区块链技术丛书

姜景锋 李 军◎编著

区块链技术的应用实践

Application Practice of Blockchain Technology

本书编著团队是国内区块链技术和应用领域的深度实践者

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书通过对数字货币的起源及区块链相关核心技术的介绍，使读者了解区块链技术发展的来龙去脉，并结合区块链的技术特点，论述了区块链技术在具体应用过程中需要注意的优势和劣势，以期让读者能够透过晦涩难懂的技术概念来真正了解区块链技术的本质。而目前区块链技术还不是万能的，在实际的区块链技术应用过程中，不是所有的问题都能够通过区块链技术来解决。因此，作者结合以往的项目经验，总结了若干个区块链技术的应用场景，向读者介绍如何将区块链技术应用到这些场景中，区块链在这些场景中解决了哪些问题，在场景中应用区块链技术时还需要注意哪些问题。最终目的是希望读者通过阅读本书能够对区块链技术有所了解和认知。

图书在版编目(CIP)数据

区块链技术的应用实践 / 姜景锋，李军编著. -- 北京 ：北京邮电大学出版社，2020.7
ISBN 978-7-5635-6014-1

Ⅰ. ①区… Ⅱ. ①姜… ②李… Ⅲ. ①电子商务—支付方式—研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字(2020)第 046143 号

策划编辑：姚 顺 刘纳新 **责任编辑**：满志文 **封面设计**：柏拉图

出版发行：北京邮电大学出版社
社 址：北京市海淀区西土城路 10 号
邮政编码：100876
发 行 部：电话：010-62282185 传真：010-62283578
E-mail：publish@bupt.edu.cn
经 销：各地新华书店
印 刷：北京玺诚印务有限公司
开 本：720 mm×1 000 mm 1/16
印 张：13.75
字 数：200 千字
版 次：2020 年 7 月第 1 版
印 次：2020 年 7 月第 1 次印刷

ISBN 978-7-5635-6014-1 定价：45.00 元

区块链技术丛书

前 言

了解比特币是在2014年，当时听说有很多人挖币，有很多人炒币。我作为一名IT从业人员，带着本能的好奇心开始到处搜索比特币的信息，当时觉得比特币很不靠谱，像游戏里的虚拟资产一样，因此并没有太在意。

大约也是从那个时候，我加入了一家从事分布式数据库研发的公司，专门负责分布式数据库产品售前及方案设计的相关工作。彼时，国内正处于大规模去“IOE”热潮，各个国内IT厂商都希望借此机会能够将原有国外厂商所占有的市场份额分一杯羹出来。当时，在硬件层面，国产的服务器、存储等都已经是有一定竞争力的产品，可以在硬件搭建上以价格优势与国外产品进行比拼。但是，在数据库层面，由于其与操作系统、中间件、业务系统紧密耦合，客户一般不愿意冒风险下决心更换业务系统数据库。因此，在数据库应用领域，尤其是在政府、金融、电信、电力等行业，国产数据库都很难打入市场。而在互联网行业，由于对数据库的稳定性、性能要求不高，更多的是考虑易用性和成本，互联网企业往往采用开源免费的数据库作为应用支撑。另外，当时云计算开始兴起，很多互联网企业也开始尝试在云内部署维护数据库，进而降低采购运维成本。

所以，在那段时间，我的主要工作就是参与各种行业客户对我们数据产

品的 POC 测试，争取在测试过程中能够赢得客户的满意，获取订单。当时，我们主攻的方向是 OLAP 型数据库，也就是主要以数据分析为主要应用。这种类型的数据一般是查询操作多，删改操作少，主要数据来自生产数据库，通过如 ETL 工具获取保存数据，并对数据进行分析处理，供生产经营使用。OLAP 数据库的思想是通过大规模集群的方式将多个 PC 服务器连接到一起，实现对大规模数据的存储。另外一个重要的工作就是如何从大量的数据中，查询符合条件的数据，这牵扯如何存储数据，如何优化数据存储结构，如果网络中的数据节点宕机坏掉了如何保障系统业务正常运行并且数据不丢失等一系列问题。这当中就涉及在网络中如何保障数据的一致性、同步性等问题。而这些技术问题，其实跟区块链技术有很多相通的地方。

认识李军是在 2016 年 11 月的一个周末。那天在清华校园的一个礼堂里，中关村区块链产业联盟正在进行区块链技术应用大赛的路演及评奖。后来才了解到，那次大赛应该是国内最早一批区块链技术应用企业的展示。在午饭的间歇我跟李军进行了简单的沟通和交流，那天他上午刚完成项目路演的答辩，感觉有些疲倦，但还是向我介绍了区块链技术发展的情况以及对未来应用的畅想。当时我还自以为是地表达了对区块链技术的一些看法，但都被李军一一指正。自那时起，我开始对区块链技术产生了兴趣，并有幸于 2017 年 1 月加入布比从事区块链技术的研发和应用推广。

此时的布比已经在行业内声名赫然，应用区块链做了好几个案例，有一定的反响。但如何将区块链技术更广泛地应用，如何结合业务场景，发挥区块链技术的优势一直都是区块链应用落地的难题。区块链技术不单单是一项技术，而是已有的多个技术组合形成的解决方案。在应用的过程中，最大的难点不在于如何技术对接，而是在于如何找到客户的痛点，并结合区块链的特点解决问题。区块链不是万能的，不能解决所有的问题，甚至有些问题使用区块链技术反而更加复杂。另外，区块链项目往往是多方参与的，参与各方都有各种诉求，这就导致项目推进和落地的复杂度更大。因此在这个过程

中，我也在不断了解学习各个行业的情况和痛点，学习区块链技术的优势和劣势，学习如何发挥区块链优势，规避区块链劣势。这些过程也成为编写本书的主要内容。

本书分为9个章节，第1章主要介绍区块链技术发展过程，通过对整个过程的了解，使读者能够了解区块链技术发展的脉络；第2章主要介绍区块链的核心技术，通过对这些核心技术的介绍使读者了解区块链技术的本质，以及区块链是如何实现其宣称的特性的；第3章主要介绍应用区块链技术的一些原则性问题，这些也是我们在以往项目中总结出来的经验和教训；第4章到第9章主要介绍区块链具体应用的场景，这里有我们在工作中项目经验的积累，也有我们合作伙伴的真实案例，还有一些是对未来发展方向的判断。

总之，这本书算是对以往工作内容的总结和梳理，仅供各位读者批评指正。书中引用的内容在章末标明参考的文献，有些是从互联网上查询得来，无法获取原始出处，如有遗漏可与出版社及作者联系，我们会及时更正。

最后，由于区块链行业变化很快，书中的观点仅代表作者个人的看法，希望书中的内容能给您一定的启发。

姜景锋

目　录

CONTENTS

第 1 章　区块链技术的起源与演进 …… 1

第 2 章　区块链核心技术介绍 …… 33

第 3 章　如何应用区块链技术 …… 68

第 4 章　区块链应用场景——政务 …… 99

第 5 章　区块链应用场景——供应链金融 …… 121

第 6 章　区块链应用场景——保险 …… 147

第 7 章　区块链应用场景——物联网 …… 168

第 8 章　区块链技术在征信领域的应用 …… 183

第 9 章　区块链应用发展方向——5G 的应用 …… 201

第 1 章
区块链技术的起源与演进

1. 从比特币说起

2008 年北京奥运会开幕后一个多月，世界上多家金融机构纷纷倒闭、破产。其中的原因主要包括以下几点。

2008 年 9 月 15 日，美国第四大投资银行雷曼兄弟控股公司申请破产保护。

2008 年 9 月 15 日晚些时候，美国银行发表声明，愿意收购美国第三大投资银行美林公司。

2008 年 9 月 16 日，美国国际集团（AIG）提供 850 亿美元短期紧急贷款。这意味着美国政府出面接管了 AIG。

2008 年 9 月 21 日，在华尔街的投资银行接二连三地倒下后，美联储宣布：把仅有的最后两家投资银行，即高盛集团和摩根士丹利全部改为商业银行。这样就可以通过吸收存款来渡过难关了。

2008 年 10 月 3 日，布什政府签署了总额高达 7 000 亿美元的金融救市方案。

美国金融危机的爆发，使美国包括通用汽车、福特汽车、克莱斯勒三大汽车公司在内的实体经济受到巨大的打击，实体产业濒临破产危机。除此之外，美国金融海啸也波及全球，影响了全世界。

这其中，雷曼兄弟公司的倒闭被认为是具有标志性的事件。雷曼兄弟公司创建于 1850 年，是美国排名第四的投资银行。雷曼兄弟公司因其投资了次级抵押住房贷款产品从而造成了巨大的损失，其 2008 年 9 月 10 日公布的财报显示，雷曼兄弟公司第二季度损失了 39 亿美元，是它成立 158 年来单季度最大的损失，其股价较 2007 年年初下跌了 95%。

围绕着是否出手救援，美国政府内部发生了激烈的争执。美联储主席伯南克主张出手相助，他打比方说："如果你有一位邻居喜欢在床上抽烟，一不小心引燃了自己的房子，你可能会说，我不会帮他报警，让他的房子自己烧去吧，反正不关我的事。但如果你的房子是用木头建成的，又位于他房子的隔壁，你该怎么办？再假如整个城市的房子都是用木头造的，你又该怎么办呢？"而美国财长保尔森公开表示"见死不救"，他坚定地认为，"大而不倒"是一种无法接受的现象，美联储没有担保债务或是注资的权力，美国财政部也不会出手，在发生挤兑的过程中，给一个分崩离析的投资银行贷款是不会成功的。就这样，2008 年 9 月 15 日上午 10 点，由于所有潜在投资方均拒绝介入，雷曼兄弟公司向纽约南区美国破产法院申请破产保护。[①]

由此，因次级抵押贷款机构破产、投资基金被迫关闭、股市剧烈震荡引起的金融风暴，导致全球主要金融市场出现流动性不足的危机。美国作为世界上唯一的超级大国，其次贷危机的爆发瞬间就影响了全世界的金融中心以

① 吴晓波《激荡十年，鱼大水大》，伯南克和保尔森都出版了自传体的回忆录，详尽回顾金融海啸爆发时的决策场景。伯南克：《行动的勇气：金融风暴及其余波回忆录》（2016），保尔森：《峭壁边缘：拯救世界金融之路》（2010）

及一些周边国家，其范围已远远不是次贷危机方面，而是蔓延到整个金融行业。为了救市，美联储开始实施宽松的货币政策，即所谓的量化宽松货币政策，以提高整个市场的流动性，而这一系列事件的结果就是，美元开始大幅贬值。正是在这样的背景环境下，一个叫“比特币”的东西应运而生，并开始发展壮大。

2008 年 10 月 31 日，在一个包含密码学专家和爱好者的邮件列表里，大家收到了一个自称“Satoshi Nakamoto”，中文名“中本聪”的电子邮件。“中本聪”到目前为止，还无法确认是一个人还是一个组织，这个人的神秘色彩也给比特币带来了无限的想象空间。在这里，我们权且把“中本聪”当成一个不愿意公开个人身份的人（当然，在比特币运行的这些年里，经常有人宣称自己就是“中本聪”本人。由于早期只有“中本聪”自己挖矿，因此他持有大量的比特币，因此，想要证明自己是“中本聪”本人，只要对早期持有的比特币账户进行交易即可，但到目前为止，还没有人能以让人信服的证据证明自己是“中本聪”本人）。“中本聪”在该邮件中写道：“我一直在研究一个完全点对点的，无须任何可信第三方的新型电子现金系统。”并引导读者连接到一个在两个月前注册的网站，网站里能看到一个 9 页的 PDF 文档，“Bitcoin：A Peer-to-Peer Electronic Cash System”。这篇文章随着加密货币被广泛宣传后，也被奉为“加密货币世界里的圣经”。在这篇所谓比特币白皮书里，首次提到了“Bitcoin”，也就是“比特币”。“中本聪”结合已有的几种所谓数字货币的情况，如：b-money、HashCash 等，希望创建一个完全去中心化的货币系统，它不依赖于任何中央机构进行货币发行、交易结算、验证，能够通过去中心化的网络对交易的状态进行确认并达成共识。这种想法能够很好地解决分布式系统中双重支付的问题。在之前系统当中，双重支付一直都是分布式数字货币系统的弱点，从而导致不得不通过引入中央清算机构或系统来完成交易的确认和清算。

比特币白皮书（图 1-1）的内容不算很长，用配图、公式甚至代码解释了

这个所谓的“电子货币系统”原理。其中，很多内容还是非常晦涩难懂的，甚至有的内容在简单描述之后，就不了了之了。例如，“我们把电子货币定义为一个数字签名链，每一个所有者把币转给下一个人的时候，是通过将前一个交易的哈希值和下一个所有者的公钥进行数字签名，并把这些追加在币的后面。收款人可以通过验证数字签名来确认链的所有者。”如果不是从事计算机科学或者密码学相关专业的人看到这样的描述，肯定会是一头雾水，但在这里“中本聪”提出了一个数学方法，从而实现了点对点交易在没有第三方中介机构参与的情况下保证交易的可信。

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.

图 1-1　比特币白皮书

在这个关于加密的讨论社区里，很多都是密码朋克运动的成员，他们是一群对高科技极度狂热的分子，早在 20 世纪 90 年代就尝试使用密码技术对国家、社会、文化进行激进的影响。其中也包括维基解密的创始人朱利安·阿桑奇 (Julian Assange)。在阿桑奇通过维基解密网站公开美国政府加密文件后，美国政府对其进行封锁和制裁，后来，阿桑奇不得不宣称接受比特币

的资助，这在当时也算是对比特币推广和宣传起到了非常大的作用。

在那个时候，在那样的一个松散的极客技术社区里面，很多人是不相信“中本聪”设计的这套系统能够成功的。这源于这些极客天生的自傲及玩世不恭的态度。很多人认为没有理由相信“中本聪”设计的系统能够比之前的极客开发的系统更吸引人。没有人相信这样的系统能够支撑数以百万的交易。

“中本聪”并没有受到干扰，依然继续着自己的开发，偶尔会针对一些技术问题进行讨论。他的系统里包含两个最大的创新点：一是一个被称为“blockchain”的账本数据结构，这种数据结构能够实现交易的快速验证；二是一套虚拟货币的激励机制，这种机制能够鼓励人们贡献计算资源，帮助账本的记录和存储。“中本聪”认为，这两种方法能够保证系统的安全可靠，并能够抵抗黑客的攻击。

北京时间 2009-1-4 2：15：5（UTC：2009-1-3 18：15：05），“中本聪”上线自己的比特币系统，并通过自己的台式机作为第一个节点，“挖矿”产生了第一笔比特币。并在创世块留言写下“The Times 3/Jan/2009 Chancellor on brink of second bailout for banks”这句话正是泰晤士报当天的头版文章标题。当时正是英国的财政大臣达林被迫考虑第二次出手缓解银行危机的时刻。“中本聪”引用这句话，既是对该区块产生时间的说明，又是对金融危机中旧有金融体系的嘲讽。这里，“挖矿”这个名词是一种形象的比喻，因为比特币节点采用的是一种工作量证明的共识算法，当节点争夺到了记账权后，会给予一定的奖励，因此就将这种奖励机制形象地比喻成挖矿获得奖励。由于当时网络中没有其他的节点，也没有任何交易，他只能让自己的个人计算机不停地运行程序。可以说，这个时候的比特币网络是一个“中心化”的网络。而如今，比特币网络节点遍布世界各地，开采的计算难度不断加大，为了争夺记账权利甚至形成大的矿池。

按照程序的计算规则，最开始“挖矿”的奖励是每生成一个区块链产生 50 个比特币。在系统上线及随后的六天时间里，按照每 10 分钟产生一个区块

的生产方式，大概有 43 000 个比特币。这在现在是一笔价值不菲的资产，而在当时，只有“中本聪”一人拥有这些，且几乎没有什么价值。因此，他需要有更多的人加入这个网络中来。

在创建了比特币网络六天之后，“中本聪”在邮件列表中告诉大家，系统已经搭建完成。并宣布一个基于 P2P 网络并可以防止“双花”（重复消费）的电子现金系统可以使用了。在邮件中，他描述这个系统是“完全分布式的，无须服务器或者中心权威的”。

一个叫哈尔·芬尼（Hal Finney）的人成为了比特币的第二个使用者。当时，芬尼已经 53 岁了，是密码朋克运动的早期成员，他本人就有多种加密创新，包括匿名邮件转发器，可以在不透露发件人地址的情况下发送电子邮件。早在 2004 年，芬尼就已经发布过自己的电子货币系统，跟比特币一样，他的电子货币系统也采用的是“工作量证明”的方式。“工作量证明”机制是在 1997 年由英国密码学专家亚当·贝克（Adam Back）提出的，用来验证和量化整个加入网络节点所需要的计算处理能力。

在这样的背景下，芬尼对“中本聪”的系统很感兴趣，他们通过电子邮件相互交流、合作、分享。按照“中本聪”的指导，芬尼下载了比特币软件，创建了一个比特币钱包，并开始开采比特币。这样，他成为了第二个比特币网络节点。作为测试，“中本聪”转移了 10 枚比特币到芬尼的新钱包，芬尼成为了从别人那里收到比特币的第一人。

两人在早期的电子邮件交流中，没有任何个人信息的交互，没有透露任何的关于“中本聪”真实身份的细节。他们不断地进行系统测试、寻找 bug、更新代码、版本迭代。芬尼用他的计算机持续运行了一个星期左右开采比特币，最后得到了大约 1 000 个比特币。不知道具体什么原因他停掉了计算机，并再也没有开启过挖矿。10 个月后，芬尼被诊断出患有 ALS，肌萎缩性侧索硬化症。日常生活完全需要妻子和儿子帮助。2014 年 8 月，芬尼去世。此时，芬尼所拥有的比特币已经具有很高的价值，按照他的遗愿，妻子将他所拥有

的比特币资助了在亚利桑那州的一个工厂对其身体进行低温冷冻，并希望未来有一天能让他“起死回生”。

在 2009 年 2 月 11 日张贴在开发者论坛的帖子中，“中本聪”写道：“传统货币问题的根源在于其运行所要求的信用。央行必须被信任不会让货币贬值，但法定货币违背其信用的事在历史上比比皆是。银行必须在保存和以电子方式传送我们的钱方面被信任，但他们在信贷泡沫中将钱借出，而准备金仅占很小一部分。”在另一篇文章中，他又说道：“逃离央行管理货币的任意通货膨胀风险！”从这些只言片语中，我们能够发现，“中本聪”是一个对传统金融行业颇有怨言的人，他的比特币项目也是其对现有金融现象和环境的一种反抗。虽然我们没有证据证明 2008 年的金融危机到底对“中本聪”有多少影响，但从其发布比特币网络的时间点以及种种言论都能看出其设计比特币的初衷是一种变革，至于比特币的价值，在当时并没有那么重要。在比特币之前，从来没有一个加密货币系统或者是模型能够摆脱集中式的架构，没有了中央权威，如何让网络中的每个人彼此之间能够相互信任，相互合作呢？

“中本聪”通过两种方法解决这个问题。一种方法是他突破性地提出“区块链”总账数据结构。交易被安排为按时间顺序排列的数据块，赋予矿工们通过比较它们账户余额的历史总账以验证其内容的能力。一旦满足验证要求，通过创建下一个区块并将其链接到已经被验证的前块，以此承认这些数据被批准。验证和链接区块，然后接受每个新的区块作为在其事实上的共识。这能够有效地让任何人“重复消费”一枚比特币变得不可能。换言之，数字伪造的可能性被排除。在“中本聪”发表的比特币白皮书，以及在比特币刚开始运行的时候，应该没有人相信这套系统能够实现其既定的目标，但在其运行的这些年中，比特币经历了无数次的攻击，甚至各种软硬分叉，但它依然能够实现加密货币的基本属性要求，并且不经过第三方验证处理，应该说这是个奇迹。

另一种方法是其设计的采矿奖励模式，即得到了联网计算机的计算和存

储能力来维护比特币网络的总账。从而奠定了整个信任网络的基础。除此之外，还需要体现比特币的稀缺感，为比特币赋予内在的升值感觉。“中本聪”用比特币未来发行的时间表来解决这个问题。在第一个四年里，程序设置在每 10 分钟发行产生固定的 50 个比特币。在 2012 年年底降至 25 个，以此类推，大约每四年生成的比特币逐步减半。大约到 2140 年，所有的 2100 万个比特币将全部挖完。这种预先的减半设计使比特币具有了稀缺感，从而支持比特币价值，并激励矿工为其提供算力。他知道光靠减半的激励只是一个美好的愿景，不足以激励矿工为其持续提供算力，于是他设计了适度的交易费用，以弥补矿工提供的计算存储资源。随着时间的推移，矿工挖出的比特币越来越少，而交易费用将成为其主要的回报。

总之，通过这样的看起来简单而又优雅的设计，精巧地解决了一个分布式点对点的电子货币系统，并且是一个真正意义上的没有第三方参与，完全靠算法实现的信任传递网络。

在芬尼退出由他和“中本聪”在两个人形成的比特币网络后，比特币并没有受到太大的影响，因为其他极客很快就加入了这个系统的开发测试中。在整个 2009 年，这一系统吸引了愿意下载的新用户，并构成新的节点，用来管理网络和开采比特币。每当有新的节点加入，就增加了整个网络的计算能力，也增加了耗电量，也就意味着“挖矿难度”的增加。人们在通过挖矿获取比特币变得越来越难，在 2009 年 10 月，社区的一些人认为有必要提供以美元为基础的汇率，来计算比特币价格，其计算标准是基于开采的电力成本，当时的价格是 1 比特币值 0.08 美分。有些人认为对于这种毫无价值的虚拟货币来说，价格太贵了。但也有一些极客愿意为此花钱购买比特币，并相互买卖转让，像游戏一样乐此不疲。这一切都是社区自发的，看起来非常自治。

在 2010 年 12 月，比特币社区就有人呼吁维基解密接受比特币形式的捐赠。但“中本聪”却急了，过去，他发声或为了学术讨论，或自证“你们找的这个人不是我”，但那天，他却措辞强烈地回应道：

“不！别把它放在维基解密上！这个项目需要渐渐地成长，这样软件才能一路上保持强劲。我在此呼吁维基解密不要使用比特币！比特币还只是一个处于婴儿时期的小规模社区实验，你们带来的热度可能会在这个阶段毁了我们！”

“中本聪”的最后一次现身是在 2010 年 12 月 12 日，这是比特币历史上最重要的一天，当时甚至很少有人听说过比特币。这一天并未让当时的社区感到震惊，但其将成为自创世区块以来最关键的日子。就在这一天，“中本聪”在 Bitcointalk 上发表了最后一篇帖子，然后默默地离开了，从此再未出现在公开场合。就在一天之前，他还就维基解密（Wikileaks）通过比特币躲避 Visa 封杀的消息发表了以上的意见，他很反对这种做法：“比特币如果能在其他情况下得到这样的关注，那就太好了。维基解密已经捅了马蜂窝，蜂群正在朝我们扑来。”不知道当时“中本聪”是感受到了自身安全的威胁了，还是对比特币的未来产生了担忧，亦或是其他的想法，总之，在那之后他就从公众视野当中消失了。他将开发代码和建设网站的任务交给一个活跃的志愿者小组。也就是从那以后，比特币真正地实现了一种完全的去中心化的网络，在没有创建者的意见和思想建议下，一直通过社区的力量开发前进，直到今天。在这期间，比特币不依赖于任何某个人的意志，只依赖于完全透明的数学法则。

2011 年 6 月，维基解密终于还是在推特上宣布，愿意接受以比特币形式提供的匿名捐赠。原因是，这位世界上最大的“黑客”网站泄密了美国的重要保密函电，甚至包括时任美国国务卿的希拉里·克林顿的邮件，美国政府封杀了网站，并迫使 VISA 和万事达卡等支付公司对维基解密关闭支付通道。由于维基解密一半的资金来源依靠网络捐赠，美国政府这一举措一下就减少了网站 90%的资金来源。他们实在没有其他捐助渠道，不得不求助于比特币。维基解密当时收到的比特币捐赠价值大约 5 000 美元，也不算特别大的款项。

但六年后比特币暴涨，获益 500 倍，创始人阿桑奇后来还发推特感谢了美国政府。

随着比特币的币值从几美分涨到了几百美元，大批的传媒行业加入了报道队伍，杂志、网站连发各种关于比特币的报道。

在此情形下，越来越多的人利用它协助违法犯罪，而投资市场上，炒家入局，比特币的价格涨跌起伏更极端，“套现”“割韭菜”每天都在发生。

比特币终究还是迎来了各国政府的“关注”。

2018 年，关于“目前各国对于加密货币的态度与看法如何”，彭博社做过一项调查。

其中，在“是否立法”“是否支持加密货币支付”“是否支持加密货币 ICO 活动”“加密货币交易所监管”等方面，各国政策不一，争议极大。

不过，除了政府的态度，人们依旧在寻找“中本聪”，因为没有人比这位比特币之父更能指出比特币未来的走向。尽管他早年也说过那么一句废话：“未来二十年内，比特币要么交易量惊人，要么交易量为零。”

事实上，通过查找关于“中本聪”的一切信息可以发现，目前我们对他的了解还知之甚少。他没有透露过任何个人信息，有时会在帖子里掺杂英式拼写，这也导致有人认为他是来自英美国家。但从名字看，是一个日本姓氏，由此不得不让人猜测“中本聪”并不是一个人，而可能是一个团队。更重要的是，“中本聪”本人被认为拥有约百万枚比特币，因此，追查“中本聪”到底是谁将一直成为人们渴望的话题。自从“中本聪”在 2010 年消失之后，已经有几十个候选人被认为是现实中的“中本聪”，然而这些人都不约而同地否认了自己就是“中本聪”。

如今十年已去，下一个十年，我们还将继续等待答案。