当一个

6 岁的孩子都能制作一个名叫“Joeycoin”的币，并且在学校里发布，这说明加密货币已经是全球化、并且扩展性很强了。不幸的是，一个竞争者，Maria 币随后也在学校里发布了，这就是那种老套的货币战争。一部分原因是因为每个孩子都可以制作货币，当你把小孩单独留在幼儿园，他们就会玩制作货币、抢银行、卡牌、积木的游戏，他们会开始储存、交易、交换感兴趣的东西，并且最终会为刚刚发明的假想货币展开抢夺，这就是人类的发展历史。

我们刚刚发明了世界上最令人惊叹的货币，你现在的任务就是创建正确的设计隐喻，让每个人的使用都变得简单。

谢谢。

第 9 章 货币是一种内容形式

比特币南部会议：新西兰皇后镇：2014 年 11 月

视频链接：https://www.youtube.com/watch?v=6vFgBGdmDgs

大家早上好！我最近致力于研究一项新课题：货币是一种内容形式。通过与传输媒介的完全分离，比特币将转变成一种独立的内容形式，而这将彻底改变人们对货币的认知。

这是什么意思？比特币交易是一种可以在世界任何地方执行的签名数据结构。很多人都认为只有在比特币网络上才能发送交易，实际上根本不是那么回事。比特币交易需要被矿工确认并打包进区块中，但是交易本身却不需要通过比特币网络发送。比特币网络没有特别之处，它只是用来生成交易和区块的，任何形式的通讯媒介都可以用来发送交易。

其中不可思议的是，比特币交易并不包含安全机制。交易的安全性是由矿工的工作量证明来保障的，并且交易的数字签名是由终端用户通过他们私钥生成的。在比特币交易中，不区分敏感交易或秘密交易，请允许我做如下说明。

9.1 信用卡：设计存在安全隐患

如果我用信用卡在商店消费，那么我需要经过一系列中间商向商家发送信用卡号码、有效日期以及卡背面的 CCV2 码，这实际上相当于发送私钥，这是在向我的银行账户发送接入码。这些都属于敏感信息，如果别人抓取到这些信息，我的帐户安全将会受到威胁。信用卡信息可能会被商家、中间商、或者黑客盗取，所以一定要妥善地保护信用卡信息。

当人们从钱包拿出信用卡的那一刻一直到这笔钱转到商家指定的接收账户上，信用卡信息一直在一连串虚拟网络节点上传送，信息会以加密形式从销售点发送到商家后端，然后以

加密形式从商家后端发送到 Visa 系统进行加密批量处理，最后以加密形式从 Visa 发送到发起银行和对方银行，过程中的每一步都需要加密令牌，这个令牌就是秘钥。如果在某一环节加密失败，信用卡安全将会受到威胁。

这些信用卡信息同时也会在许多中转站点存储，这是为了保存历史记录。这种方式实在是太可怕了，因为这会产生一个中心化的信息宝库，一旦黑客侵入这个宝库并藏匿于此，后果不堪设想。这种现象屡见不鲜，美国两大零售商 Target 和 HomeDepot 系统曾遭到黑客入侵，大约五、六千万份信用卡资料被窃取。最近摩根大通也有 7500 万个银行账户面临安全威胁，这都是因为这些公司未能尽责保护用户的信用卡信息。

实际上有两类公司：一类公司是采取必要措施后，仍未能成功保护委托的信用卡信息；另一类公司是采取必要安全措施后，信息保护也即将失败。也就是有两种情况——你的账户已经遭到黑客入侵了，或者即将遭受黑客入侵，没人幸免于此。没人有能力保护数百万安全令牌免于蓄意攻击，这是不可能实现的，我们也不知道该怎么做。没有任何信息安全手段可以让我们免受各种网络攻击，信用卡的设计毁了它，因为令牌本身就是秘钥，如果你发送令牌，会使整个帐户暴露在风险之下。

9.2 比特币交易：设计保障交易安全

比特币交易与信用卡交易完全不同，我们发送的不是私钥，而是签名之后的信息，这代表授权。此授权有两个外部参照：（1）通过在区块链上参考未花费的输出来获取转出账户的信息；（2）通过对谁能花费这笔钱设置新的障碍、或使用限制，即公钥或比特币地址，来获取转入账户的信息。比特币交易不包含任何所谓的敏感数据，即便交易信息被窃取，所有能了解的也只是转出账户地址、转入账户地址以及交易金额。仅此而已！哪怕是将这些交易数据打印出来张贴在广告牌上，甚至是爬到屋顶上将这些数据喊出来也不会透露任何信息。

比特币交易可以通过极度不安全的 Wi-Fi 进行，也可以使用烟雾信号、灯光信号、甚至是信鸽来完成，交易信息的泄露不会破坏账户安全。

9.3 货币是一种内容形式

绝大多数人都不明白货币转换为内容形式意味着什么。我们现在得到一个长度仅为 250 字节的交易数据，并且将它与传送媒介完全分离，所以它不依赖于网络安全。任何全节点都能独立验证交易的真实性，交易验证在几秒钟内就能完成。它要做的就是连接网络上的某个节点，通知矿工进行确认，仅此而已！一旦交易被添加到比特币网络并进行广播，基本上就可以确定这笔交易最终会打包进区块，而且这笔交易将会是有效的。如果我在区块链上查询任何一笔交易，都能算出这笔交易手续费是否足够，然后可以设想矿工将会如何处理这笔交易。因为我了解共识网络的操作规则，我知道一旦交易信息在网络上广播，它很快会被记录到一个新的区块中。

9.4 比特币交易不可能被禁止

比特币交易并没有什么魔力。让我们想一想：如何把一笔 250 字节的交易加密，并且在网络上发送。

最近有人问我一个问题“专制政府禁止不了比特币交易吗？”答案是无法禁止，但我认为人们并不知道其中的原因。下面，我会举几个实例加以说明。

9.4.1 通过 Skype 发送比特币交易

我的第一个例子听起来很荒谬，即把比特币交易编码为 Skype 中的符号表情或笑脸符号。Skype 中有一个长度为 128 字符的表情符号字母表，你可以发送各种表情，如皱眉、

开心、赞扬、反对、天晴、心跳和生日蛋糕等等——相信大家对这些表情符号已经习以为常了。现在，我们从信息内容的角度来分析。那是一个字符集，对吗？如果我是一名计算机科学家，我会说“这可以是一种新的编码方案”。我可以发送一条长度为 250 字节的交易信息，也就是 500 字符，500 个表情符号。所以，比特币交易就是表情符号。

我可以写一个简单的脚本，可能是两行 Python 代码，如果进一步精简，也可能是一行。这里不需要程序库。在脚本中，比特币交易可以是十六进制，并且可以用表情符号进行编码，然后我可以把它复制到世界任何地方的 Skype 聊天窗口，只要收到该表情字符的人将其输入到解码器脚本中，然后添加到比特币网络，此次交易就会顺利完成。

现在你能解释清楚为什么政府不能通过关闭 Skype 来禁止比特币交易了吗？如果他们关闭 Skype，我们会使用 Facebook；如果关闭 Facebook，我们会使用 Craigslist；如果关闭 Craigslist，我们会把交易放到 TripAdvisord 的评论栏中；如果关闭 TripAdvisord，我们会将其作为维基百科的评论进行发布；如果关闭维基百科，我们会在假期照片中将其作为 JPEG 图片背景进行发布。

现在货币是多种完全不相关的信息内容形式，当我们今天有如此丰富的多媒体通讯机制时，他们绝对没有办法禁止信息在世界上的传播。

9.4.2 通过短波无线电的方式发送比特币交易

假设我们没有互联网，我想到了一个更加荒谬的计划，即通过短波、跳频通讯、突发无线电的方式发送比特币交易。如果你想开展全面的游击战的话，可以采用这种方式。

在第二次世界大战的法国沦陷区，盟军从飞机上扔下数千个短波无线电的整套设备，陆地上的游击队员将它们藏在谷仓、树洞、废弃的大楼或桥底，并且使用它们与欧洲各地的盟

军指挥中心进行通信，就在驻扎此地的纳粹部队眼皮底下。无线电的一个特点是，不仅包含许多波段，而且无线电信号在某些特定频率上可以从平流层弹回。那时，盟军就用它来进行语音或密码通信。

今天我可以把一台笔记本电脑和一个非常简单的短波无线电发射器通过 USB 连接起来制成整套设备。天线可以由一根足够长的金属导线制成——铁丝、晾衣绳、断开的电线、栅栏线、铁丝网等等。我在新西兰留意到你们有很多这样的线，就在那些羊群四周，遍地都是。

现在，发送一条比特币交易信息只需要打开笔记本电脑，连接无线电，再按“回车键”，25 秒钟后交易就能发送成功。只要在附近 1000 英里内有能连接上比特币网络的接收站——并且你可以将接收站隐藏在任何地方，那么它就能成为一个被动式监听器——监听设备可以将交易信息添加到网络上。如果我是游击队员，我会先建立好离线交易，当我准备交易时，跑到场地中间，将无线电发射器夹在晾衣绳上，按“回车键”，25 秒钟后交易会发送成功，我再收起设备，然后消失在森林里。如何才能防止交易发生呢？不能！答案很简单，因为你根本不知道怎样做才能阻止交易的发生。但这仅仅只是一个开始。

9.5 媒介与信息的分离

当你意识到货币已经成为一种内容形式并且交易与媒介已经无关，那么一些非常重要的次要特征就出现了。某位名人曾说过，媒介即信息，意思是媒介约束、改变并且可以扭曲信息。

当媒介是电视时，一条 18 分钟的信息会被多次插播广告，这是你获得信息的唯一途径，没有其他的播放模式可供选择。所以，你根据信息价值等于生产成本这一错误假设，来衡量信息的价值。例如，电视台把一部分成本强加在视频制作上，从事这个行业的人会错误地认

为电视节目的生产成本与那个节目的价值是一样的，成本越高，价值也会越大。

所以当类似 YouTube 的媒介出现并将生产成本降到零点时，你可以想象，在那一刻，他们的内心有多么的恐惧！你觉得当时电视行业的人立即联想到了什么？如果成本为零，那么内容将会一文不值！当信息与媒介分离时，你对价值的理解就会从生产成本决定价值转变为信息内容决定价值。

“当制作成本昂贵并且印刷设备掌握在极少数人手中时，唯一能印刷的书籍就是古腾堡圣经。”

接下来，我举个古老的例子。当制作成本昂贵并且印刷设备掌握在极少数人手中时，唯一能印刷的书籍就是古腾堡圣经。媒介界定了信息的内容，并且仅限于社会上最宏伟、最重要的信息，它通过巨额生产成本限制了信息的内容。

推特将生产成本降到零点，当它成为主流媒介，变得无处不在，供人们免费使用，你认为古腾堡将会如何看待推特呢？从印刷古腾堡圣经到推特上的一个符号，当某人说“比特币的价值将变成零”时，我可以用一种表情（捂住脸并摇头）来表达我的意见，仅仅三个字符，我就向全世界表达了我的观点。从客观上看，这条信息肯定是毫无价值的。当你认为如果生产成本为零并且信息看起来价值不大，那么整个媒介和信息必定是毫无用处、微不足道、没有任何价值的——这是人们在历史的转折点都会犯的错误。

当推特首次出现时，人们认为它只会用来做一些毫不起眼的事情。然而，一年前，我们看到 CNN 国际新闻网络报道埃及革命，报道的内容是开罗街头埃及革命者直播的推文，然而 CNN 的主播们什么都没有做，他们只是指着电脑屏幕说“快看，我们看到了另外一条推文，在那儿又有另一条推文等等。”他们已经成为电视节目的背景模特了。能看到像安德森·库珀这样的新闻节目主持人阅读屏幕上的推文，我甚感欣慰。

因为他们轻视它所以就错误的认为——如果生产成本为零，则信息的价值也将会为零。这是没有真正理解信息的媒介，他们觉得对媒介的控制是质量的保证，在质量不复存在后的很长一段时间，他们仍然不放弃对媒介的控制。这绝对是最糟糕，并且丝毫不加掩饰的精英主义。他们认为自己是信息的“守门人”，是信息质量的来源，他们觉得拥有昂贵的媒介就意味着他们的信息值得被人们倾听。

当信息与媒介分离并且当信息可以表达所有的内容时，虽然它包含一些最不起眼的内容，比如那些表情符号，但是它也会是最有趣的信息。

今天，在美国的学校里，学生们正在学习*《联邦党人文集》*，就是托马斯·杰斐逊、约翰·亚当斯、本杰明·富兰克林与许多其他创始人之间的书信。100 年内，人们将会阅读*《开罗革命党人推文》*。这个想法并不疯狂，这是人类文明发展之路，这种事情还会再次发生。

现在他们嘲笑推特无足轻重，因为他们不了解信息和媒介之间的区别。人们曾嘲笑电视是一种平凡的消遣，因为它掩盖了电影艺术的魅力。人们曾嘲笑电影是一种平凡的消遣，因为它使剧场艺术更廉价、更通俗化。人们曾嘲笑剧院是维多利亚时代一种低俗、廉价的消遣，因为它使罗马人和古希腊人伟大的戏剧变得平淡无奇。沿着这个思路走下去，你会最终遇见亚里士多德，他会说，哲学已死，因为现在孩子们都喜欢看戏剧表演，而不是阅读他们的哲学书籍了。每一代人都误以为媒介就是价值，并认为媒介的下一次迭代是无足轻重、低俗的，并且会贬低信息价值。

他们不明白的是当媒介被贬低时，随着新信息的发布媒介的价值会相应提高，而新的媒介又能帮助人们更广泛的表达信息内容。是的，最初表达的内容可能是毫无价值的，它可能会包含那些毫无意义的表情符号，但同时也会有开罗革命这样的实时推文。到他们明白这是怎么一回事时，这种新媒介已经是高质量的信息了。接着，他们可以继续贬低下一代新生媒

介是低俗、廉价的。

9.6 货币是脱离媒介的信息

货币是一种内容形式，我们帮助它从媒介中挣脱出来。媒介曾经是将货币按照交易规模和收款人分类的一系列相互连通的网络。我们有小额支付网络、大额支付网络、快速支付网络和慢速支付网络。我们还有企业之间的支付网络、政府之间的支付网络、消费者与企业之间的支付网络和消费者之间的支付网络。哦，等等，我们没有消费者之间的支付网络，也没有小额支付网络，因为传统媒介不允许这种表达方式。

“货币是一种内容形式，我们帮助它从媒介中挣脱出来。”

在世界上任何地方，我都不能寄 20 美分给你，因为媒介限制了信息，生产成本不允许这种交易形式。但是现在我们已经将信息和媒介分离了，我们把货币看成是一种内容形式。现在货币几乎以零生产成本来表现的交易形式——从小额支付到大额支付、从消费者向消费者支付、从政府向政府支付。

接下来会发生什么？守门人会告诉你，这个网络并不严谨。他们误以为支付网络成本就是他们服务的价值。他们认为，这种新的支付形式是低俗、廉价的，只能用来做些毫不起眼的事情，所有严谨的人都将继续坚守过去稳固、优质的支付网络。其实并不是这样，这只是膨胀的生产成本，这就是赤裸裸的精英主义。至今他们仍然不愿意放弃媒介，并且不明白现在信息可以瞬间以零成本的方式在任何媒介上发送。

这种新模式、新媒介首次会应用在哪里？现在我们可以发送非常小额的交易，我可以从推特中收到小费，这个示范清楚地向人们表明支付媒介之间的差异，我们可以做到一些以前做不到的事情。但对大多数人来说，这是毫无价值的。对于大多数人来说，我向他们展示基

本的信息表达方式只是强调了这是一种廉价、低俗的媒介。他们没有弄明白，这种媒介不仅仅可以用来做毫不起眼的事情，它还扩大了交易的表达范围。

“区块链可以涵盖交易全部的表达范围，从 10 美分的推文到 1000 亿美元的债务清算。”

有一天，某个国家将会在区块链上支付石油账单；有一天，你可能会在区块链上购得一家跨国公司；有一天，你可能会在区块链上以废金属的形式出售一艘航空母舰。区块链可以涵盖交易全部的表达范围，从 10 美分的推文到 1000 亿美元的债务清算。然而，我们还没有注意到这些。事实上，作为一种内容形式，交易可以通过 Skype 笑脸符号发送。我们已经解除了潜在交易媒介所有的制约因素，我们已经成为了“内容之王”。

9.7 技术大圆弧

当内容受限于排他性、精英主义和有限访问领域时，大师们会用它来创作自己的杰作：古腾堡圣经、第一张照片、人类登上月球（首次通过电视直播）、最伟大的电影等等。

紧接着媒介发生了变化，因为技术变得越来越普及了。人们开始将媒介用于更广泛的表现形式，但守门人仍然固守那些传统的观念，他们仍旧用他们的媒介去做那些宏伟的事情，他们还在制作那些精装的、覆有厚重皮革封面的书籍。然而随着媒介越来越广泛地被人们使用，书本的封面变成了软封面，照片也越来越普及。守门人仍在坚守着过去，但是现在他们已经不能装着若无其事了，所以他们只能哗众取宠。他们说“电影真是妙不可言呐！”“黑胶唱片的特定品质是 CD 永远无法赶上的。”“电视主播都很有权威，你不记得沃尔特·克朗凯特了吗？”“报纸是权威观点的来源，它值得上整个价。”这是哗众取宠。现在再也没有所谓的宏伟或者高品质了，他们只能执着于控制，并且假装控制代表着品质。

最终，在技术大圆弧中，技术发展到了最终阶段。在技术的最终阶段，只有我们的“祖

父母”一辈才仍然相信那些过时的媒介是“宏伟的”，那些超凡的大师作品现如今只能被一些老头、老太太所欣赏。皇室的第一笔支票被用来资助那些“伟大的冒险事业”，例如东印度公司开辟香料之路或东方的贸易之路。在那个时期，只有皇室有支票簿。今天，如果你走进一家超市，在你前面排队结账的奶奶做出祈求上帝保佑她的动作，然后打开钱包并拿出支票簿，后面排队的 15 个人绝对会大声抱怨，因为他们知道填写那笔交易将会耗费 15 分钟。当你在超市用支票购买豆子和烤面包时，皇室用支票资助东印度公司的昔日辉煌早已荡然无存。这是它最后的使用阶段。

现在唯一看福克斯新闻频道的人是我们祖父母一辈，因为现在我们都在互联网上看新闻了，曾经被认为是毫不起眼的东西现在是权威新闻和信息的重要来源。对此，你无法向旧技术的守门人解释清楚。现在我们阅读的是电子书籍，有人说“这与读纸质书感觉差不多。”对的！在背包里放 20 本书实在是太重了，并且我需要在四五周内读 20 本书，我无法随身携带那么多本书。有人认为读电子书没有一点儿读纸质书的感觉，这是在执着于过去。

当我们进入货币演变为内容形式的时代，传统支付系统的守门人仍然固执的依恋只有银行才能进行货币交易这种假象。他们可以控制、审查和限制资金交易，但这并不能决定货币的表达形式，我们已经把货币的表达形式扩大到了以往难以想象的范围。他们仍然执着于过去那种“宏大的”的观念：那些带有拱形天花板和铬合金金库的古老银行。你可以在周日参观，了解银行曾经的样子，你可以去世界各地的城市看看，那些古老银行的金库如今变成了酒吧，你可以在金库里面喝鸡尾酒，因为银行再也没有能力负担得起这些建筑了。除了宏伟之外，现在没有其他任何用途。但他们仍会试图说服你，通过他们的控制会让你远离邪恶、恐怖分子和洗钱的伤害。事实上，他们所做的一切都只是为了保护自己的利益。

现在，我们已经将信息与媒介分离了。现在，货币是一种内容形式。

谢谢。

第十章 构成信任的要素：释放创造力

区块链集会，柏林，德国，2016 年 3 月

视频链接：https://www.youtube.com/watch?v=uLpSM3HWU6U

今天，我要介绍一下货币的化学成分，尤其是比特币的化学成分。这是比特币中让人感到激动和有趣的一方面，这是我们中间某些人研究了比特币一到两年仍会忽略的一方面。比特币就像洋葱，你要把它拆开，才会发现里面其实有更多层。我是从五年前开始的，直到现在我仍在研究比特币，每天我都会发现更多令人惊奇的事情。

10.1 关于发送者、接收者和账户的错觉

当我第一次看到比特币，我感到很惊奇，因为它跟银行系统看起来如此之像。当我访问那些出名的比特币网站，比如 blockchain.info，我可以查询交易记录，点击某条交易，我可以看到发送方，接收方和账户地址，这跟银行系统非常类似。然后，我决定查看一下比特币的源代码看它是如何工作的。

作为一名计算机学家，我试着去理解比特币系统是如何做到此类事情的，但我在源代码里查询发送方、接收方和账户的时候，什么都没查到。因为比特币系统里面并不存在任何此类东西，这让我觉得非常奇怪。你本以为这是类似于银行系统，它看起来也的确如此，但比特币系统实际上根本不是这样。

你们中有多少人查看过比特币的源代码并且理解它的基础技术结构？很少一部分人。当你深入研究代码的时候，你会发现这里没有资产负债表，没有发送方，这里只有 UTXO（未花费的交易输出）和输入，但这些输入实际上并不是与发送方对应的，比特币交易输出同样

也不与接收方对应。突然间，你会意识到你看到的几乎就是比特币的原子本质。

10.2 比特币的原子结构

在化学领域，我们有铜、铁、氦这样的元素。化学给予你如此巨大的复杂性使你可以用不同化学元素结合成不同有趣的东西，就像人和烤面包机都是由不同化学元素构成。但是当你深入钻研化学，你会认识到铜不只是一样东西。铜是质子、中子和电子的一种构成模式。铜事实上并不存在，一个质子和另外一个质子完全相同，它并不在乎成为铜或者成为氦的一部分。并没有一种特殊的质子来构成铜。

化学只是一层，下面还有原子物理学。那层很简单，只有几个元素，这几个元素构成了我们所知的所有化学元素。自然界的 100 多种元素都有着独一无二的特性，有些是液体形式存在的，有些是金属，有些是气体。它们的行为各有不同，有些是呈酸性的，有些则不是。但这些都不是它们的基本构成，只是模式不同而已。

比特币也有这种基本的原子结构，或者说元素结构。比特币的元素是组成交易和脚本语言的基本部分。它的元素与传统银行毫无关系，它没有任何账户、资产负债表、付款人和收款人。相反，比特币的元素是在找寻根本的数学性质和加密图形特性——比如一个哈希值是否与另一个哈希值相等，一个椭圆曲线签名与另一个椭圆曲线签名相匹配，数据是否伪造等等。你在表面看到的——比特币交易——只是元素的结构而已。它是用一种特定方式把元素混搭起来的东西，看起来像一个银行。假如你是刚接触到比特币，有人告诉你，“嗯，这里面有账户，付款人和收款人，”你就会觉得，好的，这很好理解。

然后你会了解到比特币系统里面有一个钱包，但是钱包里面并没有币，它包含私钥，并且这些私钥可以被复制。或许你现在会想，我有点糊涂了，这不太符合我的经验。事情变得

复杂是因为比特币并不是你想的那样，它是一个平台，而并不是一个支付网络。它不是货币，同样也不是银行系统，它是一个保障特定可信任功能的平台，你可以在上面创建货币和支付网络，甚至其他的更多东西。

10.2.1 搭建乐高积木

当我小时候，最喜欢的玩具就是乐高。我喜欢它的原因不是因为它可以拼成玩具盒上面的样图，而是可以拼出许多其他的东西。如果盒子上面的图案是一个消防车，我就可以搭成一条龙，或者是混搭出又像河马又像长颈鹿的东西，或者是其它一些实际上并不存在的东西又或者我脑海里产生的一些奇怪的念头。这就是我喜欢它的原因，我可以用这些积木创造出任何我想要的东西。

从抽象的角度来看，乐高一团糟，因为我搭建的东西既不像消防车也不像宇宙飞船。如果有人给我一个消防车，一个塑料铸成的、边角光滑的、鲜艳的红色消防车，那么这将会是一个完美的玩具。但它永远只是一个消防车而已，我可能会玩上 20 分钟，然后就感到无聊。但是我自己用乐高积木搭建的玩具，既可以像河马与长颈鹿混搭的动物，又可以像西红柿或者宇宙飞船，乐高可以让我做到更多。

10.2.2 烹饪的积木

随着年龄的增长，我开始爱好烹饪，因为那是科学和艺术的完美结合。如果你从根本上了解这些原料是如何工作的——当它们结合在一起的时候，当你添加盐这样的催化剂的时候，当你加热的时候，它们会产生什么样的化学变化，那么你就可以做出美味的饭菜。只要你理解这些原料是如何工作的，你就可以操作并且创造出任何你想要的东西。

10.2.3 创造力的积木

比特币包含着最基本的元素，它不会给你一个最终的结果，它只会给你一套配料和配方。它给你一套乐高积木，盒子外面的照片看起来像是一个红色的消防车。当我们向世界展示它时，金融公司会这样说，“嗯，你这部车边缘太锋利了，并且它只是由愚蠢的积木搭成的。”

在比特币中，我们把这些成分组合在一起，搭建了一套银行支付系统。银行看着它，会说“嗯，这个汉堡做的不错，但在麦当劳我们 45 秒钟就可以完成一个，并且可以卖出十亿份。我们现在已经能够大规模生产了，为什么还另外需要多余的厨师、配料和配方来重新制作呢？”他们这么说其实并没有抓住要点。

重点并不在于制作数以亿计的伪劣品拷贝，注塑成型的消防车 5 秒种就会使我厌烦。关键在于释放创造力，我需要工具和原料来创造一些不寻常的东西。

我不能像麦当劳那样又快又便宜的做出汉堡，我自己制作的消防车也不像批量生产的玩具复制品那么光滑漂亮，但是我可以用番茄酱制作西班牙肉丸汤，我可以拼搭出既像河马又像长颈鹿的玩具。你不可能用预制品玩具做成这件事，你也不可能在麦当劳的厨房做出别的东西。我释放了我的创造性。

10.2.4 比特币的积木

人们已经认识到了比特币是一组原料，目前我们已经有了一个配方，但是你可以制作新的配方。

我们通过结合比特币的原子交易，输入与输出总和以及数字签名技术来建设新的众筹项目。把这些元素组合起来，我们可以创建一个由多人提供资金的交易，但只有满足资金阈值的情况下，这笔交易才会生效。这与我曾经在比特币网络上做的小额美元支付程序是同样的原理，但是你可以用不同的方式重组它们，这样你就有了一个新的众筹平台。

我们正在通过结合双重签名，多重签名和交易时间戳功能来建设一个新的支付通道，这使得我们可以按秒对视频流进行收费，这是一个全新的配方。

通过添加新的成分，我们可以在支付通道上建设更多的东西。例如哈希时间锁定的智能合约，它可以让我们进行多通道连接。然后我们有了闪电网络，这是一个全新的配方，以往从来没有人见过。

银行会这样说“你的消防车边角太锋利了，你做的汉堡太贵了并且耗费的时间太长了。”他们真正的意思是“你的交易费用太高了，交易速度太慢了并且无法做到大规模交易。”他们并没有领会问题的关键所在。关键在于，我们并不是想把 45 秒钟就可以制成的汉堡卖出上亿份，我们是想释放整代人的创造性。我们正在创建一个新的系统，上面会有上千种可信任的应用。

10.3 焦点小组（主持人通过与一个小组的被调查者交谈研究市场）经济

当你有了原料，当你有了那些最基本的成分，你想做一个什么样的配方完全取决于你。那些人制作消防车玩具时，他们需要建造一整座工厂，并且只能生产这种玩具。我可以确定他们会这么说，“听着，我们的统计数据表明，95%的儿童只想要注塑成型的玩具消防车，我们已经通过焦点小组和市场调查团队证实了这一点。我们已经生产了百万个这样的产品，每个成本只有 3 美分。虽然它们含有少量含铅油漆和有毒、致癌的碳氢化合物，但这全都不成问题。我们可以非常有利可图。”

当你建造一个麦当劳那样的厨房，每 45 秒就做出一个汉堡，但你做不了西班牙肉丸汤或是其他的东西。你可以精简到只做一件事，只要有利润在里面就行。但这是一种可怕的经

济模式，一种可怕的金融系统，一种可怕的支付网络。

10.4 银行的特权与监管

我们需要面对这样一个事实，世界上有 40 亿人口享受不到银行服务的真正原因是——交易的双方都需要进行身份认证。因为我们建立了一个集权主义的监视系统，监视来自地球的每个角落的每一笔金融交易。我们自己说服了自己，我们的资产阶级安全感得到了保证，不是通过解决贫困，也不是通过减少贫困，而是通过轰炸其他国家，或者是当人们去买汉堡的时候，监视每一个人。

我们服从现在这个精简的机制，它是这样一个系统，只为少数的精英人口提供金融服务的特权，并且伴随着极权主义的监控，各个国家的边境都设置障碍不允许自由国际贸易。它是这样一个金融系统，政府可以施加压力阻止你与维基解密交易，但是你却可以捐款给 3K 党——这可不是玩笑，这是正在发生的事实。

他们创建了一个只能做一件事的系统：奴役我们。这个系统只能做一件事：让贫富分化更加剧。该系统以最有效的方式提供利润，从而消除了自由。但这个系统已经完了，它无法再继续大规模扩张。

相比之下，我们用比特币建立的这个小的、疯狂而混杂的系统，虽然有出错的方面，低效缓慢的方面并且不成规模，但它不像国际银行系统那样危险而复杂。它提供自由，并且允许我们释放创造力。

谢谢。

第十一章 扩容比特币

比特币加密组织集会，布拉格，捷克， 2016 年 3 月

视频链接：https://www.youtube.com/watch?v=bFOFqNKKns0

11.1 关于扩容的故事

今天，我想要谈一下扩容的问题。你们中的大部分人已经注意到了关于比特币有一个非常有趣的讨论，那就是如何扩容。这正是我接下来要讨论的话题，不是从技术的角度，而是从更广泛的角度来理解如何实现扩容。

11.1.1 新闻组（基于网络的计算机组合，完全交互式的超级电子论坛）将会摧毁互联网

1989 年，互联网还处于拨号上网的时期，不仅仅是用户与互联网之间的连接，在大多数情况下，互联网上的主干网都是拨号上网。那时大学之间，研究所之间有一些永久性的高速连接——256k, 512k，但主要仍是拨号上网。那时电子邮件还没有真正开始广泛应用，但网上有一个特殊的地方叫 Usenet(新闻组），它是这样一个系统，在那里你可以以文本的方式发布信息，其他人可以看到并做出回答。

这不是即时信息传递，这是缓慢的信息，为了使新闻组正常工作，所有的信息都是通过拨号系统传递，并且通过一个节点到节点的，称之为储存和转发的系统进行传播。你可以发布信息，但这需要花费 24 至 48 小时才能推送给每一个人。然后，如果他们做出回应，你需要等待 24 至 48 小时才能看到。这个情形与影片《火星救援》里面，地球与火星上的马克达蒙联络非常相似。

在那时，互联网工程师之间有一个比较大的争论，由于新闻组的模式变得非常受欢迎，并且规模变得越来越大，千兆字节的文本信息需要被传播。最初，在拨号连接上把新闻组里所有的信息和数据上传需要 30 分钟，很快，这个系统变得越来越受欢迎，更多的信息意味着更大量的数据和更多的上传时间，这就需要 1 小时，2 小时，3 小时。然后，专家们预测了结局，他们说，如果你在我们今天所在位置画一个点，在 6 个月以前的位置画另一个点，并且划条线把它们连起来，你会发现不久后传播一天的信息量需要 26 个小时，这里就会产生一个麻烦，因为我们一天只有 24 小时。

所以，接下来会发生什么？互联网就会崩溃！很明显，它无法扩容，这行不通。

11.1.2 替代组将会摧毁互联网

在那时，新闻组上分为两部分，有常规部分，这里包含了非常严谨的学术讨论小组。另外还有一小部分，称为 Alt，替代组。作为用户，你可以选择使用 Alt 但这并不是强制性的。但是真正有趣的东西都在替代组里面，这里有一些早期的令人惊叹的民间团体，比如 alt.folklore.computers, alt.security, 当然，还有和互联网上其他那些推动规模的应用一样——alt.sex。

这些替代组是那次大争论的焦点。我们应该继续支持它吗？在那时我们看到了世界上首封垃圾邮件。我记得我收到的第一封垃圾邮件，它是由几个律师发给每一个新闻组用户的。人们不应该这么做，这并不酷。有几千个用户都告诉他们这并不酷，这是互联网史上第一次集体抵制。

我们应该支持替代组吗？如果我们支持，互联网肯定会崩溃，并且它的容量将再也无法进一步扩大。如果替代组变得更受欢迎，人们将会在上面讨论更多东西，如果人们讨论的更

多，我们将没有足够的容量来处理这些数据。这次大争论持续了两年多的时间，有几个大胆的服务器提供商使用 5 兆的超大硬盘来提供支持。再一次的，主要矛盾又回到了“我们现在所在的这个点永远达不到将来的那个点”，我们遇到了瓶颈。

因此，互联网无法扩容，这是它最开始遇到的一个基本问题，互联网上有些系统甚至几十年来都无法稳定扩容。很明显，许多人会写出一篇博士论文论证它为什么无法扩容，然而最终获取成功的确实它们。

最后，我们解决了新闻组的问题。数字连接的升级，越来越多的系统使用专线连接。拨号上网被专线取代，人们开始投资于基础设施建设，我们可以很容易的支撑起新闻组。然后，人们开始使用电子邮件。然而这时，扩容性的限制又重新回来了。

11.1.3 电子邮件及其附件将会摧毁互联网

随着电子邮件的流行，它开始取代和超越新闻组。那时由于人们希望直接联系，我们甚至遇到了更大的麻烦。这时，一条信息不需要花费 24 小时，通过互联网传递 2 个小时就可以，这意味着人们开始拥有实时通讯——好吧，几乎实时，电子邮件的用量开始呈爆炸式增长，再一次的，互联网遇到了扩容问题，因为如果你看一下电子邮件今天的用量，然后对比一下 6 个月前的用量，划一条线连接这两个点然后延长，你会发现它的容量无法再继续扩大，互联网将会崩溃。人们写了更多的博士论文来论述在电子邮件超负荷的状态下互联网将会如何崩溃，并且无法扩张。

逐渐的，我们开始学会如何去进行优化，并且解决了电子邮件的问题，当我说“我们”，我那时只是在观望，因为我那时只有 16 岁，完全不知道当时发生了什么事，但是我们作为人类整体解决了这个问题。接下来，当互联网成功解决电子邮件的容量问题之后，有些聪明

的“混蛋”接着发明了 MIME,多媒体互联网信息，这意味着你可以添加附件到邮件里面。通常，附件的大小都有文本信息的 10 倍那么大，因为人们开始发送格式更大的东西，比如图画、照片，再一次的，有关色情的东西。

因此，我们可以承受电子邮件的规模却承受不了其中附件的规模，所有人都开始骚乱起来，“我们将永远无法满足电子邮件附件的扩张，互联网肯定会崩溃。”随后我们解决了这个问题，某个来自英国的家伙，Tim Berners Lee 爵士，发明了网页，此后你就可以把照片上传到网站上面。

11.1.4 网站将会摧毁互联网

1992 年我下载并运行了第一个网页浏览器，NCSA Mosaic，在我大学的图书馆里。我们聚集了三、四个朋友，用了几个小时才把 NCSA Mosaic 浏览器下载下来并且完成安装。然后，我们启动了它并且开始浏览网页，我敢说一句大部分人都不敢说的话：1992 年，我用一个下午的时间就浏览完了互联网上所有的网页！因为当时总共只有两个网站。当时我在想，“噢，天呐，这个东西（网站）将来会发展的非常巨大，但是互联网的容量永远也满足不了它们，想象一下你可以利用网站制造出多少色情内容。”当然，色情是一个可以推动规模化的应用，我们都知道这一点，它从一开始就推动了互联网的发展，但是在得体的场合我们不应该讨论这一点。

互联网不能为这些网站扩大容量，人们说“我们永远都处理不了这些图像和超文本文档，它永远都行不通。”更多的博士论文被发表出来，更多的讨论都在进行，互联网仍然不能扩容。但到现在为止，它不能扩容已经超过 10 年了。

11.1.5 VOIP（由 IP 传送语音的技术服务）将会摧

毁互联网

然后，有人发明了通过 IP 传输语音的技术，另一些人决定，我们为什么不用互联网替代整个电话系统？这真是一个疯狂的想法。电话公司发起大规模的运动来告知我们，为什么分组交换式网络永远支撑不了语音。他们说改善声音品质永远都是靠那些国家垄断性的电信公司所掌握的多层交换式网络，因为互联网的规模不可能支撑的起全世界的电话通讯。

就是那些电话公司，现在把他们的电话通讯全部部署到了互联网上。最开始，他们并不想要互联网使用他们的电话网络，然后，他们开始慢慢接受这个新生的事物，最后，他们的电话网络全部都建设在了互联网之上。

11.1.6 宠物视频将会摧毁互联网

接着，我们开始发送视频。再一次的，互联网遇到了扩容问题，因为 YouTube 将会堵塞整个互联网。很明显我们需要视频内容质量控制，因为我们不可能允许每一个傻瓜都把他们宠物猫视频发布到网上。他们说，“这里已经有几千种关于猫咪的视频了，如果你划一条线把昨天猫咪视频的数量和今天猫咪视频的数量连接起来，然后进行推算，十年之后，互联网上将会有一百万种猫咪视频！”事情完全就是这么发展的。

但是我们扩容了网络，现在，我们拥有了 3D 和 4K 视频。

11.1.7 Netflix（美国在线影片租赁商）将会摧毁互联网

当 Netflix 出现的时候，我们看到了同样的事情。在 1992 年，当我访问互联网上首个网站时，当时的想法是，哇，电视要完了，因为总有一天我们可以实时传输电影。然而，如果

你在 1992 年对某个值得尊重的网络研究员说这样的话，他会说你是傻瓜。原因很明显，假如我们在 1992 年就有了 Netflix，单用户的单个视频流就会堵塞整个网络。然而今天我们却实现了。

顺带一提，互联网在那时无法为 Netflix 和其他视频直播公司进行扩容。但不久之后，我们就开始实现全息 3D, 4K 和虚拟现实。可以预见，人们仍将会撰写博士论文来论述这些大规模的应用将会给互联网造成崩溃。

11.2 扩容是一个动态目标

扩容是一个动态目标，它定义了现有的能力边界。随着扩容的发展，能力也会相应的增强。原因很简单：因为扩容不是一个随时可以实现的固定目标，而是用来定义现在可以用网络做些什么。当你能力提高时，这个定义随之发生变化。因为完成某次扩容之后，就会有人说：“等一下！你的意思是我现在可以做某件事了，它的需求量是以前的 10 倍，那我们开始吧。”然后，扩容又会失败。

比特币也缺乏扩容能力，如果我们足够“幸运”，比特币会像互联网一样，在未来的 25 年之内都无法扩容。那时一些公司说互联网永远不可能被用来发送电子邮件、进行高质量语音通话和传输高质量的视频，现在这些公司也在进行同样的争论：比特币永远不可能被用来进行零售支付，不能满足 Visa 那种规模系统的扩容以及进行全球扩容，如果真的被采用，它会面临崩溃。现在有许多人正在撰写关于比特币将会如何失败、比特币已经失败、比特币正在迈向死亡、比特币已死和比特币将会再次死亡的博士论文。

“比特币也缺乏扩容能力，如果我们足够幸运，比特币会像互联网一样，在未来的 25 年之内都无法扩

容。”

有一个名为 bitcoinobituaries.com 的不错网站，你可以在这个网站上你可以看到 2009 年以来关于比特币死亡的所有声明——就像定时闹钟一样，每隔三到六个月都会有主流报纸、科学家说“就是这样，比特币已死!”事实上，这已经成为出人意料的吸引比特币新用户的机会，因为你所要做的就是等待人们听说关于比特币死亡、比特币首席执行官被逮捕或者比特币被普京关闭的消息，然后四个月后，另一些人说“你知道吗？这里有一些关于比特币的有趣新应用。”这时人们就会问“比特币仍然活着吗？”

“比特币仍然活着”是这个社区的营销口号，如果我们一直宣称“比特币仍然活着”，人们会感到惊讶、困惑，因为这不符合他们的预期，他们觉得比特币不可能一直活着，因为在大公司供职并且具有重要头衔的人告诉他们比特币将会死亡。但是，比特币仍然活着，虽然我们未能成功扩容。

11.2.1 费用优化和扩容

当我们在进行压力测试或者容量测试期间，当网络上有太多交易时，会发生些什么？一些用户感觉非常槽糕，他们像往常一样以 0.0001 比特币的交易费进行交易，并且需要三天的时间才能确认交易。那段时间他们吓坏了，特别是新用户。因为新用户会认为这笔钱已经不在他们的账户了，并且正在发送到转入账户，因此交易处于两者的中间状态。实际上这笔钱仍然在他们的账户中，只是他们的钱包显示交易还未被确认。这笔钱要么在转出账户中，要么就在转入账户中，从头到尾只有一笔交易，没有中间状态，因为比特币中没有发送，只有结算，所以交易不可能处于中间状态。

有些钱包非常智能，它们通过增加交易费用，有时甚至增加 100%来解决交易确认问题。

这意味着向世界任何地方发送一笔需要被验证和公开的交易，不再是收取 4 美分，而是 8 美分！显然，这一事实连同等待三天都无法确认交易的情况都表明：现在比特币肯定已死。有些开发人员说“哦，我放弃。比特币已死!”报纸上写着“比特币已死，交易无法完成了。”

但比特币交易正在进行，我使用了智能钱包，它可以计算交易费用。在这次交易拥堵之后会发生什么呢？我们得到了更好的钱包。

这实际上是应对压力的动态系统本质，当我们获得更好的钱包后，这些钱包会更准确地计算费用。如果有些不那么智能的钱包计算出 0.0001 比特币的交易费用，那么这很容易堵塞网络，但是在那时，你只需要支付 0.00011 比特币的交易费用，你就会在交易中会脱颖而出。如果别人支付了 0.00012 比特币的交易费，你将需要支付 0.00013 比特币。现在我们正在竞赛，并且在你意识到这件事之前，你会花费 0.0005 比特币。噢，天呐，如果你是合法用户，这算不了什么。假如你试图堵塞网络，你的交易成本将会变得非常昂贵。

11.3 垃圾交易、合法交易、非法交易

这就带来一个很有趣的问题：什么是垃圾交易？什么是合法交易？什么是非法交易？有两种方法可以解决这个问题。第一种是专制的、自上而下的方式，明确规定什么是可以被允许的，我们可以通过过滤交易来阻止部分交易进入网络，但这会打破比特币网络的中立性。比特币不关心发送人是谁，接收人是谁，也不关心交易价值有多少。它关心的是，你是否支付了交易费？如果已经支付，那么你的交易会被定义为合法。如果我们从一开始就决定什么是垃圾交易，那么我们就是在选择比特币的未来，并且将其限制在我们可以想象的应用中。天才创建出一个我们无法想象的应用——虽然上面有些所谓的垃圾交易——并且目前网络无法支持这些交易，但是这是因为我们做出了一个自上而下的决定：认定某些交易是非法的。

另一种方法是，我们利用市场来解决这个问题：通过市场来设定最低的交易费用以满足矿工快速出块的需求，和比特币用户对新应用的需求。如果你支付了交易费，那么你的交易就是合法的。这里没有所谓的垃圾交易，没有非法交易，只有被矿工确认的交易和交易费不足无法被确认的交易。

11.4 数十年来扩容未能如愿

这就是比特币未来的发展趋势，扩容问题无法解决，也许在未来的几十年里，我们每年都要讨论扩容问题。每一年下一代应用都无法扩容，而上一代应用都能成功扩容。只要我们做得更好，人们又会发明新的应用，而新应用又将导致无法扩容。

“每一年下一代应用都无法扩容，而上一代应用都能成功扩容。”

25 年来，互联网从未成功扩容。让比特币也无法扩容吧，比特币仍未死亡。

谢谢。