一本书读懂区块链

作者：吴建刚

第一章 创世区块链

一、突如其来

（一）天上掉下来的比特币

谈论区块链不能不好好研究比特币，不仅因为世界上第一个区块链——创世区块链源于比特币，还因为区块链的基础理论和核心技术也源于比特币。其实，比特币与区块链最早的历史是重叠的。

比特币在 2009 年出现后的两三年也是默默无闻的，到 2013 年比特币积攒了一些名气后，人们才发现原来其背后的技术大有用途，区块链技术才逐渐独立发展起来，并有了后来“币圈”与“链圈”的区分。

区块链独立发展起来，但比特币技术仍然是区块链技术的出发点和标准模版，而类似比特币的加密货币的发展则成为区块链在货币领域的一种应用，并且区块链在这一领域的创新仍然是区块链技术创新最火热的领域。所以，在专门讨论区块链之前，我们将花比较大的篇幅讨论比特币，而这里先短暂回顾一下比特币的发家史，或者说区块链的初创史。

这个时代新事物层出不穷，大家都有些免疫了，要让人惊呼“哇”，是越发困难了。但比特币的确令人耳目一新。

有所耳闻的人不禁心生疑问：比特币到底是什么东东呀？！虚拟货币？与我有关吗？但是大家都太忙了，比特币背后的技术也太难了，背后的经济学原理太反直觉了。这个时代奇葩的事也太多了，大家初期选择性忽略了。

但是比特币从各种新闻里冒出来，标题还挺夺人眼球的，内容也足够惊悚，我们心里有各种疑问再次如万马奔腾而过：比特币也是用矿机挖的吗？ 2040 年就挖完了？最大的矿机就在中国深山？一枚比特币在一年之内从十几元涨到了七八千？德国竟然承认比特币合法？美国 FBI 查获专门合用比特币从事毒品等非法交易的网站？最大的比特币交易所门头沟在 85 万个比特币被盗一空后突然宣布倒闭？

另外，我们发现身边似乎越来越多人开始讨论比特币了，并且有的人还颇为狂热。类似比特币的山寨币也纷纷进入视野，甚至身边有人在用传销的方式兜售这些货币了。甚至有人认为比特币会升值到一万美金一枚。

从陌生到熟悉，从怪物到正常，我们有一种再不弄清楚就有 out 的感觉了。可是，想归想，要真搞清楚可不太容易呢。可是好多人，就算在网上搜过一些资料，听身边声称懂行的人讲过，可过了较长一段时间了，还是不甚了了。

是的，比特币就这么忽然地闯入我们的生活，神秘又难解。它给人一种错觉：这玩意儿难道是天上掉下来的？

某种程度上说，的确如此。

（二）中本聪了无响应的首场秀

2008 年 10 月 31 日纽约时间下午二时 10 分，一个自称中本聪的新人（或集体或公司）在密码邮件组贴了篇论文，即比特币白皮书：“Bitcoin: A Peer-to-Peer Electronic Cash System”（比特币：一种点对点的电子货币系统）。这篇仅有 9 页的文章用清楚但干巴巴的文字，配上插图、公式、代码和注脚，解释了一个数字“货币”系统，并声称据此可以实现了一种全新的能够避免货币重用、无需第三方信任中介介入的货币转移系统。

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust,

图 1.1 比特币白皮书

中本聪选择发布自己研究成果的加密邮件组其实大有来头，这是赛博自由主义运动的一个分支——密码朋克运动的最早活动场所。

但是，在大牛林立的加密邮件组上，当一个突然出现尚未建立声誉的新人宣称自己解决了一个困扰专家多年大家基本放弃的老问题时，大家自然提不起兴趣，只是觉得这是多次失败的电子货币的又一次注定失败的尝试罢了，论文也没有引起多大响应。

但是邮件组里的天才们没有想到，他们正见证了一场伟大的区块链革命的诞生，而他们万万没想到他们错过了一次轻而易举的发财机会。

所谓“山雨欲来风满楼”，比特币终究不是突然冒出来的。要理解比特币出现的意义及中

本聪当时解决的问题，我们需要回顾一下比特币的“前世”——密码朋克运动及密码朋克们在“加密-无政府主义”理想号召下在数码货币方面的努力。

（三）密码朋克运动

1、密码朋克的成立

密码朋克运动肇始于 1992 年，可以说是互联网诞生伊始就随之诞生了。它随着在这一年蒂姆·梅[1]、埃里克.休斯与约翰·吉尔摩开创的密码朋克的邮件列表而诞生，而这正是 16 年后中本聪发表比特币白皮书的邮件列表。

事情是这样的。在 1991 年的下半年，位于互联网创新的核心地区的几位密码专家蒂姆.梅、埃里克.休斯和约翰.吉尔摩创建了一个小团体，他们每个月都在吉尔摩的位于加州湾区的公司见面讨论互联网隐私保护的问题，而“密码朋克”一词在最早的几次聚会就被创造出来了。密码朋克（cypherpunks）来源于加密（cipher）和赛博朋克（cyberpunk）两个词。

第二年休斯就开发出了一个叫做“密码朋克邮件名单”的加密电子邮件系统，简称“密码朋克”。 到 1994 年，该邮件组已经成功吸引了约 700 个定阅者，形成了一个非常私密的圈子。

2、密码朋克的理念

为了阐明该运动的理念，蒂姆.梅在 1992 年发表的重要声明《加密无政府主义者宣言》。宣言提出：

“计算机技术，接近于提供这样一种能力，即，为个人或团体之间完全匿名地进行沟通与互动。两个人之间可以交换信息，开展业务，不需要知道彼此真实名字或其他合法身份即可协商电子合同。这样通过网络的互动将不可追踪，……几乎完美地保证了不可篡改。信誉将变得无比重要，在交易中更甚于今日的信用等级。这些发展将彻底改变政府监管的性质，征税能力与控制经济活动的能力，保证信息机密性，甚至将革新信任与声誉的意义。”

图 1.2 蒂姆.梅

埃里克.休斯在 1993 年《密码朋克宣言》中提出：

“密码朋克致力于建立匿名系统……电子时代，隐私是开放的社会不可或缺的……我们

[1] Timothy C. May 译作蒂莫希.梅，但更为人所知的是他使用的另一个名字 Tim May，即蒂姆.梅，2003 年退休前是英特尔的电子工程师和资深科学家，也是美国科技和政治方面的作家。他在 IBM 因为“阿尔法粒子问题”的研究广受赞誉。从上世纪 90 年代到 2003 年写了大量的加密和隐私保护的文章，是密码朋克运动的早期创始人。

不能期望政府，企业或其他大型的，匿名组织来保障我们的隐私……如果期望拥有隐私，那么我们必须亲自捍卫之。我们使用密码学、匿名邮件转发系统、数字签名，以及电子货币来保障我们的隐私”。

蒂姆.梅结合此前的宣言，在 1994 年写下《密码朋克常见问题解答（FAQ）》，成为密码朋克运动的指南。该指南提出密码朋克的“宏图”：

“强大的加密技术已经到来。它正被广泛使用。这意味着世界的运作方式会发生许多变化：为两个素未谋面且永远不会遇见的人提供了私人渠道。它既完全匿名，也不会消逝；通讯内容无法追踪但交流又是可行的。

由于买卖双方相互不知道对方身份，且能随时退出，所以交易只能是出于自愿。这对由政府或其他集团对当时人使用的武力威胁的传统方式，产生了极其深远的影响。需指出一点，这种威胁必将会失败。

加密技术会产生什么效应我们尚不得而知，但我认为会是一种被称为‘加密-无政府状态’的无政府资本主义市场体系（只有自愿交流，无第三方介入）。”

这一“加密-无政府状态”描述的互联网乌托邦的愿景很有影响力。这一指南启发下，1998 年，戴伟发表了《b-money》白皮书，提出一种能加强匿名用户之间契约关系的途径。在其引言中，他描述了密码朋克运动的内涵：

“我被蒂姆·梅所描述的加密-无政府状态吸引。加密-无政府状态不像其他‘无政府’传统社区，在那里政府不是暂时而应当是被永久禁止且不被需要的。在这个社区里，暴力威胁是软弱无力的，因为暴力不可能存在。为什么呢？因为没人能知道参与者的真实姓名和物理位置。”

同样在这一指南启发下，尼尔.斯蒂文森在 1999 年写题为《密码宝典（Cryptonomicon）》的密码朋克发展史上的经典小说。小说主角的活动背景设定于 1990 年代，小说主人公们使用密码学、电信技术与电脑科技构建一个地下数据避难所，他们致力于这样一个使命，使用电子货币与数字化类黄金货币体系来构建匿名互联网银行。

3、从加密技术、赛博自由到密码朋克

1992 年出现的密码朋克运动出现得可谓相当及时。互联网的原型在 1991 年才刚进入商用，而菲利普.齐默曼在 1992 年才发布了用于邮件加密的 PGP 加密系统。

回顾加密技术的发展，我们发现在 20 世纪 70 年代以前加密技术仍然仅限于军事和情报领域。想到二战时图灵参与的解密德军情报的重大成功以及接下来“冷战”的激烈对抗，政府对加密技术如此敏感也算情理之中。

然而，在 1976 年，随着两个出版物的出版，这项技术进入到公众的视野：一是美国国家标准局（NBS）公布了至今仍广泛使用的《数据加密术标准》；另一个则是惠特菲尔德·迪菲和马丁·赫尔曼出版的《新密码技术指南》。后者是第一部关于密码技术的公共出版物。

随后，人们开始公开讨论加密技术，并反思其在政治和社会方面的后果。人们发现密码技术是一把双刃剑：既可以用来保护个人的隐私、政府与企业的秘密，也可以被罪犯用来隐

藏他们的方案或者利益。那么，加密技术到底应该被自由使用还是严格禁止呢？这个问题从加密技术诞生的第一天起，就一直被人们争论不休。

随着互联网的出现，加密技术与赛博自由的讨论相互关联起来。从上世纪 80 年代，万维网发明者蒂姆·伯纳斯-李爵士、赛博自由主义政治活动家约翰.巴娄，以及华盛顿大学经济学教授尼克.萨博等，他们的研究和哲学体系对密码朋克运动有着极大的贡献，可以说他们间接成就了密码朋克运动。

到 90 年代初，当互联网首次进入商用时，关于加密技术的讨论很快蔓延到对于互联网上收发电子邮件的隐私保护的讨论了。而在当时，美国政府对于加密技术还是偏保守的。齐默曼就因为在 1992 年开发并开源了自己 PGP 软件受到美国政府为期三年的调查，原因是他违反了美国政府关于加密软件出口的规定。因为在当时，美国国务院有规定，凡与密码技术有关的出版物、磁盘，如果要出口，就必需获得许可。

对于加密技术、赛博自由的讨论和思索逐渐酝酿了“密码朋克”运动。但是密码朋克运动能够发展起来还与美国宪法文化有关。

1789 年，美国国会通过了宪法前 10 条修正案的第一条，即著名的美国宪法第一修正案。修正案规定，国会不得制定关于下列事项的法律：确立国教或禁止信教自由；剥夺言论自由或出版自由；或剥夺人民和平集会和向政府请愿申冤的权利。

这项修正案对美国影响相当巨大，它使美国媒体享有极大的自由并形成极大的政治影响力，甚至被人称为三权分立之外的“第四权”。这一修正安也几乎成为美国媒体或个人言论自由的护身符，不可动摇。以至于美国人把它颂扬为“美国生活方式”的主要内容。密码朋克就常常运用该修正案保护自己才得以将此运动推向前进。

4、密码朋克的活动

密码朋克的邮件组最初仅是几百个密码专家和爱好者，但其中藏龙卧虎，有著名邮件加密软件 PGP 的开发者菲利普·齐默尔曼、太阳微系统公司的明星员工约翰·吉尔摩、美国贝尔实验室研究员兼哥伦比亚大学计算机科学教授斯蒂文·贝洛文、BT 下载的作者布拉姆·科恩、英特尔公司前首席科学家蒂姆·梅，以及后来很火的维基解密创始人阿桑奇等等。

邮件列表里的密码专家吉姆.贝尔、大卫.乔姆、菲利普.齐默尔曼、亚当.贝克、哈尔.芬尼、阿桑奇、戴伟（音译，一个神秘的中国人）等因由他们为保护信息时代人们的隐私权做出了重要贡献现已广为人知。

“密码朋克”的成员曾多次运用美国宪法第一修正案，与美国政府机构对簿公堂。1994 年，“密码朋克”成员菲尔·卡恩（贝尔实验室研究员）指控美国国务院对密码技术的出口管制。当时，美国国务院规定，有关密码技术的出版物、磁盘如果要出口，必需获得许可。1995 年加利福尼亚州大学伯克利分校学生丹尼尔·伯恩斯坦恩在“密码朋克”的支持下，起诉美国国务院，理由是国务院对有关加密技术源码出版物的出口管制违宪。他赢了这场官司，对出版物出口管制的规定也因此作废。因此在 1992 年对齐默曼的指控也在 1996 年取消了。或许也是由于第一修正案的影响，美国政府没有对阿桑奇采取强硬措施。

阿桑奇于 1995 年加入“密码朋克”，2002 年离开。他曾在组件组提出要建立“维基解密”，并曾指出，美国一直在提倡和标榜“新闻自由”，“维基解密”也属于新闻自由的范畴。他享有自由去做自己认为正确的事情。阿桑奇在写于 2001 年 10 月 23 日的一封邮件中说：

“谁重塑战后美国的自由？人权活动家推动强大的游说集团，而游说集团又推动国会中虚伪的立法者，结果是，自由的本质变了味。或许，把这个链条缩短是个好主意。或许，让每个人都自由行事，率性而为，这个办法至少在荷兰很管用。”

密码朋克的活动在 1997 年前后达到顶峰，人数达到近两千人，而约翰·吉尔摩的一个邮箱显示：从 1996 年 12 月 1 日开始到 1999 年 3 月 1 日，这个“名单”平均每天发送 30 条信息。有关估计认为邮件组最高峰时，平均每天有能达到上千条。

这个圈子讨论的话题包括数学、加密技术、计算机技术、政治和哲学，也包括私人问题，有时候还会互相扔一些垃圾邮件，整垮对方的邮箱。阿桑奇在这里曾发过上百封邮件，按约翰·扬的话说，这些邮件充分体现了阿桑奇的能力、智慧、口才以及对政府的蔑视。

（三）无政府货币

1、数字现金系统

密码朋克运动一开始就想到了除了要保护网络通讯自由和隐私外，还需要保护电子交易的隐私，但当时的维萨、万事达等电子交易支付系统，包括后来流行的贝宝之类的支付系统都是有中介的，而且要求身份验证，这就使中介掌握了大量个人隐私和交易信息。所以，密码朋克的理想首先是要构建去中介的加密支付系统，更大的理想则是为无政府的社会提供可供交易的电子货币。

密码朋克的数字化货币体系最初的雏形是最引人注目的电子货币先驱大卫.乔姆 1983 发明的电子现金系统（Digicash）。这一系统实际上并没有取消中介，但它是一种私人发行的货币，同时它做到了使中介不掌握货币使用者的隐私的情况下可以进行匿名转账支付。

乔姆的做法是，让货币发行人向人们发放数字签名的电子纸条，上面写着“拿到此条的人可以来我这里领取 1 美元”。假设人们信任发放纸条的人不会食言，而纸条也不可伪造，那这些纸条就可以像银行汇票一样流动起来。事实上，银行汇票最初就是这样由银行承诺支付的情况下发行的。

但乔姆的电子纸条遇到恼人的“双重花费”（double spending，简称双花）的问题，即收到表示一定金额的电子纸条时，这些电子纸条不过是一些可以复制的信息，支付人可以重复将其传输给其他人。由于其他人很难识别这些信息中哪些是初始信息，哪些是复制品，重复传输这些电子纸条就可以达到重复支付的目的。

乔姆的解决方法是由发行人记账并验证。具体做法是：发行人除了在电子纸条上登记用户的数字签名外，还在每张电子纸条上印一串独特的序列号，并将这些信息记录在账簿上。当有人把电子纸条发给你时，你可以打电话给发行人，告诉发行人这些电子纸条的序列号，并且询问这些电子纸条是否已经使用过了。发行人查阅账簿发现没有使用过，就注销掉这些电子纸条，并且给你带有你的数字签名的相同数量的印有新序列号的电子纸条，并记录在账

簿上。这就解决了双重花费的问题。另外，这里的数字签名并非真名，只要可以区分不同的用户的一串不会重复的随机产生的数字就可以了，所以乔姆的方法也解决了隐私保护的问题。

看来这个方法是可行的，虽然在通过打电话、记账、核对等实施起来会非常烦琐，但在互联网上可以很容易实现，只需要设置一台服务器，用它来自动完成数字签名和序列号记录即可。

乔姆提供的创造性的解决方案是第一个真正意义上可以保护隐私的电子货币方案，但它需要一个大家信任的中心机构来管理运行的服务器，而这个服务器需要参与每笔交易，如果服务器停止工作，交易就不得不暂停，另外交易记录也有被篡改的可能性。

虽然数年之后的 1988 年，乔姆与另外两位专家阿莫斯.菲亚特和摩尼.纳欧尔合作提出线下电子货币的概念，他们研究出复杂的机制将个人身份通过加密方式嵌入到电子货币中，只有所有者可以解密，通过这种方式电子货币所有者可以在没有联网的情况下到银行之类的线下机构通过证明自己的身份来提取线下电子货币。

在商用互联网还基本没有形成的 1989 年，乔姆开了一家叫数字现金（DigiCash）的公司，开发了数字现金系统，这因为是世界上第一家提供在线支付服务的公司。甚至在美国有几家银行以及在芬兰至少一家银行确实使用了他们的系统。能够说服中心化机构为保障客户隐私使用该，不能不说是不小的成就。由于金融监管当局要求货币交易需要了解客户身份，监管机构对这几家银行的纵容态度也颇为微妙。

在乔姆之后还有为数众多的无政府货币的尝试，比较有名的是：1998 年戴伟提出的 b-money，它提出货币用于加强匿名用户之间契约关系的想法；2005 年，尼克.萨博的比特金（Bitgold）提出一个可以使用工作量证明。另外，尼克.萨博还早在 1990 年代就已经提出过关于智能合约的几个想法。

2、后续努力及失败原因

乔姆的数字现金系统，以及该系统的魔法货币系统、PGP 邮件转账系统、Lucre 系统都没能获得成功。后来另辟蹊径的 Beenz、Flooz、E-cash、B-money、比特金等虚拟货币先驱都失败了。类似的可能有上百种的虚拟货币的尝试都失败了。

这些系统中的大部分的问题是他们都没有跳出中心化支付系统的思维设置，只是在匿名和支付技术上进行了完善。同时，这一失败还证明私人发行的电子货币体系无法在类似“反洗钱与了解客户”这样法规和强力的政府监管体系下存活。另外，没有明显的成本优势很难形成广泛的网络，在互联网不发达的初期他们的便利性和用户界面也不够友好，从而很难说服商家和客户使用。所以，他们都没办法挑战根基深厚的信用卡公司。

所有这些系统中，1998 年戴伟提出的 B-money 和 2005 年尼克.萨博提出的比特金特别值得一提，因为它们是分布式的，而且与比特币已经很相似了。B-money 被认为是比特币的精神先导，比特金的理念已经与比特币很相似了。

戴伟首先想到了分布式架构下发行货币，但戴伟发行货币的机制是不可行的。他的的设

想到了解决难题的计算工作量的多少来发行货币，但是他认为每个人只要解决了难题就可以发行货币，这是不可行的。另外，1998 年互联网还并不发达，计算成本这类信息很难获得也不准确，而且随着计算技术的发展，计算成本在不断降低。他也想到这个问题，于是在白皮书的附录中提出计划、拍卖计算量的方式来决定成本，但这引入了太多的复杂性。但戴伟的分布式设想是很新颖的，他想到了分布式记账的想法，而且在白皮书中还提出了智能合约、仲裁机制和多重签名机制等先进的设想。所以，戴伟这个神秘的中国人，对中本聪的影响应该是最大的。

萨博 2005 年的比特金设想用户通过竞争解决数学难题，再将结果用加密算法串联在一起公开发布，以此来构建一套产权认证系统。比特币的求解哈希难题并广播给大家来验证的做法应该是吸取了比特金的想法。但比特金并不是一套货币系统，他也只是在某一方面得出了创建，没有能力把一系统技术和关于货币的理念结合在一起形成一种新的非政府货币。这套设想已经很类似比特币的理念了，而且发布日期与比特币的日期已经很近了，所以有人认为他就是中本聪。

萨博是乔治·华盛顿大学的法学教授，也是一名出众的计算机科学家。除此之外，绍博还是一位活跃的作家，其涉猎之广、产量之高令人惊叹，博客撰文涉及诠释学、深海资源开发和密码安全等领域。但萨博应该不是中本聪，因为他擅长理论不擅长编程，他一直找人合作实现比特金，但一直没有人响应。绍博本人在 2011 年 5 月也发文否认了这种猜测。

虽然乔姆、戴伟、萨博、芬尼等电子货币没有取得成功，但他们如此早就试验了密码技术在现金支付中的应用，而且还取得了一些理论和实务的成就，真是让人惊叹。乔姆的数字现金系统还取得了一些专利，尤其是盲签技术，可以有效保护所签署消息的具体内容，在以后电子商务和电子选举等领域有着广泛的应用。后来，许多密码专家对这一机制进行完善，产生了很多技术都为比特币的出现奠定了基础，包括找零的技术、分割电子货币技术中采用的梅克尔树技术、萨博提出的智能合约概念、1997 年英国密码专业亚当.贝克提出了工作量证明、2005 年提出的“零知识验证”等等都是后来被运用于比特币的关键技术。

其中特别提出的是：乔姆的系统遇到的如何解决双重花费的问题是电子货币系统遇到的基本问题，而乔姆提出的通过记账来解决为比特币提供了思想基础；贝克提出的智能合约是比特币使用脚本语言进行智能转账的基础；萨博的比特金提出的“凭空”发行货币的思想是比特币的重要思想准确。

虽然基础技术已经存在了，但这些成百种的失败似乎证明，摆在密码朋克的无政府货币梦想前的困难是很难逾越的。进入 20 世纪，除了很少的尝试，密码朋克们似乎对上世纪 90 年代的理想已经疏远了。在密码邮件组上，他们对一个日本名字的新人的虚拟货币的白皮书提不起兴致就很好理解了。

（四）创世主

1、身份成谜

虽然中本聪现在已经非常有名，甚至被提名为 2016 年诺贝尔奖经济学奖的候选人，虽

然人们到处“人肉”这个人，至今仍然不知下落。

自从 2011 年 4 月最后一次在比特币社区以“中本聪”的账号名称露面回帖之后，这位比特币的发明者，传说中的数学家、密码学家至今没有在网上或现实生活中公开露面过。根据 Tech2ipo 的一篇报道，截止至 2014 年，外界估算“中本聪”本人可能持有多达一百万枚比特币，按照今天的美元比价计算，大约价值 7 亿美元。

我们甚至不知道“中本聪”这个网名背后代表的是什么：是男是女，是美国人还是日本人，还是任何其它国家人，是一个团体还是一个公司……都不知道。虽然媒体几次声称找到真身，最后都被大家否定了。也有人主动出来承认，但得不到大家认可。所以，此问题至今悬而未决。有人利用网上的邮件内容及比特币白皮书的论文进行文本分析，认为中本聪应该是一个人，英语流利，英文夹杂一些英式拼法，但很难断定属于哪个国家。

中本聪隐藏自己身份，一开始就是有意为之。中本聪行事缜密细致，与任何人交流都使用 PGP 加密和 Tor 网络。加文·安德列森（比特币基金会首席科学家）曾向记者透露，有很多人都冒充中本聪写信给他，但被他轻易识破，因为他们没有使用 PGP 加密。中本聪哪怕与最亲密的合作伙伴交流也使用加密，而且从不透露个人信息，加文、尼克·萨博、哈尔.芬尼均对他知之甚少。中本聪把项目的领导权移交给加文，仅仅是通过邮件的简短交流。他甚至在白皮书和社区发言中，有意的伪造一些身份信息与个性化特征，误导一些错误的猜测。比如伪装英式拼读，格林威治时间的作息规律，日本名字，论文中“WE”的第一人称，使用生僻的科技术语，模仿密码学同仁的写作风格，反复使用‘of course’无逗号隔离，不同于惯用的方法（‘the problem of course is’）；使用‘preclude’一词（仅在 1.5%的密码论文中出现）……他的这些障眼法取得了不错的效果，已经有无数研究者、情报人员调查过他的真实身份，候选人多达几十位，有天才数学家，有技术大牛，还可能是团队，但没有一个得到核实。

比较有名的被怀疑者有乔治·华盛顿大学的法学教授尼克.萨博，它也是一名计算机科学家，在 1998 年至 2005 年期间，绍博曾致力于虚拟货币研究，并开发了一个“比特金”体系，这被视作比特币的前身。他因此被高度怀疑是“中本聪”真身。

名列“嫌疑榜”前茅的还有道纳尔·奥马奥尼团队。奥马奥尼是都柏林三一学院的计算机科学家，1997 年，他和两个同事合著完成一本关于电子支付体系的书。该书被视为比特币蓝图。

另外，《纽约客》记者乔舒亚·戴维斯一直怀疑曾迈克尔·克利尔。他就读于都柏林三一学院，几年前受雇于爱尔兰联合银行改进其货币交易软件，还合作发表了一篇关于点对点技术的学术论文，该技术是比特币的理论基石。

但以上三位的否认了这种猜测，所以也并没有引起太多新闻的反响。克利尔还表示自己仅仅在技术层面欣赏比特币，却对其中蕴含的无政府主义倾向感到不安。但美国一位 64 岁的多里安·中本和澳洲的克雷格·赖特则引起了巨大的新闻效应。

美国《新闻周刊》记者利娅·古德曼认为，如果真想匿名行事，比特币发明者完全没必取“中本聪”这种不常见的名字。她在搜索常住人口数据和国家档案馆材料后发现了与“中

本聪”同名的“嫌疑人”。

这个“中本聪” 是一位定居加利福尼亚州的美籍日本物理学家，1959 年从日本移居美国，从小天赋过人，精通数学、工程学和计算机，在生活中是个沉默寡言且情绪化的人，格外注重保护隐私。自从 40 年前大学毕业至今，他一直改用“多里安 • 中本”这个名字。

于是，2014 年 3 月《新闻周刊》发表了一篇封面故事，宣称找到了比特币创始人。但据《华尔街日报》之后的采访报道，事情并非如此。

真实情况是这样的。在遭遇几个小时的“围困”后，一位貌似所描述的“中本聪”的男子从屋里走出来，走向聚集在外面的记者，并称希望获得免费的“昂贵”午餐。在美联社的记者表示会向他提供一份寿司餐厅的午餐后，该男子和这位记者穿过人群，进入记者的车子，随后驶离现场。不过，在车子开走前，该男子向众记者表示，他和比特币没有关系。

中本聪的弟弟称，自己的哥哥在科学和数学方面很有天赋，但不太相信老哥是比特币创始人。弟弟说，哥哥“中本聪”并没有隐藏什么，也没有那么聪明，因为他从来都没有担任过首席科学家或首席工程师之类的职务。

这位中本聪后来说，他之前是与《新闻周刊》的记者交谈过，当时表示自己已经不干了，现在都交由他人负责，这指的是过去曾参与过需要保密的军工活动，可《新闻周刊》的撰稿人把这些话理解为“中本聪”是在秘密从事比特币的编码工作。

由于《新闻周刊》仍旧一口咬定此“中本聪”就是彼“中本聪”，逼得 64 岁的退休科学家不得不求助于律师替他发表了一份声明，再次表明自己与比特币没有丝毫关系。“中本聪”在声明中说，自己已经 10 年没有稳定的工作了，迫于窘迫的经济状况，去年还取消了网络服务，对于比特币，也是直到 2 月中旬儿子告诉他有一名记者询问这方面的事情，他才知道一二。

64 岁的老人称，“《新闻周刊》的报道给我本人、我 93 岁的妈妈、我的兄弟姐妹及他们的家庭带来了诸多困扰和压力”。“中本聪”最后表示，这是他最后一次就此事发表公开声明。今后，无论他还是他的律师都不会再对关于此事的言论给予任何回应。

Juola & Associates 公司拥有一项名为“文体测定”的技术，它能被用来确认匿名作品的作者，其首席科学家小约翰 • 内克尔用这位老人发表的邮件和网站贴子与比特币创始人的文本进行比对发现，两人的写作风格并不匹配，可以比较有信心的确认，这位老人并非比特币创始人。

这场乌龙可谓相当有名，这说明新闻界多么想挖出中本聪来，但看起来很不容易。直到两年后的 2016 年 5 月 2 日，BBC 报道，澳大利亚企业家及计算机专家克雷格 • 赖特已经公开证实，他就是所谓的比特币创始人“中本聪”。这一下子掀起轩然大波。

赖特已向三家媒体机构公布了他的身份，包括 BBC、《经济学人》以及《GQ》。在与 BBC 会面时，赖特对使用了密钥的加密消息进行了数字签名，该密钥被认为是比特币开发早期所创建的。赖特表示，著名密码学家芬尼是协助他将创意转化为比特币协议的工程师之一，但他才是比特币的主要构想者。赖特称，他已计划发布信息，让其他人从密码学上确认他就是

中本聪。

事实上，比特币社区曾经还弄出了一份中本聪的怀疑名单，其中就包括克雷格·赖特。当这份名单被媒体公布的时候，赖特极力否认。

在赖特承认自己身份后不久，比特币基金会首席科学家嘉文·安德森发布博文，支持赖特的说法。但是比特币社区很多人对此表示怀疑。有不少资深的比特币代码维护者认为现在赖特提供的证明并不能证明什么，认为赖特是在欺诈，认为他只是在公开途径拷贝了中本聪的签名，但不能证明可以动用那些资产，而且赖特只提供了第 1 区块和第 9 区块的签名，而创世区块是第 0 区块，只有第 0 区块才百分之百被认为是中本聪本人创建的。

“如果赖特真的想证明自己就是中本聪，那很简单，”早期的比特币企业家杰德·迈克卡勒伯说。“如果他能证明自己能够控制创世纪区块的关键部分，那他就能终结质疑。”

但就在 5 月 6 号赖特突然在自己的博客上发文表示收回证明自己身份的承诺，并因此向支持自己的安德森表示歉意。赖特说自己在严密关注之下他没有“勇气”这样做，还在文中表示自己“不够坚强”，无法面对不断浮出水面的关于他的资历和性格的指控。他表示，他不会公布自己能够获取比特币秘钥的证据。他供应商：“我曾相信我可以抛弃多年的匿名和隐藏。但随着本周事态的发展，随着我准备发表访问最早秘钥的证据，我垮掉了。我没有这个勇气。我做不到。”

我们已经知道比特币区块链能够永久记录所有发生在网路上的交易。带有公钥和私钥的加密哈希能够用来与其他使用同样私钥的签过名的交易进行比较。在克雷格·赖特事件中，比特币区块链所提供的透明性使公众能够很容易拿莱特的签名与区块链上现有的条目进行对比。比特币社区发现了赖特签名中的一些差异，由此证明赖特提供的证明是虚假的。

如果不是区块链数据的透明性和不可更改性质，整个事情可能就被忽视，进而直接认定莱特就是中本聪。尤其是在两位比特币社区著名人物安德森支持莱特声明的情况下，人们可能就会很容易接受莱特的说法。

此事不了了之，似乎到赖特家里搜查的警察也一无所获。

图 1.3 究竟谁是中本聪

中本聪为何不公开自己的身份呢？在密码邮件组中出没的大多人虽然通信都是加密的，但在邮件内容中都不隐晦自己的身份，毕竟这是一个专家交流的地方，也是大家积累声誉的

地方。我认为中本聪想到比特币的点子时，已经天才的预料到了比特币与以前的货币都不同，必将在未来货币体系中扮演一定的角色，所以他进行了一系列的有意识的运作。首先是到密码邮件组中以化名注册并发布比特币白皮书，这方便隐藏自己的身份的同时找到容易接受这一项目的人士，然后极其认真的把比特币当成一个严肃的工程项目加以完成，最后持续挖矿直到挖矿变得困难为止。隐藏身份是密码朋克的一个文化，当然也可能是比特币创始人的个性使然——作为顶级的黑客，当然应该有意愿和有能力隐藏自己的身份了。那么为什么直到现在还不现身呢？可能创始人对名声并不是在意，甚至害怕出名。

我们也可以想像，如果作为比特币的创始人出现，那么就不得不抛头露面，接受媒体的采访，而那样跟中本聪的性格真的是格格不入。他可能确实已经不想再当比特币的领军者。他无法忍受做什么事情却不能做到称职的感觉，而且他也已经认识到，这个项目即使没有他的存在也能继续下去。

另外，比特币可能只是一个实验项目，中本聪有更多理想需要通过隐藏身份才方便完成。正如他最后的留言："我转做其作事情了。"

不过，还有一个比较现实的原因：比特币被美国政府视为一种资产，如果知道创始人是谁，会被征收一大笔税收。中本聪一直没有使用大约 100 万枚比特币，这在现在大约是 7 亿美元。可能的一种解释是：如果中本聪想要出售他所拥有的比特币，那么他很可能就不得不到一个合法的比特币银行或交易平台上来进行这项操作，而这不仅会泄露他的身份信息，而且还会让美国国内税务署（IRS）和联邦调查局（FBI）都注意到他的行动。虽然比特币允许其用户匿名交易，但在互联网上，所有交易都形同透明。也就是说，如果中本聪想要把这种虚拟货币转变成能在现实中使用的货币，那么就会让他在政府面前变得无所遁形，而他希望跟政府越少瓜葛越好。多一事不如少一事嘛。联想丝绸之路站长被 FBI 安排的卧底钓鱼，中本聪显然要高明得多。

还有一种可能性是，中本聪已经遗失了能使其使用这笔财富的访问密钥，但比特币基金会首席科学家盖文·安德森对《新闻周刊》表示：中本聪是个"严守纪律"的人，不会犯那样的错误。

2010 年 12 月，比特币已经崭露头角，一家名为"维基揭秘"的自称反对权威、倡导自由的网站宣称愿意接受比特币形式的捐赠。在"中本聪"的追随者为之欢呼雀跃时，中本聪却发言表示："不，别这么做……我请求维基揭秘别用比特币。"他说，"比特币尚处于测试第二版婴儿期，你最多从中捞点零花钱，但因此引发的热度却足以就此毁掉我们。"

看来，中本聪的确很小心的呵护着比特币，他不希望比特币成为反政府的力量，害怕人们将比特币与反政府划上等号。两个星期后，中本聪留言说："维基揭秘捅了马蜂窝，现在蜂群直奔我们铺面而来。"一天后，即 2010 年 12 月 12 日，"中本聪"在比特币论坛留言后在网上露面越来越少。2011 年 4 月，他最后一次公开留言"我转做其他事情了"，从此踪迹全无。

2、个性分析

中本聪身份成谜，然而中本聪是怎么样一个人呢？从“中本聪”近十万字的网络留言中，人们能为这个比特币发明者拼凑出一幅“网络肖像”，比如“厌恶银行”、“小心谨慎”等。

我们分析，中本聪应该对虚假货币发展史很熟悉，并进行了反思，认为失败的致命原因是其中心化组织结构。使用中心化结构为虚拟货币信用背书存的问题是：不符合无政府的思想；中心机构也可能倒闭；中心机构的保管总账的中央服务器被黑客攻破；中心机构可能被内部人员出卖……总之，中心机构不可信。这样的机构与同样是中心化组织并且其发展已经根深蒂固的信用卡生态系统是很难匹敌的。

2009 年 2 月，中本聪在自己注册的网站 bitcoin.org 的聊天频道写道：“政府擅长击溃 Napster 那样拥有中央控制的网络，但是 Gnutella 和 Tor 这样完全 P2P 的网络看起来依旧安枕无忧。”这样的文字透露了他的心路历程，即其出发点是要用分布式的支付网络替代类似乔姆电子系统的中心化结构的支付网络。

一旦认识到中心化组织架构的问题，并且有意识地要走向分布式组织架构后，整个无政府电子货币问题的解决方案一下就明朗起来了。双花的问题可以用分布式账本代替，众所周知的分布式通讯的拜占庭将军问题恰好可以跳出计算机技术通过货币发行机制加以解决，前途晦暗的无政府货币理想突然变得一片光明！

中本聪对自己的想法可以说是倍儿有信心。而且，还可以肯定的是中本聪是个十足的实干家。他在发表比特币白皮书时就已经注册了 bitcoin.org 域名，并且那个时候已经开始对比特币进行编程实现了。虽然白皮书在加密邮件组上无甚反响，他并没有停止编程工作。中本聪对比特币的工程实现相当游刃有余，虽然现在看来比特币某些设计有待改进，C++编程也被某些牛人认为不算特别优秀，但更多专家不断赞叹其工程设计上巧妙架构。中本聪能在众多设计的选择中先出最有利于工程稳定运行的方案，并且在熟练的使用前二三十年发展出的众多加密货币技术，并在这些技术的基础上进行了大量的创新，在某些重要方面和技术细节上相当具有前瞻性。

中本聪的密码学造诣可以说是十分精湛的，许多曾经被当时的密码专家认为是冗余的设计错误，后来被证明都是正确的和很有讲究的：比如，精心挑选的 Koblitz 曲线，有可能是为了避开了美国国安局在加密标准中暗藏的后门；再比如，在椭圆曲线数字签名算法加密的基础上再哈希两次可能是为了应付量子计算机的威胁……总之，中本聪既是理论天才又是技术天才，他以意想不到的方式让比特币躲开了一系列潜在陷阱或密码学子弹，让比特币能在无人值守的情况下成功运行长达 7 年之久，并且不断状大。这一工程堪称人类工程史上的一大典范。

中本聪曾在其邮件中曾经说，自己的想法如果没有想好实现路径就难以形成文字。可以认为中本聪是天才的理论家和老练的工程师，再加上他的神秘性，早期“皈依”比特币的人们对比特币使用“创世纪”、“创世主”、“创世区块”类似这样的宗教语言就不难理解了。

实际上，与比特币相关的类似宗教的意味在语言和概念中无处不在：“创世区块”用于描述中本聪第一批开采硬币；绰号“比特币耶稣”给了罗杰.威尔是社区里“布道者”里最突出的

代表之一；“信徒”是指那么比特币“真相”尚未显示出来就顿悟的社区成员。而 2008 年神秘的出现又在三年后同样神秘的失踪的中本聪奠定了宗教基础，因为不管他/她/他们是谁，中本聪给比特币带来了创世神话。

3、谁是中本聪并不重要

中本聪是密码朋克文化养育的孩子，乔姆、戴伟、芬尼、瑞特、拜克和萨博等都为这一文化做出贡献，也许中本聪对于加密货币临门一脚的作用比其他人更关键，但由于他的神秘，他成为一个重要的象征被刻入历史。他是黑客帝国反抗矩阵压迫的尼奥，赛博自由主义的英雄，来自威廉.吉布森小说所说的一个“政府是被永久禁止或永远不需要的”的地方，他是数字货币时代的先知，他集齐了赛博空间的后宗教文化所需要的全部元素。

我们处于一个后宗教文化中，尼采在“上帝已死”，但我们还生活在互联网寡头、银行寡头、跨国公司巨头、政府特权等的阴影中。我们无力对抗对我们信息进行监督和审核的中央权力，无力对抗政府滥发货币的威胁，无力对抗在世界四处布点的金融巨头。谁能领导我们对抗那些利用我们对钱的属性愚昧无知来获利的利益集团呢？我们无力对抗根深蒂固的寡头和国家垄断，我们只能降低道德要求对政府与商业巨头们的相互勾结？或者选择逆来顺受？

中本聪的形象让我们想起像来自 V 字仇杀队的 V，中本聪从数字地下世界的黑暗中浮现，像一个后宗教时代的先知，领导公众对抗企业寡头和政府特权。赛博自由主义者的心目中，他是全球黑客和网络自由战士组成的松散联盟的象征。他像摩西一样，从西奈山上获得摩西十戒，并通过血腥的清洗，从而让从埃及强权下的奴隶在精神上获得神性，能够团结起来为自由而奋斗。

密码朋克文化滋养着自由主义战士的灵魂，朱利安·阿桑奇、布拉德利·曼宁和爱德华·斯诺登……他们都对网络监控深恶痛绝，宣称他们将终结腐败。他们是信仰非暴力的和平主义，他们的泄密代表着对互联网自由主义理想的忠诚。在政府眼里他们可能是持不同政见者的异类，但在赛博朋克眼里他们是真正的英雄。

中本聪是谁已经不是特别重要了，因为比特币一旦运行，只要还有信奉者，只要这种精神还有继承者，就没有办法关闭。这台似乎永不停息的无政府货币机器“怪兽”，代表着对旧秩序的挑战、对更公平社会的向往和对特权的鄙视。总而言之，对那些追求一个更公平的世界的人来说：我们都是中本聪。

4、创世先驱

还有一个加密专家在比特币软件开发中也起到了重要作用，可以认为是创世先驱。他就是哈尔.芬尼（Hal Finney），早期比特币的二号人物。他在读了中本聪贴出的比特币白皮书，很快识别到这个论文的价值，并在几乎一开始就联系中本聪参与了比特币的软件开发工作。在中本聪开发出比特币软件后，他与中本聪进行了大约两周的高强度的软件测试，遇到问题后就用简单的语言进行纯技术的交流，直到软件调试成功并能够健壮地运行。

哈尔·芬尼，那时 53 岁，是由菲尔·齐默尔曼创立的 PGP 公司一个顶级开发人员，著名

邮件加密软件 PGP 第二作者，是一个传奇色彩的加密活动家。作为密码朋克运动的早期的和重要的成员，芬尼本人有多种加密创新，包括匿名邮件转发器，它让人们可以在没有透露邮件起源的情况下发送电子邮件。2004 年，芬尼甚至已经推出了自己版本的电子货币，并在其中使用了 “工作证明”的功能。这一功能可以验证和量化记账者是否有相应的处理能力，是比特币的关键技术之一。这样的背景使芬尼有能力发现中本聪的比特币白皮书所说的货币系统真的有所不同，并很自然地投入到其中。

遗憾的是，他在比特币推出后的第五年去世了，去世时年仅 58 岁。他去世时已经和肌肉萎缩硬化症（ALS，即“渐冻人症”）抗争了 5 年，可见在与中本聪开发比特币软件时已经知道自己时日不多了。自 2009 年从中本聪那里通过试验性的转账得到第一个比特币后，他通过自己和中本聪合作开发的比特币系统作为“节点 2 号”继续开采，但比较遗憾的是他由于自己电脑 CPU 太热，散热风扇因此太响而关闭了比特币软件并停止开采。芬尼让他的电脑持续开采比特币一个星期左右，最后得到约一千个比特币。不过，芬尼一直没有动用这些比特币，在他去世时已经价值约 300 万人民币。根据芬尼的愿望，他的比特币现在用于资助在亚利桑那州的一个工厂对其身体进行低温冻结，他满怀希望，有一天能起死回生。芬尼也成为人体冷冻术技术的首位使用者。或许有一天芬尼被解冻并治愈时，比特币已经成为宇宙货币。谁知道呢？这算是我们对这位比特早期创始人的美好祝愿吧。

（五）创世区块

2009 年 1 月 3 号中本聪在位于芬兰赫尔辛基的作为“节点 1 号”的一个小型服务器上挖出了第一批 50 个比特币，并且形成第一个货币记录区块——创世区块。他在创世区块的信息备注栏里写下如下字句：

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

这句话的意思是“《泰晤士报》，2009 年 1 月 3 号，大臣处于第二轮救助银行的边沿”，这正是泰晤士报当天的头版文章标题。当时美国的次贷危机正蔓延到欧洲，受质疑的大臣是英国财政大臣阿利斯泰尔•达林，他当时正奋力阻止英国银行体系的彻底崩溃。当时英国政府已经抽出 5000 亿英镑用于向银行提供贷款和担保，其中包括 500 亿英镑用于收购苏格兰皇家银行、莱斯银行集团和 HBOS 公司这三家摇摇欲坠的金融巨头的大部分股份。

这是黑暗的日子。雷曼兄弟已经破产，美林证券在同一个周末被美国银行救出。数天后世界最大的保险公司 AIG 爆出的坏账导致政府救助膨胀到 1820 亿美元。西方经济体陷入信任危机，股市崩溃，世界贸易陷于停顿。如果有人寻找时机推出一种替代货币体系，他们再也找不到比这更好的时机了。

中本聪在这时推出比特币，并在创世区块上写下这样的字句，真是显得老谋深算又意味深长。

图 1. 4 2009 年 1 月 3 日《泰晤士报》头版

2009 年 1 月 3 日，中本聪在邮件组中宣布：“比特币首次发布：一个使用点对点网络以防止重复花费的新的电子现金系统。”并且附上了宣传口号：“这完全是分布式[2]的，无需中央服务器或中央权威。”

再次，针对中本聪的反应不温不火。立刻反应出来的普遍批评是：开采比特币区块链所需要的电能比开采出来的比特币的价值还大，更别提其灾难性的环境影响了。美国印第安纳大学的天文学教授，乔纳森·索恩伯格，看到了一个更大的政治挑战：“没有哪些大国政府愿意让比特币以当前方式大规模运作。”

虽然创世区块被挖出来后发现软件还老板娘调试，第二个区块五天之后才被挖出来，在五天之中，中本聪和芬尼不断调试软件，但软件总算顺利运行了，信心满满的中本聪让软件持续运转，并有条不紊地让节点 1 号每 10 分钟产生 50 个比特币。由于当时在网络中虽然陆陆续续有人加入，但没有人像节点一号这样觉得有义务让软件持续运行，除了他试验性地进行了向芬尼转了十个比特币外，可以说一开始除了挖矿也根本没有交易，很少有人意识到比特币的价值。可能只有中本聪让自己在芬兰的服务器一直运行比特币软件，将产生的比特币不断地存到只有他自己知道私钥的作为数字“钱包”的地址里。

甚至中本聪重要的助手哈尔·芬尼，第一个接受比特币转账的人也没有意识到比特币未来的“钱途”。他虽然热情饱满地参与了最早的软件开发和调试，但更多是出于理想主义和试验的心态，或许也是因为得了绝症，没有把比特币过于当真，所以在发现自己电脑 CPU 太热时，把作为“节点 2 号”比特币软件关闭了。

在中本聪和芬尼的调试的最初几天的通信中，我们得知他们发现有其他不知名的人下载并运行了比特币软件，这些人是比特币最早的追随者。随后比特币使用的人越来越多。虽然现在仍然不知道谁是中本聪，但这似乎也不重要了，因为技术是透明的、代码是开源的、参

[2] 本文中将较多使用“分布式”这一计算机术语。分布式是一个形容词，常用的有分布式系统、分布式计算、分布式数据库等，是指由多个平等的节点共同承担。之与相对应的是中央集中式或中心化的系统、计算或数据库。

与者是自愿的、程序是分布式的，只要有信奉者，一切都会自动运行下去。

（六）并非偶然

现在看来，比特币又不尽然是天上掉下来的。可以说，万事具备，只欠有心人。比特币的成功，实际上得了天时、地利和人和之便，只需要创世主出来大呼一声就会一呼百应。

地利，是美国本来就是一个鼓励多元化和技术革新的国家，也是一个无政府主义文化盛行的国家，拥有各种分支文化，如科技极客、硅谷文化、赛博自由主义、开源文化、隐私保护文化等文化。这些文化的滋养下才能产生密码朋克文化。这些文化的流行有比较长期的历史渊源。

美国的创始人是一批最初被政府迫害的清教徒，当他们乘船到美国的时候，他们认为政府应该是一个小政府，所谓“夜警政府”，晚上打打烊保证大家的安全就可以了。这个文化在美国一直比较盛行的，即对政府不信任。美国 27 条宪法修正案的前 10 条都是为了保障平民免遭政府迫害的修正案，所以又通称权利法案。美国允许私人持有枪支，而且枪支协会在美国政坛有非常大的影响力。背后原因就是，国家创始人们认为平民拥有枪支才有能力随时推翻作恶的政府，而持有枪支的平民反过来又成为让政府不作恶的威慑力。

在互联网时代信息美国人的那根不相信政府的神经又敏锐起来，有识之士意识到网络隐私可能会被政府监听，所以想通过赛博自由主义运动来保证大家的权利，而倡导加密通信的密码朋友运动就是这个运动的一个分支，其主要目的是保障大家的隐私和网络言论自由。在这个过程中还涌现出阿桑奇、斯诺顿这样的激进人物。对于政府的不信任自由的延伸到对于政府滥发货币的担心和大型金融机构的不信任，这些作为赛博自由主义斗士的科技极客一直在想让大家通过互联网在金融方面摆脱政府的控制办法。他们首先想到的办法就是哈耶克曾经设想过的让私人发行货币，并且让这些货币自由竞争。这并非不可能的，有些时代民间钱庄发行的银票等由于可以流通，就拥有类似货币的功能。而科技极客有了要把这套系统移到互联网上的想法也是很自然的。

人和，是指有一邦志同道合的密码朋克能够相互交流、矢志不渝、不断尝试，并最终开发发一系列必不可少的技术，包括电子记账技术、零知识验证技术、工作证明技术、电子找零技术、分布式数据同步技术等，而将这些技术在去中心化的分布式记账思想下进行组合其实只是呼之欲出了。在密码邮件组的天才中正酝酿了这样的人才，能够突破传统思维将技术和经济两个维度相结合，通过将经济学的激励机制和通缩货币等原理与加密技术武装的分布式记账结合起来，从而完成惊人的一跳，发明出了比特币。

天时，是指金融危机频仍，让人们对政府一次次地失去信任，特别是 2006 年到 2008 年美国次贷危机为比特币的出现和流动提供了难得的时机。次贷危机中表现出来的大型金融机构的不负责任，和被绑架的政府必须求助这些“大而不倒”的金融机构的无奈，加上相继的欧债危机，让人们对现在的主权货币系统进一步产生疑虑，并让密码朋克们行动起来，并重拾无政府货币的思想，发明了比特币。比特币也在这样的背景下得以快速流行起来。

二、运作原理

（一）背后技术引人入胜

比特币与早期无政府货币的尝试的本质区别是：比特币完全是分布式的。所有下载比特币软件的计算机节点会作为一个平等的新的节点自动加入到比特币网络，享有平等的权利。正如中本聪在软件首发时在邮件组中所宣布的，比特币“一个使用点对点网络以防止重复花费的新的电子现金系统”，并在宣传口号中强调比特币“完全是分布式的，无需中央服务器或中央权威”。

比特币继承电子货币先驱们发明的一些技术，包括工作量证明、零知识验证、不对称加密、智能转账技术、凭空发行货币、用记账防止双花问题、找零技术等等，但中本聪的比特币现金系统与早期上百种电子货币的主要区别是，它完全是分布式的，它用分布式的架构创造性的将所有这些技术集成在一起，并且突破性地解决了分布式架构下才存在的一些特殊问题。

我相信当中本聪想到用分布式架构替代乔姆的系统并将自由的系统命名比特币后，他就发现比特币需要解决以下四个特有的问题：

（1） 如何让人们相信各节点是完全平等的？

（2） 如何发行货币并让人们相信整个货币体系不是通胀货币？

（3） 如何在分布式架构下解决双花问题？

（4） 如何在分布式架构下解决数据库同步并让数据不可篡改（即拜占庭将军问题）？

第一个问题还是比较好解决的，将软件开源，以方便参与者对程序进行审核，同时辅之以让数据透明，让参与者可以对数据进行校验，为了保护隐私和让参与者不以身份相区分则使用匿名机制。软件开源、数据透明和匿名机制，三者结合可以很好的解决参与者信任机制的问题。

第二个问题也比较好解决，凭空发行货币，并引入逐步减少的现金发行机制，直到停止发行货币，从而控制了货币的总量。

但是第三个和第四个问题则是中本聪天才的创造，更加引人入胜。这两个问题的解决方案形成了比特币最主要的技术基础。这一技术后来被人们命名为区块链技术，它是人类相互不信任的伴随着战争、欺骗、尔虞我诈的黑暗进化阶段进入新的相互信任的进化阶段的黎明的一线阳光。这一新的进化阶段就是价值编码进化阶段，这将在第八章加以讨论。

中本聪对货币的本质有深刻的理解，在此基础上才可能创造性的解决双花问题。要理解中本聪设计背后的巧妙，我们需要一探“货币”这样一种司空见惯又无比神秘的存在的本质。

（二）货币本质

1、货币是人类合作的基础

试着把一个人放到荒野中，生存的能力是很差的。人类，就单个人而言是很没有竞争力的，但一小群人，生存和延续的可能性就增加了很多。虽然 1620 年到达北美的五月花号上的 102 人在当年冬天就死去一大半，只剩下 44 人，虽然如果没有心地善良的印第安人给移

民送来了生活必需品，还特地派人教他们怎样狩猎、养火鸡、捕鱼和种植玉米、南瓜等，这一百多人最后的命运还很难讲，但是一群人的力量是很强大的。这可能是智人小分队们能走出非洲分散到其它各大洲的原因，也是近 10 万年内包括猛犸象、欧洲野牛、剑齿虎等几乎所有的大型哺乳动物都在各大洲灭绝的重要原因。

人类能在 250 万年前在动物中脱颖而出，可能是因为人类更擅长使用工具和合作，而直到 10 万年前几十种直立人中的叫智人的一支才让人类能够大规模繁衍，并最终替代其它直立人。

我们直立行走的祖先经历了上两百多万年使用石器的时代，却一直进步不大，仍然活在缺衣少吃，朝不保夕的生存的恐惧中，直到 10 万年前才突然长出息了，能够大规模协作征服全球。这原因是什么呢？至今依然成谜。有考古学家认为这可能是因为智人突然进化出了语言，使人类可以通过交流更好的合作。人类在黑暗行走了如此长久的岁月，睁着恐惧的大眼，却没有语言可以很好的思考和交流。想起动物世界里草原动物们相互捕食，而我自己却能在家里安然写作，不禁产生一种很幸运的感觉。

但是人类合作的基础不仅是语言，蚂蚁、蜜蜂、狼群也能很好的合作，但是动物的合作只是捕食、建巢穴、自卫等简单的无意识或应激性的合作，而人类的合作是复杂的社会分工和相互交易。

由于社会分工也最终表现为交易，可以说人类合作是以交易为基础的。交易是一种基于等价交换的分工合作机制。越是复杂多样的交易网络越能构建复杂多样的合作网络，创造出璀璨的文明。

但是，交易的达成是要满足一定条件的，正是这些条件影响着分工合作的规模。因为交易是一种等价互换的行为，需要交易双方都能提供对方满意的交易对象才能够达成。

针对频率高、期间长的交易行为，人们并不一定每次交易都要结算，只要相互亏欠着，并相信未来会返还，并在长期内能够平衡就可以，这就需要一种信任机制。最早的人类部落只能依靠血缘关系才能维持相互信任，所以人类首先进化出比较容易了解血缘关系的组织形式，即母系社会。

人类中等强度的交易还可以在部落、村庄这样的范围内以集体互助或暂时亏欠的形式展开，这就需要中等强度的信任。营销学有一个“250”法则，认为一个人大约有 250 名亲朋好友。可见一个人能了解和信任的其它人的规模不可能很大，所以这种模式的交易规模也不可能很大。虽然可以通过规则、法律和强权等契约形式在城邦甚至国家层面进行合作，但只能是特定的方面才能合作，比如国防、教育等，并且容易偏离公平交易，这样的合作并不能达到多样、高频和高效的。

通过相互暂欠或缔结长期合约，都需要比较强的信任关系才能完成。但最好的方式是能够立刻结清的交易方式，并将需要的信任关系降到最低。早期的人们没有找到共同认可的中介物，只能实行以物易物，但这种方式只能较小的规模地开展。人类要展开更大规模的合作就必须找到在较大范围人群内共同认可的交易中介，即一般等价物，因此各种类型的货币就应运而生。这就是货币的起源。货币，实际上是人类大规模分工合作的基础。

2、金龟子和符号主义者

既然需要一般等价物，不同地区的人们都在尝试着。最开始肯定是用一些大家都容易接受的东西。但人们逐渐发现，人们比较容易接受的东西需要以下一些特点：

（1） 容易分割和验证，方便结算；

（2） 不易变质和损坏，容易储藏；

（3） 比较稀缺，体积小、价值大，容易携带。

人们使用过贝克，到现在汉子里与钱有关的还主要是贝字旁的。人们使用过一般金属。但最好的还是贵金属，即黄金和白银。它们的特点是：比较软，容易分割；化学性质稳定，

容易储藏；比较稀缺，体积不大，容易携带。

喜欢黄金，这甚至被一些人类学家认为是刻在基因里的。他们发现从来没有看到过黄金的部落，一旦看到黄金这种东西，就愿意用比较值钱的东西进行交换。

历史上研究货币的人人，认为黄金天然是货币的人，就被称为贵金属主义者，又可以戏称为“金龟子”。

但也有人不同意这样的观点，认为货币不必然是黄金。实际上在历史上毛皮、食盐、铁等都担任过一般等价物，充当货币职能。只是随着交易的扩大，一般等价物才逐渐固定在体积小、价值大、不易损坏、易分割、便于携带和保存的金银等贵金属上。但即使贵金属也有其问题，一是称量的麻烦，二是化验的不便。

在纸币流行开来之后，黄金的货币属性已经不断降低了，人们认识到货币可能只是一种基于某种信任的“符号”即可，这些符合不论是钱庄银票、银行本票还是国家纸币，只要让人们相信大家都愿意授受并且不容易贬值就可以充当货币进行流通了。

3、雅蒲岛石币之谜

历史上的确早有人在一种封闭的环境下无意中采用了符号主义的思路。甚至他们走得更远，他们认为货币体系本质上是一本关于交易的账本，而货币只是账本上可以任意不可伪造的的记账符合即可。

1903 年，William Henry Furness III 在雅蒲岛居住了几个月。由于对该岛居民所实行的货币体制印象深刻，他就根据雅浦岛居民的风俗和习惯，写了《石币之岛》。

雅蒲是在太平洋西部加罗林群岛中的一个岛，它是世界上最大货币所在地，雅浦岛的居民在土地和房屋的买卖交易时，仍用直径达 4 米、最重 5 吨的石材当货币使用；这些巨大的雅浦岛石币 (Fei)，是特地从帕劳岛上的石灰岩切割下来后渡海运回雅浦岛，可以说石币的制作也颇不容易。看起来石币不符合我们说的实物货币容易切割和携带的特点。其实，虽然石币也是实体货币，其背后的本质是一套大家相互信任的记录货币由谁手里转到谁手里的账本。

雅蒲岛人做交易时，只需要把相应的石币登记到对方的账上，并在自己账上划掉即可，并不需要把这些石币搬来搬去。所以，实体货币并不需要进行转移。如果还可以登记几分之几转移到对方账上，几分之几留在自己账上，那就并不要求三体货币容易分割了。石币存在的作用是为了限制货币发行、不能造假，所以货币可以是观念的，只要不能无限发行即可，而石币体系本质上是各人手上的账本。但还有一条，账本不能篡改。雅蒲居民比较可爱，他们相互信任，不篡改账本。

图 1.5 雅浦岛硬币

雅蒲岛居民对雅蒲账本是很信任的。岛上有一家在很久远的祖上曾经开采到一个很大的

石币，但是该石币快运到雅蒲岛时掉到了海里，大家一商量就说：算不，不必打捞了，我们都知道你家有这么大个石币就可以了。于是祖祖代代大家都知道他家很有钱，并且可以用这个石币进行交易，但后来的人谁也没有见过这个石币。

另一个轶事可以说明雅蒲岛名是很把这个货币系统当回事的。二战期间，德国人想在岛上建机场，需要修路，并要求岛民提供帮助，但岛民都不愿意。德国人了解到雅蒲账本体系之后就威胁，如果不修路就在每家的账上取消一定数量的石币，岛民权衡了一下，居然就范了。

雅蒲账本给经济学家很大启发，著名的提出直升飞机撒钱思想试验的弗里得曼写过一本书叫《货币的祸患》，书一开篇就通过雅蒲岛石币还说明货币的本质。

雅蒲货币体系给我们的启示是货币是一种制度体系，其实本质是一种不可篡改的分布式账本，其实主要特点是：

（1） 货币体系是一个登记用户及余额的账本，每个货币使用者需要证明自己的余额是确实存在的；

（2） 货币中账本上用于衡量所有交易价值的符号，可以是纸币、电子货币、积分、站内币或任意符号。

这样的货币体系还需要有两个附加特点：

（1） 货币不能造假，也不能无限发行；

（2） 账本不能篡改，即交易记录篡改，这是为了解决重复花费的问题。

以上各点似乎才是“货币”这种东西的更本质的特性。我们发现中本聪的比特币能够符合以上特点，比特币实际上是互联网时代的雅蒲石币。当然，由于是互联网实时记账，比特币还有额外的特性，即用户匿名、交易透明、支付与记账实时同步等。

4、黄金和纸币的本质

货币实际上是一种分布式记账技术，这实在有点烧脑。我们用这种思路来分析一下历史上出现过的货币，然后我们再分析一下比特币是怎么做到的。

（1）金本位记账体系

在金本位货币体系里，账本及记账符号是一种什么形态呢？这里黄金是记录符号。由于账本主要记录余额，每个人手里持有的黄金就可以用于信息记录，因为一验证和称量黄金即可知道用户和余额。如果这个人把黄金保存在钱庄，由钱庄出具证明，这时钱庄就代为记账，表明该人手里有多少余额的黄金，所以钱庄出具的银票就可以作为货币使用了，其本质还是记录用户和余额的账本。

在金本位体系还必须符合货币体系的两个附加特点，即货币和账本不能造假。由于货币是黄金，它是没办造假的，也很难大量供应，而每个人手里的黄金足以证明账本中关于自己的余额是真实的，这样的信息也难以篡改。

（2）纸币记账体系

我们再看在纸币体系里，账本及记账符号是一种什么形态呢？纸币是一种记账符号，实际上，现在社会常常不用现金就可以交易，更加体现了其符号的特性。而用户如何证明自己账上的余额呢？一是纸币，这是难以造假的，而且如果造假会是违法的；二是通过银行的转账记录来证明自己的余额。前一种方式类似于黄金，持有者即证明有这样的余额；二一种方式有点像是通过钱庄来记录。

纸币也是不能伪造的，一定时间其供应也有限定的。但纸币也可能因为大量供应而失去货币的功能。另外，交易由银行记录，不一定安全，但安全度已经能够满足大部分场景的需要。

5、读者乌托邦社会的货币系统

通过观察黄金和纸币体系，我们发现实物的黄金和实物的纸币由分散的个体持有，用于记录自己的余额并证明自己拥有这些余额，这还是分布的记账体系。但是通过钱庄和银行来记录就是中心化的账本形式了。雅蒲居名的创造在于他们使用了分布式的记账体系。

为了更加清楚的说明分布式记账体系是如何运作的，我们举一个例子来说明。

假设有一群人，比如所有读本书的人构成的一个团体，我们准备在一起做交易，但我们不能使用其它任何货币，我们需要建立一个“读者乌托邦社会”并且自己发明货币。

传统上我们有三种选择：

（1）使用黄金，即金本位制；

（2）由某个人持有大量黄金，以此为准备金发行可以兑换黄金的纸币，即联系金本位制；

（3）由某个人或我们选择出来的某些代表凭空发行纸币，并且立法让读者乌托邦成员表决通过，即法币。

以上方式各有优缺点，但当读者乌托邦的成员知道雅浦岛的货币系统后，心有向往，我们已经知道货币的秘密，其实是一个大家相信的账本，账本上记录的东西不需要真实的商品货币只需要一种符号就可以了。

另外，大家都有智能手机，摆脱黄金、纸等的货币形态，直接使用“符号”似乎更容易了，比如互联网时代，一切东西都比特化了，为什么不能使用比特化了的货币呢？

于是我们设想一种叫“比特币”的货币，而且不需要黄金或印刷而是凭空发行该种货币。当然，我们为了和比特币相区别，我们称这种货币为“读者币”。

假设读者乌托邦社会有一万名成员，我们让每个人都事先持有一万枚读者币。接下来的问题是怎么记账才能让大家相互信任账上的用户及每个用户的读者币余额是真实的呢？我们想到两种方式：

（1）推选出某个人或某些代表，比如读者币记账委员会，即中央化记账系统；

（2）每个人都把所有的交易记录下来，即分布式记账系统。

我们先看看第一种方式。

我们先建立了一个读者币记账委员会负责记录所有交易，要求每个人交易之后必须将交易通过手机发送到记录处，记录处有一个软件可以接收这些记录，并将其审核和记录下案。如果交易双方发送的交易相符，而且购买方的确有足够的余额，就在购买方减记相应的交易额，并在销售方增加相应的交易额。这实际上就是乔姆的电子现金货币系统。

中央化记账系统容易受到黑客攻击，容易内部人员被篡改，甚至断电、死机、一场火灾或炎灾都可能让整个读者乌托邦的货币系统崩溃。我们需要一个更加可信、健壮的货币系统。看来我们只能选择分布式记账了。

我们发现雅蒲岛的居民并不需要把每笔交易发送给政府，而是交易双方记录下来就可以了。但这样的系统有一个“双花”问题，即购买方已经花钱购买了，但他不承认，接着又把这个钱用于购买其他人的商品。所以，雅蒲岛石币系统并非真正的分布式记账，之所有没有（或者不严重）是因为这是个小岛，要核查并不难，而且一但被查出来将声誉扫地，这对于很小的熟人社会来说是很严重的事。

但读者乌托邦社员分布在各地，甚至我们并不知道对方姓名，比如，我们只是某读者网站上注册为读者乌托邦成员而已。

于是我们在网站论坛上商量决定我们需要一个分布式的读者币软件，每个安装软件的节点都是平等的，都拥有一套完整的账本，软件在每过一段时间就把这段时间的交易记录到一个区块里，每个区块里的交易都经过事先达成共识的方式进行了审核，都是合法真实的交易，而下一个区块继续这样操作，这样的区块在时间上形成一个链条，我们称为区块链。

我们称这种由平等的各方共同记账的系统为分布式记账系统，其背后的技术称为分布式记账技术。所以，雅蒲岛石币也是分布式记账技术，是一种线下的分布式记账技术。如果在互联网上使用分布式记账技术，我们可以每过一段时间产生一个区块，记录所在这段时间发生的所有交易，而所有交易区块在时间形成一个链条，我们可以称这种分布式记账技术为“区块链分布式技术”。

但是要使区块链可以实际投入使用我们需要解决几个问题：首先，要让分布各地的读者相信软件是可行的，大家也是平等的，所以我们决定由自愿者开发一个开放源代码的软件，所有热心人都可以审查软件。其次，我们要使软件能同步所有愿意持有账本的读者手上的账本信息是同步的。第三，我们要求软件能够防止有读者悄悄的伪造交易信息。最后，我们还需要制定一套读者币发行制度，总不能像雅蒲岛居民挖石头吧。

具体来说，我们希望软件做到以下几点：

首先，让每个人同时记账是不可行的，这不仅由于网络存在传播快慢，大家记的账可能不相同，检验起来太麻烦，谁对谁错也没有标准。所以每次要选出一个我们信任的人来记账，如何选择呢？这需要一个大家认可的共识机制。

其次，就算选到这个人，如何防止这个人乱来或者不够谨慎呢？必须要给他一个比乱来更大的激励，而且要激励记账人任劳任怨的认真记账。这是一个激励机制问题。

第三，如果一般人都愿意授受激励，但如果有人使坏，想更改账本，把一笔钱花两次呢？这就是双花问题。

第四，如果有人掌握了大部分算力，比如51%的算力，就可以任意篡改账本了。这就是所谓的51%攻击问题。

第五，就算这个人认真记账，如何把记账的结果广播给大家的过程中不出错呢？这是一个通讯安全问题。在分布式通讯问题上有一个著名的“拜占庭将军问题”，已经证明要保证所有节点信息同步是不可能的。所以，必须要容忍部分读者的账本与大家的账本不同步的问题。这就需要记账者在多路广播的账本中加以选择，这就可能产生区块链分叉的问题。

第六，如果这个人愿意记，而且广播过程没有出错，那要每个记账人相信这段时间的交易是真实的，是不是要让交易都是透明的，而且每个人记账都能够在验证之后才记录下来呢？这就是验证问题。

第七，如果账本是透明的，那如何保护读者乌托邦的人们的财务隐私呢？这就有个匿名机制的问题。

最后，货币如何无中生有，数量如何决定呢？这不是一个小问题吧。每个人发一笔钱，但后来的读者也享受同样的待遇？这是不公平的。总之，货币发行也伤脑子的。

中本聪的天才之处是，它几乎完美的解决了以上问题。实际上解决了以上问题，就解决了分布式账本的基本问题，那区块链技术的基本问题，但分布式账本其实不仅可以用于货币系统，这套系统大有用处的。所以，中本聪又可以称为“区块链之父”。

6、货币体系本质和货币本质

不过，在讲述比特币是如何解决我们读者币面临的问题之前，我们需要总结一下货币体系及货币的本质。

通过对黄金系统、纸币系统以及读者乌托邦读者货币系统分析，我们知道了货币系统其实是一套具有公信力的记账系统。

当然要成为货币系统需要两个条件：第一，货币系统是一个账本，能够记录参与人的货币余额，并且能够证明货币属于该所有者；第二，参与人相信该账本。

货币的本质是某一大家信任的货币系统的记账符号。黄金之所以能成为黄金货币系统的货币，是因为黄金的特性和大家的天生的信任，纸币系统中的纸币能成为货币中因为人们对国家的信任。另外，黄金和纸币作为实物货币能做到记录货币余额和所属人的账本的作用。

读者币系统是一套记账系统，其公信力来源于系统的可靠性和大家达成的共识，读者币则只是一个记账符号。

（三）货币发行和交易记录

1、选谁记账的共识问题

现在我们要看看中本聪是怎么漂亮的解决我们在构建读者币系统时遇到的问题的。要建成一个可信的分布式账本一共要解决八个问题：选谁记账的共识问题、激励记账人的激励问题、双花问题、51%攻击问题、验证问题、分叉问题、匿名机制问题和货币发行问题。

中本聪的想法是选择记账最快的人，为此他选择了工作量证明机制。具体的做法是，让记账人们一起解决某个数学难题，谁能解出来说明谁的计算机最快。当然这个数学难题必须符合一个条件，即解题很难，而验证是否解对很容易。

另外，最好这个数学难题有随机属性，不能让最快的那台计算机垄断记账，而只能让它以一定的概率解出该题。

最后，这个题的难度最好是可以调整的。因为中本要求记账的间隙最好是固定的，在比特币需要把解题时间大约控制每 10 分钟一道题，由于参与计算的计算机的算力不是固定的，所以题的难度还需要可以调整。

中本选择了 SHA-256 哈希算法。哈希算法是一类函数，函数能把任何长度的数据转化为一个等长度的数据摘要，我们称其为哈希值。其形式如下：

119c506ceaa18a973a5dbcfbf23253bc970114edd1063bd1288fbba468dcb7f8

哈希函数有一个特点，如果原数据有任何改动，哈希值就会改变，这就是说，我们可以把哈希值看成该数据的指纹。如果出现两个不同的数据有相同的哈希值，在密码学上叫“碰撞”，好的哈希函数出现碰撞的概念应该是很低的，甚至应该比两个人拥有同样的指纹的概率还要低。如果被发现碰撞办法，让这个加密技术就算是作废了。

安全散列算法 SHA（Secure Hash Algorithm）是美国国家安全局 （NSA） 设计，美国国家标准与技术研究院（NIST） 发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。SHA-1 被人发现用一个算法可以让破解时间缩小到 10 天，这就算是作废了。在 2008 年 SHA-256 是公认最安全的哈希算法，在现代仍然是安全的，具体细节将在后面介绍。这里主要说明中本是如何用 SHA256 函数来构建一个数学难题的。现在只需要知道：SHA256 函数能够让任意长度的数据产生一个 256 位的数据摘要，这个哈希值的大小是随机的，同时数据固定后，出现的哈希值就是固定的。

每 10 分钟产生的交易数据是原数据，中本聪要求在原数据前随机加一个整数，然后求这个构造数据的哈希值，如果这个随机产生的哈希值小于某个数值上限就被认为解出了难题，被选为记账人。其他人要验证此人解出了难题也很容易，记账人会把随机数的哈希值广播给大家，验证人只需要把原数据和随机数放在一起求出哈希值就可以比较这个哈希值是不是给出的哈希值，以及这个哈希值是不是小于数值上限。

由于这个难题只能不断选择随机数暴力破解，所以只能拼算力，而且那个选到随机数并最选广播的人并不一定是计算最快的，而是运气比较好的。事实上，大家解出难题的概念是按算力占比分配的。另外，难题的难度很容易控制，只要把数据上限按一定时间大家计算时间重新设定就可以了。如果一段时间平均计算时间大于 10 分钟，就减少难度，即把上限提高，如果小于 10 分钟就磁加难度，把上限减小。

好了，记账人算是选出来了。由于记账人需要拼算力，算力竞争越来越激烈，想要获得记账权，就需要采购更快的机器，并且这样的机器耗电也越大。这类似于在矿场挖矿。所以，争取记账权的过程又被称为挖矿，这些计算机又称为矿机，而拥有这些矿机的人又称为矿工。而且因为挖矿的确有机器采购、磨损和电力消耗，这里争取记账权的工作量证明的确是产生了工作量，也被人认为比特币的确是付出代价和是有价值的。

2、激励记账人的激励问题

这套方法的确可以产生记账人，但矿工们干嘛那么努力却解一个看起来无意义却很耗电的难题来争取记账权呢？我们都想到了，把在这 10 分钟产生的交易的交易者都给记账人一定的记账费好了，这也是应该的。

中本聪采用了两种激励机制：发行激励机制和交易收费机制。

发行激励机制的做法是把记账激励与比特币发行结合起来，记账的人可以获得比特币，这样就可以产生比特币了。比特币无中生有了。

为了让比特币不会无限发行，每过一段时间就对比特币减半发行，这样比特币就会指数式的减少，最终停止发行，使比特币固定在某个数值。比特币的做法是让最开始每 10 分钟发行 50 个比特币，然后控制在大约每 4 年减半发行，这样从 2009 年 1 月到 2040 年发行结束时比特币总共发行大约 2100 万枚。

减半发行的确可以控制货币发行数量。这样做的好处是，让先参与的人获得更多的比特币也是合理的。但发行越来越少，激励也越来越弱，而且发行完之后激励就没有了。为了解决这个问题，中本聪也设计了交易收费机制。

但是最初的发行激励已经足够了，而且作为通缩货币，虽然每四年减半，但货币升值会弥补数量的减少。所以，最初并不需要收费，这也有利于货币的推广和避免过度激励。

但是细心的中本聪考虑到货币系统可能会受到分布式拒绝服务攻击，所以对小额转账收费并把费用交给记账者的收费激励机制。当然比特币只设了最低收费的标准，但交易者为了激励矿工先给自己的交易入账，可以自行设交易费用。

分布式拒绝服务攻击指攻击者借助多个计算机联合起来作为攻击平台在一个设定的时间将大量服务请求向攻击目标倾泻，以达到让对方服务器瘫痪的目标。中本聪的做法可以避免类似攻击，而且在未来发行激励机制减弱之后可以顶替上来。而且如果货币系统运行良好，交易规模扩大之后，虽然每笔交易收费甚微，但总量是可以达到激励目的的。

3、双花问题

记账人账本造假收益与激励比较，必须让记账人觉得还是老实记账来得划算。但这不仅是技术问题还是一个经济学的问题，这需要与记账人斗智斗勇啊。

简单来讲，乔姆的中央记账系统是可以避免双花的，但是分布式系统如果记账人造假，并且广播给大家，大家会对这个账本进行验证，如果账上有 1 万元，要花 100 万元就没办法通过其他人的验证，其他人就不会认可这个账本。所谓双重支付是指，造假的记账人同时向两个人同时转账 1 万元。

对于这种情况，一方面，由于每一笔付款都会被广播给系统中所有节点，任何人都可以使用收款者的公钥来验证这个交易的合法性，如果付款者试图双重支付，就必须先删除这个交易记录，否则新交易无法通过验证；另一方面，由于工作量证明机制使得生成下一个区块的节点和矿工几乎无法被预测到，所以删除交易记录几乎不可能。当然，矿工也可以选择将其中一笔入账，矿工有自己的挖矿算法，有的会选择先看到的交易先入账，有的会让给交易费多的先入账。

4、51%攻击问题

如果所有这些节点中有节点要以掌握 51%的算力，那的确可能让系统处于该节点的控制之中，但这似乎是没办法的事，只能改变工作量证明，或者各节点分散算力。那么各节点会怎么想呢？

首先，如果系统小到能够被某个节点控制，那么这个货币系统并不是很重要。

其次，如果系统足够大，那么要控制某个整个系统要付出的算力的代价将是非常高的，这样的能力不如用于挖矿。

第三，如果有某些恶意的人只是想攻击该系统并且不惜代价，那这个节点被发现后，其

它节点的人可以一起商量把被攻击之后的区块作废，并转移到其它区块链上。

最后，如果该货币系统被攻击，这个系统也可能消亡，但这样的货币系统很容易被复制出来，这些货币本来就是自由竞争的私人货币，有众多货币相互竞争，这样的攻击花费很大，但并不是很管用。

实际上，现在比特币主要算力集中在中国，而且很多矿机联合形成矿池一起挖矿，以增加获得记账权的概率。曾经有过某矿池算力过于集中的情况，但首先矿池为了减少嫌疑，不再接受新的矿工加入矿池，其次有的矿工自动退出了矿池以获得矿池之间的平衡。

总之，这似乎是一种分布式、去中心、自组织的行为，是一种生态系统的自我调节，并不需要过于担心。

5、验证问题

记账人选出来了，记账人也很愿意记账，并且愿意诚实记账，但不是所有交易都是合理的，所以需要验证。转账发生后，支付者会把信息广播给所有节点，但现在的互联网节点之间的联系是通过 TCP/IP 协议，通过路由找最近的路径，所以并不是所有的节点同时获得信息。采用的做法是，收到信息的点再把收到的信息全部广播出去，这样就可以像瀑布一样，很快把 10 分钟以内的交易发送到所有节点。但是，各节点收到的交易并不相同，矿工只能把自己收到的交易打包形成一个区块，所以有的交易并不能及时被记录。

验证的内容主要是根据地址验证是否有足够的比特币用以支付即可，但比特币实现的方式要比这个复杂，主要是引入了脚本语言。付款时需要通过“签名脚本”确认资产的使用权，同时需要知道接收方的“赎回脚本”才能正确付款。普通用户恐怕无法直接记住并使用这些脚本。那么他们如何才能进行交易？为了简化日常使用的交易过程，核心开发者们引入了“比特币地址”这一概念。通过一些协议约定，使得各种类型的钱包软件可以用某种通用的方式自动推算出所需的的脚本。实际应用中，这些脚本是由钱包软件代替用户来实现的。核心开发者们约定了某种特定数据格式，以及由该格式的数据演算对应脚本的方法。

如果是乔姆的中央化的记账模式，似乎没有必要引入脚本语言来验证，把“赎回脚本”约定为公钥，把“签名脚本”约定为签名，就可以了。因为中心化的方式下，如果日后发现某种方式无法满足新的交易类型，或是发现某种方式存在安全隐患，那么推出一个升级包或补丁，或是另外发行一个新版本就可以解决。然而，去中心方式下就行不通了。某种协议一旦确定，任何变更都需要提前经过讨论并取得共识，除非问题简单到一目了然，并且只有唯一的解决方法，那么取得共识几乎是无法实现的。脚本的引进不仅为增加灵活性而已，还使智能合约成为可能。当然，比特币的脚本语言没有循环语句，这造成这样的脚本语言不是图灵完备的，但中本聪也是为了首个无政府货币系统能够成功，因为如果循环是死循环就会造成系统崩溃，而要避免崩溃就需要引入新的机制，这就增加了复杂性，可能会造成比特币流产。

6、区块链分叉问题

在争夺记账过程中，可能在某一小段时间产生了数个记账人，但由于网络通讯的滞后，某片区的节点跟着某一个记账人确认记录，而另一片区的节点跟着另一位记账人确认记录，所以会出现区块链分叉的情况。矿工面对这种情况都有自己的算法，一般可能会同时保存某几个记账人的区块链，直到某一个链远长于其它几个链时才删除那些较短的链。而交易者要确认自己的转账成功了，可能不止等 10 分钟。如果是小额的交易那到没问题，如果是大额交易一般要等六个区块即一个小时才可以确定交易被记录在案了。虽然大额交易对于全球转账系统要一两天完成交易已经算快了，小额交易，比如买杯咖啡要等 10 分钟都被认为是太长了。当然，中本聪是考虑到 2008 年时的网速及同步时间，出于谨慎的考虑，设计了 10 分钟的时间段。中本聪还限制了每个区块的大小只有 20 兆，这也是考虑到当时的网络速度能够承载的可以安全同步的数据量。区块的大小和结算的周期成了后来比特币想要升级的重要

的方面。

7、匿名机制问题

比特币里唯一识别的是私钥，通过私钥可以生成地址和公钥，通过地址和公钥就可以验证地址里是否有足够用于支付的钱，就可以进行验证，经过验证正确就可以产生交易了。所以比特币不认人的，只认私钥。

私钥是一串随机产生的由 256 位由 0 和 1 组成的二进制数，为了方便识别比特币中通过 Base58 编码将私钥转化成一串 32 位的字符串以便于人眼识别。

当然私钥就代表着比特币现金，一定要好好保存，一旦丢了就和丢了现金是类似的。如何保护私钥不丢失不被盗取，这也是一门技术活，很多人在想这方面的办法。

8、货币发行问题

比特币采用了凭空发行的办法。这成为了很多人感觉比特币神秘的原因，并且在比特币一路上扬后仍然认为这是一场骗局。但货币只是记账的符号而已，是黄金、纸币还是比特币并没有太大的区别，想明白这一点很有必要。

通过上面激励机制我们已经知道，货币发行被用于记账激励，或者说通过记账激励来发行比特币。从 2009 年 1 月开始，大约每 10 分钟会产生一个区块账页，并生成 50 个比特币，但大约每四年会减半激励，到 2016 年 7 月已经减半两次，现在的激励是每 10 分钟 12.5 个比特币。这个数量到 2040 年由于太小就停止发行了，届时由交易费提供激励。通过这样的发行方式会产生大约 2100 万枚比特币。

货币作为记账符号还要解决不能造假的问题，其实这就是避免重复使用的问题，即上述的双花问题。由于比特币有一个分布式的不可篡改的账本，比特币是没办法造假的。

（四）节点互信问题

1、 两军问题

现在看来比特币最重要的贡献不是发明了一种电子货币，而是它一举攻认为不可解的互联网节点间的相互信任问题，即拜占庭将军问题。因为分布式账本需要每过 10 分钟就进行同步，同步时使用的互联网多点通讯可能出现问题，有些节点可能会采用欺诈行为获得不当收益。如果把网络节点看成人、公司或国家，节点之间互信问题似乎是人类历史上的普通问题，需要信任才能搞定的事通常很麻烦，隐瞒、欺诈、胁迫甚至战争就是这样发生的，而种种策略和战略也围绕信任机制来展开，但有没有办法可以一劳永逸的解决这个人类合作时存在的痼疾呢？似乎中本聪找到了办法，或者说，至少是在分布式账本互信机制上中本聪的办法是很管用的。不过，在讨论多节点复杂网络的互信问题之前，我们先讨论一个比较简单的两节点互信问题。

如果比特币节点只有两个那没有必要采用分布式账本，只要两个人以物易物就可以了，但两个节点之间的通讯或信任问题是理解多节点通讯或信任的基础，所以我们从两节点通讯说起。

两军问题是计算机领域的一个思想实验，用来说明在通信的链路不可靠的情况下，试图通过通信以达成双方意见一致存在缺陷和困难，也有些学者称之为“两军悖论”、“两军难题”、“协同攻击问题”等。两军问题及其无解性证明 1975 年被首次提出，当时用来描述两个匪徒团伙之间的通信，在 1978 年有专家将这个问题命名为“两军问题”后才沿用至今。

两军问题是在计算机通信领域首个被证明无解的问题（虽然量子通信可能会解决此问题），由此也可以推出，随机通信失败条件下的“拜占庭将军问题”也同样无解。但这里的无解是指只采用“通信技术”，并没有考虑通过激励机制来解决。

两支军队，分别由两个将军领导，正在准备攻击一个坚固的城市。两支军队都驻扎在城市旁边的两个不同的山谷里。两军之间隔着第三个山谷，两个将军想要通讯的唯一方法就是

穿过第三个山谷传送信件。问题是，第三个山谷被城市的守卫军占据，并且经此传送的信件可能会被守卫军截获。

虽然两个将军商量好要同时对城市发起攻击，但是他们没有约定特定的攻击时间。为了保证取胜，他们必须同时发起攻击，否则任何单独发起攻击的军队都有可能全军覆没。他们必须互相通信来决定一个同时攻击时间，并且同意在那个时间发起攻击。两个将军彼此之间要知道另一个将军知道自己同意了作战计划。

比如将军 A1 收到将军 A2 的作战计划，并且同意了作战计划。这时 A1 将军会想 A2 是否知道信已经送到了呢。于是 A1 将同意作战计划的信发给将军 A2。但这时还有不确定性，因为接下来 A1 将军还是担心信没有送到，所以需要通知将军 A2 告诉对方自己已经同意了作战计划。将军 A2 收到信知道 A1 同意作战计划，但他也意识到 A1 并不知道自己是否收到了信，害怕自己发起进攻时 A1 犹豫不进攻，造成自己全军覆没，所以将军 A2 还需要在收到信息之后再发信息给 A1 表示已经知道了对方同意此次攻击。由于送出去的信容易丢失，这个怀疑还将无限循环下去，所以两军要达成对作战计划真正的统一是不可能的。不过，上述循环次数越多，可靠性应该越大，但问题的复杂性还在于通信还可能被敌军拦截和造假。

这个思想实验致力于考虑两军怎么做才能达成一致，而把两个将军替换成两个节点之间的通信算法，相应的问题也同样存在。所以，两点通信时就某个问题达成一致是无解的。

当然，可以用一些方法来减少不一致的发生的概率，但是没办法杜绝。一个解决两军问题实际可行的办法就是接受而非试图去消除通信信道的不可靠性，但是要将这种不可靠性降低到可以接受的程度，即转变成容错问题。例如，A 将军可以送出 100 个信使，并预期所有信使被抓的可能性是极低的。用了这种方法，A 将军无论如何都会发起攻击，B 将军只要收到一个信使的信，也会发起攻击。

一个类似的方法是，A 将军发起一连串消息，B 将军对每一个消息都返回一个应答消息。两个将军对每个返回的消息都感觉是充分的，比如，约定收到 4 个消息就发起进攻。

2、拜占庭将军问题

多节点信任机制其实是两军问题的扩展板，在分布式通讯领域中的大神级人物莱斯利·兰伯特的文章中用“拜占庭将军问题”这个大家容易理解的故事来描述这个问题，但实际上历史上并没有相应的事件。拜占庭将军问题也不是要解决网络通讯时的完全一致的问题，因为从两军问题看，这是无解的，只能解决某些经典问题要能达成能够容忍多少通讯错误，所以这个问题又称为拜占庭容错问题。

拜占庭将军问题的故事有各种版本，故事中有多支规模比较小的军队的将军们，比如有十支，他们需要大多数人达成一致，以决定在某一个时间同时攻击某一支规模比较大的敌军。在故事中这些小军队可以理解成小城邦，敌军可以看成是一个比较富有的大城邦，小城邦分布在大城邦周围。大城邦很是富有，而且强大，对小城邦构成持续的威胁。同时小城邦也很是垂涎大城邦的财富，想攻而分之。

问题是这些将军在地理上是分隔开来的，必须要通讯兵在中间送信，但信不一定能送到。另一个严重的问题是，将军中存在叛徒。叛徒为了达成目的可谓不择手段，他们可以通过欺骗某些将军采取进攻行动，或者误导大家促成一个不是所有将军都同意的决定，又或者迷惑某些将军使他们无法做出决定等来达成目的。但是大城邦墙高壁厚，如果小于 6 个将军展开进攻，进攻就会面临失败，而且自己的城邦还可能被别的没有参战的城邦给攻占了。但只要有 6 个及以上的将军同时进攻就可以成功，如何才能在地理阻隔的情况下，通过通讯兵达成大部分在进入时间上的致呢？这就是拜占庭将军问题的主要内容。

拜占庭假设是对网络通讯的现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机网络的通讯可能出现不可预料的行为。所谓拜占庭失效指一方向另一方发送消息，另一方没有收到，或者收到了错误的信息的情形。

拜占庭容错协议就是为了解决这些问题而制定，并且这些协议还要满足所要解决的问题要求的规范。很多经典算法问题只有在错误小于通信进程总数的三分之一时才有解。这对于比特币似乎是不能接受的。

3、比特币如何解决拜占庭将军问题

传统的做法是，为了使十个城邦中至少六个达成一致，所有的城邦将同时派出骑马的通信兵送信，每个城邦派出九个通信兵，那就有 90 个通信兵，每条信息都包含类似如下的内容：“我将在 10 月 4 日早上 6 点发起进攻，你愿意加入吗？”。

如果收信人同意了，他们就会在原信上附上一份签名了的/认证了的/盖了图章的/验证了的回应，然后把新合并了的信息的拷贝再次发送给九个邻居，要求他们也如此这样做。最后的目标是，通过在原始信息链上盖上他们所有十个人的图章，让他们在时间上达成共识。最后的结果是，会有一个盖有十个同意同一时间的图章信息链最先产生，而其它只包含部分图章的信息链将被抛弃。

但是，问题在于如果每个城邦向其他九个城邦派出一名信使，那么每个城市将分别收到九个写着不同的进攻时间的信息。除此以外，部分城邦会答应超过一个的攻击时间，还存在故意背叛发信人，不断重新广播过程中这个系统迅速变得矛盾且不可信了。

比特币采用的办法是从所有将军中随机选出一个将军，并且给这个将军成本和奖励以增加这个将军造假的机会成本，这就保证在一个时间只有一个城邦可以进行广播，而且这个城邦不太可能造假。比特币加入的成本是解决一个难题的“工作量证明”，而奖励是每次发行的比特币。

我们想像拜占庭将军系统里，这些将军每次随机产生一个将军将信送出，而且给这个将军大量的奖励，这个将军就不太会造假。而且，如果大家对一次通信不太信任，可以再次随机产生一位将军，将上次广播的信息再次广播给大家，大家再次核对是一致的，就容易就某个时间进行进攻达成一致。由于每次是随机产生的，将军数量越多，广播次数越多，信息可靠性越高。

当然在线下情景下如何随机产生一个送信将军会是一个问题，但在线上情景就容易了，大家一起解一个难题，谁选解出来就把信息和难题的答案发给大家就可以了。由于难题虽然难解，但容易验证，大家很容易搞明白这个发信人是不是真正解出了难题。

比特币通讯系统在节点很多的情况下是很健壮的，不容易受到攻击。要能攻击，需要 50%以上的计算能力，而且由于解题能力除了拼算力还带有随机性，即便如此也不能保证每次获得记账权。但即便是 50%的容错力已经大大高于拜占庭将军三分之一的容错了。而且如果一个系统 50%以上的节点都叛变了，还能认为是“叛变”吗？分明是一半以上的将军已经不想再进攻了。所以比特币系统实际上是解决了拜占庭将军问题。

另外，在比特币的情景下，造假也是有限度的，即只有私钥才能运用货币的情况下，造假也只能针对自己的钱进行造假，而且造假的限度也不能高于自己所有的钱，造假的方式主要是“双重支付”，但双重支付其实是容易被验证的，所以要保障双重支付不被发现。由于比特币是每 10 分钟进行一次记账，而且每个区块都加盖了时间戳，所以要达成双重支付实际上需要随便篡改总账的能力，即回到 51%攻击的问题上，而要达成 51%攻击是很难的，而且有这样的攻击能力最好的选择是获得比特币记账奖励而不是双重支付。

最后，这一对于拜占庭将军问题的解决方案，可以推广到任何核心问题是在分布式网络上缺乏信任的领域。人们意识到，在系统中添加一个简单的时间延迟，随机产生一个广播节点，同时使用公钥加密算法以验证每笔交易，可以解决这个问题。

这是一个重大的突破，这是互联网走向分布式的开始，分布式账本已经可在改变整个金融领域，未来还会产生分布式的域名系统、分布式的投票系统、分布式单纯的文件分享系统等，比特币解决方案和协议才刚刚打开洪水的闸门。

（五）比特币系统的特点

比特币实际上是多种已经存在的技术的改进和组装，而其中最重要的技术至少包括不对称加密机制、网络通信同步及容错机制、货币经济原理和自由货币发行机制、基于博弈论的共识和激励机制，最后当然包括计算机编程技术。除了这个特点外，至少包括以下特点：

一是去中心化和节点平等。比特币不需要中心机构的系统，任何一个节点的损坏，不会影响整个系统的运行，所以没办法关闭该系统。这是比特币系统最大的特点。任何中心化的节点，总有被攻破的那天，但比特币运行了八年，没有一次被攻破，也没有记错过一笔帐。

二是共识机制和开源。由于是分布式的，每个节点是平等的，所以需要一套逻辑让大家相信，这就是共识机制。要达成共识机制就需要先有白皮书，然后将软件开源，这样愿意参与的就是形成共识的。这些共识包括很多方面，愿意接受比特币，同意其记账机制等。

三是高度透明和匿名机制。比特币系统里的每一笔交易都可以看到的，这是为了能够验证每笔交易。但交易信息又不能和个人身份信息联系到一起，所以他同时采用了匿名机制。

四是不可篡改和无需信任。这个系统采用加密算法，比较高的容错机制来防止攻击，所以基本是不可篡改的，这使系统不需要建立在人与人的信任基础上，只要相信背后的密码数学和计算机通讯机制就可以了。

三、迅速发展

（一）比特币大事记

1、项目启动

加密货币的许多尝试都失败了。2008 年 10 月 31 号纽约时间下午 2 点 10 分，一个自称中本聪的用户在一个密码邮件组说他研究出一个新的数码现金系统，这完全是点对点的，无需任何可信的第三方，并在邮件中给出了比特币的白皮书，实际上是一篇名为“Bitcoin：A Peer -to-peer Electronic Cash System”的论文。这篇仅 9 页的论文中留了一个邮箱，可以看到邮箱是以 bitcoin.org 结尾的。这说明中本聪写论文时已经注册网站了。

2009 年 1 月 3 号他就挖出了第 0 号区块，即创始区块，获得第一笔 50 个比特币的奖励，之后和芬尼又调试了五天，然后比特币软件就算正式启动了。到现在一直运行了超过八年，没有出现任何问题。

任何人都可以在网络上免费下载代码，并作为一个矿工开始运行它。社区的人们通过下载软件并运行，投入时间和计算能力，而所有这些运行的节点就是比特币币系统。保持软件运行的人们就构成了愿意为这个事业付出的比特币社区。

最开始，社区缓慢地在密码界和各种在线论坛扩展，可以说整个 2009 年下载仍然寥寥无几。中本聪设立 bitcoin.org 论坛每月吸引几十名新用户。他们大部是被新的和有趣的想法吸引的程序员，其中有些是很严肃对待这个开源项目的。

其中一个住在马萨诸塞阿默斯特的程序员，名叫加文·安德烈森，他在 2010 年 5 月浏览一篇关于开源软件项目的文章时偶然发现比特币。在被激起兴趣后，他持怀疑态度的本性使他严肃的核查起整个项目。起初，他认为这是不可能的工作。但是在他读了聪的白皮书，阅读了开源代码，又读了一些介绍文章后，他说明了自己，认为这是个靠谱的项目，于是他下载程序并且运行它以确定软件是不是某种会感染他的电脑的讨厌病毒。最后，他确定软件可以按要求运行，然后他在 5 月 28 日注册为比特币论坛用户，成为比特币社区的一员。

这位毕业于普林斯顿大学曾工作于马萨诸塞州阿姆赫斯特大学的程序员就此迷上了比特币。2010 年下半年，他建立了一个名为“比特币龙头”的网站，这是他的第一个比特币相关项目，当时也很有名。加文向每个访问者发放 5 个比特币。他在早期的比特币交易市场之

一的“比特币市场”买了万枚比特币，花了 50 美元，并把他们全部分发出去了，其目的是增加使用量，扩大了社区，并夯实货币。之后，他开始向中本聪提交代码，以优化比特币的核心系统。他成为比特币的核心开发人员，负责开发了中本聪的多个项目，并且出席众多会议宣传比特币项目。中本聪逐渐对加文的代码信赖有加。最终有一天，中本聪问加文是否可以把他的邮件放在比特币的主页上，他同意了。从此，中本聪退到了幕后，加文变成了这个项目的领导者。他现在已经是比特币基金会首席科学家，也是比特币社区的仲裁者和架构师，同时负责协调比特币核心程序的优化。

图 1.6 比特币基金会首席科学家：加文·安德烈森

2、第一笔交易

在比特币软件开始运行之后，了解比特币的人越来越多，陆陆续续有人从网站上下载并运行比特币程序。大家相互帮助开发出了不同操作系统的程序版本，中本聪也常常亲自作答。由于每个节点都是平等的，所以都有机会获得每 10 分钟 50 个的记账奖励。由于比特币可以在无需中介的情况下点对点转账，所以也有人开始使用比特币进行交易了。

第一次转账发生在最开始调试时，由中本聪在 2009 年 1 月 12 日转给芬尼 10 个比特币，虽然我想说“这是人类货币史上最值得注意的一次转账”，但在那个时候到是波澜不惊的，就像两个大孩子在玩过家家。但第一次购买商品，现在看来真有点惊世骇俗了。

那位有名的发现基于 GPU 开采比特币的程序员名叫拉兹洛.哈涅克斯，事实证明，哈涅克斯对比特币发展的贡献并不止于发现新的挖矿方法，还因为他促成了第一笔比特币商品交易，使比特币从概念走向现实。

这个佛罗里达州杰克逊维尔市的程序员使用 GPU 方法比一般计算机节点获得比特币的概率高了约 800 倍，当时开采的人可能也就几百名，所以大部分比特币都被他赚去了。他唯一苦恼的是不知道拿这些比特币怎么办。

他想破了脑子，才想到一个点子。他在 5 月 18 日在比特币论坛发贴说，“我将付一万比特币买一些比萨饼，也许是两人吃的大小，这样我可以留一些第二天吃。”那个论坛当时只有大约两百多名会员。没有理由认为任何人同意他。当时也从来没有人在现实生活中使用比特币。当然，在佛罗里达州也没有比萨饼店会接受比特币付款。

哈涅克斯为了吃到披萨饼也颇费周折。他想到了需要一个中间人。当时比特币市场价格大约是一万个比特币 41 美元，哈涅克斯想吃的两个披萨饼大约值 25 美元，他考虑多出来的钱可以补偿他给中间人带来的麻烦。

三天后，一个聊天论坛上名为 jercos 的英格兰的比特币用户挺身而出。Jercos 在网上向

在杰克逊维尔市的棒约翰定购了比萨饼，并在网上用信用卡进行了支付。不久之后，送货员派给哈涅克斯的住处送来了两个比萨饼，并满脸疑惑地说，“新鲜的披萨饼……来自伦敦的。”

哈涅克斯把披萨饼的图片传到了网上，并且从他自己的比特币钱包向在英国的收款人传送了比特币。这是比特币进行商品购买的第一次，虽然过程颇费周折。根据当前的价格，就算每个比特币 5000 块钱吧，这位叫哈涅克斯先生用了 5000 万人民币买了两块披萨饼。真可谓是世界上最贵的披萨饼了。

我们善良的吃瓜群众肯定开始心疼哈涅克斯了，可是我要说的是，因为这些披萨很美味，拉丝勒此后又买了三次，总共花了 40000 个比特币。事实上，他后来接受《纽约时报》时说，“在那时比特币不像是可以值这么多钱，所以那时用比特币能买到披萨是一件很酷的事。”

事实上，回到当时，虽然比特币软件运行一年多了，人们对比特币能做什么，并不确定。比如，在 2010 年 3 月，一个绰号“吸烟太厉害”（SmokeTooMuch）的早期社区成员在网站上以 50 元起拍卖一万个比特币，却无人还价。

哈涅克斯在买了一次披萨饼之后想，他搞清楚一件事，如果他能挖到足够比特币使他一个星期得到一个披萨，这也是不错的。于是他又买了三次披萨饼，但他很快发现他的机器很难再挖出什么比特币了。GPU 挖矿和披萨饼购买事件对社区触动很大，很快有人跟进使用 GPU 进行挖矿，哈涅克斯的优势很快就丧失了。事实上比特币的争夺越来越厉害，一个星期后，难度飙升到如此之高，一般人已经挖不到矿了。他曾经一个月获得几万的硬币，但很快只能一天挖到一个比特币了，而他已经把比特币都用来买棒约翰的比萨饼了。早期参与者的好运气也就此用尽了。

3、社区更加活跃

比特币社区越来越大。自从发现可以用 GPU 挖矿后，比特币挖矿也越来越难。比特币价格也越来越高，就在披萨事件的次年的 2 月 9 日，比特币价格首次达 1 美元。就在同一个月就有人想到用比特币进行匿名黑市交易，这就是后来非常有名的丝绸之路网站，不过，这家网站万万没有想到美国联邦调查局一开始就注意到这家网站并且派了卧底开始混迹在这家网站。

围绕比特币的配套服务也逐渐发展起来。比特币与英镑、巴西币、波兰币的互兑交易平台先后开张了。但是比特币创业还处于拓荒的早期，一家在 2011 年年初成立的叫门头沟的交易所到 7 月份竟然处理了 80%的比特币交易，要知道这是一个由个人创建的很不规范的网站，在 6 月份就有人发现他们的账户在网站上消失，但事实上，人们并没有太多的选择，只能相信该网站。虽然这次危机很快平息了，但这家网站在 2014 年却因为出现大规模的比特币“丢失”而关闭。

2011 年 8 月提供比特币转账服务的比特速递公司（BitInstant）成立，随后提供支付处理服务的比特付公司和比特基地公司也出现了。关注的人越来越多，2011 年 9 月《比特币杂志》的创立标志着比特币社区进一步走向成熟。

顺便提一句，杂志创始人 Vitalik Buterin（中文名字：维维）是后来著名的以太坊项目的创建者。这位俄国裔的加拿大人在 2011 年通过比特币第一次发现了区块链和加密货币技术，为这一技术的潜力感到兴奋和着迷，当年他才 17 岁。在 2011 年 9 月就与朋友联合创建了《比特币杂志》。他在随后的两年半时间内研究了现有的区块链技术和尚未被创建出的区块链应用，在 2013 年 11 月写出了以太坊白皮书，短短时间就筹集到 1.5 亿美金，可谓区块链创业史上的一段佳话。维维相当聪明，他经常参加中国的区块链会议，并用很短的时间学会了中文，其中文水平似乎是可以在会议问答环节比较自如的使用中文了。他在《比特币杂志》上大量发表文章，他似乎涉猎很广，其文章除了讨论技术之外也涉及到经济政治等方方面面，为比特币的推广立下汗马功劳。

图 1.7 以太坊创始人维维

2011 年夏天位于西雅图的孵化器比特币实验室公司（Coinlab）成立了，说明已经有草根风投注意到比特币了，到 2012 年已经有大约 2000 万美金的风投了，但是比特币要受到风险投资的严肃对待还要等到 2013 年，那是比特币飞速上涨的一年，风投的确不可能不关注到。

2012 年中期赌博网站聪的骰子成立，比特币创业进入拓荒的中期。2012 年 12 月 6 日，世界首家官方认可的比特币交易所——法国比特币中央交易所诞生。

4、跌宕起伏的 2013 年

2013 年是比特币大力开疆扩土的一年，也是比特币的多事之秋。政府首先注意到这种虚拟货币的价格正在疯狂上涨，同年三月底，按市值换算成美元后，全部发行比特币总值已经突破 10 亿美元。在 3 月份，美财政部金融犯罪执法系统也及时发布《虚拟货币个人管理条例》。2013 年 4 月 10 日，比特币价格已经从年初 13 美元上涨到 266 美元。当年最高价甚至到了 1242 美元，虽然年末回落到 811 美元，但当年上涨了 60 倍以上。除了美国外，其它国家也纷纷出来表态。德国表示支持，出台政策给持有比特币一年以上的人免税，俄国、泰国则禁止比特币交易。中国可能意识到没办法禁止比特币，虽然认为这是金融科技的一部分，除了禁止银行系统参与外，并没有采取其它禁止措施。

2013 年还发生一件有意思的事，当年 7 月有一对克雷格夫夫妇的实验，想要从 7 月 23 日开始仅用比特币生活三个月。

故事的男主角克雷格夫做企业宣传片的，妻子贝希是一个图形艺术家。他们既不是程序员或也不是企业家，当然也不是密码朋克。所以，他们应该不是说客。

克雷格夫在 2011 年听说了比特币后，对比特币背后的文化吸引了，在向贝希求婚后，他建议在他们蜜月后要进行一个实验——他们将在 90 天里只使用比特币生活，并拍摄整个事件的纪录片。这是克雷格夫一时兴起的提议，但令他吃惊的是，贝希欣然接受了挑战。

他们真是“臭味相投”，他们似乎觉得挑战还不够，克雷格夫妇增加了难度，他们决定开车横跨美国，然后飞往欧洲、亚洲，最后再飞回犹他，而他们在这一环游世界的旅程中的每一个阶段仅使用比特币付款。

他们虽然发起了一项名为 Kickstarter 的电影基金，并且募集了 72000 美元，并聘请了摄制组，但他们的想法放在 2013 年年中还是太不切实际了，因为当时几乎没有企业接受比特币，其实大多数商家根本没有听说过。他们采取的办法是不断的说明人们接受比特币。他们一开始还很不熟练，但他们很快完善自己的说词，实际上成为比特币布道者。那些杂货店老板、房东、披萨店等，他们在付款时会说，“我们能用比特币付款吗？”对方问用什么时，他们就给对方解释起来。当他们向他解释了比特币卡和信用卡之间的费用差异时，对方就同

意了。另外，在他们行程的每一站，在美国和海外，他们都会遇到至少一位比特币信徒想要向他们伸出援手。

最后，到 11 月 2 号克雷格夫妇仅靠比特币存活了 101 天。他们证明，虽然不方便，这个在五年前仅是中本聪一个人的项目，已经如雨后春笋般发展到一个全球性的社区，其成员已经能够形成一个没有中央权威的密切联系的社区。不管人们是否认可比特币，假装比特币不存在，不认为它是一种货币，但在这个社区里，他们已经像我们假想的读者乌托邦一样，有了自己的分布式账本和可以信任的记账符号了。只要社区存在，比特币就不会灭亡，只要社区扩大，比特币就会壮大。类似比特币的山寨币也是同样的情况，只要有人相信，有社区存在，货币就不会灭亡。当然，社区不存在了，货币也就灭亡了。

顺便补充一下，比特币的确演变为一种文化现象，而克雷格夫妇也成为文化名人。人们没有为信用卡写歌，也没有为贝宝写歌，但约翰•巴雷特在他东田纳西州纳什维尔的一个工作室录制的歌曲《咏聪》中这样唱到：“哦，比特币，我知道你会统御，将会统御……直到每个人都知道，每个人都知道，直到每个人都知道你的名字。”劳拉.撒格斯写了名为《一万比特币》的爱情歌曲。YTCracker 创作了《比特币男爵》的说唱歌曲。还有其它一些。

与此同时，德国艺术家久野乡田画了一幅《200 比特币》的画，画布上比特币标志重复出现了 200 次，安迪•沃霍尔排了《200 张一美元钞票》的戏剧，加利福尼亚戴夫.金受到多利安.中本聪的故事的启发，画了一幅他在他的草坪面对媒体的大规模绘画。他为其取名“免费的午餐”。LA 摄影师梅根•米勒做了一系列的作品展示在日常生活中比特币。

就在克雷格夫妇全球比特币布道般旅行的时候，美国政府也没有闲着，就在 10 月 2 日美国联邦调查局执法人员关闭了丝绸之路，这个又被称为“暗网”的网上毒品交易市场，同时逮捕了该网站涉嫌人罗斯威廉 • 乌布利希。丝绸之路网站用户的超过 26000 枚比特币被查封，此外还有 144000 多枚比特币是从据称是乌布利希的地址查获的。受此消息影响比特币的汇率从 141.93 美元开始在接下来的几天之里跌到 110 美元。

就在克雷格夫妇回到家刚过一周，美国政府机构坐下来听取包括比特币在内的虚拟货币的积极与消极之处的讨论，多个证人为比特币贴上了“合法”的标签，认为它能够在金融行业产生“深刻的变革”。批评者则普遍认为，比特币可以用来洗钱。但听证会对此毫不含糊地指出，“现金仍是洗钱的最好方式”，而在进行大规模的犯罪用途中用虚拟货币来洗钱的情况实际上十分鲜见。在听证会的积极影响下，比特币的价格达到了一枚 900 美元的历史新高。

虽然 2013 年里比特币社区张开双臂试图拥抱中国市场，却只能眼睁睁看着中国的人民银行发布通告，禁止中国的银行和支付与直接或间接参与比特币的兑换交易。比特币在 12 月 5 日比特币在中国央行的通告后大跌，到 18 日在门头沟的价格降到最低 455 美元而在中国则曾经降到了 2011 元人民币（约 330 美元）。而这一年最高记录仅是人行通造几天前的 11 月 29 日创下的，即 1242 美元，这到现在都还没有突破。

但是，2013 年 Blockchain.info，这个最流行的网络比特币钱包，声称到 2013 年年底钱包数量将达到近 100 万个。同时 Coinbase 也有 18,000 个商户和 732,000 个钱包，而 BitPay 拥有超过 12,000 个商户签署了这项服务。泡沫是人性使然，但只要社区扩大，比特币就在扩大地盘。

2013 年的确是比特币充满戏剧性的一年，也是突飞猛进的一年。

5、稳步发展的 2014 和 2015 年

2014 年则要理性反省的一年，看起来有些缺乏生气，但却是暗流涌动。

一方面，泡沫继续磨灭。14 年 2 月门头沟的倒闭使得比特币的价格严重下滑，从高峰值 951.39 美元跌至 309.87 美元，跌幅高达 67%。

另一方面除了大量增加的小企业接受比特币外，像微软和戴尔这样的大品牌商支持比特

币支付，更是扩大了比特币的接受范围。经过 2013 年的折腾，关注的人大增，比特币自动取款机的数量增长也很快。虽然价格大跌，但这一年比特币总交易量比 2013 年增长了 50%以上。风险投资在 2014 年已经累计到 4.33 亿美元，是 13 年的 3 倍。12 年也才两千万美元，到 13 年就到了 1 亿美元，到 14 年更是跃升到 3.35 亿美元。14 年的风投数额已经超过了早期对因特网的投资。接受风投的国家从 13 年的 8 个增长为 14 年的 18 个，新增的国家包括：日本、荷兰、巴拿马、丹麦、卢森堡、瑞典、德国、印度、墨西哥、阿根廷。与 13 年相比，14 年风投加大了对交易平台、支付处理、矿业、金融服务和钱包的投资。实际上，人们不仅关注比特币，也注意到背后的区块链技术。

进入 15 年后，比特币可以说是，步上正轨了。虽然这一年开局不利，其价格进入新年的不到两周时间内就已下跌约 13%，从 320 美元下跌至 278 美元左右。但先抑后扬，年终收盘上涨了 40%。但 2015 比特币最大的收获不是价格上涨，而是使用人数和交易量，还有风投资金的上升。风险投资超过 5 亿美元。当然，这一年已经有一些比特币创业公司开始倒闭，这证明这个行业不是一路高歌猛进，而是有进有退的良性迭代。另外，也有很多投资投向区块链创业公司，币圈和链圈开始分化。比特币总市值达到 70 亿美金，按 GDP 算已经排到了 2015 年全球各国的第 66 名，超过了 150 个国家。

实际上，2015 年的确很多政府对比特币表示了支持。新泽西州为数字货币创业提供税收的减免以及相关的激励措施。美国加利福尼亚州使比特币在内的其他数字货币在该州成为合法货币。纽约 BitLicense 试图创建一种全新的技术许可比特币和其他虚拟货币公司在该州的运营，在 8 月份开始生效。美国美国商品交易委员会在 9 月份最终为比特币定性，认为比特币是商品。美国证券交易委员会将挖矿合同定性为证券。另外，香港表示比特币不需要监管，可见香港有让自己成为全球知名的数字货币中心的想法。欧盟法院裁定比特币不应该征收增值税。英国财政部决定通过反洗钱（AML）监管标准对数字货币进行监管。

6、乘胜追击的 2016 年

经过 2014 和 2015 年的默默高速和稳步发展，比特币在 2016 年迎来一波反弹行情，以人民币计算，1 月最低价 2300 元到年底已经是 6791 元，美元标价则以 968.23 美元收官，是年初价格的近三倍。这一方面是因为比特币受到更多人理解和支持，另一方面也是因为这是全球动荡的一年。政府公信力缺失，让更多民众意识到用区块链技术保障个人财产不可侵犯的重要性。比特币一定程度表现出了类似黄金的避险属性。。

6 月 24 日，英国脱欧公投结果揭晓，超过半数民众支持脱离欧盟，英国首相卡梅伦也宣布辞职。英镑跳水，比特币价格应声上涨，涨幅近 20%，价格稳定在 4300 元上下。

11 月 9 日，随着美国大选选票统计结果不断出炉，多种资产创下英国退欧以来的最大振幅，而比特币毫无意外的大幅上涨，接近人民币 5000 元。原因是市场普遍认为，围绕特朗普政策提案的不确定性将推动避险资产的价格。

11 月 8 日，印度总理纳伦德拉•莫迪宣布，废除分别相当于约 7.5 美元和 15 美元的面值为 500 卢比和 1000 卢比的纸币。随后，这一“废钞”规则又经历了一系列变动。首次宣布“废钞”时，莫迪强调主要是为了切断恐怖主义的资金来源。之后他又强调，此举更多是为了追回逃税的黑钱，后又改口称，是为了鼓励印度人更多地使用数字支付。印度前总理辛格批评这是一场“合法抢劫”。取现难的印度人民开始寻求替代资产，一时间印度比特币一币难求，价格也超出国际市场价格近 10%。无独有偶，委内瑞拉废除了 100 元面额的玻利瓦尔纸币，发行 6 种更大面额的新纸币。澳大利亚政府和印尼似乎也有 “废钞”打算。而一枚比特币的价格，已从 11 月初的 4800 元人民币，到年终的 6800 人民币上下。短短不到两月，涨幅超 40%。除此以外，人民币的不断贬值和外汇管制给比特币市场带来了强大的需求，比特币价格水涨船高。

2016 年除了价格上扬外，监管也逐渐上了轨道。日本金融厅比特币将其定义为商品，

韩国金融监管机构成立数字货币工作小组进行比特币交易所的监管，澳大利亚税务局将比特币定义为“无形资产”而不是货币，俄罗斯放弃实施比特币禁令。对比特币来说，监管并不是一件坏事，监管在一定程度上意味着“承认”。在 2017 年，相信有更多监管政策实施，数字货币社区将实现更为良性的发展。

融资虽然可能不及 2015 年，但 ICO 方式融资则颇为火爆，可以被称为 ICO 元年。2016 年前九个月中，区块链和比特币初创公司在 92 起融资事件中共募集 4.92 亿美元。按照这个速度，2016 年投资交易活动将比 2015 有所下降。与之相反的，2016 多个项目通过 ICO 方式获得融资。ICO 的说法来源于 IPO，为数字货币社区特有。这种方式主要是数字货币和区块链项目向早期爱好者出售项目代币，项目团队将通过 ICO 获取的资金用于开发和拓展市场。

2016 年仅 TheDAO 就通过 ICO 获得 1.5 亿美元的众筹，WAVES、Lisk、国内项目小蚁、领萌宝、元界等都成功完成了 ICO，也随之诞生了一批区块链众筹平台，国外包括 bnktothefuture，国内有币众筹、云币网、ICO365。

2016 年还是区块链茁壮成长的一年。各种国际机构纷纷组成各种联盟，发布白皮书，各种会议也突然如雨后春笋般冒起来。各机构纷纷申请区块链相关的专利，这显示大家对待区块链是认真的，这也有利于区块链生态的建立。虽然这一年以太坊由于智能合约漏洞遭受黑客攻击，但这一最大的区块链项目经受住了考验，算是区块链诞生初期难免的阵痛。这一年还发生了一个重要的事件，即一月份中国央行行长周小川表示要研究区块链发行人民币，一时众说纷纭，但却成功调动机国内各种机构的研究热情。由于链圈发展与币圈会有所不同，虽然 2016 年区块链项目大多还处于概念验证阶段的探路阶段，但是随着链圈生态的逐渐完善，相信 2017 年会在概念落地上有一定的突破。

（二）比特币淘金

1、早期采矿阶段

讨论比特币不能不说一说比特币采矿。2009 年 1 月 8 号开始，比特币软件就稳定的开始运行了，以每 10 分钟 50 个的速度产生比特币。中本聪在芬兰的服务器是节点一号，而芬尼的个人电脑是节点二号。虽然芬尼很快退出了比特币网络，但并没有给比特币带来什么影响，因为陆陆续续有人加入到比特币的开采行列中。

中本聪的 bitcoin.org 网站有聊天频道，每个月有几十人注册使用，到 10 月份开通了以编程为主要聊天内容的 bitcion-dev 聊天频道，11 月份以“比特币论坛”（Bitcoin Forum）命名的聊天论坛就正式成立了。比特币用户的社区正在形成。

每当一个新人将自己的计算机登录比特币网络，它就增加用于争夺比特币记账权的总的计算能力，也增加了总耗电量，这也意味着开采新一批 50 枚硬币的竞争加强了，同时每个计算机节点获得新币的机会下降了。随着时间的推移，为了保持在大约每 10 分钟产生一位记账人，核心程序会自动增加数学难题的困难。这是为了使增加的总算力并不会造成比特币过早发行。

这一时期大家还只是被这一新事物吸引，没有太多人认为比特币是真正的货币，所以没有特别的动力去改进挖矿的设备。在那时用大型主机来采矿一定会被认为是疯子吧。可以说这个时期还处于概念验证阶段，参与人以是尝鲜为主。

在采矿的同时，大家开始在网站上讨论比特币与美元的汇率。由于开采比特币需要使用计算机计算难题以争夺每 10 分钟的发行，这是需要耗电的，所以在 2009 年 10 月，有人张贴上在一个称为“新自由标准”的新闻网站上一个基于开采的电力成本计算的汇率，是 1 比特币值得 0.08 美分。虽然有人认为新自由标准定得有点高，但至少有了一个可供参考的价值。

比特币立即表现出波动性，11 月 13 日价格跃升 70％，至 0.14 美分，12 月又急跌至 0.06

美分。由于交易的标的都不大，这给交易者带来一些乐趣。另外，由于社区仍然较小，还没有人想使使用自己的电脑在解数学谜题上打败所有其他人，所以这一阶段电费支出在矿工之间是比较公平的。

2、GPU 采矿阶段

原始采矿阶段的公平在新的一年改变了。在佛罗里达州一位名叫拉兹洛.哈涅克斯软件工程师想到，他可以编一个程序用他的电脑显卡（或 GPU）接管 CPU 来解比特币的哈希难题。这个方法是他的电脑解决数学难题的能力成倍增加，增加的倍数可能达到 800 倍，让他在本来不大的社区里获得每批 50 个比特币的机会也成倍增加了。

2010 年之前基本是 CPU 在挖矿，全网算力一直在每秒 1G 哈希以下，2011 开始显卡加入挖矿大军，下半年全网算力一举突破每秒 10T 哈希，一年增长了 10000 倍，第二年算力继续快速增长，显卡矿机迎来了全盛时期。

不用说，这很快引起了很多人的关注。尽管每个比特币的价值如此小，越来越多的社区开始相信它的升值潜力巨大。正当比特币核心软件升级为更强大的 0.2 版本时，比较正规的名为“比特币市场”比特币交易市场成立了，有消息称那个叫汗涅克斯的家伙搞到很多比特币，就好象 100 多年前加州萨特磨坊的淘金热一样，社区的人们眼红得不得了，新的淘金者也迅速加入。当然，军备竞赛也随即展开。

人们纷纷把装有显卡的家用电脑用于开采这个神秘但已经有市场交易价格的数字货币，这很快变得不是社区爱好者的行为，而变成一种商业行为，而一旦商业机构开始加入比特币淘金热，大量吞噬电子的专用矿机也就开动起来，比特币核心软件不断调整难题以平衡货币发行节奏。随着事情变得更加疯狂，技术社区里这些行事古怪的密码朋克和程序员们立刻被挤掉了，商人们成为拥抱数字淘金的新阶层。

随着价格一路上扬，采矿变得越来越专业化。2013 年 1 月比特币价格很快达到 100 元人民币，接下来以每月翻倍的态势发展，虽然中间有大跌，但在年末就突破了 7000 元，以美元表示首次超过 1000 美元。2013 年之后虽然发生了一系列负面事件使价格一路走低，但并没有给这个产业带来严重的打击，2015 年之后又慢慢走强，到 2016 年年末价格再次突破 1000 美元。

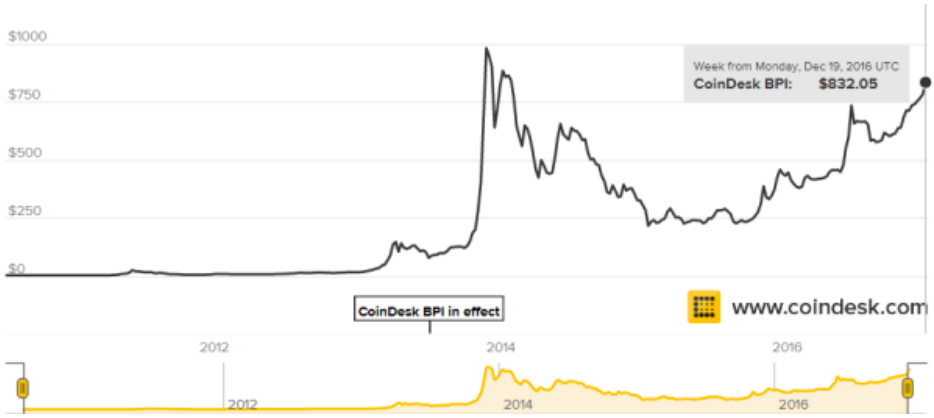

图 1.8 比特币价格

随着价格的疯狂走势，采矿产业链很快形成，而产业利润则很快摊薄。

早在 2012 年 12 月第一家名为“臭名昭著的蝴蝶”专门目的集成电路（ASIC）的矿机厂商就诞生。这是一家来自美国的团队，其商业模式很快被中国公司拷贝，青出于蓝而胜于蓝，市场也很快被中国公司占领了。蝴蝶是以期货形式销售产品的，它成立后就宣布将于 2013 年 3 月份陆续发货，同时开始接受预订，价格极具诱惑力，在当时的难度下 3 天内即可回本，在短期内便吸引了上万个订单的投资，而实际上蝴蝶在 2013 年 7 月才开始小规模出货，从而导致大规模的退款潮，虽然到 9 月份发货规模加大，直到 2014 年 1 月才完成所有订单

的发货，但在当时算力环境下，蝴蝶已经成为废铁。蝴蝶一度成为骗子的代名词，这对期货矿机市场造成了不良影响。

美国市场算是搞砸了，而中国则开始疯狂。在蝴蝶刚发货的 2013 年 3 月份就出现了全球第一台现货矿机，即西瓜 FPGA 矿机。但是，由于性价比并不高，加之当时国内挖矿者寥寥可数，到 5 月就无疾而终，出货量不到 200 台。终结的原因很简单，随着挖矿难度的增加，生产成本已远超挖矿所得。接下来几个月产品像走马灯， 2013 年 5 月南瓜张开发的南瓜机开始在淘宝销售，由于当月下旬央视首次播放了比特币相关的新闻，南瓜机很受市场欢迎，但比特币挖矿难度随之提高，到 2013 年 6 月份，烤猫推出了 USB 矿机后南瓜机就被淘汰。而从 2013 年 7 月开始，矿机就进入百花争鸣的季节，大量 ASIC 矿机如雨后春笋般出现，接下来的 5 个月，每月算力增长平均达到 30%以上。同年 7 月还有部分矿机商发明了一种新玩法，即算力出租，以每 G 算力定价多少钱出租给客户，但随着难度提高，这种模式随着客户的觉醒最终流产。

当年 8 月份，南瓜张团队设计出一种专门挖矿的叫“阿瓦隆”的矿机开始在淘宝上销售。这种机器插上电线和网线，设置好比特币账号就可以挖矿了。当然，这种机器只能用于比特币挖矿。随着当年比特币价格一路上扬，市场还出现了贝壳、蚂蚁、花园、夏级等，阿瓦隆也不断升级。矿机产业越来越专门化，购买矿机的人并不需要接触到矿机，直接委托相关机构代管即可，大量矿机放在一些服务器托管中心，就形成了矿区。为了节约电费，甚至有机构把矿区设在了四川的山区的小水电附近，那里电费便宜，气温较低，较节约空调费。这个行业已经完全走上专业化。后来出现其它山寨币之后，比如莱特币，矿机供应商也提供这些货币的挖矿机。购买专业矿机的人们为了增加获得比特币记账权的可能性还把自己的机器与其它机器联合在一起，形成可以并行计算的“矿池”。

图 1.9 比特币矿区

不知道中本聪对正在发生的一切会不会感到惊讶，我想应该是惊得合不拢嘴了，一切已

经与他的关系不大了。他是在庆祝还是在哀伤他所缔造的这一切？我们不得而知。一年后，他就从比特币世界消失了。

（三）比特币灰色面

1、黑市交易：丝绸之路

比特币神秘难懂，糗事迭出，很多人，稍一提起，抵触之情，溢于言表。说了那么多光明伟岸，也让我们正视比特币的灰色面。比特币相关的负面新闻影响最大的是比特币用于黑市交易，其次是与比特币交易所有关的，还有拷贝比特币的山寨币有关的犯罪，最后也有人利用比特币进行庞氏欺骗的。庞氏骗局比较简单，例如特伦顿.希维尔斯（Trendon Shavers）通过被称为比特币储蓄信托（Bitcoin Savings and Trust，BCS&T）的投资服务来欺诈投资者，筹集了 764000 个比特币（在当时价值 450 万美元）。希维尔斯承诺了一个每周 7%的夸张回报，那么一年下来总共就可以获得 36 倍的回报。这种欺骗只要是不那么贪婪是比较容易识破的，这与其它币种的庞氏骗局没有什么不同，但与加密货币特性相关的犯罪则对比特币的声誉影响比较大，这里主要举将比特币用于黑市的丝绸之路、作为比特币交易所的门头沟和拷贝比特币源代码相关的山寨币的三个故事一探究竟。

由于比特币的点对点转账特性和匿名特性，将比特币用于黑市交易的应该是有的，其中被查获，而且影响也特别大的是丝绸之路电子商务网站。这其实是一家地下网站。有人认为能够用搜索引擎搜到的网络实际上是冰山一角，还有很多被称为暗黑网络或暗网的地下网站。暗网则隐藏在深层网络里面，同样不能被搜索引擎搜到，但与深网又有重大区别：暗网由主动想保持匿名的人和网站组成，其用户用加密软件隐藏自己。除非使用类似洋葱路由技术的浏览器，否则几乎不可能看到它。比特币被用于这方面的交易也是可以理解的。

2013 年 10 月 2 日，FBI 高调宣布，他们在旧金山逮捕了一个名叫罗斯.威廉姆斯.乌布利希（Ross William Ulbricht）的人。罗斯当时年方 29 岁，住旧金山，毕业于德州大学物理学系，曾在宾州攻读学位，没有前科，素来默默无闻。

让我们看看罗斯是怎么想到用比特币犯罪的。罗斯其实是个聪明而且有想像力的人。他生长在德克萨斯的奥斯汀，家庭非常和睦。他天资聪慧，经常会冒出一些很惊人的想法，虽然没自私学习，但 SAT 考得很好。高中毕业后德州大学主修物理学，虽然成绩出色，但是他厌倦了实验室枯燥的工作。随后他去了滨州州立大学攻读硕士，专业是晶体学，但他不想从事学术研究，并对经济学产生了浓厚的兴趣，他对政府干预市场的态度是无情的蔑视。另外他在大学期间就开始体验迷幻剂，阅读东方哲学，还自学了编程。在参加了一个集体鼓乐俱乐部，在这里他认识了正在读大学的朱丽叶.维（Julia Vie）。还做了一个水晶戒指给她。两个很快相爱。

2009 年获得硕士学位以后，他回到了奥斯汀，并给朱丽叶买了一张机票，让他过来同自己一起生活。朱丽叶离开大学，同他一起住进了一间很狭小的房子，但是他们并不觉得艰苦，还幻想着结婚的生活呢。但是，乌布利希做生意、开公司都不成功。他和朱丽叶也渐渐产生了分歧，分分合合数次。2010 年他发现比特币后谋生了建立基于比特币的地下网站的想法，和许多自由意志主义者一样，他相信毒品的使用与否只是个人选择，想把丝绸之路是一个毒品交易市场，但没有货源，于是决定先自主研发一种毒品。

2011 年 1 月中旬，“丝绸之路”（Silk Road）的网站诞生，它利用比特币进行非法买卖的匿名黑市，由于采用了一种“洋葱路由”（Tor）的技术，让追踪变得更加困难。没多久罗斯自主研制的 10 磅毒品就卖完了，网站上也陆续有毒品商入驻，并在不久之后网站上各类商家也在日益增长。许多边缘人群，很快意识到了它的超级安全性，放心大胆的在“丝绸之路”网站上开始进行各种非法买卖。丝路网上 70%左右的交易都和毒品有关，剩下的 30%是黑枪、盗取的信用卡用户资料、色情服务、黑客服务、悬赏暗杀等违法交易，甚至还包括一些

儿童色情作品。

网站发展很快，但也很快被美国缉毒局、国安局和联邦调查局盯上，都想尽快拿下它。他们扮成商家和顾客，还联系到丝绸之路站长代号为邪恶海盗罗伯茨（Dread Pirate Roberts），简称 DPR，即罗斯，与其讨论网站经营和网站投资，在近两年的时间里建立了良好的“信誉”。办案人员也对网站管理员有了一些了解。

他们通过不知什么方法找到了在冰岛的服务器，并侵入分析“丝绸之路”建立之初的数据，怀疑叫“奥托伊德”（Altoid）的用户是网站创始人，因为他曾在一个比特币论坛里发帖招聘技术人员，而这时网络上第一次有人提到了“丝绸之路”网站。这个帖子留下的电子信箱“rossulbricht@gmail.com”，成为了追查工作的起点。通过谷歌公司的配合了解到该账号是通过一家位于旧金山一家咖啡店的电脑建立的。

通过线下调查很快缩小了嫌疑人范围，其中就包括乌布利希。随即，乌布利希的所有网络通讯都被秘密监控起来。接下来进入收集证据的阶段。

乌布利希收取每笔交易额的 8%～15%作为佣金，日子渐渐富足。到网站关闭时，它的用户超过 100 万，交易总额保守估计超过 10 亿美元。罗斯这下致富了，赚了上亿美元。但他不敢露富，在租来的房子过着简朴的生活。挣钱不错，但乌布利希经常把丝绸之路当成一个政治行为，经常在 网上发出“丝绸之路远非买卖毒品那么简单，它是要夺回我们的自由、我们的尊严和追求公正”的申明。

乌布利希的成功带来隐瞒供应商和卖家的身份的挑战，在 2013 年三四月间当他被人威胁要求 50 万美元的封口费，否则就透露一些供应商和卖家的身份。在 7 月份时，乌布利希终于忍受不了，在网站上买凶杀人，并且在网站上寻购伪造护照。护照很快收到，照片都是乌布利希本人，制作精良，简直就是以假乱真——和他联系的卖家，其实是国土安全部的探员。乌布利希的嫌疑陡然上升，FBI 推测他正在做外逃的准备。

很快杀手也找到了，原来是卧底探员立即毛遂自荐。乌布利希告诉该“杀手”，某人敲诈了他一大笔钱，威胁说不给钱就公布他的真实身份，所以，他想找人“折磨”、“杀死”这个用户。讨价还价之后，双方敲定了报酬是 15 万美元，以比特币支付，做掉该用户后拍照为证。卧底探员把他们之间的交谈作为证据固定下来，并且很快实施逮捕。

收网行动定在 2013 年 10 月 1 日，在一家公共图书馆，趁着 乌布利希打开自己电脑输入密码登录后，探员迅速实施抓捕。

在此之前乌布利希表现得不像毒品犯或地下王国的首领，或许更像一个哲学家，一个有抱负、懂科学的自由主义者。

“我已经挥霍了我的青春，我知道你必须夺走我的中年，但是我恳求你让我安度晚年，”他写道，“请在无尽的黑暗隧道的尽头为我预留一盏明灯吧，为了我的健康，为了在漫长服刑之后能够梦想更好的生活，请给予我一丁点宽恕吧，也为了在去造物主那里报到之前能够在自由的世界完成自我救赎，请给予我一个机会吧。”

但是主审法官福瑞斯特拒绝承认丝绸之路是一个幼稚的实验，或者是年轻时候犯的错误。“它是一个精心策划的生活作品，”她说，“你希望它成为你的遗迹，是的，它就是你的遗迹。”

最终，在 2015 年 5 月，年轻的乌布利希被判处终身监禁，证据包括探员钓鱼的聊天记录、毒贩、谋杀等。

或许丝绸之路网站的发展给其它暗网启示，发明更加安全的暗网交易模式，但这并不是比特币的错，技术发展从来是这样，方便了生活，也可能方便犯罪，但后者不是主要方面。同时，打击犯罪也需要更加先进的技术，最好的办法不是指责和限制技术而是使用更先进的技术来防止犯罪。

2、平台倒闭：门头沟

实际上交易所倒闭的事情经常发生，这有几个原因：一是经营不善，宣布停止营业；二

是当地监管太严，银行不愿意合作；三是被黑客攻击；四是被骗。第四种负面影响最大，而出现较早，影响最大的要属比特币交易网站门头沟的倒闭了。这一事件让多少比特币热心人心凉，又让多少发财梦惊醒啊。

14 年 2 月 10 日，中国人刚过大年初十，那些手持比特币的人一定在为下午六点三刻位于日本的全球知名比特币交易平台门头沟发生的离奇事件心惊不已。比特币交易在盘中惊现 6000 个单位的抛盘，引起比特币交易价格在盘中数秒内一度跌幅高达八成，从逾 600 美元直接跌至最低的 102 美元，而在很快时间内，比特币的价格出现了快速反弹。这一惊情造成比特币价格 K 线图出现一条长长的下影线。

虽有“专家”猜测这只是一次乌龙指，但谁曾想到两周后的 25 号门头沟网站就永久关闭了，并且 28 号就申请破产，并且承认该公司在 24 号发现被黑客盗取 85 万个比特币和银行账号上的 2740 万美元，在当时总计价值约 5 亿美元，已经严重资不抵债。被盗比特币包括客户的 75 万个比特币和公司自己持有的 10 万个，当时约占全球比特币发行量的 7%，当时价值价值 4.73 亿美元。虽然在次月 7 号承认找回 20 万“冷保存”的比特币，但大部分用户损失惨重。

部分投资人在 Mt.Gox 的办公室外高举“门头沟，我们的钱到哪里去了？”，和“门头沟，你是不是破产了？”的抗议标语。然而并无甚用。

虽然有黑客声称此次事件是网者所有者卡佩勒斯等人自编自导，也有调查报告显示丢失的比特币是从 2011 年开始逐渐被偷走的，但真相至今扑朔迷离。

比特币交易网站 Mt. Gox（业内俗称“门头沟[3]”）由杰德. 麦凯莱布（Jed McCaleb）创建于 2010 年 7 月，起初想做游戏卡交易网站，但是很快决定改做比特币交易所。虽然网站很快火了起来，但是也让创始人觉得难以应付，于是他把 88%的股权卖给了马克.卡普勒斯（Mark Karpeles）。

创始人麦凯莱布的确很忙，他是一位连续创业者。在加州大学伯克利分校退学后，在 2000 年就创建了当时很大的 p2p 文件分享网络 eDonkey，12 年又与克里斯·拉尔森共同创立了 Opencoin 公司并随后推出后来极为成功的瑞波币。2014 年他兴趣再改，转而独立创建恒星币。后来接受采访问当问及他为什么卖掉门头沟时，他说：“门头沟很酷，也被市场所需要，但是它在技术上缺乏挑战，我没有长期经营它的兴趣。“看来，麦凯莱布很有极客风范，真乃有为青年。

但门头沟的继任者就逊色很多了。虽然在继任者卡普勒斯任内，门头沟一度为世界上最大的比特币交易所，截至 2013 年，该交易所处理了全球约 70%的交易，通过每笔 0.25%到 0.6%的交易费，该公司已经赚取了约 10 万比特币，当时价值 5000 万美元。但这更多是运气使然。

卡普勒斯，法国人，2009 年，年仅 24 岁就只身赴日。然而，让人意想不到的是，在收购门头沟之前，他本应该在家乡法国服牢役。2010 年，他因为欺诈指控在缺席的情况下被判监禁一年。来自法国的法庭文件显示，卡普勒斯在法国还有一起民事和非民事未决诉讼等着他。除了一年监禁外，他还欠 4.5 万欧元。起诉卡普勒斯的原告是他的前雇主，他被控偷窃客户的用户名、密码和域名。他选择逃到日本据说是喜欢日本动漫，但也可能是喜欢日本女人，因为他在日本和一日本女人结婚，还育有一子，在此期间日本知名媒体《读卖新闻》还曾报道他涉嫌挪用交易所的钱去嫖妓。

[3] 即 Mt.Gox，“门头沟”是业内俗称。至于为什么业内这么称呼，可能首先是因为两者音很接近（读做：Mount Go），其次可能是极客聚集的北京恰好有一个区叫门头沟区，说起来顺口，也有一些调侃意味，就此流行开了。英文名的来源也有些绕。原创始人 Jed McCaleb 创建 Mt.Gox 网站本来是一个魔法风云会线上买卖交易平台，其命名源于魔法风云会英文名称（Magic: The Gathering Online eXchange）的首字母略缩字。

图 1.10 门头沟控制人马克.卡普勒斯

其实，在门头沟申请破产前，他在日本遭到过客户的起诉，原告称支付了 1.5 万欧元建网站但网站从来没帮人家建成，东京地区法院裁决他归还客户的钱。

门头沟申请破产后，该公司声称，资金失踪归咎于一个软件缺陷，然后卡普勒斯就声称因为没有个人律师，然后就玩失踪了。

面对这样的大事件，虽然日本金融主管机关宣称虚拟货币不在管辖范围，但东京警视厅展开对他的调查，并在 2015 年 8 月 1 日以篡改系统数据虚报自身现金账户余额涉嫌非法制作并使用私人电磁记录为由逮捕了他。警视厅称，2013 年 2 月门头沟交易系统中卡普勒斯的美元账户的数据被两次改动，现金余额虚报了共计 100 万美元。卡普勒斯可能用虚报的现金购买了比特币，他还可能虚报了自身比特币账户的余额。警方正在加紧调查取证，而能进入公司服务器和数据库对余额进行违规操作的只有作为系统管理者的卡普勒斯一人。

实际上门头沟前员工表示，门头沟管理相当混乱。卡普勒斯是个 PHP 程序员，热爱编程，也是个吃货。在接手门头沟后，他很快重写了网站的后端软件，最终让它变成了世界上最具人气的比特币交易所。网站在 2011 年 6 月就曾被黑客攻击，损失数百万美元，并且下线数日之久。但是卡普勒斯并未隐瞒此事，而是以坦率的态度在比特币领域赢得了良好声誉。

在 2013 年比特币从年初 13 美元飙升至逾 1200 美元之际，卡普勒斯也身价暴涨，卡普勒斯也成了比特币领域举足轻重的“大腕”，还资助了“比特币基金会”（Bitcoin Foudation）5000 个比特币，并且成为了这个非营利性比特币软件开发及游说组织的董事会成员。

门头沟总部在东京涩谷边上的现代化办公楼里占据了 3 层楼，卡普勒斯喜欢被赞美、喜欢被称为“比特币之王”，而且经常炫耀他是门萨（Mensa，一个面向高智商人群的国际化俱乐部组织）会员这件事。但是门头沟的管理相当业余。门头沟根本不使用任何“版本控制软件”，也就意味着任何程序员都有可能覆盖掉其同事在同一文件中编写的代码，而且软件改动都是未经测试就直接向顾客推出了——这种情况在专业金融服务网站上不可能出现。

内部人士称卡普勒斯意识到安全问题，但并没有重视，而是把时间用在开比特币咖啡馆、修理服务器、搭建网络和安装设备等这些琐事上。

此外，有一个不可忽视的事件是，只有卡普勒斯掌握着网站源代码的改动大权，修复漏洞甚至解决安全问题动辄需要花费数周时间，一切都要等卡普勒斯说了算。这里面是否隐藏着什么秘密，到现在一直不得而知。

管理的混乱让门头沟到了 2013 年秋季已经一团糟，一度停止提现，全球排名也跌至第三。2013 年 7 月份，日本最大、最受尊重的信用评级机构帝国征信公司对门头沟的评估是 D4，是这个规模的公司所能得到的最糟糕评级。

卡普勒斯在 2016 年 7 月保释出狱，但必须呆在日本。刚刚出狱他就通过推特嘲笑比特

币社区的无能，讽刺他们对区块容量问题无能为力。年过三十，虽然历经波折，仍霸气不减啊。或许其底气来源于他仍然持有那些丢失的比特币，谁知道呢？

在比特币世界里，已经发生过很多次类似的危机：比特币期货矿机不发货事件、GBL 跑路事件、比特币曾经最大的两家股票交易所 BTCT 和 Bitfunder 的倒闭事件，比特币钱包监守自盗事件……但从后来发生的情况来看，比特币的境遇似乎越来越正规了，这似乎是野蛮生长的新生赖特难免的阵痛。

3、山寨币困局：狗币

除了交易所的野蛮生长造成不少问题之外，由于很容易将比特币的开放原代码略加修改然后取个新名字就可以将新的一种货币“招摇上市”，有比特币在前，新的山塞币也层出不穷，不免鱼目混珠。越是假的币越是到处兜售，什么珍宝币、唯卡币，名字又炫，简直真假难辩。

只能看是不是在真正挖矿，有没有技术突破，有没有程序员或者极客跟进，有多大热度等等。如果打着新币的幌子，很容易变成传销、圈钱，类似卖出提成，发展下线之类的，这就肯定是假的。甚至人许诺一个月给多少个点的利息的，那就是旁氏类型的骗局了。

2016 年央视紧急宣布有 350 个资金盘全是骗局，其中大多打着加密货币的幌子，真是智商税一波未平一波又起啊。

当然，有些货币可能也不一定一开始是有理想的，但挣扎着，活不下来，被错认为是骗局了。比如，唯卡币煞有介事，到底是真是假，还很难断定，但除了比特币，其它货币如果没有特别的创新，生存空间真的很小了，但这不是一般人能判断的。

在央视的列表里，狗狗币（Dogecoin）也被认为是骗局，但这个货币一开始虽然因为一个玩笑而生，但的确不是骗局。这个币 2017 年 1 月初的排名大约是 15 名，市值约 800 万美元。这也说明是否是骗局真的很难分辨，不过狗狗币社区的确也出现过犯法的事。不过，我们还是从头说起。

狗狗币或狗币，又音译为多吉币，在华人圈又有一个可爱而且吉利的名字“旺旺币”。这种山寨币开始于澳大利亚品牌与市场营销专家比利•马库斯和澳大利亚品牌与市场营销专家杰克逊•帕尔默在 2013 年 12 月的一个笑话。

先解释一下词源。“神烦狗”是从一个网络流行词，在 2005 年以木偶表演的形式出现在 YouTube 上，视频中木偶将狗（dog）拼错了，拼成 doge，另一个也发音错发成“多吉”（dohj）。实际上是一种日本柴犬。

2013 年 11 月，正是比特币大出风头的月份，在 Adobe 公司悉尼市场部门的杰克逊•帕尔默一直在研究电子货币，看了 Doge 后突发奇想，在 Twitter 发了个推文：投资 Dogecoin，这就是下一个大机遇。随后不久他得到了不少回复，都是鼓励他继续完成这个想法。而一个礼拜后他买下了 Dogecoin.com 的域名，该域名被 Doge 的大本营 reddit 收录。其一出生，就带着强烈的搞笑和吐槽色彩。是 Doge 的爆炸式审美情趣被延续到了货币。总之，我们只要知道有美国人觉得很搞笑就可以了。

而与此同时，在波特兰的比利•马库斯一直想创造属于自己的电子货币，他希望这种货币能够满足更多人的需求，而不是像比特币那样为投机者服务。在 Dogecoin.com 刚注册没两天，他偶然知道了这个网站，顿时觉得找到了归属。于是他给帕尔默发了条推文，表达合作之意。在帕尔默回复之前，他就开始重新排列比特币的源代码，并加入了 Doge 文化元素。后来两人一拍即合，在帕尔默半开玩笑的推文发布后一周左右，Dogecoin 诞生了。

狗币很重视宣传，发布第一天，其官网、钱包、数个专用矿池、Block Explorer、官方博客、论坛、Wiki、新手指南等就一同发布了，甚至还开了狗币赌场，准备充分，配套完善，几乎没有虚拟币在发布之初就如此完备，很多虚拟币一开始就一张帖子、一个钱包而已。

在其软件方面，多吉币借用了一些莱特币的创始人查理.李的想法，他曾调整采矿系统，以使矿工们不那么相互竞争。另外，多吉币可以挖最多 1000 亿个。基于 Scrypt 算法，交易

过程比比特币更加便捷，狗币一个确认时间只要 1 分钟。

一开始很多人想用多加密货币给小费，但比特币太贵，大家就想到了用多吉币。但更重要的是，多吉币的有趣性，以及他专用于慈善的定位。

2014 年当它的价格在加密货币市场上升时，对多吉币的兴趣上升了，它可以与比特币交换，然后可以再换成美元。这意味着多吉币有了真正的价值，因此，可以用来为一些事筹集资金。多吉币基金会的一个成员了解到牙买加雪橇队缺乏参加 2014 年奥运会的旅途资金，就提出为其筹集资金。通过在 Reddit 及其他地方的活动，并指示把多吉币转到哪个钱包，他们很快筹集到等值 25,000 美元的比特币。接下来，有人建议清理为肯尼亚的水井筹资。他们为肯尼亚水井筹集到 30,000 美元。他们也为英国曼彻斯特一家咖啡店筹资。多吉币赵是做慈善项目，人们就越喜欢。

在大约四个月的时间里，社区获得数千成员。他们的激情和热情，已经捧红了他们的品牌，使其从一个笑话一跃变成是一个相对合理的加密货币。

但狗币社区也发生了一些犯法事件，而且给社区的生态带来严重破坏，甚至创始人帕尔默在 2014 年因此离开了社区，并声称这个社区已经变成“邪教”。

2014 年当时他 27 岁的英国人莱恩.肯尼迪（Ryan Kennedy）开始用化名 Alex Green 出现在狗币社区，他很快创建了狗币的交易平台 Moolah，收购了另一个交易平台 Mintpal，并将两者合并，但不久后 Moolah 申请破产了。他被指控拿了 Moolah 用户价值 140 万美元的加密货币，声称 Mintpal 被盗损失 200 万美元后，也被控告从狗币社区盗取了约合 28.5 万美元的 750 个比特币。这些指控还在审时，他在 2016 年 2 月被控与 14 起犯罪指控，其中 11 起是强奸罪。在 2016 年 8 月，其中三起强奸罪已经坐实，分别判 4 年、4 年和 3 年，一共 11 年。似乎有些轻，因为在英国一般要判 24 年。

如果盗窃罪不能宣判，莱恩可能在出狱后使用这些钱。比较理想的情况在，莱恩在押期间能够宣判，这样损失者可能可以挽回一些损失。

比特币的兴起，以及比特币开源的特性，让山寨币很快发展起来，他们有的打技术革新的牌，有的在推销上下功夫，有认真的，也有打着幌子的，也有开始认真后来蜕化的，自由发行私人货币的时代可能就是这样的，总有鱼目混珠，总有优胜劣汰，但不能因此就否定这种自由。或许这就是自由的代价。

（四）比特币的未来

比特币是一场社会实验，是有可能失败的。比特币的失败一定是社区的失败，即越来越小的人相信比特币了。这有点像是传说中靠着人类的信仰才能越来越强大的神。

有几种力量影响着社区的成长：

（1）有更成熟的加密货币或区块链法币系统推出，夺走了社区成员；

（2）大量国家规定比特币不能与法币兑换，因此不能提现；

（3）矿工收入越来越低，收费却越来越高，而且费用具有高度的不可预测性；

（4）容量太小，积压了大量请求，支付极其脆弱；

（5）处于某不确定的力量的控制之下，比如被中国矿工控制，而中国政府的防火墙及对矿工的政策带来不确定性；

（6）社区，特别是服务公司和开发维护成员出现持久内讧。

可能还有很多力量可能影响比特币未来，但以上力量单独都不太可能对比特币带来重创，但多条同时出现就会影响社区的信心。比如，容量太小、积压的请求太多，而社区在升级上出现内讧，问题迟迟得不到解决，在技术上更加有效的货币的出现，从而造成社员流失。

最大的问题可能是容量，现在每个区块理论上 1 兆的大小实在太小，只能执行每秒三到七笔的交易，这造成容量枯竭，但由于算力过于集中在少数矿工，而这些矿工对于升级是很

谨慎的，同时由于矿工主要在中国，而中国的防火墙使跨国转账带来很大的问题。中国现在的跨国连接速度刚好能支撑现在的转账容量，如果升级容量，对中国矿工的记账权争夺是不利的。另外，长远看，扩容受到网络通讯带宽的限制，所以比特币难以应付大量小额的交易请求。

不过，8 年来的稳定运行和价值的不断上升已经很有说明力了，至少在这段时间是很成功的。在未来尚未见到特别大的危机，扩容问题也应该可以解决，所以比特币还会保持壮大。

当然，比特币的特点使比特币并不适用所有的支付场景，容量小、算力高、转账时间偏长，这使小额支付可能逐渐变得成本较高，但对于大额转账则是比较好的选择。另外，比特币的这些特点使比特币还有其它的用途，比如利用比特币的交易脚本的信息备注段可以用于写入一些留作证据的信息，比如有人通过比特币写下结婚誓言并由婚姻双方数字签字确认。这说明比特币的区块链可能成为一种基础设施，而相关的应用可以嫁接在基础设施上。