区块链启示录

[美] 菲尔·尚帕涅（Phil Champagne）编著

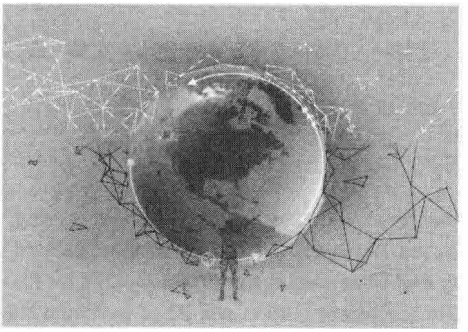
陈斌 胡繁 译

中本聪文集

THE BOOK OF SATOSHI

The Collected Writings of Bitcoin Creator
Satoshi Nakamoto

机械工业出版社
China Machine Press



区块链启示录

[美] 菲尔·尚帕涅（Phil Champagne）编著
陈斌 胡繁 译

中本聪文集

THE BOOK OF SATOSHI

The Collected Writings of Bitcoin
Creator Satoshi Nakamoto

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链启示录：中本聪文集 /（美）菲尔·尚帕涅（Phil Champagne）编著；陈斌，胡繁译 . —北京：机械工业出版社，2018.9
书名原文：The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto

ISBN 978-7-111-60924-7

I. 区… II. ①菲… ②陈… ③胡… III. 电子货币－文集 IV. F830.46-53

中国版本图书馆 CIP 数据核字（2018）第 211982 号

本书版权登记号：图字 01-2018-2512

区块链启示录：中本聪文集

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：唐晓琳
责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司
版　　次：2018 年 9 月第 1 版第 1 次印刷
开　　本：147mm×210mm 1/32
印　　张：12.125
书　　号：ISBN 978-7-111-60924-7
定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066　　投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259　　读者信箱：hzit@hzbook.com

•• 赞誉 ••

中本聪创立的区块链技术到现在已经10年了，区块链以其去中心化、去信用中介、透明和难以篡改而广受人们的关注。尽管中心化是人类社会发展的进步，是信息化发展的必然结果，但是现实中仍然还有很多非中心化的应用场景，特别是像供应链金融、跨境支付等涉及范围窄、频度不高的交易，非常适合区块链技术的应用。因此，我们要科学地研究和探索该技术，不要对其神秘化，既要看到优势，也要看到劣势。希望读者能通过阅读本书开拓视野。

——陈静

中国人民银行科技司前司长

国家信息化专家咨询委员会委员

译者陈斌先生，专注于互联网前沿技术的探索和创新，并以忠于民族计算机网络技术领先发展的意志和谦诚不变的教诲精神，出版了《架构即未来》《架构真经》《数据即未来》等译著。新

作《区块链启示录》比较系统地介绍了比特币和区块链技术的诞生和发展过程，有助于我们结合现有的业务在数字经济时代不断地创新。

——姚世全

国家技术监督局标准化司副司长

中国电子商务协会高级技术顾问

本书中阐述的比特币系统的实操技术实质上是现在被统一命名的区块链技术。区块链技术是达尔文揭示大自然自组织、自生成机制在金融领域映射产生的应用技术。因此，随着区块链技术的推广普及，它必将渗透到人类社会的一切领域。任何代表人或与人相关事物的网络节点的价值也必将加速倍增，从而引起了一场非凡的网络价值革命。

——余晓芒

中国信息大学校长

联通集团前副总裁

区块链和比特币是这几年热度最高的词汇。回想过去 20 年互联网创新，热度往往代表趋势；但不明就里的热度，对很多人却常常是看不懂的烫手山芋。追，怕烫手；不追，怕错过！春天时听陈斌兄讲区块链，从前世今生、数字货币、应用领域、量子计算等视角，深入浅出，讲发展、讲机会、讲局限，通俗易懂，实战代入，印象深刻！陈斌兄翻译的《区块链启示录》是我看到的最为全面诠释比特币发展、深刻解读区块链思维的好书。必将会

和《架构即未来》《数据即未来》一样，为志在创新的人带来区块链的启发！

——杨彬

易观国际共同创始人

易观天马云商总裁

如果说比特币是区块链的第一个应用，那么区块链对这个世界的重构才刚刚开始。包括对信用体系的重构，对资产流动性的创造，以及对生产关系和商业模式的彻底颠覆。拥抱区块链，从阅读本书开始！

——李大学

磁云科技创始人

京东终身技术顾问

系统地学习比特币的创造者中本聪先生的思想观点，可以帮助我们更好地理解和掌握区块链技术，便于发现潜在的、巨大的商业机会，有助于创新出符合数字时代要求的金融科技产品。

——苏文力

阳光保险总裁助理

本书对比特币的运行机制和底层技术进行了全面且深入浅出的解读，介绍了比特币的主要概念和核心原理，并从技术层面阐述了比特币的运作模式，为广大读者打造了一个极佳的实验和学习平台。希望通过这样的优质内容，让更多人真正了解区块链技术，让

更多构想中的项目得以落地，让区块链技术真正普惠大众。

——阮安邦

Trias 创始人 CEO

牛津大学计算机博士

区块链的发明者中本聪是具有创新精神的神秘人，他所开启的价值互联网时代，必将激励无数创业者前赴后继。而他自己的消失更酷，成为了这个世纪之谜，而在我所在的中关村创业大街，区块链热潮几年前就已经开始了。

——苏茹

中关村创业大街早期开拓者

车库咖啡创始人

•• 推荐序 ••

与陈斌相知多年，一直以来在我心目中他对前沿技术研究深刻，并且有自己的洞察和视角。有人说老酒历久弥新，我赞赏的是推陈出新，这就是时代进步的特征。

今天在我们周围可能会充斥着各种各样关于比特币的讨论，有人奉其为神明，有人视之为恶魔。姑且不论其是神明还是恶魔，我们把时针拨回到 1010 年以前……

坐标：中国成都

1008 年，成都 16 家官商联合用楮树皮纸印刷凭证券，上有图案、密码、花押、图章等印记，面额依领用人所交现款临时填写，然后作为支付凭证流通。存款人把现金交给铺户，铺户把存款人存放现金的数额临时填写在用楮纸制作的券面上，再交还存款人，当存款人提取现金时，每 1000 文收手续费 30 文，这种临时填写存款金额的楮纸券便谓之“交子”。

当时“交子”出现所引发的争议我们现在已经很难想象了，它出现的过程也不再可能重现在我们眼前。现在我们只知道它成了纸

币的起源，是人类货币史上的一大飞跃，甚至直接奠定了千年后的货币格局。

让我们再把时针调回到 1000 年以后……

坐标：任何地方

2008 年 11 月 1 日，一个叫中本聪的人（也可能是一群人，不排除是外星人）在网络上公布了一份白皮书《比特币：一种点对点的电子现金系统》的链接，之后一种新的货币形式——比特币出现了，当时的你我可能不曾注意到它，当它家喻户晓后我们着了魔地想要了解它，但有什么能比参与它出现的过程更直接明了呢？本书给了我们一次时光倒流的机会，以一名网友的身份去重新见证比特币的出现。

让我们一起去经历这个过程吧，至于它是神明还是恶魔也许你会有自己的答案。把过程留给自己，至于未来就交给时间吧！

赵卫星

2018 年 7 月，中国成都

•• 译者序 ••

2008 年中本聪发表了《比特币：一种点对点的电子现金系统》，并据此创立了比特币，从那时开始到现在已过了十年。比特币及其所依赖的区块链技术从早期的寥无人知迅速发展到今天的家喻户晓，而且已经风靡全球。

美国政府的多次量化宽松，特别是为拯救次贷危机所采取的一些措施促使中本聪开始认真思考这些危机背后的深刻原因，由此对传统的基于可信第三方所构建的支付体系提出了质疑，从而创造性地提出了以哈希计算、工作量证明、非对称加密、P2P 网络、分布式存储等为核心的区块链技术，通过比特币的具体实施有效且完美地解决了在没有可信第三方存在的情况下的支付问题。

作者菲尔·尚帕涅将中本聪所发表的比特币白皮书、在几个网络论坛的对话精选以及部分相关的私人往来邮件整理成册，翔实地记录了比特币和区块链的孕育、创立和发展过程，以及围绕着理念、逻辑、原理、实施、安全、设计和普及所进行的深入讨论，并按照不同的主题组织起来呈现给广大的读者。

本书见证了新思想和新技术推动时代变革的又一创举。某种程度上讲，中本聪所创建的比特币和区块链技术不仅是一次技术革命，更是一场伟大的思想革命。中本聪通过互联网的在线讨论亲自参与并引导了这场具有重大历史意义的思想革命。本书就是这场思想革命的完整记录。从这个意义上讲，其价值可以与达·芬奇手稿媲美。

今天，区块链技术已经从最初以解决支付问题为主的全球账簿阶段发展到了以智能合约为主的全球计算机阶段。虽然在金融监管政策、交易并发处理能力以及数据安全性方面仍然还存在着不少需要进一步发展和优化的空间，但是人们已经越来越多地认识到区块链技术在供应链金融、有价证券交易、数据资产保全、个人与企业征信等方面的巨大潜在价值。包括中国在内的世界正在快速地向数字时代发展，而区块链技术有希望成为数字时代数字经济完成价值交换的基础，因此区块链技术全面开启了崭新的价值互联网时代。

译者期待广大读者能够通过阅读本书，更深入地理解中本聪的精髓，掌握区块链技术的核心理念，并能够在各自的领域中有效地应用。

谨以此书纪念比特币诞辰十周年！

陈斌　胡繁

2018.7.30

•• 封面照片的故事 ••

封面照片由丽莎·韦克尔拍摄（flickr.com 用户名 lisa_aw）。这张照片拍摄于阿根廷圣克鲁斯省的手洞。手洞是一系列洞穴的统称，得名于许许多多人将手掌按在墙上绘制而成多种作品。这些绘画作品最早出现在 13 000 年前，最晚距今也有 9000 年以上，它们在那里静静地走过了漫漫岁月。

选择这张照片作为本书封面，是因为它体现了比特币的许多概念——大量的个体跨越时间参与合作以达到一个共同的目标，但同时仍保持了自己的独特性。然而手洞岩画在规模上却远逊于比特币。

虽然几千年来很多代人参与了这些画的创作，但是艺术家的数量还是无法与数以百万计的比特币用户相比。此外，分散于不同地域的比特币用户通过分布式系统协作，与手洞是少数几个不同部落人民的作品不同，比特币开放给所有愿意使用的人，它超越了国界，具备了成为真正世界货币的潜力。

•• 致谢 ••

谨向以下各位表示深切的谢意，感谢他们为本书出版做出的贡献。

达斯汀·特拉梅尔分享了他与中本聪之间往来的电子邮件。

加文·安德森是比特币项目的首席开发者，我们感谢他为比特币做出的贡献，也感谢他分享与中本聪之间的电子邮件。

感谢 DollarVigilante.com 的杰夫·贝里克为本书撰写序言，并感谢他对自由和解放的倡导。

还要感谢我的儿子塞缪尔、女儿薇薇安、妻子玛丽·加尼翁，感谢他们的支持。最后，我要感谢所有帮助我完成这本书的人，特别是编辑玛丽·格雷比尔，她承担了大量的工作，另外还有为本书提出伟大设计的约翰·莱因哈特。

最后，真诚地感谢中本聪。要不是他，还要等多久才能发现比特币这个如此伟大的革命性概念呢？

•• 本书的目标读者 ••

本书包含了从比特币发行到企稳的两年多时间里，比特币之父中本聪通过电子邮件和论坛文章而流传下来的大多数思想。有兴趣了解比特币，特别是其创造者思想过程的人都会欣赏本书。有计算机软件背景的读者很容易理解本书内容。但是因为这些文章里讨论到了经济学概念，所以经济学家、投资者等非信息技术背景的读者也可能对中本聪的文章感兴趣。由于不同的背景和兴趣，读者可能会对特定章节感兴趣。

为了让读者能从中本聪的文章中获得最大的收获，本书第 2 章介绍了比特币的主要概念和基本原理。这将有助于读者理解后续章节中的大部分内容。章节的内容按时间顺序排列，从中本聪最早提出比特币的最初想法到他发出标志着退出公开活动的帖子。

本书的部分内容来自网络论坛 p2pfoundation.org、bitcointalk.org，以及密码学电子邮件档案。

访问网址 TheBookOfSatoshi.com 可以轻松得到书中引用网页的链接地址。地址按章节的顺序排列。

•• 序言 ••

比特币改变了一切。它在货币和银行业的进化过程中发挥了举足轻重的作用。请注意，这里没有用“革命”一词，因为我认为比特币是从现行陈旧的货币和银行系统中发生的一次彻底的“进化”。

对刚接触比特币的人来说，最大的问题就是它的神秘感。

本书为世人揭开其神秘的面纱。虽然中本聪的真实身份可能永远是个谜，且不管那些主流媒体将多里安·中本聪之流认定为中本聪妥当与否，但至少在丰富翔实的史料中能让我们获得自比特币创世以来的理论基础和设计思路。

从世人认识比特币的第一天起，顶级密码学和编程专家之间就有了非常深入的对话。2008 年 11 月 1 日是历史性的一天，它很有可能被几代人所铭记。

当中本聪在网络上公布他的创造时，说出的第一句话简单而铿锵：“我一直在研究一种全新的完全点对点（peer-to-peer）的电子现金系统，抛弃第三方信用机构。”正是这句话即将改变整个

世界。

接着，他留下了一份白皮书链接。剩下的事情大家就都知道了。

这些公开发生在 bitcointalk.org 论坛上的讨论一直持续到 2010 年 12 月 12 日。在此之后，中本聪就彻底地消失了。

在比特币社区中，这些网络论坛的文章众人皆知，但是普通人需要好几个小时从头到尾翻阅一遍才能够搞清楚到底说了些什么。为了完成这本书，菲尔·尚帕涅阅读了每一篇网络论坛的文章，并从中筛选出了最重要的那些，同时也给出了那些文章发表时的背景及重要性。这些都是由中本聪直接完成的比特币进化大事记，实际上可以作为一本比特币的传记。

在撰写本书的 2014 年 3 月，比特币前途未卜。它可能会继续翻天覆地，使人们摆脱对中央银行和依靠免费资金生存的庞大政府机构的依赖。或者，也可能因为某些可能的事件而就此灰飞烟灭。

无论如何，比特币带来的影响已经确定。其最核心的概念已经改变了世界对合同、信用和交易的看法。平台上已经建立起数以千计的应用，而且这些应用已经扩展到金融交易领域之外。

菲尔·尚帕涅以易于阅读的方式向我们展示了这个振奋时代的最重要的技术创新。在完全分布式的平台上进行支付交易，不再需要可信的第三方。其重要性仅逊于互联网的演进。第 2 章为不熟悉比特币的读者概述了其技术和哲学基础以及运作机制。几十年后，当人们回首看待这项创新时，会像现在的人们看待互联网或古腾堡印刷机一样，将比特币的出现看作是人类文明史上划

时代的时刻。而本书收录了中本聪的文章和邮件，形成了一个合理的时间线，是了解比特币如何开始和发展的最简单的方式之一。

杰夫·贝里克

美元侠客网主编 (http://DollarVigilante.com)