区块链：定义未来金融与经济新格局

张健　著

ISBN：978-7-111-54109-7

本书纸版由机械工业出版社于2016年出版，电子版由华章分社（北京华章图文信息有限公司，北京奥维博世图书发行有限公司）全球范围内制作与发行。

客服热线：+86-10-68995265

客服信箱：service@bbbvip.com 官方网址：www.hzmedia.com.cn 新浪微博 @华章数媒

微信公众号 华章电子书（微信号：hzebook）

目录

后记

对话作者：区块链离我们还有多远

大家谈之《区块链大革命》

未来已经来临，只是尚未流行。

——威廉·吉布森（William Gibson）

推荐序一

随着互联网金融向纵深发展，区块链技术及其应用成为人们日益关注的热点。区块链技术开始从概念走向实际应用，越来越多的资金流向区块链的创业企业以及相关领域的创新，随着各国的金融机构甚至一些大型传统企业加入区块链技术的探索行列，一场真正的革命正悄然到来。

2015年10月，《经济学人》发布封面文章：制造信任的机器——比特币背后的技术将如何改变世界。理解这句话的意思并不难，然而理解其背后的机理却相当不易。这不仅需要对于区块链本质有认识，更需要诸多跨学科的背景知识，远不是一两句话就能够解释明白的。这也是我们推荐这本书的原因所在。通读本书，最大的感受是，作为区块链行业的从业者，作者的视野和知识结构都没有局限于自身的职业。本书开篇通过简述人类社会信息转播方式和价值传递方式的演化路径，勾勒出一个从信息到信用、从互联网到区块链的发展轨迹，引出了区块链这种高效的价值传递方式出现的必然性。谈到区块链的本质，作者又从货币开始讲起，同时引入大量背景知识，让读者对区块链的内涵有更为深刻的理解。这种系统化的论述，对一项新兴技术甚至思想的推广普及，无疑有着非常重要的意义。

区块链的优势在于能够用非常低的成本解决网络交易的身份识别和个人征信，以及使用点对点的交易避免了传统集中式的清算结构，从而能够大大提高金融系统甚至整个经济体系的运行效率。除了区块链的诞生背景及本质，本书还围绕区块链的各个方面分别谈了区块链带来的新机遇、各种应用场景以及具体的技术原理等内容。比如谈到互联网金融，作者提出了“区块链将成为互联网金融梦想照进现实的关键技术”这样让人印象深刻的观点；提及物联网与共享经济，作者从理论的角度分析它们目前面临的问题，并引出区块链对解决这些问题的价值与意义。虽然本书涉及的领域非常宽泛，很难做到面面俱到，但书中所讲的各种观点以及独立思考的精神，是难能可贵的。

与常见的新技术布道者不同，本书体现了少见的冷静。作者坦承，现在的区块链处在它的婴儿时期，各方面的基础设施还很不完善，而这种不完善限制了区块链的大规模应用。在我看来，中国需要更多的这种不虚美、不隐恶、冷静务实的金融科技从业者，而这也是整个国家的金融体系稳步改革和发展的基本保证。

廖理

清华大学五道口金融学院教授、博士生导师

互联网金融实验室主任

推荐序二

2011年，已经连续创业多年的我无意中听到朋友介绍比特币；2013年下半年，火币网成为当时我们只有20多人的创业公司里并行的第四个项目。2013年9月，在火币网上线后不到3个月的时间，比特币涨到8000元一枚，火币网一跃成为行业的领军交易平台。截至今日，我们已经为超过30个国家和地区的150万用户提供交易服务，累计交易额突破1万亿元。

在火币网做出一些成绩后，经常有人来问我成功的秘诀。鸡汤也不是没有灌过，但回首往事，我清楚地知道火币网能有今天，除了全员上下的不懈努力，运气的成分必不可少。创业维艰，九死一生，不是所有的努力都能有结果，我们只是在对的时间做了一件对的事情。这件事总的来说，便是认识到了比特币乃至其背后的支撑技术——区块链的价值。

区块链可能是21世纪最让人兴奋和值得期待的技术创新之一，它创造性地使用技术的方式为交易双方建立信用，而无需第三方机构参与，从而极大地降低了交易成本。如同互联网技术革命性地降低了人类信息交互的通信成本，区块链技术的广泛应用，在未来将极大地降低价值交换的信用成本。

火币网作为行业的领军企业，因此有责任和义务向公众客观全面且深入地介绍比特币的底层技术，这也体现了我们要长期扎根数字货币产业的诚意和决心。2015年以来，随着区块链技术的蔚然成风，市场上陆续出现了一些相关书籍，但质量良莠不齐。本书作者张健力图以高屋建瓴的视角、深入浅出的文字，让普通读者也能领悟这一创新技术的价值和奥秘。本书从整个人类文明的发展讲起，从信息交换和价值传递的路径提出区块链出现的必然性，在全面地介绍这一技术突破的同时，保持研究者的冷静和客观。我作为比特币这个新兴行业的资深从业者，推荐读者阅读此书，本书可作为了解区块链技术的入门书籍，相信你在本书中可以体会到一个研究者应有的专注和专业。

2014年6月，我第一次见到本书作者张健，当时他在做国内最大的区块链查询网站（qukuai.com）。同为连续创业者的我们志同道合，相谈甚欢，很快确立了合作意向，张健也以此为契机加入了火币网团队。经过两年的共同创业，张健最为打动我的是他对区块链事业的热爱，以及对于创业的专注、坚韧和执着。2016年年初，为了更好地推进区块链业务的研发和开拓，火币网成立了区块链研究与应用中心，张健以火币网技术副总裁的身份任中心负责人。本书是该中心成立后第一项向公众展示的成果，之后我们还会有一系列的研发、教育、公众科普与商务合作项目，致力于全面推动比特币乃至区块链产业的发展。

人生的大方向很多时候是由一些微不足道的瞬间决定的。如果不是在几年前的饭桌上听到比特币的理念，我可能不会做火币网；如果不是因为火币网，我便没有机会结识张健和其他在火币网工作的同仁，也不会为了我们共同的理想而奋斗。希望对于各位读者来说，在翻开这本书的这个瞬间，也能让你们开始对区块链这个令人激动的创新技术产生兴趣，希望有越来越多的人才进入这个方兴未艾的行业，与我们共同创造一个科技引领改变的未来。

李林

火币网创始人兼董事长

序言

有幸成为新时代的亲历者

价值互联网时代

我有幸亲历的这个新时代，是价值互联网时代。而正在拉开这个时代大幕的，却是在诞生初期并不起眼，但目前越来越受到关注的区块链技术。

区块链虽然以技术的面目诞生，但是其所带来的，已经远远超越技术范畴本身，正如互联网所给我们带来的一样。在我看来，区块链不仅仅是一项技术、一个工具，更是一种思想。开放、共享、去中心化，区块链的这些核心精神与互联网不谋而合。而与互联网不同的是，区块链把这样的思想从信息的传递进一步拓展到价值的传输。

互联网时代的来临，使得信息传输的成本趋于零，这已经深刻地改变了社会的经济格局及每个人的生活。这促使我思考，当未来市场交易成本趋于零的时代到来时，整个世界经济格局及社会结构将发生怎样的变化？

我们必须为这样的变化做好准备，因为这个时代正在朝我们走来。

我与区块链的缘分

区块链作为比特币背后的技术，于2009年年初正式诞生。而我真正关注到这项技术是在2013年。当时，随着价格的暴涨以及媒体的报道，比特币第一次走进了大众的视野。与大多数人关注点不同的是，我对比特币背后的技术产生了非常大的兴趣，于是开始一探究竟。而当我真正懂得了比特币背后的逻辑，即区块链的原理时，我被这样优雅的设计深深震撼了。这开启了我与区块链的缘分——由兴趣到事业的过程。

2014年年初，我开始着手创建一个区块查询网站。创建这个网站的初衷是，当时国内并没有这样的平台，而国外的平台对于国内用户来说，无论是速度还是体验都不尽如人意。经过一段时间的努力，2014年3月，国内首家比特币区块浏览器“区块”（Qukuai.com）正式上线。通过这个网站，任何人都可以非常方便地查询区块链的数据。网站上线以后，逐渐获得国内比特币用户的支持与青睐，这让我萌发了把这个兴趣当作事业的想法。

于是，基于区块网站，我做了一系列的功能升级，并推出了一个比特币钱包——“快钱包”。在这个过程中，我有幸结识了火币的创始人李林。怀着对这个新兴行业共同的理解与对前景的认同，我选择加入火币。作为一个年轻的品牌，火币于2013年下半年诞生并迅速成长为国内最大的比特币交易平台。通过一系列的产业链扩张，火币立志成为数字货币领域的基础服务商。如今，火币已经颇具规模，成为行业内名副其实的领军企业。这使得我们有能力也有责任来做一些基础工作，为推动整个行业的发展贡献力量。于是2016年年初，我牵头成立了火币数字货币与区块链研究中心，专注于数字货币与区块链技术的研究及行业基础设施的建设。

创作此书的初衷

最近两年，区块链从不为人知到获得越来越多人的关注，甚至正在成为一个热门的新兴领域，其实有着深刻的内在逻辑。然而，除了少数已经投入其中的公司或研究机构，大多数人对于区块链的了解还处在概念阶段，可能知道一些特征或技术术语，但并不真正知道它究竟是什么。

2016年以来，我多次参加区块链相关论坛活动，也接受了很多采访。然而没想到的是，讲得越多，似乎越觉得难讲。首

先，你想把这个概念讲清楚，并不是一两句话就可以做到，因为它涉及各种各样不同领域的知识与背景。更大的挑战在于，由于听众的背景与知识结构各不相同，在短时间内通过口述让所有人理解区块链是什么以及它能干什么，简直是一件不可能完成的任务。

于是，我萌发了创作一本区块链书籍的想法。利用这本书，我可以把我对于区块链的所有理解系统且完整地呈现出来，让所有对于区块链或者对于新事物、新机会感兴趣的人，都能够在不需要太多背景知识的情况下理解区块链是什么、当前的发展如何以及可能拥有怎样的未来。最后，在火币联合创始人兼CMO杜均的提议和鼓励下，写作此书的任务正式排上日程。

时间意味着什么

不过想法虽好，要真正做到并不容易。最大的敌人是时间。由于日常工作的繁忙，想抽出大块的时间完成书稿本已非常难，加之我对于本书的内容又有着较高的要求，这对矛盾就变得愈加尖锐，在写作的过程中始终困扰着我。幸运的是，我不是一个人在战斗。若是没有团队的协助与鼓励，以及公司的大力支持，本书的完成不知道还要等上多久。

即便如此，成书的过程依然仓促，再加上我知识结构的局限，错误之处在所难免。不过我依然坚定地认为，让此书尽快面世远比把内容修订得“完美”更有意义。在一个各方面边际成本正逐步趋于零的社会，“时间”越来越成为我们最大的成本。知识可以长久存在，但机会往往转瞬即逝。我们可以学习过去的知识，却无法抓住过去的机会。我们越早一点了解到新事物，就越有可能抓住时代前行带给我们的机遇。

对于区块链这样一种协议式的、需要大规模社会协作与参与的颠覆性技术，越快让更多人了解到它的意义，就会使其越快体现出自身的价值。

让我们一起期待并拥抱价值互联网时代的到来吧！

张健

2016年5月18日于火币

致谢

本书得以面世，离不开很多人的帮助。

感谢中本聪（Satoshi Nakamoto），他开创性的工作拉开了数字货币与价值互联网的大幕。

感谢我的同事李志阔、赵海涛、张智茹、焦锋，在写作过程中我们常常进行热烈而卓有成效的讨论。李志阔协助修订了大部分章节，赵海涛参与了第4章区块链技术原理的写作，张智茹协助修订了部分章节，焦锋绘制了书中的部分插图，没有他们，本书的精彩程度将大打折扣。

感谢火币市场部的同事吴兴、安鑫鑫、张晓萌，没有他们的耐心督促，这本书的面世还要推迟很久。

感谢机械工业出版社的编辑老师李华君、张梦玲，感谢他们容忍我对书稿的反复修改，感谢他们专业细致认真的编校工作。

感谢火币创始人李林、联合创始人杜均，没有火币这个积极向上、充满活力的团队，这本书的完成是不可想象的；感谢火币总裁办刘月雯，她为这本书做了大量的协调工作。

感谢区块链爱好者魏然对书稿的宝贵建议及其提供的精彩文章。

要感谢的人还有很多，难以一一列举。惟愿这本书能够为区块链技术在中国的推广和发展做出尽量多的贡献。

第0章　必然的出现

这些力量并非命运，而是轨迹。它们提供的并不是我们将去往何方的预测，而是告诉我们，在不远的将来，我们会向哪些方向前行，必然而然。

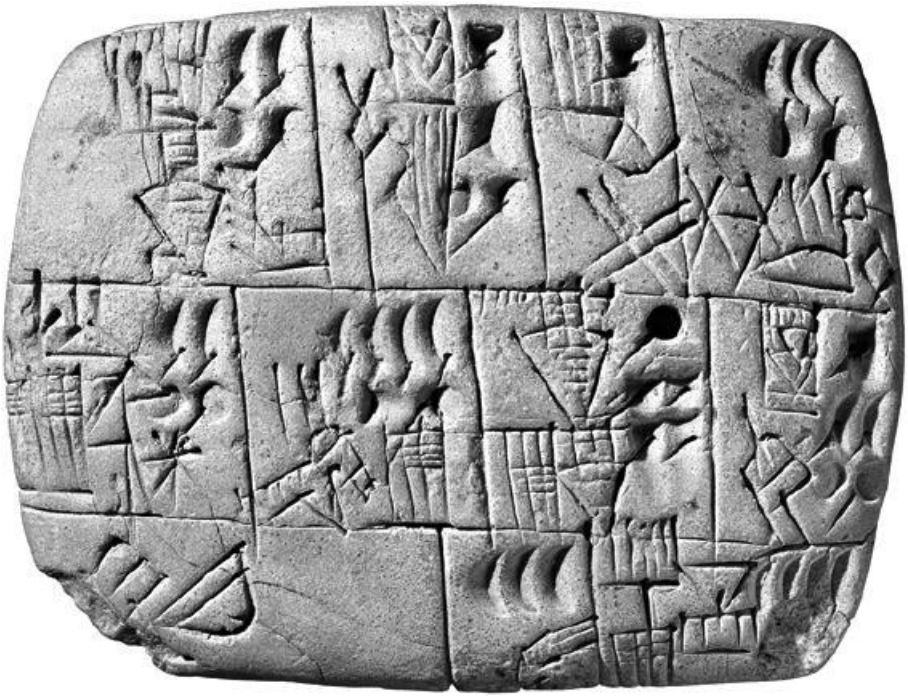
——凯文·凯利（Kevin Kelly）

文字与货币

人类在演化过程中，凭借智慧创造了无数事物，这些创造推动了人类文明的加速发展。特别是在进入信息时代以后，每天甚至每时每刻，创造都在不同领域发生着。

然而在人类文明的历史长河中，有两样东西的诞生具有极为特殊的地位，甚至其他任何创造都无法与之相提并论，它们就是文字与货币。文字的发明，使得人类能够在精神层面做到可靠的交流与传承；而货币的发明，则让人类在物质层面能够做到这一点。如果没有这两者，人类作为一个群体将无法获得知识与财富的迭代与累积，也就不会有人类辉煌的文明成果。

现今发现最早的使用文字的记录来自于公元前3000年左右，美索不达米亚平原[1]南部的苏美尔人用削成三角尖头的芦苇杆将文字刻写在泥板上，然后将泥板烘干以便于保存。这就是最早的文字形式——楔形文字。巧合的是，货币制度也同时在这一地区诞生，苏美尔人发明了已知最早的货币——大麦货币。他们将定量的大麦作为通用单位，用来衡量和交换其他各种货物和服务。更有意思的是，当年的泥板上记载的内容不是诗歌也不是哲学，而是生意。美索不达米亚文明属于城邦文明，发展出了丰富的商业行为。他们记录在泥板上的，就是经营相关的事项和账本。正如一位学者[2]所说：文字不是一种深思熟虑后的发明物，而是伴随对私有财产的强烈意识而产生的一种副产品。



图片来源：可汗学院，https://www.khanacademy.org/humanities/ancient-art-civilizations/ancient-near-east1/sumerian/a/cuneiform

而在中国，公元前210年，秦始皇统一六国之后，在全国范围内统一文字，把小篆作为全国通用的书写规范；废除各国原来的货币，统一使用圆形方孔的秦半两。统一的文字对推行法令、传播文化起了重要的作用，而统一的货币改变了过去货币的混乱状态，促进了全国各地的商品交换和经济交流。这两个举措都被作为秦始皇最重要的功绩载入史册。

《圣经·创世纪》里有一则著名的故事：起初人类有共同的语言，并且一起居住在与幼发拉底河相距不远的地方。人们利用河谷的资源在那里建筑城和塔，以聚集全体人类。上帝降临视察，认为人类过于自信和团结，一旦完成计划，人类将无所不能。上帝决定打乱人们的口音和语言，并使他们分散各地。于是高塔停工了，人们操持不同的语言，互相之间难以交流。这个塔就是巴别塔。

图片来源：维基百科，Pieter Bruegel the Elder

抛开宗教方面的意义，故事本身已经很值得玩味了。它告诉我们，如果全人类能顺畅地交流，那么所能产生的能量和带来的改变是不可估量的。而人类进行交流的载体不仅仅是语言。我们审视一下当今的世界，在全球经济一体化的背景下，人类还是被不同的货币所分割。我们不由得遐想，如果有一天建成货币的巴别塔，人类的经济生活将会面临怎样的飞跃。

如果我们进一步追本溯源，文字与货币都是人类进行更高效交流的手段。本质上，文字作为一种人际交流的手段，承载的是信息；而货币作为一种价值传输的载体，承载的是信用。自这两者诞生以来，人类信息传播和价值交换的手段也一直没有停止迭代和进化。下面将简要回顾它们发展和演变的历史。

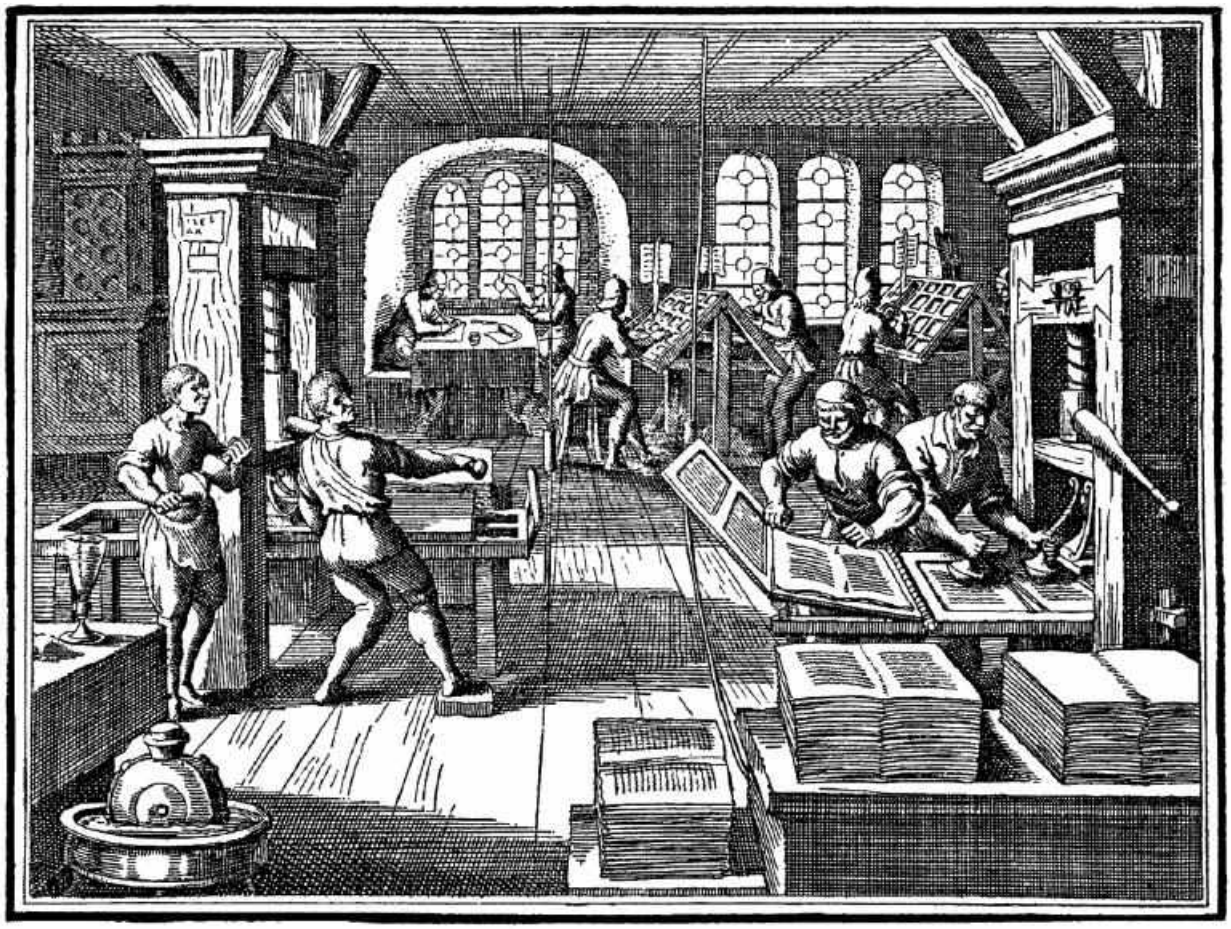
[1] 位于今天的伊拉克境内。

[2] Cf. E. A. Speiser,“ The Beginnings of Civilization in Mesopotamia,” J. Amer.Oriental Soc., Supp. 4, 59, 17 ff., esp. 25–28（1939）.

信息的演化

在文字出现以前，人类的信息主要通过语言来传递。个人的知识来自族人的口授，集体的记忆来自祖辈的传说。文字的出现使信息不再稍纵即逝，可以更好地跨越时空。甚至有些人认为，书面文字（持久存在的文字）是我们所理解的有意识思考的前提条件。它触发了人类灵魂不可逆转的大规模变化。逻辑是书面文字的产物，是文字造就了人类的思维和历史[1]。

印刷术的发明是信息传播方式里程碑式的进步之一。印刷术使知识传播的范围和有效性得到了极大的提高。在人类走出中世纪，迎来文艺复兴、启蒙运动和科学革命的进程中，印刷术扮演了重要角色。



图片来源：http://www.gutenbergsapprentice.com Copyright ©2016 Alix Christie|Main images courtesy of the Mainz Stadtarchiv，Gutenberg Museum Mainz and University of Gottingen 时间推进到19世纪后期，随着第二次工业革命的到来，电力得到广泛使用，信息传输技术也得到了又一次跨越式的发展。人们发明了电报，文字被转换为莫尔斯码；人们发明了电话，电流承载着信息。从此以后，一个以“信息”为关键词的时代慢慢拉开了它的大幕。20世纪40年代，信息时代迎来了它最伟大的推手：香农。

香农曾向麻省理工学院的万内瓦尔·布什透露，研究传递信息的一般系统的某些基本属性是他一直的兴趣所在[2]。

图片来源：维基百科

1948年，香农发表了《通信的数学原理》，这篇具有划时代意义的论文奠定了现代信息论的基础。在文章中，香农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。如今比特作为衡量信息多少的单位，已经与米、千克、分钟一样，成为人类生活中最基本的量纲之一。1949年，香农又有了重量级的发现，他公开发表的《保密系统的通信理论》一文，开辟了用信息论来研究密码学的新思路。这一发现将密码从艺术变成科学。

通信的基本问题是，在一点精确地或近似地复现从另一点所选取的信息[3]。从密码分析者的角度来看，一个保密系统几乎就是一个通信系统。待传的消息是统计事件，加密所用的密钥按概率选出，加密结果为密报，这是分析者可以利用的，类似于受扰信号[4]。在香农的理论里，信息传输、处理、检测和接收过程，与密码系统中的加密、解密、分析和破译过程都可以用信息论的观点进行分析和研究。密码系统本质上也是一种传递信息的系统。

在香农对信息的概念加以简化，并用比特（bit）作为量纲衡量后，人们发现信息几乎无处不在。比特（bit）的出现在后来引领了计算机、网络、摩尔定律以及如今发达的信息和互联网产业。

互联网的诞生标志着信息时代的真正到来。从此信息的产生与传输开始以前所未有的速度进一步突破时空限制，我们甚至正在迎来一个信息爆炸的时代。而互联网带来的信息革命，已经深刻地改变了全球的商业格局及我们每个人的生活方式。

[1] 詹姆斯·格雷克，《信息简史》，人民邮电出版社。

[2] 引用自http://ethw.org/Oral-History:Claude_E._Shannon。

[3] Claude E. Shannon, Warren Weaver. The Mathematical Theory of Communication. Univ of Illinois Press, 1949. ISBN 0-252-72548-4.

[4] 引用自http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf。

尝试定义信用

自古以来，人们就认识到了信用的重要性。司马迁在《史记·季布栾布列传》中记载：得黄金百，不如得季布一诺。英国哲学家约翰·穆勒认为：互相信任可以弥合人类生活中的每一个裂隙[1]。然而，或许正是因为信用的无所不在，就像对空气一样，人类在绝大部分历史时间内都忽略了对信用的定义和分析。

在刚刚过去的几十年中，随着科学和经济的进步，信用成为交易成本理论、博弈论、社会经济学等不同学科和理论中的重要话题。然而，由于不同的研究主体和研究层面并存，信用的概念依然是一个混乱的大杂烩。

在经济学意义上，一般来说，信用意味着一些群体将自身置于因其他群体的不确定行为所造成的风险之下[2]。

信用与货币

现代经济学认为，现代市场经济从根本上是一种信用经济，因为随着分工的深化和市场的扩大，信用出现在借贷活动和其他一切市场经济活动中。信用是维系商品交换的基本前提，是市场经济良好并高效运行的基础。

货币在市场经济中扮演着核心的角色，而信用与货币之间的关系则更为密切。尤瓦尔·赫拉利（Yuval Harari）在《人类简史》中说：“金钱就是一种互相信任的系统，而且还不是随随便便的某种系统——金钱正是有史以来最普遍也最有效的互信系统。”

最早发明钱的时候，人们还没有这种信任，所以要当作货币的事物本身就得有实际的价值，比如苏美尔人的“大麦货币”制度。而随着信任的建立，货币就开始向基于纯粹的信用而不需要有内在价值的方向演化。

传统的货币理论认为货币的本质是商品或一般等价物，随着金本位制的瓦解，以20世纪70年代布雷顿森林体系的崩溃为标志，金属本位彻底退出了历史舞台。事实上，目前世界上几乎所有国家的货币都已是信用货币。信用货币是货币发展中的现代形态，不再代表任何贵金属，并且其本身价值远远低于其货币价值，已经和商品属性彻底脱钩。

在实物货币阶段，货币以实物商品的形式表现出来。从表面上看货币是有价值的商品，但是，人们出卖商品换取实物货币时需要的不是实物货币本身，而是实物货币交换其他商品的能力，即购买力。换句话说，人们之所以能接受实物货币，本质上并不是因为实物货币是有价值的商品，而是因为其相信实物货币是信用的象征，它可以提供一般购买力。所以无论是实物货币还是信用货币，信用都是货币更为本质的属性。也可以说，信用是货币的创造者[3]。

信用的可计算性

区块链是作为比特币底层技术与基础架构而诞生的。比特币是一个可以点对点进行支付、不依赖任何第三方的电子现金系统。借助密码学技术，比特币的发明者中本聪构造了一个极为巧妙的经济系统，解决了在去中心化的结构下，如何创造一个可信的价值传输系统这个难题。

香农作为信息论的开创者，解决了“如何用数学方法定义信息”这个关键的问题，让信息有了量化的单位“比特”并可以被精确计算，从而奠定了数字通信的理论基础。类似地，在我看来，区块链的诞生给了我们解决另一个宏大问题的机会——如何用数学方法定义信用。

在经济学的语境内，作为一个风险要素，信用被定义为一个主体评估另一个主体将采取某种特殊行为的主观概率水平[4]。信用关系的建立前提在不同的学者看来是不同的，这种分歧主要体现在信用是否具有可计算性（Calculativeness）上。

只有存在不同选择的时候，才可能出现信用的问题。当一个主体将自身暴露在对方会投机取巧的风险之下时，就可以认为

是信用的展现[5]。从这个意义上讲，信用是一种行为策略，而行为策略的选择，从数学和博弈的角度看，似乎是可以计算的。最容易想到的是，只要潜在收益与信用行为的概率之乘积大于潜在损失与不守信行为的概率之乘积（潜在收益×信用行为的概率>潜在损失×不守信行为的概率），信用就是占优势的行为策略。1990年科尔曼就以代数的方式提出了这种计算方法[6]。

尽管持信用可计算观点的学者很多，而且他们也给出了不同的可计算概念和方法，但是都无法回避一个问题，就是可操作性不强。另一个持信用可计算观点的学者就在他的文章中承认[7]：归根结底，人是有限理性的社会动物，不同的社会环境会改变经济主体在面对交易时所做的行为选择。如果将社会环境的多样性以及个体并没有绝对理性这些事实考虑在内，那么我们就会发现，所谓信用并不是一个单纯的计算概念，因此社会层面的信用行为也不能总是被单纯地简化为基于计算的主体间的相互影响[8]。

或者可以说，不是信用不可计算，而是我们还未构造出可以精确计算它的环境或系统。

区块链的信用表达式

这里所谓的定义信用，不是计算人或参与主体的信用，而是计算信用行为（比如交易）的可信程度，或者说计算一个信用行为在未来发生违约（欺诈）的可能性。违约的可能性越低，该行为的可信程度就越高；反之，违约的可能性越高，该行为的可信程度就越低。

从经济学的角度看，解决这个问题的阻碍其实源于违约的成本与收益很难在违约行为发生之前被精确地计算出来。区块链这种通过数学算法构造的经济系统，本身是一个对所有人都公开透明的系统，更为重要的一点是，在区块链这样的系统中，可以精确计算发生违约（欺诈）行为[9]所需要付出的成本以及可以预期的收益。

比如，我们这里可以将信用行为的可信度简单定义为违约成本与违约收益的比值（信用行为可信度＝违约成本/违约收益）。对于在区块链上发生的任何交易，我们都可以用此公式得出一个精确的结果[10]。

比特币从诞生到现在已经在争议中走过了7年，在这样一个去中心化的经济系统内部，在没有任何可信的第三方担保的情况下，却没有发生过严重的欺诈行为，其主要原因在于，欺诈行为的成本往往远大于预期的收益。这也符合中本聪在创造区块链时的计算及预测[11]。显然，当欺诈行为所要付出的成本远大于其所能带来的收益，并且成本和收益都可以事先被精确计算时，任何一个理性的参与者都不会有欺诈的动力。

[1] Principles of Political Economy with some of their Applications to Social PhilosophyMill, John Stuart.

[2] L. Hosmer,“ Trust: the connecting link between organizational, behavior and philosophical ethics ”, Academy management Review, 20(2), 1995,pp. 370–403.

[3] 熊彼特，《经济分析史》，第一卷第480 页。

[4] Cyer t R.M., and DeGroot, M.H., 1987, Bayes ian Analysis and Uncertainty in Economic Theory,London: Chapman and Hall.

[5] Sugden, R., 1994, ‘ How people choose ’, in S. Hargreaves-Heap, M.Hollis, B. Lyons, R. Sugden, and A.Weale, The Theory of Choice: A Critical Guide, Oxford: Basil Blackwell: 36-50.

[6] Coleman, J.S., 1990, Foundations of Social Theory, Harvard University Press.

[7] Williamson, illiamson, O., 1993‘, Calculativeness, trust, and economic organization’ , Journal of Law and Economics, Vol 36 No 2: 453-486.

[8] Humphrey, J. and H. Schmitz, 1996, ‘ Trust and economic development ’ ,mimeo, Institute of Development.

[9] 区块链的违约或欺诈行为就是双花问题，即同一笔钱重复消费的问题。

[10] 引用自http://qukuai.com/calculations。

[11] 引用自https://bitcoin.org/bitcoin.pdf。

从互联网到区块链

更高效的信息传递和价值传输是指引人类文明前进的两座灯塔。实际上，信息与价值密不可分。从广义上理解，任何形式的信息都是有价值的，尤其是人们有意识发出的信息。纵观人类社会的发展进程，信息传递和价值传输的技术发展存在着深刻的联系，你无法想象在原始部落使用移动支付，也同样无法想象在现代社会使用贝壳消费。

互联网的出现

1946年2月，世界上第一台电子计算机在美国宾夕法尼亚大学诞生，这是一个重30吨的庞然大物。1969年，美国国防部主导建立阿帕网（Appanet），斯坦福大学和加州大学洛杉矶分校的计算机首次连接了起来，这标志着计算机网络的诞生。1982年，TCP/IP协议的最终规范被确定下来，1986年，美国国家科学基金会（NSF）资助建立了基于TCP/IP的主干网，这是第一个真正意义上的互联网，并迅速连接到世界各地。1987年9月14日，中国的第一封电子邮件从中国发往德国，内容为“跨越长城，走向世界”。1990年，万维网（World Wide Web）协议完成，互联网开始向社会大众普及。

在人类文明的发展过程中，信息的传递方式经历了语言、文字、印刷术、电等一系列飞跃。香农以比特（bit）为单位将信息量化，奠定了现代信息传输的理论基础，并最终将我们带进以互联网的广泛应用为特征的信息时代的大门。互联网的出现第一次使信息可以在全球范围内做到瞬时传递。互联网带来了信息的自由传输，极大地拉近了人与人之间的距离，使全人类得以更好地交流协作。

信息传递方式的跨越式发展给人们带来的不仅是某个行业和领域的改变，更是全人类社会组织形式和行为方式的深刻变革。一种司空见惯的说法是，互联网的核心精神是开放、共享、去中心化、自下而上、多元价值等，这些说法没错，但绝不是由于互联网的出现才产生的，而是因为市场这只看不见的手导致人类社会本身就有这种天然倾向。技术的进步导致交流更为高效，这样的倾向也就被进一步放大。所谓互联网精神，只是由于拥有了新的信息传递工具，是人类行为的自然投射。

从互联网到区块链

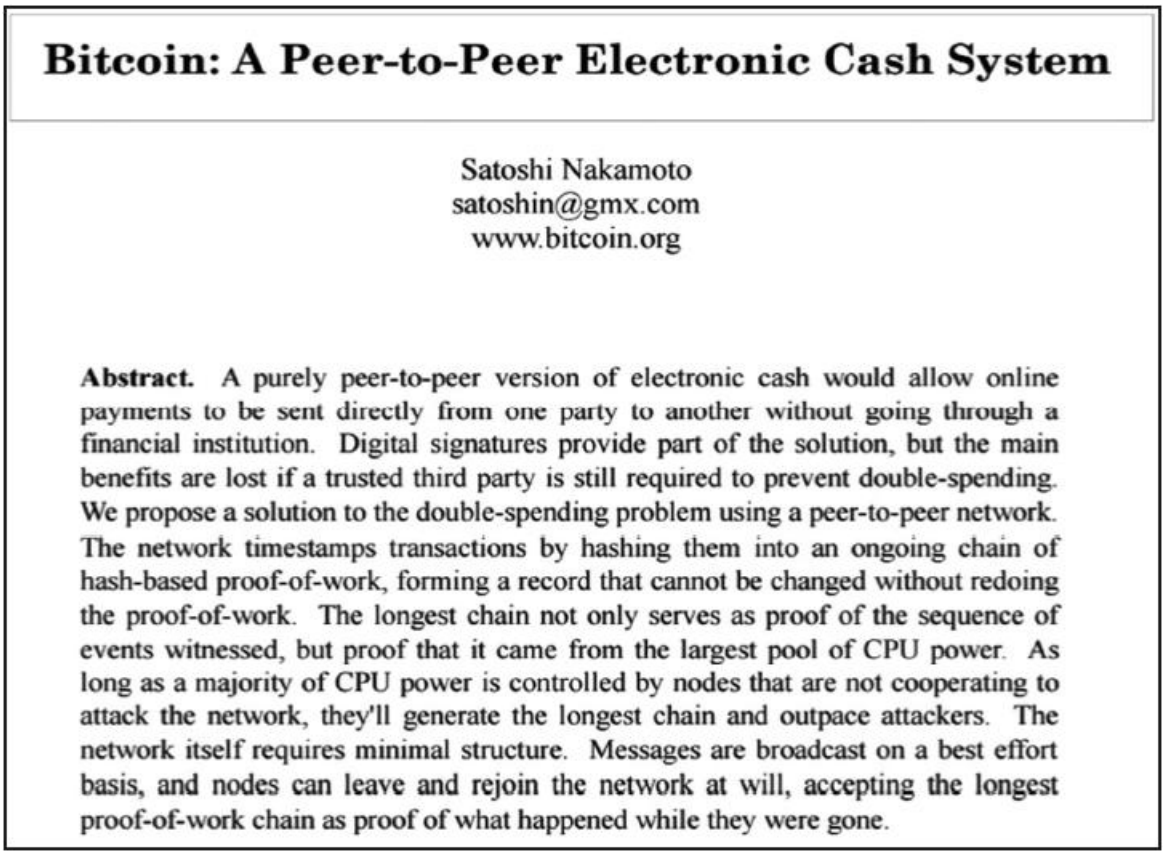
自第二次工业革命以来，从电报、电话到互联网，信息的传递方式不断升级，价值的传递方式也因此得到了同步发展。以信用卡、网银、移动支付为代表的电子货币就是在这样的背景下产生的。

互联网是为了解决信息的高效传输而被发明的，在这个网络中，信息在全球范围内的点对点传输变得异常高效与廉价。然而，这种信息传输网络并没有对有价值的信息进行保护的内在机制，在网上复制、传播乃至篡改一条信息的成本几乎为零，我们无法点对点地传递带有所有权的信息。一些传统行业（比如唱片业、出版业）在互联网诞生后受到了很大冲击，就是这个特征带来的必然结果。虽然目前各国政府对网上内容的版权保护力度越来越大，但仍然很难从技术层面上杜绝侵权问题。

从电子货币的诞生与发展来看，虽然我们已经做到了让货币以数字化的形式高效流通，但这种数字化还相当初级。我们不得不依赖大量的第三方中介机构才能保障电子货币的流通，而这种形式不仅引入了中心化的风险，也提升了传输的成本。

区块链就是在这样的背景下诞生的。由于信息与价值的密不可分，我们有了互联网这个全球范围的高效可靠的信息传输系统后，必然会要求一个与之匹配的高效可靠的价值传输系统。也就是说，区块链的诞生不是偶然的，其背后有着深刻的必然逻辑。“区块链”这个名字或许是偶然，但行区块链之实的系统的诞生则是必然。

信用是制造货币的真正原材料。而区块链通过构造一个可以量化信用的经济系统，使得一个点对点的电子现金系统——比特币[1]的出现成为可能。或者说，区块链创造了一个数字化的、可以点对点传输价值的信用系统。



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.

综上所述，我们可以看到，在传递信息的路径上，人类从文字开始，最终创造出了互联网这样高效的信息传递网络；为了传输价值，人类从货币开始，也必将创造出与互联网相匹配的价值传输网络。区块链的诞生，正是人类构建价值传输网络的开始。其实，跳出我们生存的时代，从更大的人类历史发展的尺度看，互联网与区块链的诞生也只有短短几十年的时间差而已，未来的考古工作者何尝不能说，人类同时发明了高效的信息传递网络和价值传输网络。

[1] Bitcoin: A Peer-to-Peer Electronic Cash System，https://bitcoin.org/bitcoin.pdf.

区块链的诞生

万物源自比特。

——约翰·惠勒

区块链作为比特币背后的技术架构，是随着比特币的出现而诞生的。因此，要讲区块链的诞生，我们就不得不从比特币的历史说起。

密码朋克

说到比特币的缘起，就不得不谈到一个略显神秘的团体：密码朋克（Cypherpunk）。这个团体是密码天才们的松散联盟，比特币的创新中大量借鉴了密码朋克成员的贡献。密码朋克这个词一部分来源于密码（Cipher），这在密码学中意为用于加密解密的算法；一部分来源于赛博朋克（Cyberpunk），这是指那个时代流行的一个科幻流派。这样的组合有很微妙的意味，散发着改变社会的激进理想。凯文·凯利曾在《失控》里写道：

所以在1992年夏天，一个由富有创意的数学黑客、公民自由主义者、自由市场的鼓吹者、天才程序员、改旗易帜的密码学家以及其他各种前卫人士组成的松散联盟开始创造、拼凑甚至是盗用加密技术，并将其植入网络之中。他们管自己叫“密码朋克”。

1992年秋天的几个周六，我参加了蒂姆·梅还有其他大概是15个“密码反叛者”在加州帕洛阿托举行的“密码朋克”月度会议……小组是通过密码朋克邮件列表这个虚拟网络空间来推广他们的努力的。来自世界各地、越来越多的热衷于加密技术的人每天通过互联网上的“邮件列表”互动，为了以低成本来实现他们的想法（比如数字签名）。

密码朋克们的观点是：现代社会不断蔓延着对个人隐私和权利的侵蚀。他们互相交流着对这一问题的关注，并认为在数字时代保护隐私对于维持一个开放社会是至关重要的。这一理念在比特币中得到体现：去中心化的追求，对匿名的拥抱，自由主义的原则。

密码朋克本身就是数字货币最早的传播者，在其电子邮件组中，常见关于数字货币的讨论，并有一些想法付诸实践。比如大卫·乔姆、亚当·贝克、戴伟、哈尔·芬尼等人在早期数字货币领域做了大量的探索。

早期数字货币的探索

比特币并不是数字货币的首次尝试。据统计，比特币诞生之前，失败的数字货币或支付系统多达数十个。正是这些探索为比特币的诞生提供了大量可借鉴的经验。在这里我们简要介绍几位之前的探路者。

大卫·乔姆（David Chaum）是一位密码破译专家，也是20世纪八九十年代密码朋克的“主教”级人物。他是很多密码学协议的发明者，他在1981年的研究奠定了匿名通信的基础[1]。1990年，大卫·乔姆创建了数字现金公司（DigiCash），并试验了一个数字化的货币系统，称为Ecash。数字现金公司来自他的一些突破性想法，包括如何分享和传输金融信息，以及管理不同身份信息的保密程度。在他的系统中，付款方式是匿名的，而收款方并不是匿名的。更精确的说法是，Ecash是个人对商家的系统。他发明的这个货币系统还有部分绕过中间商的特质，数字现金公司作为可信的第三方来确认交易，避免重复消费，保证系统诚实。

大卫·乔姆迅速与荷兰政府签订了合同，并从德意志银行、澳大利亚高级银行、瑞士信贷和日本住友银行获得了执照，乔姆曾与微软和VISA及其他大公司讨论如何使用新的支付系统。然而在1998年，数字现金公司宣布破产。失败的主要原因在于，将技术理念转化为实用系统的过程中缺失了很多东西。首先，数字现金公司很难说服银行和商家大规模采用他的系统，另外由

于Ecash对个人之间的交易没有很好的支持，因此当银行和商家没有动力接受它的时候，个人用户也就无从使用它。

亚当·贝克（Adam Back）是一位英国的密码学家，1997年，他发明了哈希现金（Hashcash）[2]，其中用到了工作量证明系统（Proof Of Work）。这个机制的原型可用于解决互联网垃圾信息，比如作为垃圾邮件问题的一个解决方案[3]。它要求计算机在获得发送信息权限之前做一定的计算工作，这对正常的信息传播几乎不会造成可以察觉的影响，但是对向全网大量散布垃圾信息的计算机来说，这些计算会变得不可承受。这种工作量证明机制后来成为比特币的核心要素之一。

哈伯和斯托尼塔（Haber and Stornetta）在1997年提出了一个用时间戳的方法保证数字文件安全的协议[4]。对它的简单解释是，用时间戳的方式表达文件创建的先后顺序，协议要求在文件创建后其时间戳不能改动，这就使文件被篡改的可能性为零。这个协议成为比特币区块链协议的原型。

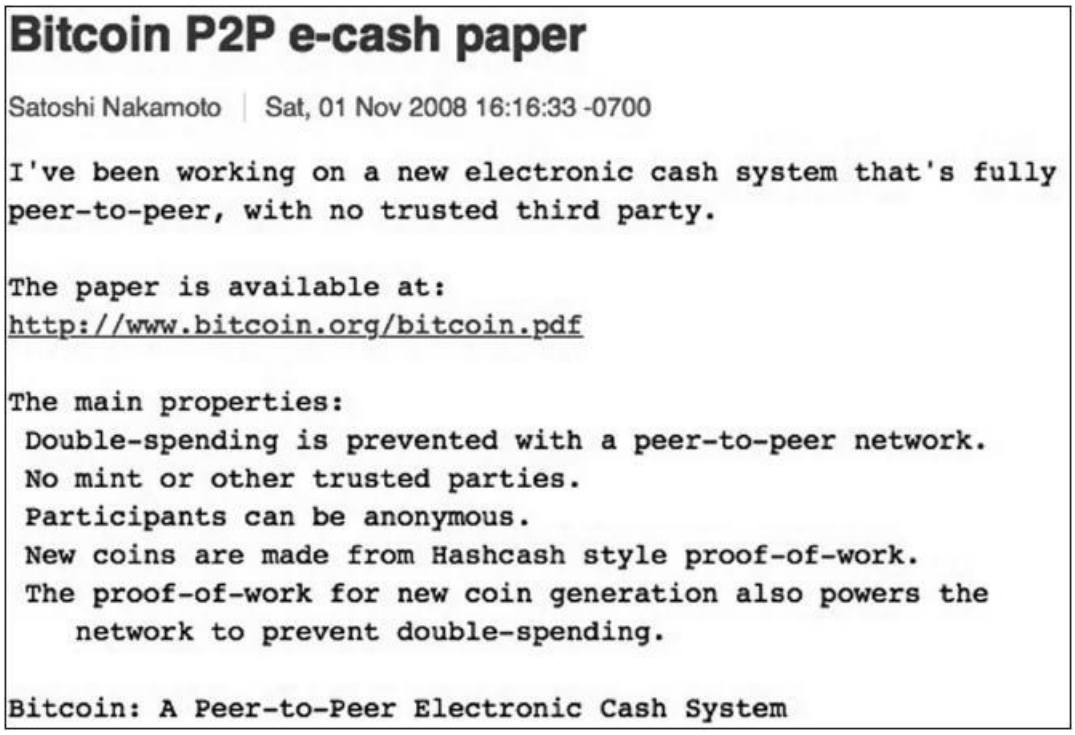
戴伟（W Dai）是一位兴趣广泛的密码学专家，他在1998年发明了B-money[5]。B-money强调点对点的交易和不可更改的交易记录，网络中的每一个交易者都保持对交易的追踪。不过在B-money中，每个节点分别记录自己的账本，这不可避免地会产生节点间的不一致。戴伟为此设计了复杂的奖惩机制以防止节点作弊，但是并没有从根本上解决问题。中本聪发明比特币的时候借鉴了很多戴伟的设计，并和戴伟有很多邮件交流。

哈尔·芬尼（Hal Finney）是PGP公司的一位顶级开发人员，也是密码朋克运动早期和重要的成员。2004年，芬尼推出了自己的电子货币，在其中采用了可重复使用的工作量证明机制（RPOW）。哈尔·芬尼是第一笔比特币转账的接受者，在比特币发展的早期与中本聪有大量互动与交流。由于身患绝症，哈尔·芬尼已于2014年去世。

比特币的诞生

2008年9月，以雷曼兄弟的倒闭为开端，金融危机在美国爆发并向全世界蔓延。为应对危机，世界各国政府和中央银行采取了史无前例的财政刺激方案和扩张的货币政策并对金融机构提供紧急援助。这些措施同时也引起了广泛的质疑。

2008年10月31日下午2点10分，在一个普通的密码学邮件列表中，几百个成员均收到了自称是中本聪的人的电子邮件[6]，“我一直在研究一个新的电子现金系统，这完全是点对点的，无需任何可信的第三方”，然后他将收件人引向一个九页的白皮书，其中描述了一个新的货币体系。同年11月16日，中本聪发布了比特币代码的先行版本[7]。



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

图片来源：http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

2009年1月3日，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了比特币的第一个区块——创世区块（Genesis Block），并获得了首批“挖矿”奖励——50个比特币。在创世区块中，中本聪写下这样一句话：

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

财政大臣站在第二次救助银行的边缘

这句话是当天《泰晤士报》头版的标题。中本聪将它写进创世区块，不但清晰地展示着比特币的诞生时间，还暗含了对于旧体系的嘲讽。


THE TIMES

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

不过正如上文所述，加密数字货币并不是什么新概念，曾有很多人试图打造这样的系统，但最终都失败了，有什么理由认为比特币会比之前的尝试更好呢？当时，即使在密码朋克内部，多数人对中本聪的系统也没抱多大的期望。

然而事实是，中本聪通过一个天才的发明——区块链，扫清了创造加密货币的最后障碍。于是，出乎大多数人的意料，比特币开始走上了一条不断成长与快速发展的道路。

小结

如今，比特币已经成为数字货币领域的翘楚，拥有数十亿美元的市值，但中本聪早已于2010年选择隐退。中本聪到底是谁是每一个关心比特币的人都感兴趣的话题，从《纽约客》到《新闻周刊》，媒体找到了数个自称是中本聪或者被认为是中本聪的人。但无一例外，这些发现都因为可信度不足遭到了读者甚至是中本聪本人的否定。中本聪是谁？也许我们永远不得而知。

[1] Danezis, George ; Diaz,Claudia（January 2008）“ Survey of Anonymous Communication Channels ”. Technical Report MSRTR-2008-35. Microsoft Research; For the paper, see Chaum, David（1981）. “ Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms ”. Communications of the ACM 24（2）: 84–90.doi:10.1145/358549.358563.

[2] 引用自http://www.hashcash.org/papers/announce.txt。

[3] Dwork, Cynthia; Naor, Moni （1993）. “ Pricing via Processing, Or,Combatting Junk Mail, Advances in Cryptology ”. CRYPTO ’92: Lecture Notes in Computer Science No. 740（ Springer）: 139–147.

[4] S. Haber, W.S. Stornetta, “ Secure names for bit-strings, ” In Proceedings of the 4th ACM Conference on Computer and Communications Security,pages 28-35, April 1997. on Computer and Communications Security,pages 28-35, April 1997.

[5] W Dai,a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help “ B-money ”, http://www.weidai.com/bmoney.txt,1998.

[6] 引用自http://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html。

[7] 引用自http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html。

第1章　区块链是什么

记账货币

记账货币可以记载债务、价格以及一般购买力，是货币理论最基本的概念。……从严格意义上说，货币只有在与记账货币的关系中才能存在。

——凯恩斯

区块链的本质是什么？区块链与比特币有什么关系？回答这两个问题前，让我们先从一个拿石头当钱的小岛说起。

石币之岛

雅浦岛（Yap）是位于太平洋西部的加罗林群岛中的一个小岛，居住人口仅有数千人，岛上风景如画，人们过着田园牧歌式的生活。然而，这个岛最出名的原因却是岛上奇特的货币。

图片来源：http://www.reefseekers.com/PIXPAGES/Yap%202013/Yap%202013%20pix.htm

一种又大又厚的石轮——“费（Fei）币”构建了当地的货币体系，这些石轮的直径从1到12英寸（1英寸=0.0254米）不等，中有孔洞。雅浦岛上的居民进行的交易很多，但交易过程一般只是债务互相抵消的过程，账款通常留待以后的交易中进行转结。即便到了最后的清算时刻，费币也很少被搬动，当地人只是在上面做标记，以显示所有权的易手，其所有者无须持有它。当地人并不在意自己对这块石头的所有权有没有实物保证，甚至不需要为交易做什么记号，石币还是原封不动地留在原来的主人那里。

威廉·亨利·福内斯[1]对雅浦岛的货币体系进行描述时，讲述了这么一个故事：

附近村子里有一家人，他们的富裕程度毋庸置疑、人所周知，然而没有一个人见过或接触过这笔财富，这家人自己也不例外。他们家的财富就是一块巨大的费币，其尺寸只是在祖辈的口中提到过，历经两三代人，这块费币一直躺在海底，直到现在！人们都承认，这块费币在运输过程中掉下海的事故本身无须多议，而且人们也承认，即便沉在数百英里（1英里=1609.344米）之外的海里，这块石币的交易价值也不应受到影响……这块石头的购买力就如同把它明显地摆在主人房外一样，仍然有

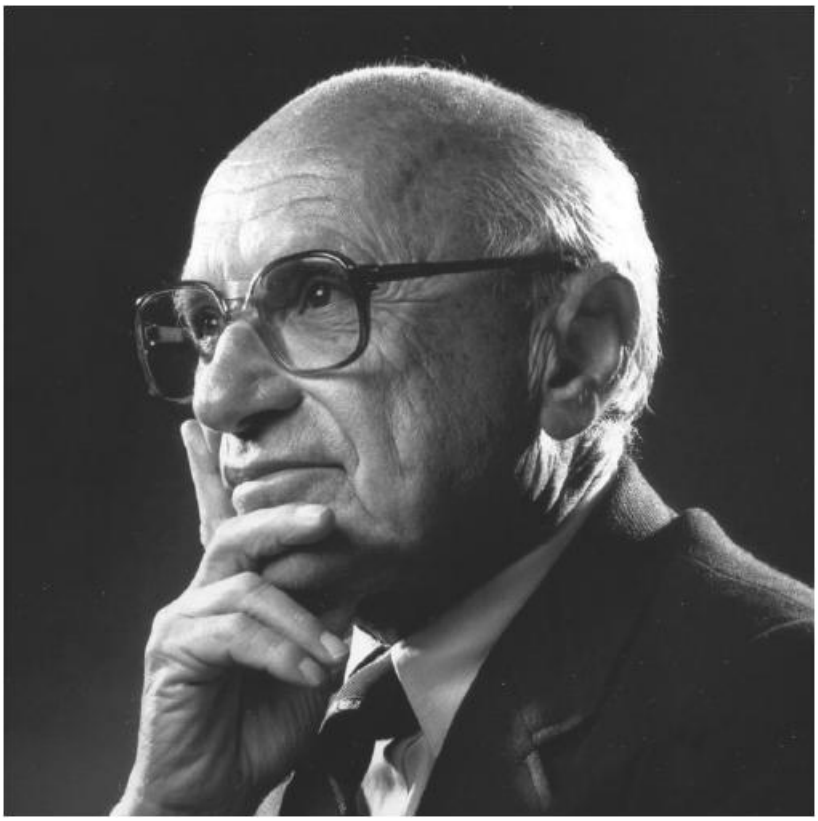
效。

这种奇特的货币制度其实并不难理解，雅浦岛的货币不是费币，而是其背后的一套由信用记录以及信用记录的清算构成的体系。费币只是用来记账的表征[2]。凯恩斯在他的《货币论》里表示：“福内斯的书让我们了解到，有一个民族对货币的观念可能比其他国家的人聪明得多。”[3]

约翰·梅纳德·凯恩斯（John Maynard Keynes，1883—1946），现代经济学领域最有影响的经济学家之一，被称为“资本主义的‘救星’”“战后繁荣之父”等。在经济学界，“凯恩斯学派”衍生了数个支系，其影响力持续至今。

图片来源：可汗学院，https://www.khanacademy.org/partner-content/big-history-project/acceleration/changing-economies/a/smith-marx-and-keynes

1991年，79岁的米尔顿·弗里德曼同样对雅浦岛有很高的评价，认为雅浦岛摆脱了商品硬币这套传统但不健康的制度[4]。该岛对公认的实体通货明显漠不关心，这说明了货币不是一种商品，而是信用与清算构成的一套体系[5]。



米尔顿·弗里德曼（Milton Friedman），美国当代经济学家、芝加哥大学教授、芝加哥经济学派代表人物之一，1976年获诺贝尔经济学奖。

图片来源：http://twitchy.com/sd-3133/2013/07/31/happy-birthday-milton-friedman-free-market-warriors-remember-their-hero/

记账货币

关于货币是什么的问题，在历史上有两种针锋相对的学说。货币金属论者认为货币与贵金属等同，货币必须具有金属内容和实质价值，货币的价值取决于贵金属的价值。货币名目论者则否定货币的实质价值，认为货币只是一种符号，一种名目上的存在。随着金本位制度的崩溃，目前世界上几乎所有国家的货币都已是信用货币，这场争论的结果也越来越清晰，货币名目论逐渐占据了统治地位。美国著名经济学家米什金在《货币金融学》中对货币的定义为：“货币或货币供给是任何在支付商品、劳务或偿还债务时被普遍接受的东西。”[6]

凯恩斯是货币名目论的典型代表，他在《货币论》中说：记账货币可以承载债务、价格以及一般等价物，是货币理论中最为基本的概念。那些在交易现场作为便利的交易媒介而存在的物体会逐渐演变成货币，这是因为它们代表了一种持有一般购买力的方式。记账货币是一种描述，而货币则是这种描述对应的事物[7]。

从纸质的信用货币发展到目前广泛使用的电子货币，如信用卡、网上银行、手机银行等，进一步体现了记账货币的特点——当你通过网银给其他人转账的时候，没有发生任何物理货币的转移，只是银行里记账系统的账务发生了变化而已。

区块链的本质

区块链[8]的本质是一种去中心化的记账系统，而比特币正是这个系统上承载的“以数字形式存在”的货币。我们可以认为区块链与比特币之间的关系就是凯恩斯所说的记账货币与货币之间的关系，也可以用菲利克斯·马丁对货币的理解[9]来说明两者的关系——比特币只是记账的表征，而区块链就是其背后的一套由信用记录以及信用记录的清算构成的体系。

[1] 威廉·亨利·福内斯三世（William Henry Furness III），1910 年。

[2] Felix MartinMoney: The Unauthorised Biography，P23.

[3] 凯恩斯，货币论（A Treatise on Money ,first published 1930），第二卷，P292。

[4] 米尔顿·弗里德曼，货币的祸害。

[5] Felix Martin，Money: The Unauthorised Biography，P25.

[6] Frederic Mishkin，The Economics of Money, Banking, and Financial Markets, seventh edition,P44.

[7] 凯恩斯《货币论》，P1。

[8] 这里的区块链特指比特币区块链。

[9] Felix Martin，Money: The Unauthorised Biography.

天才的发明

要了解比特币的内在优雅。不是软件使得比特币如此有效，而是经济学。[1]

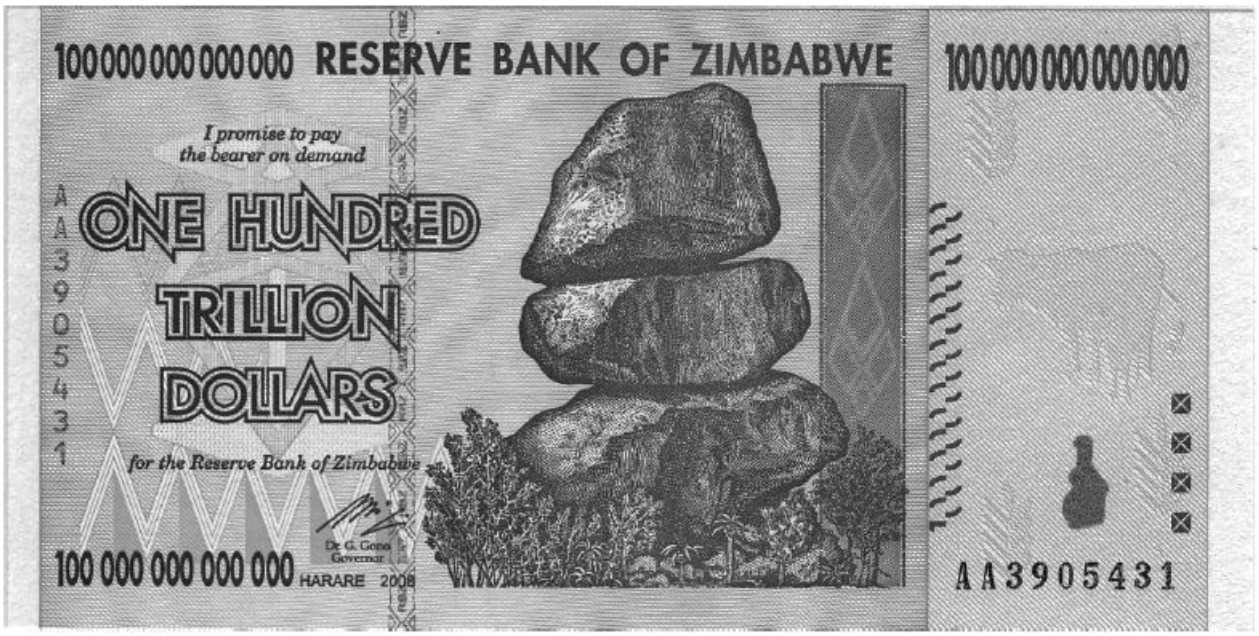
——罗伯特·沃伦斯基

从技术的角度看，区块链就是比特币的基础架构及实现方式。没有区块链，就不会有比特币。也就是说，我们谈论比特币的发明，与谈论区块链的发明是一回事。

中心化的记账方式

因为账本上的内容必须是唯一的，所以就导致记账是一种天然的中心化的行为。在通信手段不发达的时代，这是必然的选择；在如今的信息时代，中心化的记账方式依然覆盖了社会生活的方方面面。然而，中心化的记账却有一些显而易见的弱点：一旦这个中心出现问题，如被篡改、被损坏，整个系统就会面临危机乃至崩溃。

一个典型的例子是21世纪初的安然事件：这家2000年披露的营业额高达1010亿美元美国能源巨头，由于深陷会计假账丑闻，于2001年轰然倒下。如果账本系统承载的是整个货币体系，那么就会面临中心管理者滥发的风险。历史上，由于货币滥发造成恶性通货膨胀的例子并不鲜见，甚至在当今世界仍然屡屡发生，比如津巴布韦。从1980年到2009年，津巴布韦共发行了4代津巴布韦元，无一不陷入恶性贬值。2008年11月，津巴布韦每天的通胀率高达98%。2015年，津巴布韦元失去了流通资格，当地只能以南非米特、印度卢比、欧元、日元、澳元、美元、人民币等他国货币作为流通工具。



图片来源：维基百科

所以，这种中心化的记账方式对中心本身的能力、相应的监管法律和手段以及参与者对其的信任都有极高的要求。

去中心化记账的难题

那么，我们能不能构建一个不依赖任何中心或是第三方但却可靠的记账系统呢？如果可能，我们就可以克服中心化记账的弱点。然而事实上，构建这样的系统远比想象中复杂。

从设计记账系统的角度，要达成去中心化的目标，显然需要具备以下两个条件：

1）账本数据的存储必须是去中心化的，不能指定任何参与方拥有特殊的保存账本的权力，或者说，我们需要让所有参与方都平等地拥有保存账本的权力。

2）记账行为本身必须是去中心化的，不能指定任何参与方拥有特殊的记账权力，或者说，我们需要让所有参与方都平等地拥有记录账务数据的权力。

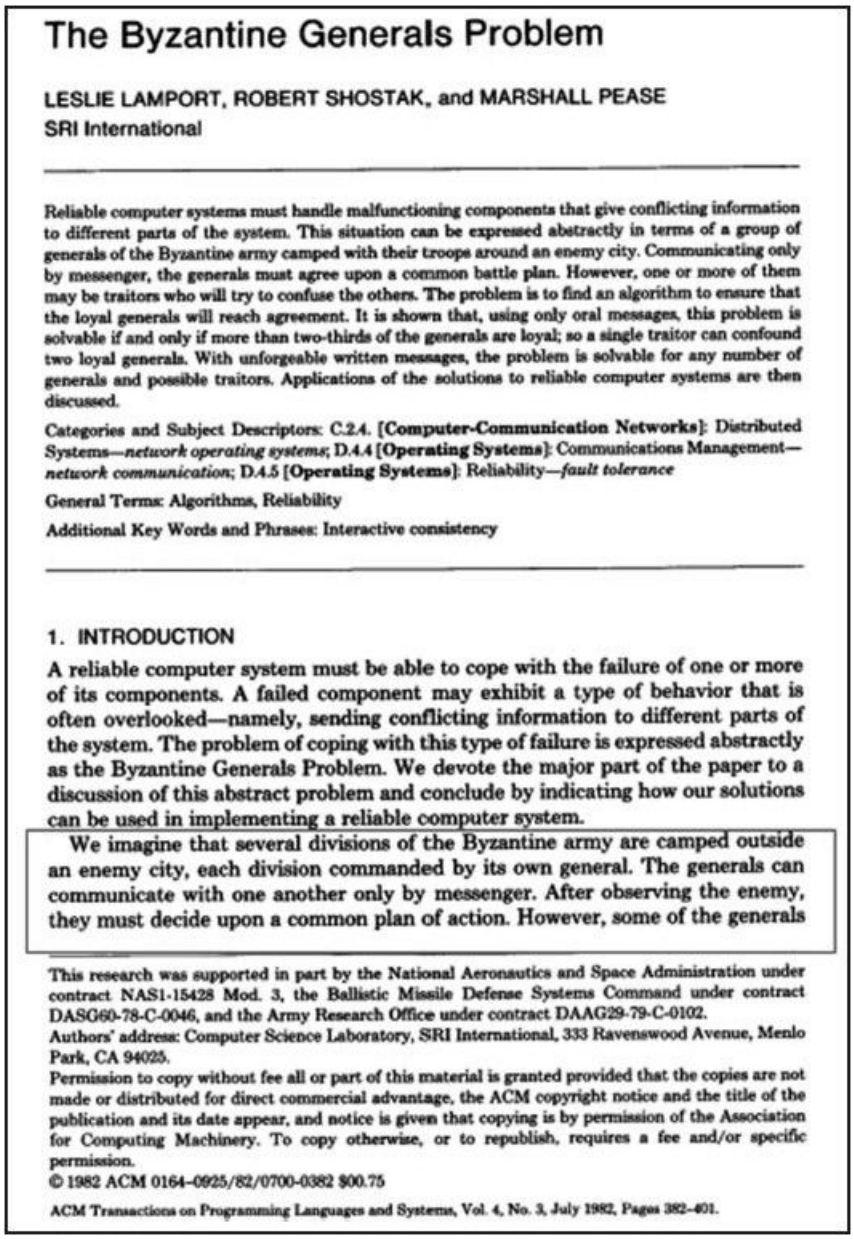
下面我们就来分析一下想同时达成以上两个条件有多么困难。

我们先看第一个条件，这个并不复杂，我们只需要让系统的每个参与方都能保存完整账本即可。接下来，我们把第二个条件加入进来，这时候发现麻烦来了：在所有参与方都可以保存账本的前提下，又让所有参与方都拥有记账的权力，必然会导致账本数据的不一致。这个道理很浅显：即使不考虑恶意的参与方，由于每个参与方所处的物理环境不同，因此接收到的账务信息不可能是完全一致的。而作为一个记账系统，数据的一致性是最基本要求，如果我们不能拥有一致的账本数据，大家记的账各不相同，那么整个记账系统无疑会乱作一团，也就没有任何价值了。

依据之前的分析，既然所有参与方同时记账会导致混乱，那么为了保证数据的一致性，我们就不得不选择让某个特定参与方拥有存储账本的权力或是记账的权力，然而这样，就会至少与上面的两个条件之一相违背……这似乎成了不可能解决的问题。

拜占庭将军问题

在揭开谜底之前，我们先回顾一个历史上的经典问题：拜占庭的将军们围攻一座城堡，军队被分散成很多分支，每一支军队由一名将军独立指挥。将军们之间通过传令兵来保持交流，以期达成一致的行动（进攻或撤退）。但是有些将军是隐藏的叛徒，他们会用虚假的信息来扰乱忠诚将军们的计划。大家并不知道叛徒是谁，那么，忠实将军们有办法达成一致的行动而不被虚假信息干扰吗？



The Byzantine Generals Problem

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.

Categories and Subject Descriptors: C.2.4. [**Computer-Communication Networks**]: Distributed Systems—*network operating systems*; D.4.4 [**Operating Systems**]: Communications Management—*network communication*; D.4.5 [**Operating Systems**]: Reliability—*fault tolerance*

General Terms: Algorithms, Reliability

Additional Key Words and Phrases: Interactive consistency

1. INTRODUCTION

A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked—namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem. We devote the major part of the paper to a discussion of this abstract problem and conclude by indicating how our solutions can be used in implementing a reliable computer system.

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals

This research was supported in part by the National Aeronautics and Space Administration under contract NAS1-15428 Mod. 3, the Ballistic Missile Defense Systems Command under contract DASG60-78-C-0046, and the Army Research Office under contract DAAG29-79-C-0102.
Authors' address: Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025.

历史上并没有拜占庭军队围攻城堡的事件，这个例子其实是研究分布式一致性（Distributed Consensus）问题的祖师级人物莱斯利·兰波特（Leslie Lamport）创造的。但这个例子完美表达了分布式一致性的核心问题，因此常常被人们引用。

其实，一致性问题尤其是分布式系统的一致性问题是个很大的概念，也是计算机科学领域很早就在研究的内容。传统上对这个问题的研究是为了增加分布式系统的可靠性。比如Twitter、Facebook这样的系统，它们有很多服务器，同时记录着系统上发生的所有行为。每一条信息分别记录在不同的后台节点上，系统具有分布式的特征。如果记录出现不一致，就有可能发生用户信息丢失的情况。时至今日，这样的系统也没有达成完美的一致性。分布式系统和去中心化系统并不是等同的概念，但是都要面对在缺乏信任的前提下如何取得一致的问题。

在任何一个系统中，不一致的信息都会造成系统混乱。去中心化的系统没有中央管理机构，因而信息传播的一致性更成为关键的问题。下面我们看一下中本聪给出的解决方案到底是什么。

区块链经济系统

中本聪构造了一个极为精巧的系统，解决了这个看起来不可能完成的任务。这个系统被称为“区块链”。从字面意思上看，“区块链”就是以“区块”这个东西组成的链条。那么区块是什么？我们可以先做一个形象的类比：如果区块链是一个实物账本，那么区块就相当于账本中的一页，区块中承载的信息就是这一页上记载的交易内容。

那么，区块链是靠怎样的架构设计最终解决了去中心化记账的难题呢？竞争记账机制成为了解决问题的关键。

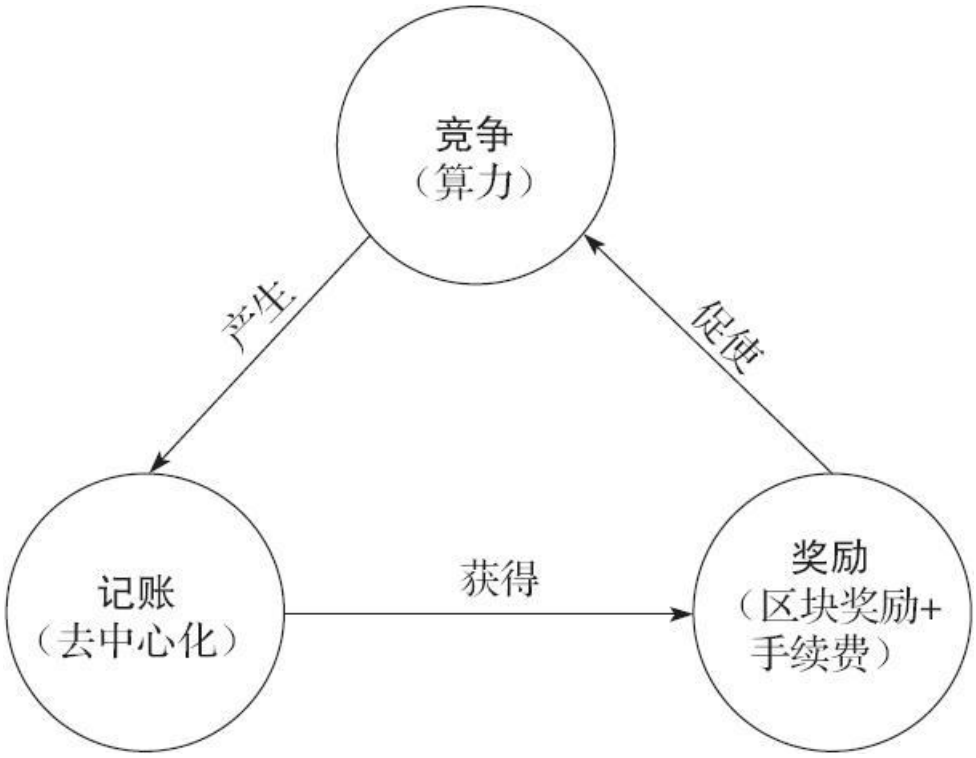
这里我们先引入一个称为“节点”的概念。在当前的信息时代，负责记账的自然是计算机，而在记账系统中接入的每一台计算机都可以称作节点。

所谓的竞争记账，就是以每个节点的计算能力（“算力”）来竞争记账权的一种机制。在比特币系统中，大约每十分钟进行一轮算力竞赛，竞赛的胜利者获得一次记账的权力，即向区块链这个总账本写入一个新区块的权力。这样，在一定时间内，只有竞争的胜利者才能完成一轮记账并向其他节点同步新增账本信息，这个过程就是区块产生的过程。

这里要指出的是，计算能力只能决定赢得竞争的概率。为了便于理解，我们可以用彩票系统做一个形象的类比，算力高的节点相当于可以一次买很多张彩票的人，算力低的节点相当于一次只能买一张或是几张彩票的人。在一轮开奖中，一次买很多张彩票的人只是中奖概率更大，却并不是一定会中奖。

那么，算力竞争是如何做到的？又由谁有权判定竞争的结果呢？区块链系统是通过一个称为“工作量证明”（Proof Of Work，POW）的机制完成的。举个形象的例子，比如要组装一批玩具，早上起来我给了你一些零件，晚上回来便看到玩具摆在桌上，虽然我没有从早到晚盯着你做玩具的过程，但我也能确定你确实做了这么多工作。这就是对工作量证明的简单理解——通过一个（人人都可以验证的）特定的结果，就能确认（竞争的）参与者完成了相应的工作量。关于POW的机制与实现细节会在下面的章节中详述。

不过，算力竞争是要付出成本的，没有激励，节点就没有进行竞争的动力。在中本聪的设计里，每轮竞争胜出并完成记账的节点将可以获得系统给予的一定数量的比特币奖励[2]。这个奖励的过程同时也是比特币的发行过程[3]。节点不停地进行计算，以期获得系统发放的比特币。这种设计相当巧妙——它将竞争记账机制与货币的发行完美结合到一起，在引入竞争的同时，解决了去中心化货币系统中发行的难题。这个过程很像现实生活中黄金开采的过程，因此被人们形象地称为“挖矿”。



最终，区块链通过构造一个以竞争-记账-奖励为核心的经济系统，解决了去中心化记账的难题。在这个系统中，每一个节点只需要根据自身利益行事，出于“自私”的目的进行的竞争，最终造就了保护系统安全的庞大算力基础，提升了系统的可靠性。比特币借助区块链打造了一个正向循环的经济系统，才使得其在没有强大的中心化机构或组织推动的情况下，自然地生长出来并发展壮大。

[1] 引用自http://www.coindesk.com/can-trust-basedprivate-blockchains-be-trusted/。

[2] 只有在最长链上完成记账的节点，才能最终获得系统给予的比特币奖励。关于最长链原则请参考本书第5章。

[3] 更准确地说，系统发放的奖励包含两部分，一部分是区块所包含交易的手续费，这部分不属于比特币的发行过程；一部分是新币奖励，新币奖励每四年减半一次，是比特币的发行过程。目前打包区块获得的奖励以新币奖励为主。

共识机制与价值载体

共识机制是区块链技术的核心，它使得区块链这样一个去中心化的账本系统成为可能；而价值载体是区块链技术的潜力所在，它使得区块链技术的应用领域远不止数字货币。这两个核心因素是区块链内生能力得以扩展的关键。

共识机制与去中心化

如何达成共识——只有在去中心化的结构下才成为问题。

在中心化的结构体系中，系统的共识由中心决定，各参与方只需要服从这个中心即可，因此，共识的建立是极为高效的。而在去中心化的结构体系中，由于系统的各个参与方地位平等，当出现分歧的时候，如何达成共识就成了问题。

市场经济是一个典型的去中心化系统，这个系统的共识机制就是市场经济制度。参与市场经济的每个主体都在遵守商业规则的基础上，按照实现自己利益最大化的原则行事，同时在客观上推动了整个市场的繁荣。“无形的手“推动了人们争取自身利益的行为，这些行为的结果则服务于更大的社会利益。正如亚当·斯密所说：“我们的晚餐并非来自屠宰商、酿酒师和面包师的恩惠，而是来自他们对自身利益的关切。”

共识机制与资源消耗

现在我们知道，比特币区块链的共识机制是通过工作量证明（POW）来实现的，这种机制的优点是显而易见的，每个节点可以平等地参与竞争，并通过激励构建了一个正循环的经济系统，从而逐渐积累了保护系统安全的庞大算力。

然而对工作量证明机制也有一些批评。一个常见的指责是“浪费”能源，因为节点进行算力竞赛是要消耗电力的。目前，投入挖矿竞争的总算力已经接近1300P（注：引用自http://qukuai.com/pools，可以近似认为1P的算力能够实现每秒10^{15}次哈希计算。），挖矿也因此成了能源密集型的行业（注：用目前主流的28nm矿机来估算的话，1300P算力每秒消耗的电力高达2.16×10^{5} kW。）。

由于存在对工作量证明机制消耗能源的担忧[1]，一些人也在探索和实践新的共识机制，即采用非算力竞争的方案来选择记账节点。其中典型的是权益证明机制（Proof Of Stake，POS），以节点持有币的数量和时间来选择记账权；还有股份授权证明机制（DPoS），它类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。另外还有燃烧证明（Proof Of Burn）、沉淀证明（Proof Of Deposit）等方案，这里不一一赘述。不过我认为，目前这些探索本质上并没有改变“需要消耗资源”的实质[2]。从目前的实践看，工作量证明机制仍然是最为有效和可靠的去中心化共识机制。

那么，未来是否会有更先进的技术来降低共识机制资源消耗呢？在我看来，对于更低成本甚至无成本的共识机制[3]的追逐，正如人类历史上对于永动机的追逐一样，是注定要失败的。虽然我们并不能说POW就是最好的去中心化共识机制，但是我真正想表达的是，当谈到区块链技术与共识机制时，我们应该知道天下没有免费的午餐。

共识机制与私有链

所谓公有链，是指比特币区块链这样的完全去中心化的、不受任何机构控制的区块链；而私有链[4]则是指存在一定的中心化控制的区块链。

相较于完全公开、不受控制、依靠加密技术来保证安全的公有链而言，私有链可以创造出权限控制更为严格的系统，其修改甚至是读取权限可以仅限于少数用户。正因如此，关于私有链和公有链的争论一直没有中断过：一方认为私有链没有任何意

义，和分布式数据库没有太大区别；另一方则认为私有链仅仅是对参与者进行一定控制的区块链，只要在有多方参与且不完全互信的环境下，需要共识机制的建立以及达成共识的过程，私有链就有存在的价值。

从本质上来说，私有链就是以牺牲部分去中心化的特性为代价，来换取对于区块链权限的一些特殊控制，并且可以使用比公有链更为高效、灵活、低成本的共识机制。我们认为，私有链确实有大量的场景可以对接现实世界的需求，有限的去中心化更容易达成共识，可以使交易速度更快、效率更高，并且可以提供更多受控的功能，比如，在特定场景下必要的交易回滚。去中心化与中心化并不是非此即彼，相反，它们之间是一种共生共存、互相依赖与结合的关系。在去中心化协议的基础上，可以衍生出各种中心化的服务，以适应不同行业及领域的个性化需求。比如，VPN（Virtual Private Network）就是一个在共用网络上构建专用网络的例子，该技术允许人们利用互联网现有的基础设施，构建有限且开放的专有网络，而无需投入大量硬件资源重新构建底层基础设施。更为广泛的例子存在于互联网的各种服务提供者中，域名注册机构、电子邮件运营商以及提供各种形式服务的网站，都是基于互联网这个去中心化的系统构建或提供各种类型的中心化服务的例子。

近一两年来，区块链吸引了全球各大主流金融机构的注意，他们纷纷对区块链进行调研，甚至专门成立实验室或部门，研究在各种金融场景中使用区块链技术的可能性。但是类似比特币区块链这样的公有链尚不能满足金融机构的一些基本要求，比如了解你的客户（KYC）、反洗钱（AML）等，因此，金融机构对私有链的兴趣更大。目前私有链最著名的例子是R3CEV公司牵头的区块链联盟，它已经吸引了全球四十多家大型银行的加入[5]，其中不乏美国银行、摩根大通等巨头的身影。

价值载体

共识机制的建立使得区块链这样一个去中心化的记账系统成为可能，而其发展潜力则体现在这个系统上所能承载的各种价值形式。

显然，作为一个记账系统，区块链上面不仅可以记录数字形式的货币，也可以记录能用数字定义的其他任何资产，甚至，由于区块链上的价值转移可以通过脚本语言来完成，这意味着区块链上还可以定义更为复杂的交易逻辑。也就是说，除了数字货币，区块链还可以承载股权、债券、产权、版权、公证、合约、投票等可以用数字形式进行价值存储或转移的任何东西。

也正因如此，区块链技术才吸引了越来越多精英人士和顶级机构的关注。这也很容易理解，正如《经济学人》的封面文章[6]所讲的，区块链是一个制造信任的机器。在任何需要信任的领域，区块链都有用武之地。

价值载体之数字货币

显然，比特币并不是唯一的基于区块链技术的数字货币。据统计，仅2015年，新发布的数字货币就有800余种。坊间笑称，发行新币最难的部分是起名字，因为常用的可以起名字的英文单词已经用完了。

事实上，自比特币诞生之日起，它的模仿者或竞争者就层出不穷。其中有很多都只是对比特币简单的复制和模仿，没有任何创新，我们将这种称为山寨币。还有一些并不是简单的模仿，而是有自己的创新和专注的领域，这种类型的币我们称之为竞争币[7]。在数字货币的市值方面，尽管比特币遥遥领先，但之后诞生的莱特币、以太坊的市值都曾短暂地超过10亿美元。

数字货币是目前区块链创造的使用最广泛也是受认可程度最高的一类应用。以比特币为代表的数字货币一度成为区块链的代名词。可以预期的是，即使在区块链广泛使用的未来，数字货币也仍然会是最为重要的区块链应用之一。

价值载体之数字资产

数字资产和区块链具有天然的亲和性。一般意义上讲，数字资产包括任何形式的以二进制格式存在并且具备所有权属性的东西。而在较为狭义的理解中，数字资产则是指以电子数据的形式存在的，在日常生活中持有以备出售的非货币性资产，比较

典型是股票、债券等金融产品[8]。

美国著名的互联网零售企业Overstock就基于区块链建立了tØ股权交易平台，并将在上面发行自己的股份。在摩根大通担任了近30年主管的布莱斯·马斯特（Blythe Masters）则担任了数字资产控股公司（Digital Asset Holdings）的CEO，寻求如何将区块链技术应用于华尔街。

另外，由于区块链公开、透明、难以篡改的特点，利用区块链技术可以非常方便地为任何数字资产或有价值的信息实现比现有中心化结构更为可靠的存在性证明，以及各种形式现实资产的登记或转移。这方面的应用可以包括产权、版权、公证等诸多领域。

如果说比特币等基于区块链的数字货币是一个刚诞生不久的婴儿，那么基于区块链的非货币形式的价值承载则还是一个孕育中的胚胎。作为价值载体，区块链可以承载的价值是非常丰富的。随着区块链技术的发展和相关基础设施的不断完善，我们相信区块链承载价值的范围会不断扩大。

[1] 对于工作量证明机制浪费能源的批评，我们认为，要达成去中心化的可靠共识，必然要付出一定的成本，考虑到这同时也是创造新币的过程，因而与新币价值相对应的成本消耗几乎是必然的。

[2] POS需要该数字货币的持有者锁定其所持有的币以换取“挖矿”收益，相当于消耗了“资本流动性”。

[3] 这里的共识机制特指类似比特币区块链这样的完全去中心化的区块链，即“公有链”的共识机制。

[4] 目前关于区块链的分类并没有统一的标准。有人将区块链分为公有链、联盟链和私有链。而我们则认为，联盟链由于存在一定的中心化控制，所以属于我们所说的私有链范畴。

[5] 引用自http://www.coindesk.com/r3-blockchain-new-partnerships/。

[6] 引用自http://www.economist.com/news/leaders/21677198-technology-behind-bitcoincould-transform-how-economy-works-trust-machine>。

[7] 分类和叫法没有一定之规。业内也有一种意见认为，应该将所有比特币之后的数字货币统一称为竞争币。

[8] 引用自https://en.wikipedia.org/wiki/Digital_asset。

当交易变得智能

在传统的账本中，账上的数据仅仅是一种纪录。而在区块链这个账本上，这些数据则有了超越账本的意义——它们是可编程的。

这是一个质的变化。由于区块链的可编程属性，使得区块链上所能承载的就不仅仅是普通的交易，而是可以基于程序自动执行的智能交易。

脚本与多重签名技术

比特币区块链上的交易可以通过脚本来实现。所谓脚本（Script），就是使用一种特定的描述性语言编写的、可执行的计算机代码。比特币的脚本语言非常简单，仅有256条指令，其中75个是被保留的，尚未被赋予任何含义。比特币脚本中的指令与其他编程语言类似，包含基本的语法、逻辑，除此之外还包括一些加密指令，如哈希函数、签名验证等。

比特币的多重签名技术就是使用脚本实现可编程交易的一个典型例子。其基本原理是，在系统里创建一个由多个人共同管理的账户，只有达到事先约定数量的人的同意，才能动用该账户的钱，并且这个过程是由系统本身保障执行的，不需要任何第三方介入。

一般来说，一个比特币地址对应一个私钥[1]，动用这个地址中的资金只需要该私钥的掌握者单独发起签名即可。而多重签名技术就是需要多个私钥的共同签名才能动用一笔资金。比如说，某笔资金对应3个私钥，而必须至少有其中任意2个私钥参与签名才能动用，只有1个私钥参与签名是无效的。这个2/3可以推广到任意的m/n，比如3/5、4/7、6/11等，当然m要小于等于n。

多重签名技术有着广泛的应用空间，一个最直观的场景就是类似于支付宝的应用，卖家、买家和作为担保的第三方可以构建一个多重签名的交易，约定其中至少两方取得一致才能决定资金的流向。其他容易想到的应用场景还有：更安全的在线钱包、共同财产、合伙经营、资金监管等。以上构想的场景都是比较简单的，具体实践中一定会有更加灵活丰富的形式。

智能合约

智能合约的理念可以追溯到1994年，几乎与互联网（World Wide Web）同时出现。密码学家尼克·萨博（Nick Szabo）首次提出了“智能合约”这一术语。从本质上讲，智能合约工作原理类似于计算机程序的条件执行语句。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。由于区块链的可编程性，因此智能合约在区块链和数字货币上的应用是水到渠成的事情。

举一个简单的例子，以西甲国家德比为例。假如你赌皇马赢，下注一个比特币，你的朋友赌巴萨赢，下同样的注。比赛开始前，你和你的朋友将你们的比特币发送到一个由智能合约控制的中立账户。比赛结束后，智能合约能够根据比赛结果，自动地将相应的资金发送到赢家的账户。

再比如网上购物，如果你从网上买了某商品，但不想立即付款给卖家，希望等到发货后再付款。这时你可以创建一个合约，这个合约可以自动查询快递的物流数据，当确认你购买的商品已经发出时，才给卖家发送货款。

以上只是简单的解释和举例，智能合约是计算机程序，所以很容易应用于其他需要的场景——增加更加细致的控制条件，完成更复杂的执行逻辑。这有点类似传统的合同，我们也可以认为，智能合约就是把合同以代码的形式搬到了区块链上，但这就带来了根本的区别：它不需要任何人监督合同的执行，订立合同的双方也无法在合同完成前单方面违约，一切都是按合同的约定自动执行的。相信随着区块链的普及和交易智能化的发展，它将会对未来的交易模式与商业结构带来巨大的影响。

从具体的实践来看，由于比特币的脚本语言并不是图灵完备[2]的，所以在扩展性上，比特币区块链目前所支持的资产定义和交易模式还比较有限。

因此，业内一些人开始尝试开发不同于比特币区块链的、支持图灵完备脚本语言的区块链，以太坊（Ethereum）就是一个典型的例子。目前，以太坊上的代币以太币（ETH）的市值已经达到了比特币的1/10，成为全球市值排名第二的数字货币[3]。

[1] 其技术细节会在第5 章详述。

[2] 所谓图灵完备，是指语言可以做到用图灵机做到的所有事情，可以解决所有的可计算问题。图灵不完备的语言常常是因为循环或递归受限，无法实现类似数组或列表的数据结构，这会导致能写的程序有限。

[3] 截至2016年5月14日，比特币价格为2971元，市值约合461亿人民币，以太币价格为65.9元，市值约合52.7亿人民币。

将区块链连接起来

如果说共识机制与价值载体是区块链内生能力得以扩展的关键，那么以侧链技术为代表的、能够将不同区块链连接起来技术，就是区块链拓展外在结构的关键。

比特币区块链的局限

很多人说比特币是目前区块链最成功的应用，这么说有一定道理，但更贴合实际的说法是：由于在创造比特币时，并没有现成的、可以支持比特币系统运行的底层技术架构，所以中本聪创造了区块链。也就是说，中本聪创造区块链的初衷是为了实现一个点对点的电子现金系统。因此，当我们对于区块链的用途有更高的期待时，它的一些局限就体现出来了。

首先，比特币区块链的设计只考虑了比特币的交易，本身并不支持定义其他资产，或是定义复杂的交易逻辑。如果要添加新功能，就要对系统进行升级，然而困难在于，对于比特币这样的完全去中心化的系统，任何改变都需要获得社区的一致同意，以至于快速改变是异常困难的。

其次，大多数改变本身是不必要的甚至是无法达成的，因为更多的灵活性往往意味着复杂度的上升及随之导致的稳定性的下降。考虑到现实需求的多样性，甚至有些需求是相互冲突的，一条区块链注定无法同时满足所有的需求。

比特币的上述局限直接导致了部分竞争币的诞生，这些竞争币采用了不同的区块链，有着各自的特点和创新。但是，由于缺乏广泛的共识与信任，绝大部分基于新区块链的竞争币并不拥有类似比特币区块链这样在强大的算力保护下的稳定与安全，同时币值的稳定性也普遍较差。更重要的是，数字资产不能在不同的区块链间直接转移，这导致了价值的孤岛，正如同一个个不能互联互通的“局域网”一样。

侧链技术

为方便数字资产在不同区块链间互相转移，侧链（Sidechain）技术应运而生。简单地说，侧链就像是一条条通路，将不同的区块链互相连接在一起，以实现区块链的扩展。侧链完全独立于比特币区块链，但是这两个账本之间能够“互相操作”，实现交互。

在侧链技术的研究方面，Blockstream是较为领先的一个公司。2014年10月，以亚当·贝克[1]为首的开发团队正式发布了侧链白皮书[2]，2015年6月，Blockstream宣布将为其侧链项目发布一个开源代码库和测试环境[3]。

侧链白皮书中提出了一种新技术——“楔入式侧链”，通过它可以实现不同区块链间资产的互相转移。由于侧链是独立的系统，因此技术与理念上的创新不会受到主链的局限，即使出现创新失败或者恶意攻击，所受的损害也只限于侧链本身。

本质上，区块链是不同数字价值的载体，而侧链技术则是连接不同区块链的通路。现在还不能断言最终成熟的侧链技术形态，甚至我们也不知道未来真正大规模应用于区块链间连接的技术是否会以“侧链技术”的名义出现，但侧链技术的理念及核心功能的发展与成熟是毋庸置疑的。

[1] 亚当·贝克是英国的密码学专家，哈西现金的发明者，同时也是Blockstream公司的总裁。

[2] 引用自http://www.blockstream.com/sidechains.pdf。

[3] 引用自https://elementsproject.org/。

区块链的未来

通过前面的讲述，相信读者已经对区块链是什么有了基本的了解。接下来大家可能会好奇，基于这些特点，随着区块链技术的进一步发展和普及，未来的区块链会是什么样子呢？

虽然没有人能够预言细节，但是对未来发展的大方向我们却可以有清晰的判断。下面我们分别从经济和技术两个角度着眼，对未来做一个简要的勾勒。

价值互联网

信息不对称（Information Asymmetry）是指参与交易的各方所拥有的可影响交易的信息不同[1]。一般而言，卖家比买家拥有更多关于交易物品的信息。由于互联网的出现，新一代的传播渠道和几乎瞬时的传播速度使人们可以更容易地得到想要的信息。今天，互联网之所以给商业社会带来了深刻的影响，正是由于它打破了信息的不对称。

然而，互联网对于信息不对称的打破还远不够彻底。在互联网上，我们有了统一的信息传输层，但是还没有统一的价值传输层。因此在进行交易（价值传输）的时候，我们仍然需要依赖大量的中介机构来保证价值的可靠存储和转移。这些中介机构的存在不仅降低了价值传输的效率，也增加了价值流通的成本。

基于互联网构建统一的价值传输层，即价值互联网的诞生，将是区块链发展及演进的必然结果。价值互联网的诞生将进一步打破信息不对称的壁垒，让以货币及数字资产为代表的数字化价值无需借助大量的中介机构，就能在全球范围内自由流动。这将让市场效率获得一次质的飞跃，甚至彻底改变目前的金融与经济格局。

基础协议与分层结构

本质上，互联网同区块链一样，也是个去中心化的网络，并没有一个“互联网中心”存在。不同的是，互联网是一个高效的信息传输网络，但并不关心信息的所有权，没有内生的、对有价值信息的保护机制；区块链作为一种可以传输所有权的协议，将会基于现有互联网协议架构构建出新的基础协议层。从这个角度看，区块链（协议）会和TCP/IP协议一样，成为未来互联网的基础协议之一。

另外，区块链的未来将是复杂的，它的复杂性并不是体现在任何一条区块链本身，而是体现在由区块链组成的层级结构中。正如TCP/IP协议栈的分层结构，不同的层级承载不同的功能。人们在统一的底层协议基础上发展出了各种各样的应用层协议，最终构建出了今天丰富多彩的互联网。

未来区块链的结构也一定是分层的，不同层级、不同类型的区块链承担着不同的作用。我们认为，未来的区块链也将会在一个统一的底层协议基础上发展出各种各样的应用层协议，从而构建出多样化生态的价值互联网。

颠覆性技术的发展曲线

变革常常更能推动人们抛弃成见，激发全新的思考，区块链的崛起将颠覆人们对很多行业和事物的认知。

然而，对于指数型发展，我们容易形成的误判是高估短期影响、低估长期影响。正如2000年互联网泡沫的崩溃，互联网从可以改变一切并受到无数资本热捧的状况中瞬间跌入谷底。大家终于发现，互联网并非如此神奇，大多数公司并没有成功依靠互联网构建出有价值的商业模式。然而，又有多少人能想到，仅仅十几年后，互联网已经深刻地改变了当今商业社会的格局，更改变了我们每个人的生活。

如同互联网的发展一样，区块链这种协议式的、需要大规模协作和参与的颠覆式技术，其崛起的周期将比大多数人预想的要长，而最终影响的范围和深度也会远远超出大多数人的想象 。区块链未来发展的过程不会一帆风顺，可能会经历过热甚至泡沫阶段，也可能会经历低谷。但我相信，区块链作为数字化浪潮下一个阶段的核心技术，最终将会构建出多样化生态的价值互联网，从而深刻改变未来商业社会的结构与我们每个人的生活。

[1] 引用自https://en.wikipedia.org/wiki/Information_asymmetry。

本章结语

本章我们在尽量不涉及技术细节的前提下讲述了区块链的相关知识，包括区块链的本质、原理、核心要素以及我们对区块链发展方向的判断。区块链是一个伟大的发明，由它构建的价值互联网是一片广袤的新大陆，是未曾探索的大海，是刚刚露出水面一角的庞大冰山。不管是区块链技术还是相关的行业发展，都有无尽的精彩在前方等着我们去发现与开拓。

第2章　区块链带来的新机遇

数字货币产业链

区块链是作为比特币的基础设施而发明的。自此之后，以比特币为代表的数字货币产业链也从无到有地发展起来。相关产业形态日渐多元，规模不断扩大。随着技术及市场的发展，利用区块链技术创造的数字货币已不再局限于比特币。不过就目前而言，无论从产业链的发展程度、全球影响力还是使用人群来说，比特币都远超过其他的数字货币。因此，本节将以介绍比特币产业链为主，让大家对数字货币产业这个略显神秘的新行业有一个结构性的了解。

“挖矿”产业

发行是比特币产业的最上游，在这一部分，目前中国的相关公司占据了绝对优势。中国的矿机厂商生产了大部分挖矿设备，中国的矿池集中了全网大部分算力。

1.“挖矿”小史

就像乔布斯重新定义了“苹果”一样，对数字货币爱好者来说，中本聪重新定义了“挖矿”“矿工”“矿机”。比特币的竞争记账过程是通过节点算力的竞争实现的。这个过程就是常说的“挖矿”，运行这些计算节点的人就是“矿工”，而这些计算的节点、矿工挖矿的工具就是所谓的“矿机”。

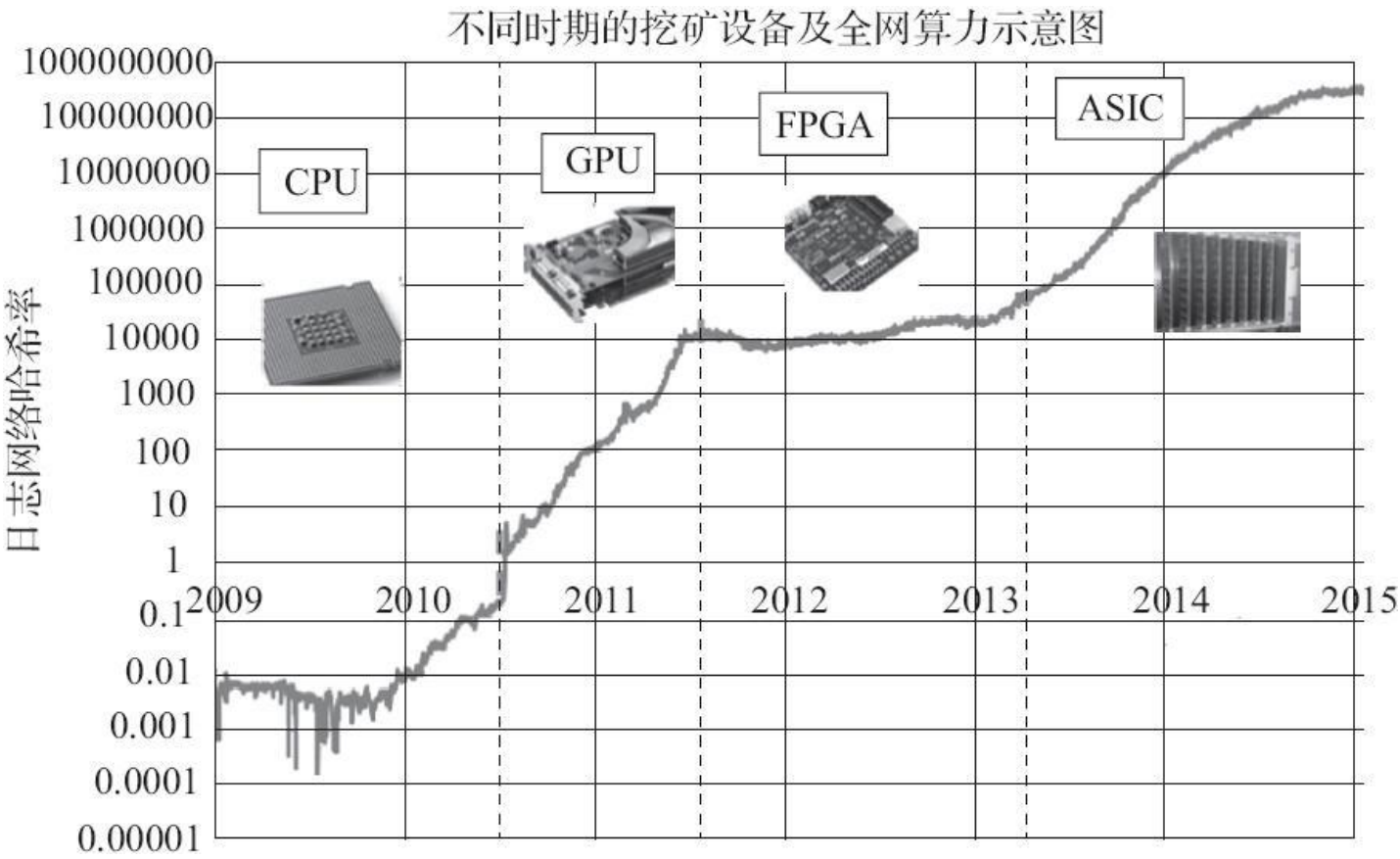
随着比特币的价值得到越来越多人的认可，打包区块获得的比特币奖励越来越“值钱”，整个系统的算力竞争也越来越激烈，挖矿工具随之经过了数次更新换代。

最早的挖矿工具是个人计算机上的通用中央处理器（CPU），较为高端的台式机CPU可以达到大约20MH/s的运算能力（约每秒2000万次哈希运算）。初期，由于挖矿难度非常低，因此普通的计算机也能挖到大量比特币，而那时比特币几乎不值钱。

比特币挖矿类似于一个暴力破解的过程。相比于CPU，独立显卡（GPU）在并行运算能力上有明显的优势，因此也更适合比特币挖矿。GPU可以使挖矿速度提升几十乃至几百倍。著名的比特币披萨购买者拉兹洛·豪涅茨（Laszlo Hanyecz）是世界上使用GPU挖矿的第一人[1]。显卡挖矿时代是比特币挖矿历史上最热闹的时期，以至于当时无论线上渠道还是线下卖场，高端显卡全部售罄。

2010年之前基本是CPU在挖矿，全网算力一直在1GH/s以下。2011年开始显卡加入挖矿大军，下半年全网算力一举突破10TH/s，一年增长了10000倍！2012年更是轻松地超越20TH/s！显卡矿机迎来了全盛时期[2]。

随后，专业矿机诞生并占据了挖矿设备的主流位置。很快专业矿机从可编程门阵列（FPGA）过渡到了高效能专用集成电路（ASIC）。而且，ASIC矿机的功能参数也在不断进化，不断有算力更强大的矿机被研发出来并投入市场，同时将挖矿效率低的老矿机淘汰出局。



图片来源：https://www.cryptocompare.com/mining/guides/how-has-bitcoinmining-changed/

当下，如果不使用专业矿机的话，挖矿事实上已经不可行了。我们简单估算一下，以当前的难度，如果使用CPU挖矿，大概需要昼夜不停地运算150万年才有成功一次的机会。工欲善其事，必先利其器，因此对于矿工来说，购买高效率的矿机是挖矿的第一步。

2.矿机江湖

每一个新兴产业的初期，都有一个各种公司野蛮生长的洪荒时期，矿机制造作为比特币产业链的最上游，自然也不外。在短短三年多的时间内，国内外众多参与者轮番上场参与角逐，在比特币的发展史上留下了自己的传说[3]。

中国的南瓜张是矿机时代的开创者。在2011年下半年，他推出了第一代FPGA矿机，引起轰动；2013年1月，又推出了首台阿瓦隆矿机（使用ASIC芯片）。后来随着市场竞争和矿机制造工艺的不断升级，其他的市场参与者逐渐占据了领先的地位。

目前，矿机制造厂商还有很多家，实力较强的有总部位于旧金山的BitFury和总部位于中国的比特大陆（Bitmain）。其中，比特大陆生产的蚂蚁矿机现在占据了大部分市场份额。

3.矿场和矿池

随着比特币的价值被越来越多的人认可，挖矿投入的人力、物力不断上升，挖矿行为从早期的单兵作战迅速演化为专业化、规模化的运作，挖矿地点也从“自家后院”转移到“专业矿场”。

参与挖矿的模式也分成了两类，除了掌握较多财力和资源的矿工可以自建矿场，继续单独挖矿外，更多的矿工选择了加入“矿池”，采取联合挖矿的模式。

单独挖矿不需要和别人分享你的收益，但是随着全网算力的不断上升，单独挖矿成功打包区块的概率在显著降低——尤其是在算力不够大的情况下。而加入一个矿池则可以增加竞争胜利的概率，但是收益要在所有矿池成员之间进行分配。

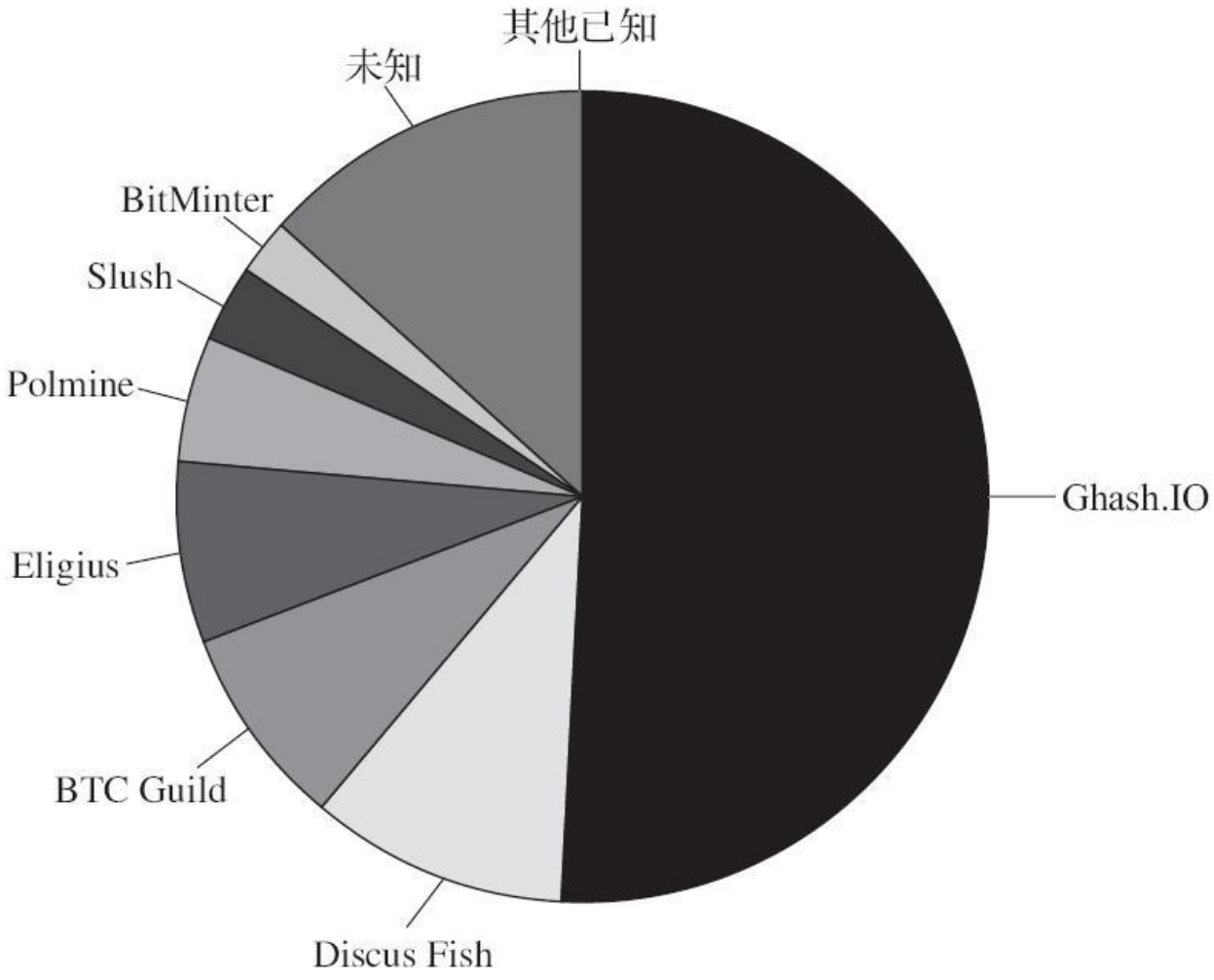
矿池属于矿工的松散联盟，矿工们将挖矿资源汇集在一起，共享算力，同时通过一定的算法，矿池管理者收取一定的管理费，矿工按各自的算力占比分享挖矿收益[4]。

现在世界上有很多矿池，人们可以根据自身的情况自由选择加入哪一个。一般人可能会下意识地相信更大的矿池，但对比特币系统来讲，选择较小的矿池会更健康，这样可以避免算力集中带来的潜在伤害。

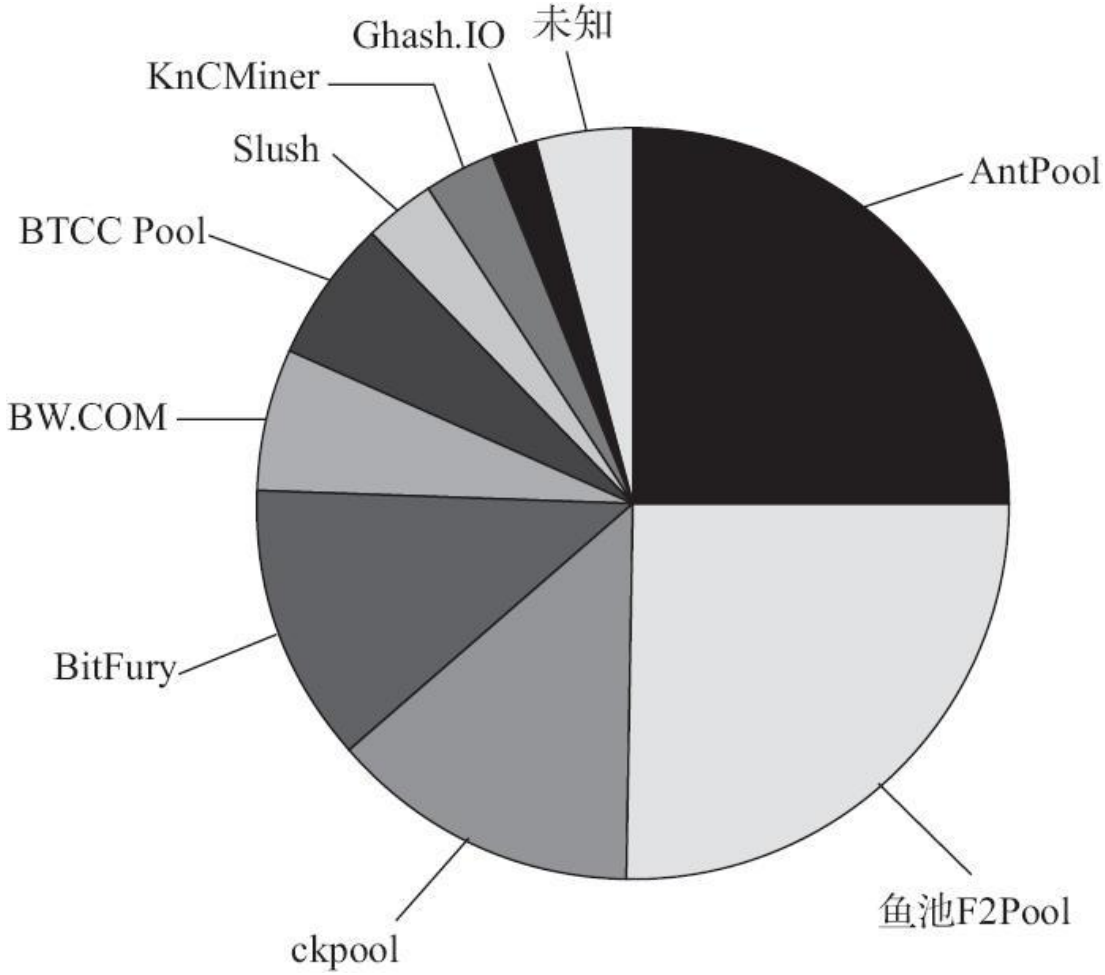
自矿池这种挖矿模式诞生以来，不同的矿池所占的算力比例就一直在变化之中。

人们一直在担心，如果单一矿池所占的算力超过了50%，系统就会面临51%攻击的威胁。Ghash.IO的算力占比就曾短暂地接近50%，之后，很多矿工自发撤离了这个矿池。不可否认的是，任何单一矿池所占的算力比例过大都是对系统的潜在威胁。

以下是2014年6月不同矿池算力占比的示意图。



以下是2016年4月不同矿池算力占比的示意图。



4.云挖矿

对个人来说，挖矿门槛越来越高。因此出现了云挖矿模式。简单地说，云挖矿就是个人投入资金，然后云挖矿平台帮你完成剩余的其他事情——包括购买机器、运行矿场并进行维护等。一般来说，云挖矿模式包括托管矿机挖矿、虚拟主机挖矿、租用算力挖矿三种[5]，目前，又以租用算力的模式最为常见。云挖矿这种模式可以为普通人解决挖矿技术资金门槛过高的问题，同时为相应平台解决（部分）资金问题，因此从商业模式上来讲，云挖矿有其生存的空间。然而，除了正常经营的云挖矿服务外，这也是最容易滋生欺诈的一种挖矿方式，Hashie.co、CloudHashing.com等提供的云挖矿服务就是前车之鉴[6]。

交易平台

随着比特币得到越来越多人的认可和使用，在比特币网络上发生的交易数量也与日俱增。

以下是比特币网络日交易数与市值随时间变化的示意图。

随着交易的增多，兑换就成为一个刚性的需求。因此交易所是比特币产业链上不可缺少的重要一环。在比特币短短七年的发展史中，诞生了许多的交易所，其中大部分都由于这样那样的原因最终消失了。

1.第一家交易所Bitcoin Market

该交易所于2010年2月6日由Bitcointalk的用户“dwdollar”创建，是世界上第一个比特币交易所。但同年6月，由于一些用户的欺诈行为，交易所撤掉了Paypal支付选项[7]，随后交易量迅速萎缩，被之后成立的交易所MtGox超越。至今仍不清楚该交易所关闭的具体日期。

2.曾经最重要的交易所MT.Gox

MT.Gox（业内戏称“门头沟”）于2010年7月18日由杰德·麦凯莱布（Jed McCaleb）创建，2011年3月被法国人马克·凯普勒斯（Mark Karpeles）接管。在比特币发展的早期，“门头沟”几乎是唯一的交易所，2011年7月，“门头沟”处理了全世界80%的比特币交易[8]。从2014年2月开始，该交易所暂停交易，关闭网站并申请了破产保护，而85万个比特币（当时估值约4.5亿美元）从用户账户中凭空消失了。CEO马克被日本警方多次传唤，而消失的资金大部分至今仍然下落不明。

3.被黑客攻击的例子

由于比特币的价值得到人们的认可，因此比特币交易所也成为黑客攻击的目标。最早因黑客攻击而遭受重大损失的交易所是Bitcoinica，这个交易所于2011年9月8日成立，2012年3月1日由于系统内部出现安全漏洞，超过4.3万个比特币被攻击者窃取。交易所对此发表了一份声明，表示储备资金足以弥补损失，但2012年5月11日该交易所再次遭遇黑客攻击，导致其立即关闭。之后黑客攻击交易所的事件仍然时有发生，现在仍在运行的知名比特币交易所Bitstamp就于2015年1月被盗约1.9万个比特币。

4.现在的交易所格局

目前全球依然有数十家活跃的比特币交易所，并且这个行业也一直处在快速的更新代谢之中。

现在占据主要市场地位的比特币交易所有中国的火币网、OKCoin、比特币中国，位于欧洲的bitstamp和btc-e，位于美国的Bitfinex、coinbase和Kraken等。

随着比特币监管政策的逐渐明确，目前位于欧美的交易所在快速走向合规化，对中国的交易所来说，这也是必然的趋势。

场外交易（Over-The-Counter，OTC）也是比特币交易的组成部分，它是指不在交易所内进行，而以买卖双方私下约定的方式进行的交易。在交易双方对私密性的要求比较高的时候，或是在对比特币不太友好的国家和地区（比如俄罗斯和委内瑞拉），场外交易往往成为首选。目前localbitcoins[9]是全球最大的场外交易平台。

钱包与支付

1.钱包

比特币的存储是比特币使用过程中的一个核心环节。随着比特币走出极客圈子，走向普通大众，钱包服务也随之成为比特币产业中的重要一环。

虽然比特币客户端本身就有钱包的功能，但它不能跨平台使用，同时存在钱包的导入/导出对普通用户来说门槛过高的问题。由于区块数据本身越来越大[10]，因此将完整的比特币客户端作为钱包使用带来的不便也越来越多。因此，市场上出现了多种钱包服务，它们大致可以分为以下三类[11]。

网页钱包。网页端钱包的好处是，不管使用什么设备，只要你能上网，就能使用它。而它的缺点也很明显，即将私钥暴露给第三方的风险相对较大。目前主流的在线钱包都使用了加密或者多重签名的措施以获取用户的信任。目前使用人群较多的在线钱包有Blockchain[12]和Coinbase[13]等。

桌面钱包。桌面钱包可以分为全节点钱包和轻钱包，全节点钱包（如bitcoin-core钱包）同步所有的区块链数据（当前在50GB以上），完全去中心化；轻钱包（如MultiBit）只有简化支付验证功能（SPV），只维护与自己相关的区块链数据，使用起来更加轻便。

硬件钱包。硬件钱包是专门用于存储私钥和进行支付的硬件设备，通常为存储大量的比特币而设计，比如Trezor、KeepKey等。

2.支付

随着比特币使用人群的扩大，到目前为止，已经有微软、戴尔、维基百科、Mozilla、Expedia、绿色和平组织、新蛋网、Overstock、steam等知名组织和公司以及数以万计中小商家开始尝试接受比特币支付，而他们接受比特币的过程绝大多数是通过比特币支付商来完成的。支付商将消费者支付的比特币转化为商家接受的法定货币，打入商家的相关账户，同时收取一定的手续费。对于传统行业的商家来讲，这种模式可以避免比特币行情波动带来的影响。从事比特币支付服务的公司也有很多，其中以

BitPay较为领先，这家公司总部位于亚特兰大，成立于2011年，2015年其日成交额达到了数百万美元。

数据与媒体

比特币系统本质上是分布式账本，对普通用户来讲查阅起来并不容易。因此为用户提供可靠便捷的数据服务也是比特币产业的重要一环，目前国外的Blockchain.info和国内的Qukuai.com是这方面较为领先的公司。

随着比特币影响力的扩大，全球各种主流媒体持续对比特币进行关注和报道，同时，专注于数字货币和区块链技术的媒体也应运而生。这些媒体专注于向外传播比特币和区块链的相关知识，报道业内动态和技术发展，消除误解，传播影响，是比特币从极客走向大众的过程中极为重要的环节。

其中较为知名的是英文站点Coindesk，它成立于2013年5月，目前是全世界最为活跃的数字货币和区块链媒体之一。中文站点巴比特成立于2011年，专注区块链、比特币以及数字货币领域的新闻报道，是中文站点中最具活力的常青树。

小结

本节大致介绍了目前数字货币产业链的主要组成部分，包括它们的简要发展过程以及相关领域的知名企业。必须要指出的是，我们只是对这个变化迅速的行业做了一个鸟瞰式的简要勾勒，挂一漏万之处在所难免。

目前整个产业还处在很初级的阶段，比特币的大规模应用还没有实现。尽管接受比特币的人和企业越来越多，但是星星之火尚未燎原。从另一个角度讲，这种局面正是资本和人才进入行业抢占有利位置的大好时机。

据统计，目前全球范围内比特币和区块链相关的初创企业有近800家，他们拿到的风投资金总计达13亿美元[14]，这个数字一点也不弱于当年互联网革命的初期阶段。人们逐渐认识到比特币背后的区块链技术的重大价值，大量基于区块链技术的新探索和新实践不断涌现出来。数字货币产业链的发展和繁荣属于未来。

[1] 《加密货币：虚拟货币如何挑战全球经济秩序》吴建刚译，人民邮电出版社，ZSBN 978-7-115-40828-0。

[2] 引用自http://www.pcpop.com/doc/1/1018/1018220_all.shtml。

[3] 国外有一家蝴蝶矿机，出售期货矿机，而期货却遥遥无期；还有烤猫，一度占据矿机市场1/3的份额，最终却以人间蒸发的方式完成最后的演出。凡此种种，举不胜举。

[4] 收益分配算法有很多种，包括PPS、DGM、PPLNS等，参见https://www.bitcoinmining.com/bitcoinmining-pools/。

[5] 引用自http://www.coindesk.com/information/cloud-mining-bitcoin-guide/。

[6] 引用自http://www.8btc.com/bitcoin-cloud-mining-service-craters-how-can-youtell-the-difference-between-a-profit-maker-and-a-ponzi-scheme。

[7] 引用自https://bitcointalk.org/index.php?topic=12678.0。

[8] 《加密货币：虚拟货币如何挑战全球经济秩序》，P74，吴建刚译，人民邮电出版社，ISBN：978-7-115-40828-0。

[9] 引用自https://localbitcoins.com/。

[10] 现在有几十GB。

[11] 引用自https://bitcoin.org/en/choose-your-wallet。

[12] 引用自https://blockchain.info/。

[13] 引用自https://www.coinbase.com/。

[14] 引用自https://www.venturescanner.com/blog/2016/bitcoin-q2-update-in-15-visuals。

互联网金融

区块链将成为互联网金融梦想照进现实的关键技术。

互联网金融是什么

随着人类的科学技术手段不断向前发展，互联网和金融已经不再是互相隔绝的两个领域，它们的有些边界已经开始接触并融合。互联网金融的概念因此应运而生[1]。随着互联网金融的实践和发展，它逐渐成为中国金融界和IT界最热门的词汇之一，越来越多地得到人们的认可并影响人们的生活。李克强总理在2014年的政府工作报告中指出要促进互联网金融的健康发展。无独有偶，在国外，金融科技（FinTech）也成为一个热词，金融科技主要是指互联网企业或高科技公司利用云计算、大数据、移动互联等新兴技术开展的低门槛金融服务。虽然在产品和服务的具体形式上，金融科技（FinTech）和国内的互联网金融并不完全相同，但本质上，它们都是新的技术手段和传统金融的结合。从这个意义上讲，无论国际还是国内，互联网金融的发展方向是一致的。

互联网金融是一个谱系概念，涵盖从传统银行、证券、保险、交易所等金融中介和市场，到瓦尔拉斯一般均衡对应的无金融中介或市场之间的所有金融交易和组织形式[2]。

金融是现代经济的基础和核心，现在，金融对经济发展的影响超过以往任何一个时期。互联网金融兴起之后，除了银行、证券、保险、基金之外，电子商务公司和IT企业等各类机构也纷纷参与互联网金融创新，演化出丰富的商业模式。事实上金融业与非金融业的界限正在逐渐模糊[3]。

要正确理解互联网金融的内涵，以下两点是至关重要的：一是互联网金融与传统金融的关系，二是互联网金融与技术发展的关系。

1.互联网金融与传统金融的关系

互联网给金融业带来的变化是形式与手段的变化，而不是内涵或本质的变化。互联网金融并不会改变金融的本质。比如电子商务与传统生意间的关系：电子商务没有改变交易的本质，但通过打破信息不对称，提升了交易效率，降低了交易成本。

互联网金融是新技术条件下金融手段的演化，它并不会改变金融服务的内涵。首先，金融的核心功能不变。互联网金融与传统金融一样，都是在不确定的环境中进行资源的时间和空间配置，以服务实体经济。第二，互联网金融不会改变股权、债权、保险、信托等金融契约的内涵。第三，互联网金融不会改变金融风险、外部性等概念的内涵。风险指的仍是未来遭受损失的可能性，市场风险、信用风险、流动性风险、操作风险、声誉风险和法律合规风险等概念及其分析框架依然适用[4]。

2.互联网金融与技术发展的关系

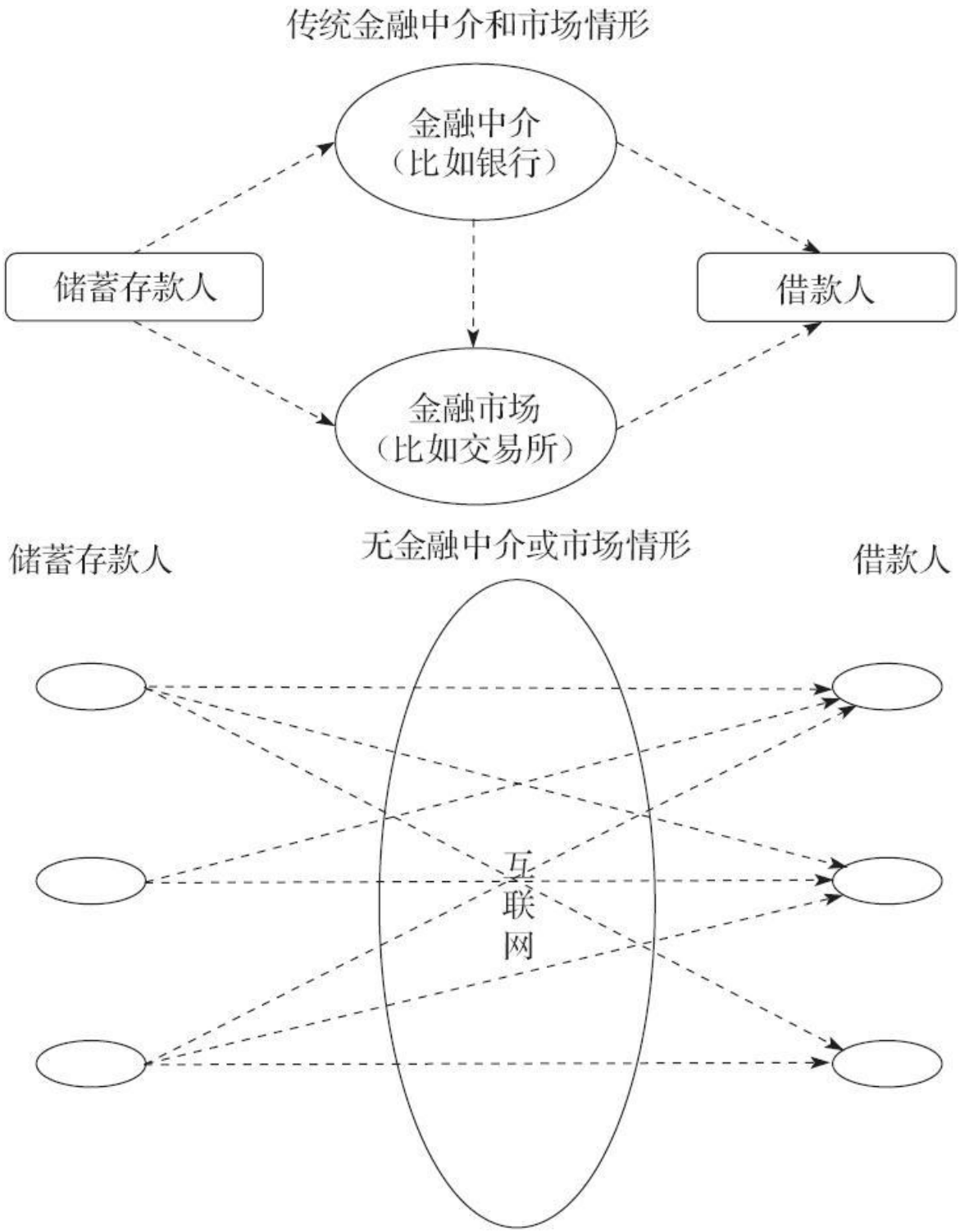
互联网金融的发展速度主要取决于互联网技术的发展速度，而不是金融自身的发展速度[5]。以互联网为代表的信息技术的发展，特别是电子支付、大数据、云计算、社交网络的发展，已经开始改变金融业的现状。而区块链技术的发展与成熟将进一步推动互联网金融向更深入和更广阔的空间发展。

理解互联网金融与技术发展的关系非常重要。很多人只看到了利用现有的互联网技术去改造金融业的机会，却忽视了技术发展本身的重要性。这会导致一种不好的倾向：拥有互联网金融的思想，但不具备相应的能力。有些人误以为现有的互联网技术能轻易解决传统金融机构无法解决的问题，并且能轻易构建超出自身能力的新型商业模式。实际情况是，以现有的技术水平，还不足以支持互联网金融的进一步发展，我们需要依赖技术本身的发展与成熟。

互联网金融的演变逻辑与发展阶段

1.演变逻辑

现实中之所以存在金融中介和市场，主要是由于信息不对称和交易成本等摩擦因素造成的。但随着互联网的发展，信息不对称的问题将大幅减少，交易成本将显著降低，互联网金融将逐渐逼近与瓦尔拉斯一般均衡相对应的无金融中介或市场情形。这是金融演变的内在逻辑[6]。



2.信息不对称与互联网金融的优势

所谓信息，就是传播中的知识差，这个差别包括信息的完整度和时间差[7]。造成信息不对称的原因主要有两种，一个是信息的传播渠道，另一个是个体间处理信息能力的不同。个体处理信息能力的不同是一种客观存在，我们存而不论。而信息传播渠道的进步（比如互联网的普及）则一直在降低信息不对称的程度。

金融的本质在于资金的融通。然而，在金融市场，信息不对称是一个普遍的特征。信息不对称存在于传统金融业的方方面面，比如中央银行和商业银行之间的信息不对称，商业银行和企业之间的信息不对称，金融服务的参与各方之间的信息不对称等。常见的情况是信息不对称导致逆向选择[8]和道德风险，比如金融机构利用自身信息优势违规经营，或者企业骗贷、银行惜贷等。信息不对称还可能导致金融秩序混乱和货币市场的无效或低效运行，加大金融风险。

信息是否对称直接制约市场的效率，应该说，互联网金融无法彻底解决信息不对称的问题，但是，它可以降低信息不对称的程度。互联网的核心精神是开放、共享、去中心化，而目标则是信息的高效流通。互联网金融最根本的意义是改善传统金融中信息不对称的问题。

在互联网时代，整个社会都在走向数字化，互联网技术在金融领域的渗透和创新是必然的趋势。具体到我国，由于现有的金融体系中存在一些低效或扭曲的因素，因而为互联网金融的发展留下了空间。比如，不能有效满足中小企业的融资和信贷需求，老百姓的投资理财需求也得不到有效满足，股权融资渠道不顺畅等。在此背景下，互联网金融演化出多种商业模式，比如传统金融的互联网化、移动与第三方支付、基于大数据的征信和网络贷款、众筹融资等。

3.发展阶段

谢平等人所著的《互联网金融手册》第一章开篇就提到“互联网金融是一个前瞻性概念”，同时给出了关于未来的预测：“我们乐观地估计，互联网金融还需要20年才能成形，主要基于两点考虑。第一，互联网金融的发展速度主要取决于互联网技术的发展速度，而不是金融自身的发展速度。我们预计，20年后，互联网技术将在目前的基础上进一步大幅度降低金融活动中的交易成本，并解决信息不对称的问题。第二，20年后，伴随着互联网成长起来的这一代人将成为社会主流，他们的互联网使用习惯将极大地影响金融交易和组织形式。”

我认为，理解“前瞻性概念”的含义，对于我们正确认识互联网金融的发展至关重要。互联网金融的发展不是一蹴而就的，需要一个较长的发展历程。以20年后才能成形的预测来看，目前互联网金融还处于非常早期的阶段，还有很长的路要走。

互联网金融面临的挑战

1.现阶段的认知误区

最近几年兴起的P2P网贷被很多人认为是互联网金融的典型。不过这些新崛起的平台中有相当一部分仅仅是民间金融的互联网化，并且很多平台由于缺乏足够的技术实力及成熟的风控体系，反而暴露出了更大的风险。这不符合互联网金融发展的特征，也完全不能代表互联网金融的发展方向，甚至某种程度上是一种倒退。

在当前的经济环境下，还有很多打着互联网金融旗号的公司把民间灰色金融的问题移到了线上，而且波及了更多的人群（强大的渠道优势）。原本线上平台能够降低成本，就是因为减少了一些监管、托管和风控成本，现在由于环境的复杂化，各种监管的介入导致成本与传统方式几乎无异了。

2.互联网金融发展的核心矛盾

传统金融体系是典型的中心化结构，而互联网则在推动着金融体系的重构，去中心化、去中介化成为趋势。然而目前的现状是，我们既想实现去中介化，但又缺乏去中介化的核心技术基础保障。也就是说，互联网金融目前的核心矛盾是：理念和商业前景已经得到了普遍接受，但技术基础还不足以支持其实现自身的理念。

在目前的技术水平上，我们虽然可以在一定程度上摆脱传统的中心化机构，实现更高的信息透明度和效率，但互联网金融服务的提供者由于受到技术的制约，依旧无法做到完全的去中心化。甚至有一些所谓的互联网金融平台，既做不到完全的去中心化，同时又缺乏传统中心化机构的信用保障及风控能力，导致尝试这些平台的消费者要冒更大的风险。最近，美国最大的

P2P借贷平台Lending Club就因为违规操作引起了人们的关注，股价一周之内暴跌40%以上。而国内P2P平台的跑路事件更是层出不穷。

区块链对当前金融行业的价值

区块链能帮助金融行业有效地提升效率和降低风险。借助区块链对金融行业内部应用场景进行改造能带来诸多好处，概括而言主要包括两个方面[9]：一是降低成本和提升效率；二是降低风险。

·降低成本和提升效率。具体体现在以下几个方面：①减少多方沟通成本，譬如证券交易市场往往需要中央结算系统、证券公司、交易所和银行等多方参与和协调，成本过高，而区块链可以通过多重签名等技术实现一条龙服务，且信息可以共享，提升整个业务的协作效率；②减少人工劳动，提高自动化程度；③更快的结算周期，区块链交易被确认的过程就是清算、结算和审计的过程；④保存监管记录和审计痕迹，为监管、审计等提供便利。根据Santander InnoVentures的报告估计，到2020年，区块链可减少基础设施成本150亿~200亿美元。

·降低风险。具体体现在以下几个方面：①由于交易确认即完成清算和结算，因此大大降低了交易对手风险；②区块链将交易过程数字化，且进行完整记录，能有效控制欺诈、手工输入错误等操作风险；③由于区块链的分布式网络和共识机制的存在，也减少了金融企业受黑客攻击等系统风险。

区块链将为互联网金融的腾飞奠定技术基础

区块链技术的发展与成熟将有效化解互联网金融面临的核心矛盾，并为行业未来的腾飞奠定坚实的技术基础。作为一个透明、可靠、去中心化的价值传输平台，区块链将进一步降低金融行业的信息不对称程度，同时提升互联网金融体系的效率和安全性。通过移除金融服务双方对过多中间机构的依赖，加速金融交易的完成，同时降低交易的成本，这将从根本上改变未来金融业的面貌。

当然，我们还应该看到，即使在大家普遍认为区块链最能够发挥核心作用的金融领域，区块链也绝非万能的，它能解决的仅仅是底层交易的成本与效率问题。比如，区块链不能消除金融领域的固有风险。不过，基于区块链所产生的信用记录数据，结合大数据、人工智能等技术在金融领域的深入发展，将能有效提高风险定价与风险管理效率。

在面对区块链技术时，前瞻性的公司会将新技术融入他们的业务。如果金融从业者对区块链技术缺乏理解，不能认识到其颠覆式的潜力，那么他们将会在未来的变革中处于非常被动的地位。因此，金融业应该早做打算，来应对这个颠覆性技术可能带来的威胁与机遇。区块链行业的很多初创企业（如R3CEV）都在尝试基于区块链技术创造新的商业模式，这可能会加速金融业的“创造性破坏”。

目前区块链技术应用于金融领域的核心阻碍，在于基础设施不够成熟。也就是说，就当前而言，它给金融业带来的实际价值还没有那么大。但它已经给金融业的未来提供了一个巨大的想象空间。未来区块链技术的演进和互联网金融的进一步发展，将使我们有能力从本质上提升金融业的效率，创造新的价值连接方式和商业模式，这不仅仅是改造或替代现有的系统，而是一个更为宏大的未来。

[1] 这个概念是谢平等人在2012年提出的，见《互联网金融模式研究》，载于《金融研究》，2012(12)。

[2] 谢平，邹传伟，刘海二，《互联网金融手册》，中国人民大学出版社，2014年，ISBN 978-7-300-19075-4。瓦尔拉斯一般均衡是指整个市场上过度需求与过剩供给的总额必定相等的情况。

[3] 《互联网金融手册》，P2，中国人民大学出版社，ISBN 978-7-300-19075-4。

[4] 《互联网金融手册》，P2，中国人民大学出版社，ISBN 978-7-300-19075-4。

[5] 《互联网金融手册》，P4，中国人民大学出版社，ISBN 978-7-300-19075-4。

[6] 《互联网金融手册》，P3，中国人民大学出版社，ISBN 978-7-300-19075-4。

[7] 谢康，《信息经济学原理》， 中南工业大学出版社，1998年6月，P14-15。

[8] 信息不对称所造成市场资源配置扭曲的现象。

[9] 中金公司，《区块链：改变金融业基础架构》。

物联网与共享经济

物联网将会成为区块链技术最激动人心的应用领域之一。

从互联网到物联网

从1995年互联网开始商业化运作，到今天已经过去了20年的时间。在这20年中，互联网给全世界带来了翻天覆地的变化。然而，在我看来，互联网带给人类社会的改变才刚刚开始，这估计会令不少人感到惊讶。物联网，这个在商业界备受关注而对于公众来说略显陌生的词汇，会将互联网的广度和深度向更高的层级推进，人类社会与数字世界将互相融合甚至难以区分。

不得不说，物联网这个词给人带来了不少陌生感，人们并不会很容易地将其与互联网联系起来，甚至一些人会误认为这是指物流行业的技术。而其英文名称就好理解多了：Internet of Things（IoT）。物联网的概念最先由麻省理工学院（MIT）的凯文·阿仕顿（kevin Ashton）提出[1]。在2010年的政府工作报告[2]中，我国将物联网定义为：通过信息传感设备，按照约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。在物联网时代，能接入网络的不仅仅是计算机和智能手机，还有汽车、健身设备、锁具、交通摄像头甚至你能想到的一切。

物联网的定义包含了两层意思：其一，物联网是在互联网基础上进行延伸和扩展的网络，其核心和基础仍然是互联网；其二，该网络的用户端延伸和扩展到了任何物品与物品之间，可进行信息交换和通信，也就是物物相连。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，也因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。

从所有权到使用权

在传统的经济模式下，租赁行业的经营范围和经营模式都是比较单一的，如果想获得某个物品的使用权，绝大多数情况下要事先获得它的所有权。而共享经济的实质则是将人们进行交易的重心由取得物品的所有权向取得其使用权转移。物品使用权的灵活转移可以更充分地提高物品的利用效率，实现生产要素的社会化，促进经济更高质量地发展。

共享经济（Sharing Economy）是一种点对点的分享产品或者服务的使用权的经济模式[3]。随着互联网的发展，特别是互联网进一步向物联网的过渡，共享经济拥有了可以爆发的技术基础。2013年3月9日，《经济学人》杂志在其封面文章第一次详细描述了“共享经济”[4]的场景，如今，出行住宿用Airbnb、用车用Uber，一个共享经济的时代正在来临，并且将重塑现在及未来的商业格局。

共享经济的实质是由所有权向使用权的转变。这一转变是经济效率提升的内在要求，而技术的发展水平则限制着共享经济能达到的高度。在现有的互联网条件下，共享经济的爆发仅仅是个开始，物联网的发展将成为拓展共享经济边界的原始技术驱动力，将使分享变得更加可靠、经济、便捷。甚至，杰里米·里夫金（Jeremy Rifkin）预言，物联网与共享经济的发展将导致一个零边际成本社会的诞生，我们熟知的资本主义社会将不复存在[5]。

物联网与共享经济面临的核心困难

在我看来，目前物联网与共享经济发展面临的核心困难不在互联网、传感器等基础设施，而是来自数据层面的挑战。我们可以从数据的存储与流动两方面进行分析。

第一，数据的存储。物联网的核心和基础仍然是互联网，而互联网上的黑客攻击、数据泄露、恶意软件、网络窥探是层出不穷的，这些问题已经给很多人造成了困扰。而如果每个人和物都连接入网的话，我们要建立怎样的界限才能保护每个人的隐

私权？

“人们已经清楚地认识到，如果无法在透明度和隐私权之间实现适当的平衡，那么物联网的发展可能放缓，甚至造成无法挽回的危害。”[6]

第二，数据的流动。首先看一看我们目前使用的支付清算系统的处理能力：Visa最新的实验室测试数据是5.6万笔/秒，实际应用中，Visa的处理峰值为1.4万笔/秒；2015年“双十一”，支付宝撑起了8.59万笔/秒的交易峰值，这被看作了不起的成就。

然而，在物联网与共享经济的时代，各种产品都接入一个庞大的智能网络，交易的主要目的是产品使用权的流转，甚至网络中的每一个节点、每一个产品都可以同时承担交易对象和交易发起者的角色。因此，交易数量会呈几何级数增加。举个简单的例子，如果购买一辆汽车（取得所有权），那么在用它代步的这段时间里，交易一次就够了，而如果仅仅是获得流转中的使用权，那么我们需要每使用一次就进行一次交易。因此，物联网中会产生天文数字的交易频率和交易数量，相关的清结算系统要分秒不停地顺畅运转，这无疑会对相关的基础设施提出极大的挑战。这将是一个复杂的网络，复杂到任何一个中心化的机构都无法承担这样的任务。

当区块链遇上物联网

通过上面的分析，我们马上能够看出，区块链的特点恰好能够解决物联网面临的核心困难，从而成为构建新一代的万物互联网的关键技术。

互联网本身就是一个去中心化的网络，在物联网时代，较之现在，接入网络的节点数量会出现极大的增长，因此，未来的物联网一定是个自组织、自调节的系统。在这样的系统中进行信息和价值的交换，必然需要可靠的去中心化点对点价值传输网络。

区块链技术可以通过可靠的数学加密算法保护用户的隐私。区块链将使设备实现自我管理和维护，使整个系统变成一个去中心化自组织的体系。在这个体系中，可以实现无需信任的、点对点的价值传输，可以实现安全的分布式数据分享，进而构造出一个健壮且可扩展的物联网。

IBM是最早宣布区块链开发计划的公司之一，他们在多个不同层面进行了区块链的研究与合作。2014年8月，IBM发表了一份报告[7]，指出区块链可以成为物联网的最佳的解决方案。2015年1月，IBM宣布将与三星联合打造ADEPT系统，利用区块链技术实现去中心化的物联网。ADEPT平台由三个要素组成：区块链（智能合约）、Telehash（P2P信息发送）和BitTorrent（文件分享）。通过该平台，两家公司都希望带来一个能自动检测问题、自动更新、不需要任何人为操作的设备，这些设备也将能够与其他附近的设备通信。2015年8月，区块链物联网项目Filament获得A轮融资500万美元。Filament的联合创始人兼首席执行官艾瑞克·詹宁斯（Eric Jennings）谈到，Filament是一个使用比特币区块链的去中心化的物联网软件堆栈，能够使公共分布式账本上的设备拥有独特身份。通过创建一个智能设备目录，Filament的物联网设备可以进行安全沟通、执行智能合同以及发送小额交易。鉴于这一设想，詹宁斯认为他的项目与ADEPT项目在本质上是相似的，不同的是它将针对工业市场，使石油、天然气、制造业和农业等行业的大公司实现效率上的新突破。

[1] Kevin Ashton, “That‘ Internet of Things ’Thing ”, RFID Journal, 22 June 2009.

[2] 引用自http://www.china.com.cn/policy/txt/2010-03/15/content_19612372_8.htm。

[3] 引用自https://en.wikipedia.org/wiki/Sharing_economy。

[4] 引用自http://www.economist.com/news/leaders/21573104-internet-everything-hirerise-sharing-economy。

[5] 杰里米·里夫金，《零边际成本社会》。

[6] 杰里米·里夫金，《零边际成本社会》。

[7] 引用自http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03620USEN#loaded。

新一代基础设施

新一代的基础设施是当前区块链行业最为重要的机会。

在社会和经济生活领域，基础设施是指为社会生产和居民生活提供核心公共服务的系统，这些基础设施往往具有先行性和基础性，若没有它们，其他生产和生活活动就难以开展。基础设施通常只有达到一定规模时才能提供有效的服务。

区块链行业目前仍处在非常早期的阶段，基础设施还远未成熟，因此基于区块链的服务、应用和商业模式常常面临难以开展的窘境。虽然价值互联网的新时代正在到来，但到来的步伐远没有想象的那么快。在区块链与各行业深入结合、产生改变金融与经济格局的巨大影响之前，当前最为重要的机会无疑是基础设施的建设。

基础设施要解决的核心问题是建立标准问题。在互联网早期，如果没有ISO、IEEE、W3C等这些组织对于标准建立的推动，大家的协议将很难统一，互联网也不会在全球迅速发展起来。而未来区块链的标准将会类似于互联网，它不是一个协议，而是一组协议，并且持续不断地进行丰富及改进。

区块链技术可以在很多行业和领域得到很好的应用，只要是和价值有关的信息，都和区块链有天然的亲和性，可以结合在一起发展出新的方式来更好地满足不同行业的需求。由于行业及领域的不同，需求是多种多样的，实现形式也是多种多样的。未来的价值互联网不可能是“某一条”或“某一种”区块链可以涵盖的，它必然是不同功能、不同特色的很多区块链共同形成的一个生态体系。

谈到区块链基础设施的具体内容，我认为主要分两类：一类是区块链的研发与构建，这里的区块链是指适用于不同目的或不同行业的各种类型的区块链；另一类是区块链间的连接设施，这些设施可以实现不同区块链之间的互联互通，让价值可以自由流动。

多样化的区块链

由于区块链的应用场景非常广泛，不同场景有着不一样的需求，因此我们不能指望一条区块链就能解决所有问题。显然，如果一条区块链上承载了太多的功能，将会使得其复杂到不可维护，从而严重降低可靠程度。同样的道理，如果一条区块链承载了各种类型的数据，也将会使其数据量过大，导致去中心化严重受限。因此，多样化的区块链将是未来发展的必然趋势。

首先发展起来的就是以比特币区块链为代表的公有链。比特币区块链是一个典型的应用于数字货币的区块链系统，为比特币的发展壮大提供了坚实的技术保障。之后产生的莱特币、狗狗币，其背后的区块链都是对比特币区块链的模仿。

最新崛起的以太坊是另一个典型，虽然其背后的区块链同样是公有链，但其目的并不是发行及运行一个数字货币系统，而是实现一个可编程的智能合约平台。

而私有链 则是最近一两年发展最为迅速及活跃的区块链类型。R3CEV是一个典型的构建私有链的公司，其发起的银行联盟的目标是制定银行间的清算标准，目前已经有40多家来自不同国家的大型银行加入。

区块链间的连接设施

区块链未来的复杂性并不是体现在任何一条区块链本身，而是体现在由区块链组成的层级结构中。而创建层级结构所依靠的基础设施，则是当前区块链基础设施中另一个关键的类别。

侧链技术就是一个典型的连接设施，这个概念最早由Blockstream公司提出，目标是构建可以让数字资产在不同区块链间自由转移的技术。他们在2014年发布了侧链技术的白皮书，并于2016年年初发布了第一个商业化侧链。

正如同多样化的区块链一样，随着技术的演进与发展，未来区块链间连接设施的技术理念及运作方式也将是多样化的，不同形态的连接设施满足不同种类的连接需求，从而构建起真正的区块链生态体系。

本章结语

“区块链+”的时代正在到来。

区块链正在构建一个全新的价值互联网。而未来价值互联网所影响的行业及领域将远远超出本章所介绍的范围。于是在本章的末尾，我们提出“区块链+”的概念，希望以此表明，区块链并不是一项普通的技术，不仅仅是带来一个行业的变革或是创造一个新的行业。它是类似互联网的一种颠覆性技术，将以基础工具或基础设施的面貌出现，拥有影响乃至颠覆所有行业和领域的潜力。

2015年3月5日上午，在十二届全国人大三次会议上，李克强总理在政府工作报告中首次提出“互联网+”行动计划。李克强在政府工作报告中提出，“制定‘互联网+’行动计划，推动移动互联网、云计算、大数据、物联网等与现代制造业结合，促进电子商务、工业互联网和互联网金融健康发展，引导互联网企业拓展国际市场。”自此以后，“互联网+”成为了街谈巷议的热门话题。

“区块链+”是“互联网+”的升级版，它基于“互联网+”，正在试图进入各个行业，并将对未来经济产生巨大的影响。在我看来，“区块链+”的实质是在“互联网+”的基础上，进一步打破信息不对称，让市场交易的去中介化成为可能，进而带来交易效率的提升及社会成本的下降，并为市场经济中的各个行业与领域带来深刻的变革。

第3章　区块链的应用场景

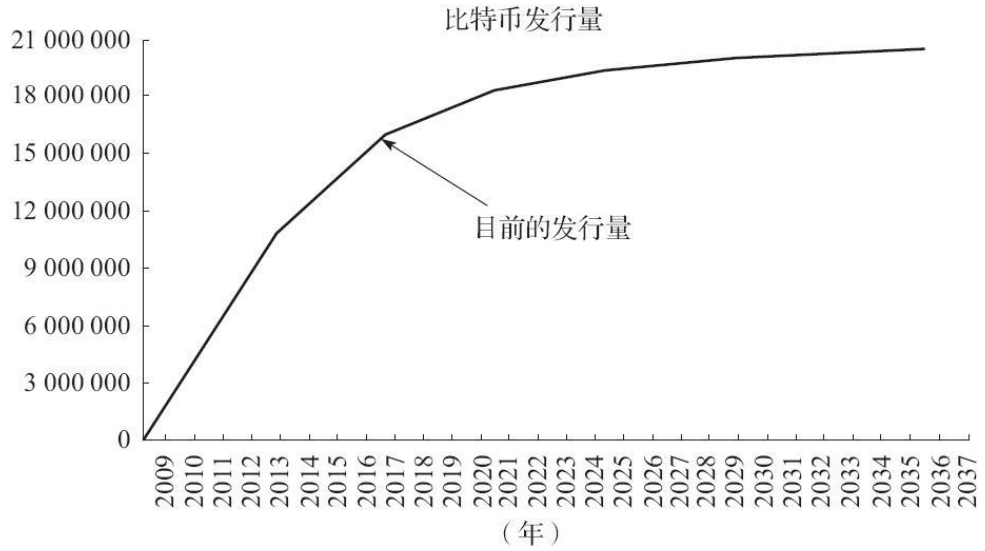
数字货币

我们知道，区块链作为比特币的基础架构，是被中本聪发明出来的。因此，换个角度讲，比特币当然也就是区块链的第一个应用，同时到目前为止，也是全球影响最广泛的一个应用。

比特币

1.发行机制

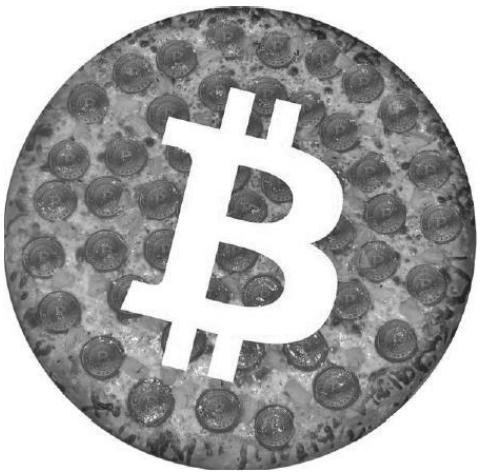
比特币采用的共识机制为工作量证明（POW），这也是第一个应用于区块链的共识机制。比特币区块链大约每10分钟生成一个新区块，同时生成新区块的节点获得比特币奖励，这也是比特币的发行过程。系统给予生成新区块的奖励每4年减半，最早为50个比特币/区块，目前为25个比特币/区块，在2016年7月即将再次减半为12.5个比特币/区块。通过这种方式，比特币的总量会在2140年达到2100万个的上限[1]。目前超过1700万个比特币已经产出。



2.轶事和涨跌

2008年11月比特币白皮书发布，2009年1月13日，比特币的创世区块被挖出，从此比特币区块链运行了起来。比特币的发明者中本聪，虽然是个匿名人物，但是一直在密码极客圈子中颇具影响力。可以这样说，比特币是极客[2]的创造。

在比特币的发展过程中，2010年5月22日是一个值得纪念的日子。这一天，一位美国的程序员拉丝勒·豪涅茨[3]（Laszlo Hanyecz）报告称，他以10000个比特币的价格成功购买了两块披萨。这次交易的意义在于，比特币不再仅仅是极客的玩具，它第一次在现实世界获得了价格——5000比特币/披萨。因此，这一天也成为比特币爱好者心目中的“比特币披萨节”。以现在的价格计算，这两块披萨无疑是昂贵的[4]。后来有人采访到拉丝勒·豪涅茨，他笑着表示：披萨味道不错，就是有点儿贵。



此后，随着比特币参与人群的扩大、相关基础设施的完善以及应用场景的丰富，比特币价格在波动中上升，期间有几次暴涨暴跌。2010年7月，比特币交易平台Mt.Gox成立，这个机构后来在比特币的价格波动中扮演了重要角色。

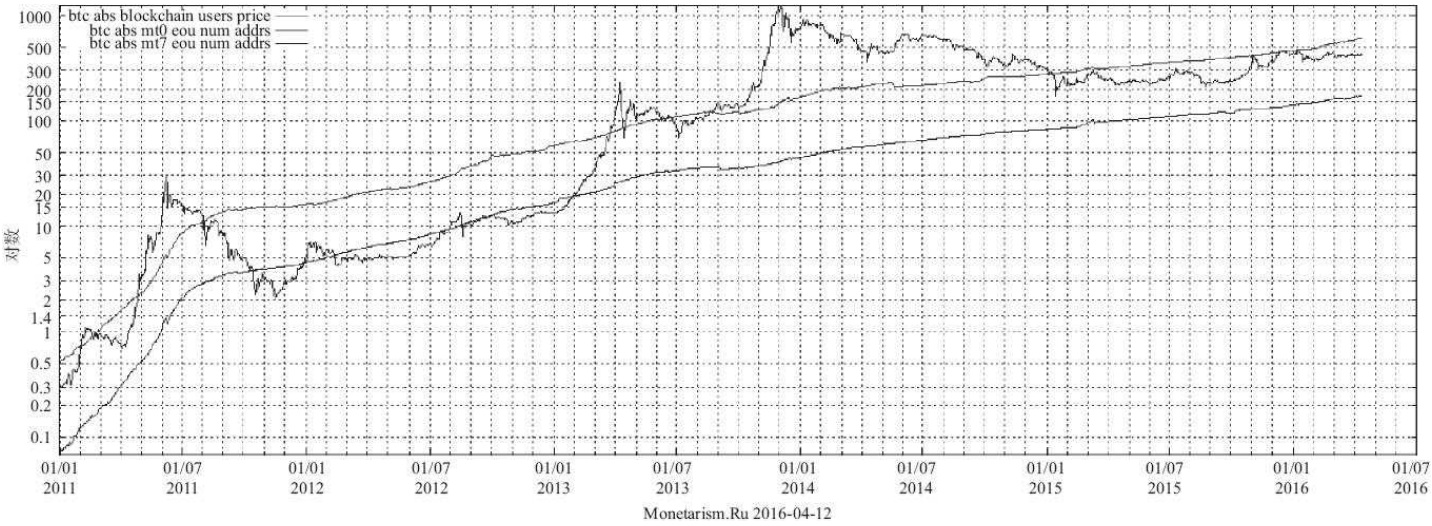
2011年上半年，比特币价格从30美分暴涨到30美元，并获得了《时代周刊》和福布斯的关注，这标志着比特币开始吸引主流媒体的目光。之后是半年的熊市，到2012年年初，比特币价格不足两美元。

2012年11月28日，比特币产量第一次减半。2013年2月，著名社交新闻网站红迪网（Reddit）接受比特币支付，成为世界上首家接受比特币支付的网站。就比特币在互联网世界中的流通而言，这件事具有划时代的意义。

2013年3月，欧盟成员国塞浦路斯发生银行危机，开始对持有银行存款的户主征收存款税。由此，比特币去中心化的特性受到人们的热捧，其价格在3周内从65美元上升到266美元。世界开始正视比特币的货币价值问题。之后比特币价格降低到50美元。而随着政府监管层面的进展[5]和媒体的不断报道，比特币的价格在2013年年底达到1200美元的历史高位。随后中国人民银行等五部委联合发布《关于防范比特币风险的通知》，比特币价格应声而落，在之后的震荡中，伴随着曾经世界上最大的比特币交易所Mt.Gox的倒闭，比特币价格最低跌至不足200美元，目前价格约

为460美元（2016年5月）。

比特币是一个新生事物，同时在全球范围内7×24h不间断交易。因此，在某种程度上，它确实是一个很好的投机标的。然而，价格只是比特币的一个方面，甚至可以说是相对不重要的一个方面。在比特币7年来的发展中，很多专家预言了比特币的死亡，但结果他们都错了。比特币系统的用户数量和应用范围在不断扩大。我们可以预言，在未来还会有无数的人会预言比特币的死亡，然而我们也可以预言他们的预言不会实现。



比特币可以方便地匿名转移给全世界的任何一个人[6]。比特币是一个工具，系统本身无法限制人们使用它的方式。一个比较灰色的例子是，早期有一个叫作比特币骰子的赌博网站，与这个网站相关的比特币交易曾经占到全网交易数量的一半。还有一个知名的例子是“丝绸之路”（Silk Road）。丝绸之路是一个进行非法买卖的匿名黑市，并且是通过比特币定价并完成交易的。目前该网站已被美国FBI查封，并查封了26000个比特币，网站运营人罗斯·威廉姆斯·乌布利希（Ross William Ulbricht）也受到多项严重指控。被FBI查封的这批比特币已经分3次拍卖，这也间接表现了美国官方对比特币的态度：犯罪的是人，而不是工具。应该看到，比特币只是一项新技术，本身不存在善恶。怎样使用新技术取决于人的选择，如果因为比特币被犯罪分子利用就反对甚至禁止比特币，那无异于因噎废食。

各国政策

我们知道，法律的制定天然具有滞后性。作为一个新生事物，几乎在所有国家的法律层面上，比特币的身份都不明朗。比特币的身份如何定义？这种新生事物是否受法律的保护？比特币是否与现行法律存在冲突？在立法和监管层面应该采取怎样的行动，以适应数字货币的发展？

虽然这些问题目前还没有在全球范围内达成共识，不同政府对比特币的归类和定义也并不相同，相关法律与政策的制定还处在探索与实验阶段，但绝大多数国家是允许比特币的使用和交易的，只有极少数国家对比特币进行限制甚至禁止。

1.中国

目前最为权威的监管文件是2013年12月5日中国人民银行等五部委联合印发的《关于防范比特币风险的通知》（以下简称为《通知》）。该《通知》明确了比特币的性质，认为比特币不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义上的货币。从性质上看，比特币是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。但是，比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由[7]。

2.美国

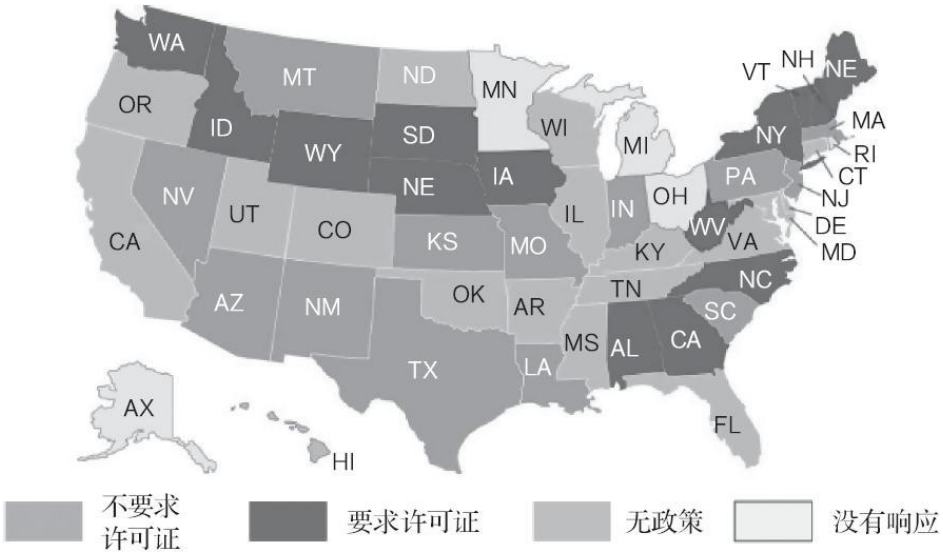
早在2013年，美国便开始比特币监管方面的研究，其中2013年11月美国参议院对比特币进行了听证，多名出席的政府官员表示，比特币不是非法货币，尽管存在被错误使用的案例，但它能够给金融系统带来好处。美联储前主席伯南克在致参议院的信中表示：美联储一直认为在虚拟货币带来洗钱和其他风险的同时，也可能带来长期益处，特别是，这种创新可能催生出一个更快、更安全、更高效的支付系统。美联储现任主席耶伦则在2014年2月参议院听证的时候表示：美联储也有任何权力去控制或者管理比特币……在我看来，比特币与美联储有能力管控的银行没有任何交集。

金融犯罪执法网络（FinCEN）将比特币的交易服务定位为货币服务业务（MSB），从业主体需要符合相应的要求，如了解客户（KYC）、反洗钱（AML）等[8]。

美国商品期货委员会（CFTC）则在其首个比特币监管法案中，将比特币归类为“商品”，进行比特币相关衍生品交易服务需要符合相关规定并接受监管[9]。

由于美国法律体系的特点，各州在比特币的监管方面具有很大的自主性。纽约州的数字货币许可证（BitLicense）一度吸引了全世界的关注。目前该制度已经投入使用，但是由于其较为严苛的规定，一些比特币企业选择了离开纽约[10]。而在加利福尼亚州，相对保守的关于数字货币的AB-1326法案最终没有生效。新泽西州的立法者则在试图推动对数字货币更友好的立法（即Digital Currency Jobs Creation Act）[11]。

对于金融服务的监管者来说，核心问题是是否应该承认像比特币这样的数字货币是一种货币或者具有货币的价值。如果承认，经营主体控制或者持有客户的数字货币时，就会被要求申请相关的许可证；如果不承认，则该经营主体还会控制或持有客户的法定货币（美元、欧元、人民币等），但不会要求货币相关的许可证。



3.欧洲国家

2012年10月，欧洲央行发布报告，将比特币定位为“第三类虚拟货币”，不具有法偿货币性质，因此，欧洲央行在信用、流动性、操作和法律4个方面对比特币等数字货币提出了风险警告。欧洲国家对比特币的政策基本沿袭了欧洲央行的政策基调。2014年7月，欧洲银行业管理局（EBA）再度发出警告，要求欧盟银行远离比特币等虚拟货币交易，直到相关监管法案出台。2015年10月，欧洲法院裁定：将比特币归类于一种支付手段，类似于传统的现金，因此比特币交易将免于消费税[12]。

尽管各欧盟成员国很早之前就针对数字货币的法律地位发布了一系列的警告或声明，但他们的立场并不完全统一。目前，在欧盟层面上，并没有针对数字货币的专门立法，也不认为数字货币具有货币的地位。不过这种情况似乎很快会发生变化。相关动议2015年11月便已提出，2016年2月，欧盟议会的经济和货币事务委员会（ECOM）发布了一份报告，相关的监管也在跟进当中，比如最近就将数字货币纳入了反洗钱管理的范围之内。

欧洲的主要国家都尚未颁布专门的法规管理数字货币的使用。英国政府发布报告承认数字货币相关技术的潜力，英格兰银行（BoE）不认为数字货币会对英国的货币和金融的稳定性造成实质的威胁[13]。法国银行管理局（ACPR）并不认为数字货币是一种威胁，但是规则应该明确，从事数字货币兑换的中间商需要获得相应的执照[14]。德国联邦金融监管局（BaFin）则将比特币作为一种“记账单位”，因此在商业交易时会涉及相应的许可问题[15]。

4.其他

2014年3月，日本政府表示，在现行的法律框架下，比特币不具备货币或者债券的性质。在此前提下，日本禁止银行和证券公司参与比特币业务，但是不禁止个人和法人实体在交易中接受比特币支付。根据最近日本《产经新闻》的报道，日本正在考虑给予比特币和其他数字货币完整的货币地位[16]。

主要国家中唯一对数字货币明确表达过敌对态度的就是俄罗斯。2014年2月，俄罗斯总检查办公室宣布，比特币不能被个人和法人实体使用[17]。2015年早期，俄罗斯屏蔽了很多比特币相关的网站，俄罗斯官方媒体则表示，使用比特币是违法的[18]。

不足与挑战

比特币自诞生以来，一直伴随着争议。通过本书的论述，相信读者可以对诸如比特币是不是庞氏骗局、比特币有没有价值、比特币是不是违法等常见的问题自行做出正确的判断。

比特币是一个仍在发展过程中的新生事物，自然不是尽善尽美的。比如比特币目前每个区块的大小为1M，这就意味着，在当前的架构下，比特币系统每秒能承载的交易数量最大只有7笔。尽管人们对比特币应该承担的角色的定位并不相同，但无论它承担什么样的角色，作为一个结算网络、货币系统或是其他，一秒最多承载7笔交易都是不足的。

因此，对于比特币扩容的问题，社区进行了旷日持久的争论。直到今天，我们也不能说得到了大家都满意的结果。这其实暴露了两个方面的问题：一个是在比特币这样一个去中心化的系统中，避免分裂很重要，达成一致又很难；另一个是比特币在开发层面上，很难说是去中心化的。Core小组的技术实力毫无疑问是最强的，绝大部分节点使用Core版本的比特币客户端。但是权力总需要制衡，我们也希望看到更多有实力的开发组的出现。

竞争币

区块链的原理是公开的，在比特币诞生，并获得越来越广泛的关注和影响力之后，出现了层出不穷的比特币的模仿者和竞争者。现在普遍将比特币之后出现的数字货币统称为竞争币（Altcoin）。下面我们挑选一些影响力较大的竞争币进行简单的介绍。

（1）采用工作量证明机制的竞争币

在采用工作量证明（POW）机制的竞争币中，莱特币（Litecoin）和狗狗币（Dogecoin）是影响力较大的两个币种，它们采用了与比特币不同的挖矿算法，比特币基于SHA-256算法，莱特币和狗狗币基于scrypt算法。基于工作量证明机制的竞争币主要是通过缩短交易确认时间使用户获得更好的体验，用更加复杂的算法实现更好的匿名性等。

莱特币 诞生于2011年11月，是在比特币的启发下诞生的产物，在技术原理上与比特币相同。莱特币试图改进比特币，与比特币相比，莱特币有三点不同。第一，莱特币网络每2.5分钟就打包一个区块，因此可以提供更快的交易确认。第二，莱特币的总量预期为8400万，是比特币总量的四倍。第三，莱特币在其工作量证明算法中使用的算法与比特币不同。莱特币是早期竞争币中较为成功的一个，曾长期占据数字货币市值第二名的位置，最高价格达到过390元/币，2016年4月莱特币的价格约为21元/币。

狗狗币 诞生于2013年12月，是澳大利亚的一位品牌营销专家与一位美国程序员合作开发的产物，狗狗币的logo是一只可爱的柴犬，交易确认时间为1分钟，总量1000亿，挖完后每年继续增加50亿，减半时间为两个月。诞生后，狗狗币以成功的营销策略迅速聚拢了一批爱好者，人气一度旺盛。

（2）采用权益证明机制的竞争币

在竞争币的探索中，还有一批竞争币采用了新的共识机制，其中以权益证明机制（POS）为代表。简而言之，权益证明不要求节点进行一定量的计算工作，而要求节点拥有一定数量加密货币的所有权，才能参与记账的竞争。

点点币 （PPCoin）发布于2012年8月，是最早采用权益证明机制的竞争币。点点币本身是工作量证明和权益证明相结合的。后续的很多竞争币都效仿了权益证明机制。

比特股 （BitShares）发布于2014年7月，采用的是权益证明机制的一个变种：授权权益证明机制（DPoS）。凭借宏伟的构思和新颖的概念，比特股也曾经风光一时。2015年，比特股的开发者改变货币总量，引发了社区的争议。

未来币 发布于2013年11月，采用百分之百的权益证明机制。未来币通过社区公开认购发行，但认购总人数只有73人，这种集中发行的方式也引发了广泛的讨论。

（3）以太坊

以太坊（Ethereum）于2014年众筹了30000余个比特币进行开发，目标是打造一个图灵完备的智能合约平台。2015年8月正式发布后，受到了社区和市场的一致热捧，市值迅速超过了莱特币，目前稳稳坐定第二的位置。以太坊前期采用工作量证明机制，后期计划采用权益证明机制。

尽管竞争币有很多，但是从市值上讲，比特币遥遥领先，排名第二的以太坊仅仅是比特币的1/10左右，再往后的竞争币的市值总和也不及比特币的1/10[19]。从这个角度看，比特币仍然是全世界影响最广、接受人数最多的数字货币，竞争币大多仅仅有“竞争”之名，但还不具备真正的竞争实力。不过相信未来，随着行业的扩大及技术的演进，一定会出现新的竞争格局。

并且，从历史的角度看，将区块链技术应用于数字货币，还是一个崭新的领域，这个领域还远远没有达到成熟和稳定的阶段。事物的演化是一个不断试错的过程，只有经过不断的尝试，我们才能看得更清楚。自由竞争是一个优胜劣汰的过程，从这个意义上讲，竞争币的实践无论是否成功，都有其不可替代的意义。

[1] 实际的数值为2099.99999769万，非常接近2100万，这里取的是近似值。

[2] 极客是美国俚语“geek”的音译。随着互联网文化的兴起，这个词含有智力超群和努力的语意，又被用于形容对计算机和网络技术有狂热兴趣并投入大量时间进行钻研的人。

[3] 同时他还是首先使用GPU 进行挖矿的矿工。

[4] 依照2016 年4 月的价格，这两块披萨的价格高达400 余万美元。

[5] 比如，2013年6月27日，德国议会决定，持有比特币一年以上的人将予以免税，业内认为这等于变相承认了比特币的法律地位。

[6] 严格地说， 比特币并不是匿名的， 而是伪匿名， 见《Bitcoin and Cryptocurrency Technologies 》Chapter 6: Bitcoin and Anonymity，Princeton University Press 出版。

[7] 引用自http://www.gov.cn/gzdt/2013-12/05/content_2542751.htm。

[8] 引用自https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html。

[9] 引用自http://www.cftc.gov/PressRoom/PressReleases/pr7231-15。

[10] 包括Bitfinex、BitQuick、BTCGuild、Eobot、Genesis Mining、GoCoin、Kraken、LocalBitcoins、Paxful 和Poloniex。

[11] 引用自http://insidebitcoins.com/news/legislators-to-introduce-pro-bitcoin-billin-new-jersey/32904。

[12] 引用自https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country# cite_note-63。

[13] 引用自http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf。

[14] 引用自https://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf。

[15] 引用自https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html。

[16] 引用自http://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-eyes-treatingbitcoins-the-same-as-real-money。

[17] 引用自http://www.theverge.com/2014/2/9/5395050/russia-bans-bitcoin。

[18] 引用自http://rt.com/news/222215-russia-bans-bitcoin-sites/。

[19] 引用自http://coinmarketcap.com/。

众筹

何谓众筹

众筹（Crowdfunding）是这样一种实践，它通过向很多人募集资金的方式来为一个项目或者企业提供支持。现在，众筹大多是通过互联网中介来进行的，是传统金融系统之外的一种替代金融形式。众筹有3种类型的参与者：项目发起人、项目投资人和众筹平台[1]。

向大众募集资金的筹款方式古已有之。最早的“众筹”多为募捐性质，比如僧侣向信众募集修建寺庙的资金。1884年，为了修建美国自由女神像，新闻家约瑟夫·普利策（Joseph Pulitzer）从12.5万人那里募集了超过十万美元的资金。现代意义的众筹正是在新时代的技术条件下开的老树新花。如今，众筹已经成为正在蓬勃发展的金融科技（FinTech）产业[2]的重要组成部分，实现方式和覆盖的领域都在不断发展。

笼统地讲，众筹可以分为回报型众筹（Rewards Crowdfunding）和股权众筹（Equity Crowdfunding）。这是一个在快速发展中的领域，有很多种细分方式，这里不进行详细的介绍[3]。

回报型众筹也称为产品众筹，是企业通过预售一种产品或服务的形式，来为业务的开展筹集资金。这种众筹形式不需要借债或付出股权。股权众筹的投资人通过付出资金支持换回公司的股份，通常进行股权众筹的公司都处于发展的早期阶段。

众筹作为一种互联网金融的融资模式，具有门槛低、项目多元、注重创意等特征，相比于传统金融渠道，众筹的效率更高。2012年，美国通过JOBS法案，为众筹扫清了法律上的障碍。目前，众筹正在以超高的增长率不断发展，自身的规模与日俱增，所发挥的影响力也在不断扩大。

据Massolution的研究报告，众筹市场连年保持超高的增长速度：2013年，全球众筹市场规模为61亿美元，2014年达到167亿美元，2015年达到344亿美元。其中亚洲也是众筹很活跃的一个区域，2014年，众筹增长320%，达到34亿美元[4]。国产动画电影《大圣归来》在创作过程中，就部分采用了众筹的方式。

传统众筹的缺点

在传统的众筹服务中，需要众筹平台作为可信的第三方来运作众筹活动。目前国外较为知名的众筹平台有Kickstarter、Indiegogo等，国内则有众筹网、云等等，京东、淘宝等巨头企业也发起了自己的众筹平台。

通常，项目支持者先将资金转到众筹平台账户，当项目筹集的资金达到目标数量时，平台将资金转到项目发起人账户；当项目筹集的资金没有达到目标数量时，表示发起项目失败，平台将资金返还给投资者。

在众筹过程中，资助者需要确认他们的钱投到了项目发起者所说的目标上，而项目发起者需要确保所筹资金到账。众筹平台是这个关系的中间人：它连接两者，促进两者建立关系，但实际上不承担更多的受信责任，并不能保证资助者的资金被合理的使用。不管是项目发起者，还是众筹平台本身，他们的行为都无法做到彻底的公开透明。众筹平台能够生存的主要原因在于人们的信任。这种信任是以什么为基础的呢？细读一下Kickstarter的使用条款，你会发现一句令人担忧的话：“公司不能保证用户提供的有关他们自己、他们的活动和项目的数据、信息的真实性”。Indiegogo在使用条款中也有类似的表述，称“Indiegogo对你们没有受信责任”“Indiegogo不保证筹资将会如项目发起者承诺的那样使用，不保证项目发起者将会提供特别优惠，不保证项目将会达到它的目标。对于项目的质量、安全、道德性和合法性，优惠及捐助额，以及在服务平台上发布的内容的真实性和准确性，Indiegogo也不作保证。”而且，众筹平台作为中心化平台的第三方，本身就存在较高的信任成本。仅仅在2015年，国内就有43家众筹平台停止运营或者倒闭。

区块链作为一种技术，不可能消灭人类的失信行为，却可以通过本身公开透明的特性，降低众筹过程中以及后续资金使用过程中的信息不对称水平，降低人们的信任成本。由于区块链可编程的特点，未来还可以在众筹过程中内置智能合约，这样就能真正做到资金的专款专用，让投资人没有后顾之忧。

另外，对于股权众筹而言，股权的高效流通可以提高用户的活跃度和股权的价值，然而这在传统的模式下是做不到的。

众筹是区块链技术最直观的应用领域之一。最原始直接的方式就是以类似于比特币的数字货币作为支付手段。在很多已经发生的数字货币领域的众筹案例中，比特币是最受欢迎的支付手段。比如以太坊2014年就众筹了30000多个比特币进行研发，当时这些比特币的价值约合1800万美元。

区块链众筹的解决方案

众筹和区块链都是金融科技的组成部分，比特币初创企业用众筹的方式募集资金，众筹企业采用区块链技术，都是必然出现的趋势。随着两个领域的互相融合，会有越来越多的众筹活动通过使用区块链技术的众筹平台来完成。

在区块链上可以发行货币，在不需要中央权威的情况下确定货币的所有权，类似地，区块链还可以承载任意类型的数字资产。因此，根据每个人支付的资金的多少来发行相应的代币[5]是在区块链上实现众筹的方式之一。理论上代币可以对应任何众筹的标的，可以是某个活动的入场凭证，也可以是未来某款产品或服务的使用权，甚至可以是一个定制版的“谢谢”。当然，这种代币最常见的形式还是作为投资某公司或产品，并获得收益的凭证。

这种代币同时也可以视为一种在区块链上发行和流通的加密股权（Crypto-Equity），一种有别于传统股权的投资方式。这种加密股权有多种可能，可能是公司发行的合规股权，但是不选择传统的股票交易所，而是以区块链作为“可供选择的交易系统”。它也可能是不代表发行方的股权，但是可以作为分红凭证，使持有者从公司的发展中获得收益。

随着区块链技术的进一步发展，依托区块链技术的众筹必然会发展出更加丰富的实现手段。

区块链众筹的优势

区块链技术将给众筹带来深刻的变化，它能够使众筹更加容易发起、管理，也能增加众筹市场的透明度和稳定性，我们甚至可以说，区块链会给众筹创造新的标准。

低费率： 使用数字货币进行众筹，可以节省交易费的支出。发起者可以抛开传统的众筹平台，采用区块链协议发起、管理众筹项目，而不再需要给第三方平台和传统的货币系统支付手续费。

容易流通： 采用发行代币的方式进行众筹，众筹的支持者可以快速、简单地将代币赎回，也可以与其他人进行交易，兑换成其他的数字货币，这相对于任何专有系统，都是一个显著的优势。

透明的规则和审计： 当投资者使用基于区块链的代币支持了你的项目，这笔支付就留下了永久不变的公开记录，这个记录不能被篡改，也不会因为技术原因丢失。这些资金的事后使用情况也同样保存在一个任何人都可以获取的公开透明的账本中。这些特性本身就提供了传统支付手段和事后审计所不能达到的信任水平与安全水平。

区块链的优势不仅在此，比如使用智能合约还可以保证：如果你没有达成预定的目标，资金可以自动退回到支持者的账户。这些都不需要第三方提供信任，不需要给第三方支付手续费。

区块链众筹的挑战

区块链众筹目前面临的挑战主要有两个方面。

一是进行众筹的载体（区块链）还处在发展的早期阶段，区块链的标准并不统一，不同区块链还难以互联互通，这种割裂会在一定程度上降低区块链众筹的优势。同时，区块链众筹本身的标准、模式也处在探索阶段。

二是现实法律的支持。各国对数字货币和区块链的立法与监管并不同步，但立法落后于实践的发展是一个整体特征。现阶段，我们应该积极实践和探索，完善区块链众筹的相关标准，而最终获得法律的支持，则是水到渠成的过程。

相关案例

下面试举一些最新的区块链技术与众筹行业紧密结合的创新案例。

2016年4月，法国巴黎银行证券服务部门宣布他们已经与法国众筹平台SmartAngel建立了合作关系，将共同开展一项试点项目，即使用区块链技术为小型公司和创业公司提供发行股份，获得散户投资的能力。SmartAngel的创始人Benoit Bazzocchi在他的博客中解释，区块链技术与众筹的合并将为许多小型公司开放大门，以使它们从许多个人和专业投资者那里获得资金[6]。

初创企业WAVES是一个新的多功能定制代币平台，致力于将区块链技术的优点应用到众筹、证券交易和法定货币转账领域。WAVES创始人萨沙·伊万诺夫（Sasha Ivanov）说：我们一开始就想要实现的使用案例之一就是将WAVES变成一种去中心化的Kickstarter——一个任何人都能为其项目筹集资金的平台，同时投资者还会受到WAVES的以区块链为基础的信誉系统的保护，投资者可以同第三方进行股票交易，并且如果交易中的一些特定条件没有满足，投资者可以获得自动退款。”[7]

根据全球最大的管理咨询和技术服务供应商埃森哲（Accenture）的报告[8]，区块链众筹初创企业Crowdaura已经成功跻身其2106年科技金融创新实验室（伦敦）。

[1] 引用自https://en.wikipedia.org/wiki/Crowdfunding。

[2] 是由使用新技术使金融服务更具效率的公司组成的经济产业，这些公司多为致力于打破现有金融体系的创业公司。

[3] 感兴趣的读者可以参考《众筹：传统融资模式颠覆与创新》，ISBN ：978-7-111-46681-9，由机械工业出版社2014年出版，盛佳、柯斌、杨倩主编。

[4] 引用自http://reports.crowdsourcing.org/index.php?route=product/product&product_id=52。

[5] 所谓代币，在现实中通常是指在一定范围内使用的替代货币的某种凭证。在区块链中则是指在特定区块链上发行的记账单位。

[6] 引用自http://www.coindesk.com/bnp-blockchain-crowdfunding/。

[7] 引用自http://themerkle.com/ultimate-custom-blockchain-tokens-platform-wavesto-launch-ico/。

[8] 引用自https://newsroom.accenture.com/news/15-innovators-selected-for-accentures-2016-fintech-innovation-lab-london.htm。

清算、结算与审计

区块链技术在金融领域有广泛的应用空间。其中在结算、清算和审计方面的应用是当前各大金融机构探索的重点。

按照传统的定义，结算 是指各经济单位由于商品交易、劳务供应和资金调拨等经济活动而引起的货币收付行为。按支付方式不同可以分为3种：现金结算、票据转让和转账结算。在当前的实践中，结算更接近不动产清算中的产权转移过程或者一个交易被执行后金融机构交换对价[1]的过程[2]。而清算则多是涉及银行间的资金结算，一般为联行业务。审计 是指由专设机关依照法律对国家各级政府及金融机构、企业/事业组织的重大项目和财务收支进行事前、事后审查的独立性经济监督活动。

金融业是一个建立在信任的基础上的行业。为了维护信任，伴随着金融业的发展，出现了大量的中介机构，包括托管机构、第三方支付平台、公证人、银行、交易所等。这些机构是传统金融业必不可少的部分，同时也天然地带有成本较高、效率较低、容易出现单点故障的缺点。比如，在传统证券交易中，证券所有人发出交易指令后，指令需要依次经过证券经纪人、资产托管人、中央银行和中央登记机构这四大步的协调，才能完成交易。整个流程效率低，成本高，另外这样的模式也造就了强势中介，金融消费者的权利往往得不到保障。一般来说，从证券所有人处发出交易指令，到交易最终在登记机构得到确认，需要“T+3”天。

区块链技术可以带来的好处

（1）增加透明度，降低信任成本

如果将相关的过程放在区块链上，将会大大增加机构、参与各方行为的透明度。由于区块链技术开源、透明的特性，系统的参与者都能够知晓系统的运行规则、验证账本内容和账本历史的真实性与完整性，确保交易历史是可靠的、没有被篡改的，这种特性相当于提高了系统的可追责性，降低了系统的信任成本。

（2）过程自动化，较少中间环节

区块链能够提升自动化水平。由于所有文件或资产都能够以代码或分布式记账的形式体现，通过对区块链上的数据处理程序进行设置，智能合约及自动交易就可能在区块链上实现。例如，智能合约可以把一组金融合同条款写入协议，保证合约的自动执行和违约偿付。

在区块链上，交易被确认的过程实际上就是清算、结算和审计的过程。录入区块链的数据难以撤销且能在短时间内同步到每个数据块中，录入区块链上的信息实际上产生了公示的效果，因此交易的发生和所有权的确认不会产生争议。所有的交易都实时显示在全球共享的分布式互联网上，区块链能将这个过程的效率提升到分钟级，从而有效降低资金成本和系统性风险。

区块链能够降低经营成本。金融机构的各个业务系统与后台工作往往面临很长的流程和很多的环节。现今无论是Visa、Master，还是支付宝都是中心化机构运营，货币转移要通过第三方机构，这使得跨境交易、货币汇率、内部核算的时间成本过高，并给资本带来了风险。区块链能够简化、自动化冗长的金融服务流程，减少前台和后台交互，节省大量的人力与物力，这对优化金融机构的业务流程、提高金融机构的竞争力具有重要意义。西班牙银行认为，到2022年，区块链技术能帮助金融行业降低200亿美元的记账成本。

（3）分布式账本，防御单点故障

区块链能够有效预防故障与攻击。传统金融模型以交易所或银行等金融机构为中心，一旦中心出现故障或被攻击，就可能导致整体网络瘫痪，交易暂停。区块链在点对点网络上由许多分布式节点来支撑，任何一部分出现问题都不会影响整体运作，而且每个节点都保存了区块链数据副本。因此区块链内置业务连续性，有着极高的可靠性、容错性。

（4）满足监管和审计的要求

区块链能够满足监管和审计要求。区块链上储存的记录具有透明性、可追踪性等特征。任何记录、任何交易双方之间的交易都是可以被追踪和查询的。

区块链在金融机构的反洗钱（AML）及了解客户（KYC）方面也有很好的应用潜力，比如德勤就提出如下的解决方案[3]。

在反洗钱领域，基于区块链，各金融机构将各自收集和验证的客户信息数字化后，上传至区块链。同时，金融机构为交易中的实体提供电子身份证明信息（类似私钥），并将用户地址与其电子身份证明信息联系起来，任何交易的发生都需要经过该私钥和银行手中的公钥验证，并由用户地址进行，这就决定了区块链上数据的可追溯性。在这种模式下，各个金融机构在区块链上实现交易信息的共享，任一交易的任何环节都不会脱离监管的视线，黑钱将无处也无法洗白，这将极大地增强反洗钱的力度。同时，通过在区块链上设置一定的规则与逻辑，区块链将自动验证交易和用户的合规性，不合规的交易及用户将被去除，整个金融企业的合规程度将得到提高。

在了解客户领域，金融机构同样可以通过区块链共享交易实体的信息，这将减少大量的重复性工作，也将为各家机构节省大量的合规成本。同时，还将为金融机构在挖掘潜在业务机会、识别风险暴露方面提供很大帮助。

除了以上的积极作用外，区块链还能够驱动新型商业模式的诞生。一方面区块链技术的特点让它能够实现一些在中心化模式下难以实现的商业模式；另一方面区块链源代码的开放和协作会极大地鼓励全社会的创新与协作。

相关案例

R3CEV是一家专注于构建下一代全球金融服务技术的区块链创业公司，它已经与全球40多家顶级银行达成合作，研究区块链在金融服务领域的应用。目前正在进行尝试的领域包括支付、结算、贸易金融、企业债券、回购、互换和保险[4]，R3CEV已经公布了名为Corda的分布式账本[5]，着眼于研究金融机构的一些特殊的隐私要求。据巴克莱银行透露，他们正在基于这一技术进行衍生品交易的测试[6]，据报道，Corda的一个关键特点就是并不是所有的节点都有同等的共享账本上信息的权限[7]，这显然对金融机构来说更为有效。

纳斯达克副总裁兼区块链主管弗雷德里克·沃斯（Fredrik Voss）表示，纳斯达克的工程师团队在两年半以前就已经开始研究分布式账本技术。2015年12月，纳斯达克的Linq区块链账本技术被用于完成、记录其家公司的私人证券交易[8]。沃斯表示，区块链技术可以将股票清算和结算时间从3天缩短到10分钟，并且可以使结算风险降低99%。澳洲证券交易所（ASX）在一月份发布公告称，他们正在认真考虑将区块链应用于其清算与结算系统[9]。

全球最大的会计师事务所之一德勤已经与5家创业公司合作建立了20种可行的区块链原型，这5家创业公司包括BlockCypher、Bloq、ConsenSys、Loyyal和Stellar。其中的4个原型在Consensus 2016区块链会议上进行实时演示。在银行业类别中，BlockCypher和ConsenSys两家创业公司正在帮助德勤在区块链上建立“数字银行”，虽然银行不会在区块链上从头开始建设，但是它们已经构建了不同的服务，Bloq致力于帮助德勤推出区块链保险产品，其余两家则专注于奖励等特殊使用场景。

[1] 对价（Consideration）原本是英美合同法中的重要概念，其内涵是一方为换取另一方做某事的承诺而向另一方支付的金钱代价或得到该种承诺的相关承诺。

[2] 引用自https://en.wikipedia.org/wiki/Settlement_(finance)。

[3] 引用自http://www.8btc.com/535352。

[4] 引用自http://www.coindesk.com/r3cev-blockchain-regulated-businesses/。

[5] 引用自http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledgerdesigned-for-financial-services。

[6] 引用自http://www.cnbc.com/2016/04/19/barclays-used-blockchain-tech-to-tradederivatives.html。

[7] 引用自http://www.coindesk.com/r3-corda-demo-barclays-distributed-ledger/。

[8] 引用自http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326。

[9] 引用自http://marketsmedia.com/blockchain-comes-out-of-the-lab/。

智能合约

合同 （Contract）又称契约、协议，是平等主体的自然人、法人、其他组织之间设立、变更、终止民事权利义务关系的协议[1]。本质上讲，合同是当事双方或多方在并没有充足信任的情况下，通过文字的约定和法律的权威，对各自的权利与义务进行的约定。

制订合同的目的就在于所签署协议的执行。传统合同的执行要求当事人的参与并消耗相应的时间，当违约发生时，还需要法律、机构等第三方的介入。可以说，人类社会投入了相当大的成本，以保证合同得到当事各方的尊重和执行。尽管如此，合同违约的事情还是屡见不鲜，时代的发展也在某种程度上放大了这个问题，因为随着经济全球化的发展，人们经常要与不了解的，甚至处在不同文化背景和法律体系下的合作伙伴签订合同，这时候，传统合同（契约）的约束力就有可能出现问题。

由于区块链有公开、透明、难以篡改的特点，所以将这种契约放到区块链上，可以有效地降低人们的信任成本。

智能合约是什么

根据区块链可编程的特点，人们可以将合同变成代码的形式放到区块链上，并在约定的条件下自动执行，这就是所谓的智能合约。这是一个宽泛的定义，然而却没有更精确的定义，越来越多的人在谈论智能合约，但这个术语的精确概念还要在进一步的讨论和实践中才能更加明确。

智能合约的概念至少可以追溯到1995年，尼克·萨博（Nick Szabo）提出了如下定义：

“一个智能合约是一套以数字形式定义的承诺（promise），包括合约参与方可以在上面执行这些承诺的协议。”

承诺指的是合约参与方同意的（经常是相互的）权利和义务，这些承诺定义了合约的本质与目的。数字形式意味着合约写入计算机可读的代码中。智能合约确立的权利和义务是由一台计算机或者计算机网络执行的。我们可以简单地认为，智能合约就是一种“程序”，只是这种“程序”处理的是人与人之间的权利和义务的约定。

这些理念出现在区块链之前，因此在区块链的语境下，可能会显得不够明确，易生混淆。而将区块链看作实现智能合约的平台的话，具体概念的区分和实现方式还处在起步阶段。

智能合约是一段涉及资产与交易的代码，只有将它放到区块链上，才能有效防止“盗版”和“篡改”，因此，在区块链出现以前，智能合约没有大的发展，随着区块链技术的发展成熟，智能合约将大有用武之地。

智能合约是一种新的参与者之间达成共识的方式。它的执行不依赖任何组织和个人，它是自我执行的，违约甚至不可能发生。智能合约将成为全球经济的基本构建，任何人都可以使用这种方式参与经济活动，而不需要事前审查和承担高昂的预付成本。在传统的合同制订中，人们必须选择信任的人和机构，而智能合约则从许多经济交易中，移除了对第三方信任的必要。

比特币区块链虽然也可以完成一些编程，但是由于比特币语言并不是图灵完备[2]的，所以对智能合约的支持非常有限。一直都有人在开发图灵完备的区块链平台，例如2015年发布的以太坊就吸引了很多人的关注。无论如何，智能合约这种新的契约制订和执行的方式，会与区块链结合在一起并得到发展。

智能合约目前面临的问题

虽然人们对智能合约充满期待，但是在智能合约发展的路径上，也还存在一些现实的阻碍。

1）目前基于区块链的资产数字化还远不够。从内部依赖条件讲，智能合约的应用要依赖于基于区块链的资产数字化，显

然，基于区块链的资产数字化还远远没有完成，目前有的只是零星的尝试而已。因此，巧妇难为无米之炊，智能合约发展的内部依赖条件尚未达成。

2）智能合约是在去中心化的系统中自动执行的。于是，如果仅仅智能合约的载体是去中心化的，实际上远远不够。如果执行合同的触发条件不是去中心化的、有效的共识机制，那么触发条件就很容易出现不一致，进一步则会极大地降低智能合约作为一个去中心化系统的有效性。因此，智能合约的发展，还必须依赖事件或事实发生的去中心化，比如去中心化预言机的出现。

通过以上分析，我们可以知道，智能合约的广泛应用远不是实现核心架构就能够达成的，而是需要一个协作体系的建立与成熟。因此，智能合约虽然是区块链非常火热的一个方向，但离大规模落地还有很长的路要走。

相关案例

目前关于智能合约的研究和实践主要集中在基础设施的完善上。

以太坊是用图灵完备的计算机语言完成的区块链系统，目前被很多人看作是新一代的智能合约开发平台[3]。

RootStock是一个建立在比特币区块链上的智能合约分布式平台。它试图以侧链的方式完成智能合约的搭载，从而为核心的比特币网络增加价值和功能。它将作为比特币的一个侧链，通过双向锚定的方式与比特币主链互联互通[4]。

Augur是一个2015年成立的基于以太坊区块链的去中心化预测市场，目前已进入Beta测试阶段[5]。

[1] 参见《中华人民共和国合同法》。
[2] 图灵完备是指一个能计算出每个图灵可计算函数（Turing-Computable Function）的计算系统。
[3] 引用自https://blog.ethereum.org/。
[4] 引用自http://www.rootstock.io/blog/sidechains-drivechains-and-rsk-2-waypeg-design。
[5] 引用自http://www.coindesk.com/augur-beta/。

版权与许可

版权和盗版

自互联网诞生以来，关于版权保护的相关争论就是经久不息的热点。一方面，我们看到，由于平等、公开、分享、协作的特点，互联网突破了地域的限制，极大地促进了知识的传播。人们从中得到的益处是不可估算的。另一方面，版权保护一直是互联网的痛点之一，尽管各国政府都在采取不同的措施，尽量完善互联网上的版权保护机制，但是盗版依然每时每刻都在发生，甚至一个作品被盗版的数量都可以成为它优秀程度的佐证，比如，现在大热的美剧《权力的游戏》就一直稳坐盗版播放榜单的第一位。

在互联网的环境中出生和成长的年轻人，只要他们想，几乎可以从互联网上免费获得任何想要的东西。因此总是有人不厌其烦地说，盗版之所以盛行，是因为人们天生不愿意合法地为互联网上的信息付费，哪怕是品质很高的东西。从表面看来，这种说法似乎是事实，但是我们认为，这种对人性的悲观是片面的。在互联网上，复制甚至篡改并传播一则信息的成本，几乎为零。互联网缺乏内生的针对有价值的信息的保护机制，这一点是事实。然而，这并不是互联网的原罪，甚至说，这本来就是人类社会不完美的常态。在互联网诞生以前，我们转述传播乃至篡改别人的观点，又何尝有什么内生的代价要付出？在人类社会的演化过程中，博弈出了现有的版权保护结构，它烦琐、低效、有局限，有存在的必要，但是并不完美。

试想一下，10年之前，作为一个在互联网中生存的个体，如果想为一本书或者一首歌支付相应的费用，他能怎么办，只能去线下买一本实体书或者一张实体专辑——是不是感觉到了哪里不对？这根本就是与互联网的大潮背道而驰。鞋子抱怨脚在长大，本身就是怪异的事情。我们不是为盗版辩护，我们只是说，互联网发展的前期，盗版之所以泛滥，很大一部分原因恰恰是相关的传统行业没有与时俱进的结果。现在，我们看到，Netflix主打收费的正版视频播放服务，Amazon在卖正版电子书，国内也有很多网站提供了收费的正版电子内容的服务，他们都在市场上获得了极大的成功。可见，人们并不是不愿意为正版内容支付合理的费用。

然而，这还不完美。

互联网上的盗版现象实际上也揭示了一些现行版权制度的不足之处。比如，在不同的国家和地区，版权登记和获取的方式、程序都有不同，版权的有效性也多种多样，而且版权保护的有效范围也常常被分割在不同的地区。宏观来看，第一，不同的国家和地区对版权保护的规定和做法并不相同，因此版权保护常常因为地域不同而发生水土不服的情况。第二，不论具体形式为何，版权保护的规则往往是比较固化和拘泥的，不大可能针对具体情况做灵活的针对性变化。第三，绝大多数国家规定，当作品以有形的形式出现时，自动获得版权，但是电子内容是很难有形的，因此当创作进入电子内容的范畴时，要获取版权证明往往更加困难。

区块链的优势

区块链可以提供更好的解决方案，区块链不仅可以记录过往和现在发生的交易，如果愿意的话，它还可以用来登记和转移版权注册，无论是数字的还是实体的作品。

在区块链上进行版权注册和证明有以下好处。

（1）突破地域限制

区块链可以作为一个去中心化的版权登记平台。在这个平台上，没有地域的限制，版权信息将以数学的形式，展现在世界上的所有人面前，无可争议。著作权人将不需要在不同的司法管辖区做重复烦琐的版权认证，这无疑可以极大地降低保护知识

产权、打击盗版的成本。而且，传统的版权登记模式是可以出现单点故障的，如果记录丢失了、被改动了或者损毁了，版权所有者想要申明自己的权益就会出现困难。然而，基于区块链去中心化的本质，每一个节点都有版权信息的备份。因此这种方式会更加安全。

（2）更低的成本

随着互联网的发展，尤其是社交网络的繁荣，大量有所有权的信息被发布在互联网上，而这些信息在传统的版权模式下，对其进行版权保护的经济成本和时间成本往往过于高昂。若使用区块链，那么你可以为这些创作进行随时随地的版权证明，即证明一则信息是在何时何地被谁创造出来的。并且一旦在区块链上创建了记录，这些证明就将永远存在。你可以为一篇博客做版权证明、为在社交媒体上分享的照片提供版权证明、为商业计划提供版权证明，几乎可以为任何你认为必要的东西提供廉价可靠的版权证明。

（3）更灵活的许可条件

利用区块链进行版权注册和保护，也许会彻底改变目前全球知识产权保护的格局，版权的许可、转让可能会诞生更加灵活多样的形式。比如，现在的杀毒软件，针对个人用户、家庭用户、企业用户常会有不同的授权条款。而在区块链上，将知识产权的消费与智能合约结合起来，就可以产生更加灵活的自动化许可协议，更好地满足买卖双方的实际需要，达到多方共赢的目的。

当知识产权登记的成本接近零时，则有可能诞生一个空前庞大的微知识产权交易市场。信息有价值，价值有归属，在区块链提供版权证明的大背景下，真的有可能实现盗版销声匿迹、天下无贼的理想。

法律总是滞后于技术的发展，但是法律也总是会适应技术的发展，我们相信，在不久的将来，区块链上的数据指纹会和生物指纹一样，具有同等的法律效力。

相关案例

位于美国的创业公司Blockai致力于帮助艺术家、摄影师和其他艺术工作者在区块链上注册作品版权，防止侵权行为。他们提出了优于费时费钱的正式注册的公共数据库注册方式，也就是在区块链上注册版权来证明著作权[1]。在Blockai平台上，你只需要做一个简单的鼠标拖放动作，就可以进行作品注册，并获得对应的版权证书。如果之后有人不经允许复制你的作品，你就可以给他发送一份版权证书来警告他。

Colu[2]是一家以色列的区块链创业公司，他们上线了新的平台，携手Revelator简化音乐版权管理，Revelator是一个基于云技术的信息提供商，为独立音乐公司提供销售和市场情报。在音乐的数字化分布中，仍然存在着复杂的权利归属和使用权链。Colu的产品将为数字资产的发行、分配提供安全渠道，包括音乐作品的上市和注册，并能够为所有市场参与者带来更高的透明度与效率。

Mine公司的Mediachain项目正在使用区块链建立全球知识产权数据库，它是一个新推出的元数据协议，允许数字创意者在他们的创作作品上附加信息，并在数据上添加时间戳，进而传送到比特币区块链，然后存储在分布式文件系统中，这将是一个整合了区块链技术特征的分布式文件系统[3]。

[1] 引用自https://blockai.com/。

[2] 引用自https://www.colu.co/。

[3] 引用自http://www.coindesk.com/mediachain-blockchain-tech-next-spotify/。

公证与记录

公证是公证机构根据自然人、法人或者其他组织的申请，依照法定程序对民事法律行为、有法律意义的事实和文书的真实性、合法性予以证明的活动。简单地说，公证就是由权力机关对一些事物提供保证和证明，这些事物可以包括文件、发明、交易、合同、身份等内容。

现有的公证组织形式，要么是公证机关统一行使公证职能，要么是公证机关与政府或者法院并行，总之是要靠一个专门的机构来提供信用背书。因此，公证其实是在信任缺失的情况下，依靠第三方提供信任。由于传统的公证需要较为高昂的制度成本、时间成本、经济成本和人力成本，导致进行公证的门槛较高。在实践中我们也看到，我国自20世纪80年代恢复公证制度以来，公证活动主要集中在合同、房产、遗嘱、声明、赠予等涉及较大经济价值的项目上。

本质上，公证是向公众证明某种东西、关系或状态在某时某刻的真实存在。在今天这个数字时代，传统的公证方式不免显得烦琐和低效。现把概念放开一点，在生活中遇到的各种证明，如身份证、学位证、结婚证、驾驶证等，其目的也是向公众提供没有争议的相关证明，因此也是一种广义上的公证。

我们可以看到，把这些记录放到区块链上，将为这些过程和相关行业带来颠覆性的改变。区块链本身作为一个达成共识的链条，任何登记在区块链上的有价值信息都是公开透明的，并且相对于传统的方式，记录的安全性和有效性都得到了极大的提升。因此，公证[1]服务——为一个文件在特定时间点的存在提供公开的“存在性证明”——是区块链应用迅速发展的领域之一。区块链公证服务可以为任何文件生成不可改变的、准确的证明，证明其存在性和完整性。相对于传统的公证方式，区块链公证的权威性、可靠性是数学保证的，它可以突破地理范围和行政区划的限制，成为一种真正全球通行的存在证明，并且，相对于传统的公证方式，区块链公证使用的时间更短，支付的费用更低。区块链的时间戳系统基本上可以扮演公证人的角色，只是这种系统更为经济和可信。

由于区块链的概念还很新，目前还没有将在区块链上使用的存在性证明作为法庭证据提交的案例。因此可以说，利用区块链技术进行公证服务的法律效力，目前还没有得到现行法律体系的认可，但是我们认为，区块链提供的信任是基于数学和逻辑的，在未来必然会得到承认。这种新型的公证方式也会得到快速的发展。

2015年10月，美国有一对新人选择通过区块链来公证婚姻，这对新人是大卫（David）和乔伊斯（Joyce），他们提交记录到比特币区块链，将誓言写入文本注释字段，并嵌入当时价值200美元的一笔比特币交易中，这条记录将永久地记录在区块链账本中。当然，作为第一个吃螃蟹的人，他们的尝试未免显得粗糙，不管在哪个国家，区块链婚姻登记也远不到获得法律认可的地步。不过我们可以想象，区块链婚姻登记作为区块链公共登记的一个尝试，如果以后能得到推广和认可，至少能带来以下好处：更加透明、公平、自由，一些隐瞒和重婚的现象将无所遁形，使用智能合约还可以对婚姻生活中的房产、子女教育等诸多事宜做更多有创造性的约定。

相关案例

Stampery是一家想用比特币的区块链代替公证人的创业公司。你可以用Stampery证明任何文件。它的创始人表示：“你可以为任何文件生成不可改变的、准确的证明，证明其存在性和完整性。世界上的任何人都可以不花一分钱自动证明某个文件是在何时创建的且之后再未改动过，相比于文件公证，Stampery的优势在于你不必带着纸质文件亲自去公证人那里，可节省不少时间。我们不是受信的证明人。这意味着即使Stampery不复存在，我们生成的每个证明依然能够被验证，我们没有会被黑客攻击的集中化数据库。由于法律证明是储存在区块链上的，任何人都可以检索这些证明。这是Stampery与其他电子公证服务的不同之处[2]。”

Uproov是应用在一款智能手机上的APP[3]，它将探索区块链时间戳的潜力，允许任何人证明实质上的任何东西，而不需

要“受信方”的参与。签名是写在区块链上的，而区块链过去的部分是不能以任何方式进行修改的。如果文件被修改了，这个哈希值就无法匹配，相关操作行为也将被系统检测到。

公证通（Factom）是一家利用区块链技术革新商业社会和政府部门的数据管理、记录的初创公司[4]。

对学校和公司来说，验证申请者的文凭信息是否造假是非常耗时耗力的。因此有些学校想通过使用区块链技术来改变这一现状。霍伯顿学校[5]和塞浦路斯的尼科西亚大学都在使用区块链记录学生的学历信息。区块链的去中心化、可验证的防篡改存储系统可以有效地解决学历造假的问题。

[1] 这里所说的公证更偏向一种存在性证明。

[2] 引用自http://techcrunch.com/2015/09/22/stampery-leverages-the-blockchainto-certify-all-your-documents/。

[3] 引用自https://uproov.com/。

[4] 引用自https://www.factom.com/。

[5] 引用自https://www.holbertonschool.com/pres。

更多

实际上，作为一种可以传输价值的协议，区块链可以应用于一切与价值相关的领域。前面小节所举的例子仅仅是冰山一角。区块链能够应用于各行各业，在未来，将成为我们赖以生存的数字世界的重要支柱。下面，我们对区块链行业在其他领域的探索和实践做一些简单的介绍。

在保险行业，业内的巨头公司对区块链技术的尝试层出不穷，埃森哲常务董事Abizer Rangwala大胆预测称“未来几年内，区块链技术将成为保险业生态系统中的主流技术。”

美国著名的保险公司USAA一直看好区块链技术的未来，它曾经参与了Coinbaser的7500万美元的融资项目，2016年3月，USAA扩大了其业务与区块链技术的融合，其账户持有人可以通过USAA.com界面接入Coinbase平台查看账户余额[1]。

2015年11月，保险巨头劳合社（Lloyd’s）表示，该公司计划使用区块链技术提高数据存取效率，并减少有关行政文书工作的成本，劳合社运营主管Shirine Khoury-Haq在声明中表示，对于保险市场而言，区块链可能会增加风险记录能力、透明度、准确度以及处理速度[2]。

德国保险业领军企业安联旗下的法国分公司，与区块链创业公司Everledger合作开发了一个区块链保险概念产品，该项目的总经理Sylvain Theveniaud在最近的一次采访中说，安联看到了区块链技术的潜力[3]。

人寿保险与金融服务巨头公司约翰·汉考克（John Hancock）已开始了多个区块链概念证明实验。约翰·汉考克公司的创新负责人Ace Moghimi表示，他的团队正致力于几个区块链应用，旨在使公司更透明、更有效[4]。

SafeShare为Uber型服务提供区块链实时保险服务。SafeShare是英国伦敦的一家新型保险解决方案提供商，专门针对基于“共享型经济”的新型创业公司，为它们提供基于区块链的实时保险解决方案。SafeShare提供的区块链保险解决方案是由英国保险巨头劳合社承保，开通了24小时索赔热线。除了提供实时、便捷的保险解决方案以外，区块链技术也有助于保险公司降低成本[5]。

全球领先的跨国金融服务和咨询公司埃森哲推出了区块链咨询服务来帮助对金融服务业有需求的公司。埃森哲与布莱斯·马斯特斯（Blythe Masters）的初创公司数字资产控股（Digital Asset Holdings）进行了合作，新公司将与银行等机构利用分布式账本技术提升安全性、工作效率、客户服务水平，以及“获得新收入的机会”。

在数据安全方面，甲骨文（Oracle）的高管Subramanian Iyer表示：各大公司通常会通过建立防火墙的方式来保护数据安全。但同时，这意味着，数据对于那些能够找到入口进入防火墙内的人来说，相当脆弱。然而，若使用区块链技术，除非所有的参与者达成一致，否则数据一旦被写入区块链就很难再被更改。这种方式完全颠覆了传统的防火墙模式，几乎可以将对数据动手脚的概率降低为零——从这个角度看，区块链对于不管是哪一个行业的数据安全来说，都有不可估量的价值[6]。

全球知名的数据存储和安全解决方案供应商Acronis，在其合作伙伴峰会上发布了基于区块链的数据保护战略倡议，希望整合现有的数据安全解决方案和区块链技术优势，变革现有系统。Acronis表示公司的技术探索会开启数据保护新纪元[7]。

电子商务方面，最近，有一个被称为“去中心化淘宝”的开源项目OpenBazaar[8]发布了beta版本。OpenBazaar是一个去中心化商品交易市场，使用比特币进行交易，既没有费用，也不用担心受到审查。因此相对于易趣与亚马逊这些提供中心化服务的电子商务平台，通过OpenBazaar不需要支付高额费用，不需要担心平台收集个人信息致使个人信息泄露或被转卖。

医疗方面，医院是信息存储量最大的地方，也是敏感信息最集中的地方，因此更要做好对信息的保护。然而，绝大多数医院都无法真正做到这点，因而还必须依靠法律的强制保护。区块链技术可以为患者的隐私保护提供可靠的解决方案，在安全隐私的前提下，还能做到公开透明，未来患者不仅不用担心自己的隐私被泄露，还能掌握自己的病历记录，医生在得到患者授权

后，才能查看患者的医疗信息。使用区块链技术，医院、医生、患者、保险公司等等相关各方都可以成为整个链条的一部分，从而降低人们之间的信任成本，减少医患纠纷和欺诈行为。将数据记录在区块链上，并使用相关的数字签名技术，只有当获得相关各方的许可的情况下，每个人的健康信息和医疗数据才能够被读取。这样，可以更好地规范患者健康数据的管理。

美国企业研究所（American Enterprise Institute）的Scott Gottlieb博士在报告中[9]，提出了一些关于医疗领域的解决方案，其中包含增加病人的保险选择以及一些其他的创新，报告认为区块链的使用是为了建设下一代的基础设施。

区块链技术机构Gem 2016年4月正式发布Gem Health项目，该项目旨在是通过新兴科技促进医疗领域间的合作。作为声明的一部分，Gem公开了首个合作伙伴飞利浦，飞利浦会协助搭建一个私人以太坊区块链，来开发企业医疗的应用程序[10]。

数据安全初创企业Guardtime宣布与爱沙尼亚电子卫生基金会合作（Estonia eHealth Foundation），利用区块链技术保证病人的医疗记录安全。该基金整合Guardtime的无钥签名区块链技术（Keyless Signature Infrastructure，KSI）和基金会Oracle数据引擎，以实现实时查看病人的病例[11]。

在政府 层面上，政府部门的低效率会导致信息的交换被延迟，从而对公共服务造成消极影响。如果将各部门的信息数据与区块链联系起来，当政府部门与公民同意数据共享的时候，就可以确保数据被实时发布。

2016年1月19日，英国政府发布了一份关于区块链技术的重要报告，这份报告名为《分布式账本技术：超越区块链》，并提到英国联邦政府正在探索类似于区块链技术的分布式账本技术，并且分析了区块链应用于传统金融行业的潜力[12]。

波兰政府数字事业部（Poland's Ministry of Digital Affairs）考虑用比特币和区块链技术进一步推进政府服务数字化进程。该机构成立于2015年，是致力于"推动政府数字化发展进程"的政府机关[13]。

英国皇家属地马恩岛的经济发展部门率先采用了基于区块链技术的公共服务系统，他们已经开始应用区块链注册系统，创建积极采用在线分布式账本系统的公司名录。该系统开发者之一称不久后英国将复制该模型[14]。

阿联酋副总统兼总理兼迪拜酋长宣布成立一个研究委员会，专门研究区块链技术。该区块链委员会将由32名委员构成，包括政府机构，如智能迪拜局、智能迪拜政府、迪拜多种商品中心（DMCC）、国际公司（思科、IBM、SAP、微软），以及区块链初创公司（BitOasis、Kraken与YellowPay）[15]。

在能源 领域，国际上，微型发电正在成为发电行业的重大趋势。新的能源项目，如家用发电和社区太阳能，正在填补电力供应的空缺。随着微型发电加入传统发电供应商，它推动建立了一种能源市场。智能仪表可以在区块链上对生产和消费的电力进行注册，允许消费各地过剩的能源，并向初始的能源生产者提供积分或货币，当他们需要额外的电力时，这些积分可以被赎回。

布鲁克林微电网开发商LO3能源和区块链技术初创企业ConsenSys共同开发了TransActive Grid项目，用户可以通过区块链技术点对点地进行剩余能源交易，参与的家庭都有连接到区块链的智能仪表，可追踪记录家庭使用的电量以及管理邻居之间的电力交易。

RWE是在全球拥有2亿消费者的德国电力公司，主要运营煤炭能源和核电基础设施。他们建立内部工作小组，以评估区块链技术怎样帮助公司减少能源传输成本。RWE与基于以太坊区块链的初创企业Slock.It合作，在最近一次访谈中，RWE区块链团队领导人Carsten Stocker谈到了一项可行的应用：可以自动识别用户和收费且使用基于区块链智能合约的充电站[16]。

关于区块链的应用场景，我们的列举必然是不完全的。不过最重要的是，我们需要看到区块链未来有无限的可能。汇集更多人的聪明才智，才能使区块链得到更快的发展。新时代的大幕已经缓缓拉开，期待着更多的角色走上前台。人们有理由期待在区块链技术范式下，又一次"大航海时代"的来临，人类这次也许将收获更多。

[1] 引用自http://www.coindesk.com/usaa-expands-bitcoin-all-members/。

[2] 引用自http://www.coindesk.com/lloyds-sees-blockchains-potential-insurancemarkets/。

[3] 引用自http://www.coindesk.com/allianz-france-exploring-use-cases-with-blockchainstartup/。

[4] 引用自http://www.coindesk.com/insurance-company-john-hancock-begins-multipleblockchain-proof-concepts/。

[5] 引用自http://www.newsbtc.com/2016/03/19/safeshare-insurance-on-blockchain/。

[6] 引用自http://www.oracle.com/us/corporate/profit/big-ideas/041316-siyer-2982371.html#userconsent#。

[7] 引用自https://itbrief.co.nz/story/acronis-launches-revolutionary-blockchaintechnology-initiative/。

[8] 引用自https://openbazaar.org/。

[9] 引用自https://www.aei.org/wp-content/uploads/2016/05/House-Testimony-5-11-16-Scott-Gottlieb.pdf。

[10] 引用自http://www.coindesk.com/gem-philips-blockchain-healthcare/。

[11] 引用自http://www.coindesk.com/blockchainstartup-aims-to-secure-1-millionestonian-health-records/。

[12] 引用自https://zh.scribd.com/doc/295987915/Distributed-Ledger-Technologybeyond-block-chain。

[13] 引用自http://www.coindesk.com/polish-ministry-digital-affairs-blockchain/。

[14] 引用自http://www.ukauthority.com/news/6170/isle-of-man-government-takes-blockchainlead。

[15] 引用自http://www.coindesk.com/dubai-government-backs-expansive-blockchain-techresearch-effort/。

[16] 引用自http://www.coindesk.com/german-utility-company-turns-to-blockchainamid-shifting-energy-landscape/。

第4章　区块链技术原理

比特币作为区块链技术的第一个应用，成功地向人们展示了这一技术的伟大。随着区块链技术的发展，区块链本身的形式也开始向多样化演进。不过虽然不同种类的区块链技术细节各有不同，但核心的理念却是相通的。在这里，将重点以比特币区块链为例来讲述区块链的技术原理。

比特币区块链大量采用了现有的技术。公钥密码学、P2P网络、时间戳服务器、工作量证明，这些技术无一不是人类智慧的结晶。比特币正是站在这些巨人的肩膀上，才得以发展壮大。要了解区块链的技术细节，就必须深入理解这些技术在比特币区块链中是如何工作的。

密码学基础

密码学概述

密码学起源于数千年以前，最早可追溯到古巴比伦时代，作为保护信息传输的技术手段，最早应用于军事、外交和情报领域。在20世纪70年代之前，密码学大都属于政府的应用范畴。有两件事的发生将密码学带入了公众领域：标准加密系统——数据加密标准（Data Encryption Standard，DES）的诞生和公钥加密算法（也称为非对称加密算法）的发明[1]。

密码学伴随着密码分析学的发展而发展。按算法思想的革新可划分为3大阶段：古典密码学、现代密码学和公钥密码学。1949年以前的密码学统称为古典密码学，它的安全基于加密算法的保密性。1949年，香农（Shannon）发表了《保密系统的通信理论》一文，文中的信息论为对称密码系统建立了理论基础，密码学开始成为一门科学。基于密钥安全而非加密算法安全的理论与技术变革，成为密码学发展的一个新的里程碑，标志着现代密码学时代的来临。1976年，Whitfield Diffie和Martin Hellman首次提出了基于数学难题的公钥密码机制；1978年，RSA公钥密码机制出现，它成为公钥密码的杰出代表并成为事实标准，这在密码学史上创造了又一个新的里程碑。20世纪90年代，公钥密码学进一步发展，基于椭圆曲线乘法、素数幂等数学函数的公钥算法诞生，这使得数字密钥和不可伪造的数字签名成为可能。

如今密码学相关技术已经深入各个领域，它们的理论共识都遵循由奥古斯特·柯克霍夫在19世纪提出的“柯克霍夫原则”——密码系统应该就算被所有人知道其运作步骤，它仍然是安全的。即算法是公开的，唯一需要保护的是密钥。密码学算法的安全性被攻破有两个可能：一是算法本身的漏洞，不需要密钥即可以破解算法；二是在可接受的时间范围内暴力破解。

1.古典密码学

古典密码学历史悠久，时间跨越了两三千年。它主要应用于军事、外交和情报领域。它的安全性是基于算法的，类似于目前经常用的编码算法。古典密码编码算法归根结底主要有两种：置换和代换。

把明文字符串中的字母重新排列，字母本身不变，位置却改变了，由此编成的密码称为置换密码。最简单的置换密码是把明文中的字母倒序排列，然后截成固定长度的字母组作为密文。代换密码则是将明文中的字符替代成其他字符，比如古罗马凯撒密码是将明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移，得到的新数据就是密文。位数就是凯撒密码加密和解密的密钥。

古典密码学大都比较简单，主要采用手工或机械操作来实现加解密，而算法是基于字符串的，由于古典密码学的安全性主要是依赖于算法的保密性，所以整体安全性不高。

2.现代密码学

1949年以香农的信息论诞生为标志，密码学的发展进入了第二个阶段。现代计算机科学与信息技术的蓬勃发展，使得基于复杂计算的密码学成为可能。同时密码学首次成为一门科学。加密算法开始时是基于密钥来进行信息的加解密，通过密钥加密明文并主要以二进制的形式进行传输。通常情况下，密钥越长，代表着密文被破解的难度越大。由于加密算法和解密算法都是同一模式，同时只用一把密钥保证加密数据的安全，因此这种加密算法也叫作“对称加密算法”。

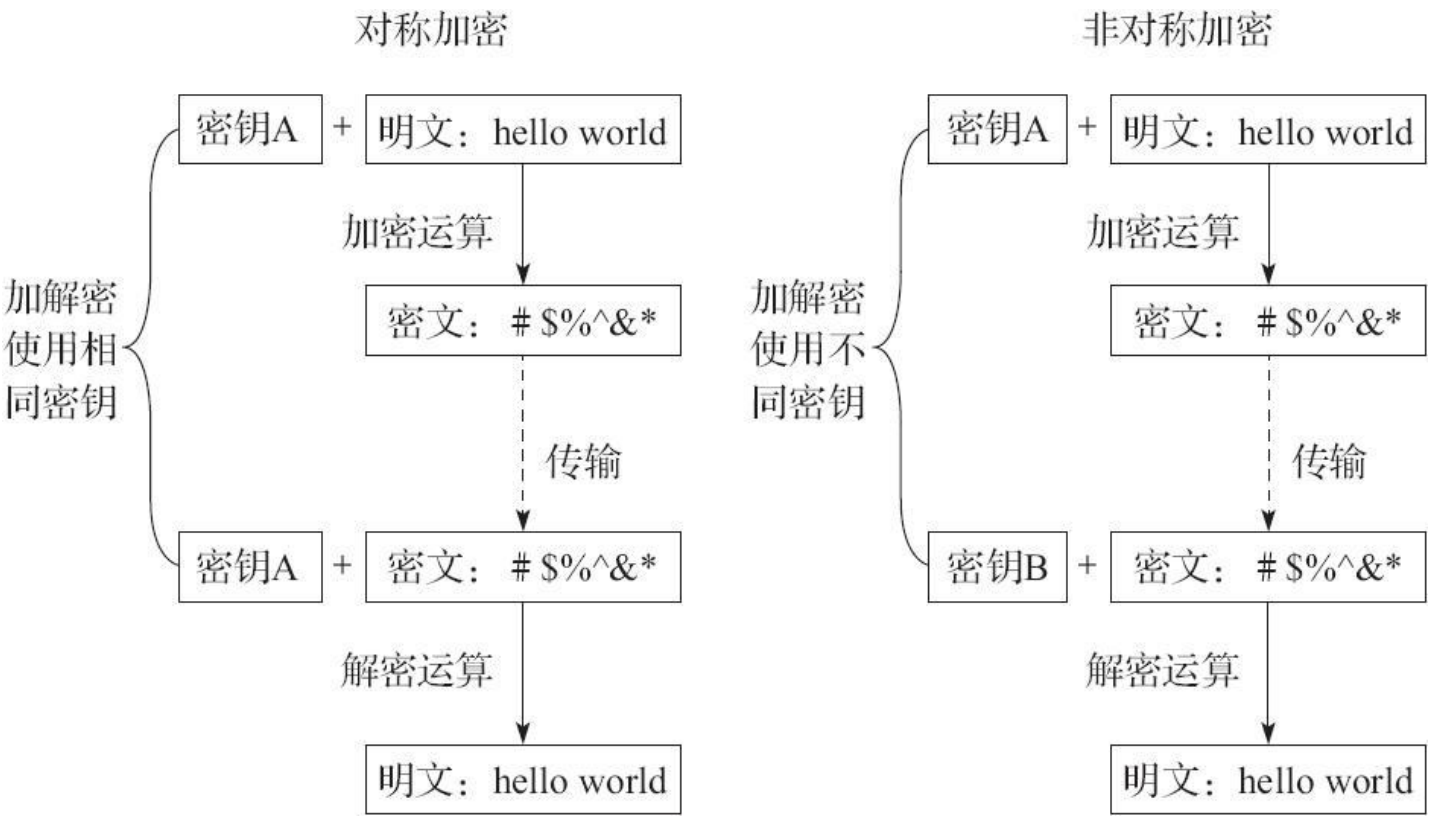
对称加密有一个最大的弱点：甲方必须把密钥告诉乙方，否则乙方无法解密。而保存和传递密钥，就成了最头疼的问题。

这个时间段是密码学开始蓬勃发展的一个开端，后期发展出来的公钥密码学、哈希算法、其实属于现代密码学的范畴。

3.公钥密码学

相比1976年以前的密码学思想，公钥密码学可以在不直接传递密钥的情况下，完成密文的解密。这个算法机制启发了其他科学家，人们认识到，加密和解密可以使用不同的规则，只要这两种规则之间存在某种对应关系即可，这样就避免了直接传递密钥。基于这种公钥机制的思想，开始出现了一系列非对称加密算法。

下图比较说明了非对称加密算法与对称加密算法的区别。



非对称加密需要两个（一对）密钥：公开密钥（Publickey）和私有密钥（Privatekey），用公钥对数据进行加密后，只有对应的私钥才能解密；反之，如果私钥用于加密，则只有对应的公钥才能解密。通信双方无须交换密钥，就可以建立保密通信。

公钥密码体制根据其所依据的数学难题一般分为3类：大整数分解问题类、离散对数问题类、椭圆曲线类[2]。

4.哈希算法

哈希函数（Hash Function）也称为散列函数，是能计算出一个数字消息所对应的、长度固定的字符串（又称消息摘要）的算法。给定一个输入x，它会算出相应固定长度的输出H（x）。哈希函数的主要特征是：

1）输入x可以是任意长度的字符串。

2）输出结果，即H（x）的长度是固定的。

3）计算H（x）的过程是高效的（对于长度为n的字符串x，计算出H（x）的时间复杂度应为O（n）），同时H（x）要相对易于计算，可通过硬件和软件实现。

而对于比特币加密系统使用的哈希函数，它需要额外具备以下的性质：

1）免碰撞，即不会出现输入x≠y但是H（x）=H（y）的情况，也就是强抗冲突性。

2）隐匿性，也就是说，对于一个给定的输出结果H（x），想要逆推出输入x，在计算上是不可能的。

3）不存在比穷举更好的方法，以使哈希结果H（x）落在特定的范围。

区块链中的密码学

在比特币区块链的整个体系中，大量使用了公开的加密算法，比如Merkle Tree哈希树算法、椭圆曲线算法、SHA-256哈希算法、对称加密算法以及一些编码算法，如Base58编码、VarInt编码、DER编码等。下面我们来了解其中的几个核心算法。

1.椭圆曲线算法

椭圆曲线在密码学中的使用是在1985年由Neal Koblitz和Victor Miller分别独立提出的。它的主要优势是：在某些情况下，它比其他的算法（比如RSA）使用更小的密钥，但提供相当的或更高等级的安全性。

比特币使用了基于secp256k1椭圆曲线数学的公钥密码学算法。它包含私钥与公钥，交易发出方用私钥进行签名，并将签名与原始数据发送给整个比特币网络，网络中的所有节点则用公钥对交易有效性进行验证。签名算法保证了交易是由拥有对应私钥的人所发出的。

数据签名算法的核心在于证明数据是签名者发出的、不可抵赖的，而不是待签名数据本身的保密性。

2.SHA-256哈希算法

SHA是安全散列算法（Secure Hash Algorithm）的缩写，是一个密码散列函数家族。这一组函数是由美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的，包括SHA-1、SHA-224、SHA-256、SHA-384和SHA-512五种变体，主要适用于数字签名标准。后4个哈希函数又并称为SHA-2。

SHA-1在许多安全协议中广为使用，包括TLS、SSL、PGP、SSH、S/MIME和IPsec，曾被视为是MD5（更早之前被广为使用的哈希函数）的后继者。但随着计算机技术的发展，SHA-1的安全性被密码学家严重质疑，且在2005年被王小云等密码学家成功破译。SHA-2的算法跟SHA-1基本相似，但至今尚未出现对SHA-2的有效攻击，安全性较高。SHA-256就是SHA-2函数中的一个，是输出值为256位的哈希算法。

3.对称加密算法

AES（Advanced Encryption Standard）是一个对称分组密码算法，旨在取代DES成为广泛使用的标准，最终成为美国新的数据加密标准而被广泛应用在各个领域。其大致运作原理和前文的对称加密算法的流程相同。

比特币官方客户端[3]使用AES算法中的AES-256-CBC来加密钱包文件，用户设置密码后，采用用户设置的密码通过AES算法对钱包私钥进行加密，确保客户端私钥的安全，从而保证资产的安全。

4.Base58编码

可读性编码算法在理论上并非密码学理论的核心内容，它类似于古典密码学里的置换算法机制。编码算法的目的不是为了保护数据的安全性，而是为了可读性。

信息以二进制的形式传输，不具备可读性，而数字与字母组成的字符串才更容易被识别。可读性编码不改变信息内容，只改变信息内容的表现形式，部分编码算法还加入了容错校验功能，以保证传输过程中数据的准确性和完整性。

Base58是比特币使用的一种独特的编码方式，主要用于产生比特币的钱包地址。相比Base64，Base58不使用数字“0”、大写字母“O”、大写字母“I”和小写字母“l”，以及“+”和“/”符号[4]。

设计Base58的主要目的是：

1）避免混淆。在某些字体下，数字0和大写字母O，以及大写字母I和小写字母l非常相似。

2）不使用“+”和“/”的原因是，非字母或数字的字符串作为账号的一部分被接受。

3）没有标点符号，通常不会被从中间分行。

4）大部分的软件支持双击选择整个字符串。

比特币使用了Base58算法来对公钥的Hash160及私钥进行编码，从而生成以1或3开头的比特币地址及WIF（Wallet Import Format）

格式的私钥。

[1] 引用自https://en.wikipedia.org/wiki/History_of_cryptography。

[2] 也有人把椭圆曲线类归为离散对数类。

[3] 引用自https://bitcoin.org/en/download。

[4] 引用自https://zh.wikipedia.org/wiki/Base58。

区块链组成

区块链数据里最基本也是重要的几个概念是地址、交易、区块、网络。比特币用地址来标识一笔交易的支出方和接收方。所有的交易最终需要被记到统一的账本上，而这个账本是通过区块确认并完成的。每一个新区块的产生，都会被打上时间戳，最终生成按照时间前后排列并加以记录的电子交易证明。每个独立节点之间又通过比特币网络来建立联系，这样就组成了一个去中心化、分布式的电子交易记录时间戳服务器系统。

比特币通过构造这个分布式时间戳服务器来解决双重支付问题。中本聪在其白皮书中曾提到：只要诚实的节点所控制的计算能力的总和，大于有合作关系的（Cooperating）攻击者的计算能力的总和，比特币系统就是安全的[1]。

如果说整个比特币区块链是一个账本，那么账本上承载的就是一笔笔由一些地址转移到另一些地址的资产交易。比特币里的各个机制及模块有机地结合，才使得区块链这样一个去中心化的记账体系成为可能。下面我们尽量从技术原理的角度来看一看这个记账体系的组成。

地址

在比特币体系里，经常提到地址，这多少让人有些费解，公钥算法用到的是私钥与公钥，跟地址有什么关系？椭圆曲线签名算法里的私钥由32字节随机数组成，通过私钥可以算出公钥，公钥经过一系列哈希算法及编码算法就得到了比特币中的地址。因此地址其实是公钥的另一种表现形式，可以理解为公钥的摘要。

椭圆曲线算法生成的公钥信息比较长，其压缩格式都有33字节，非压缩格式有65字节。地址是为了减少接收方标识的字节数。比特币地址的生成步骤如下：

1）生成椭圆曲线私钥与公钥。

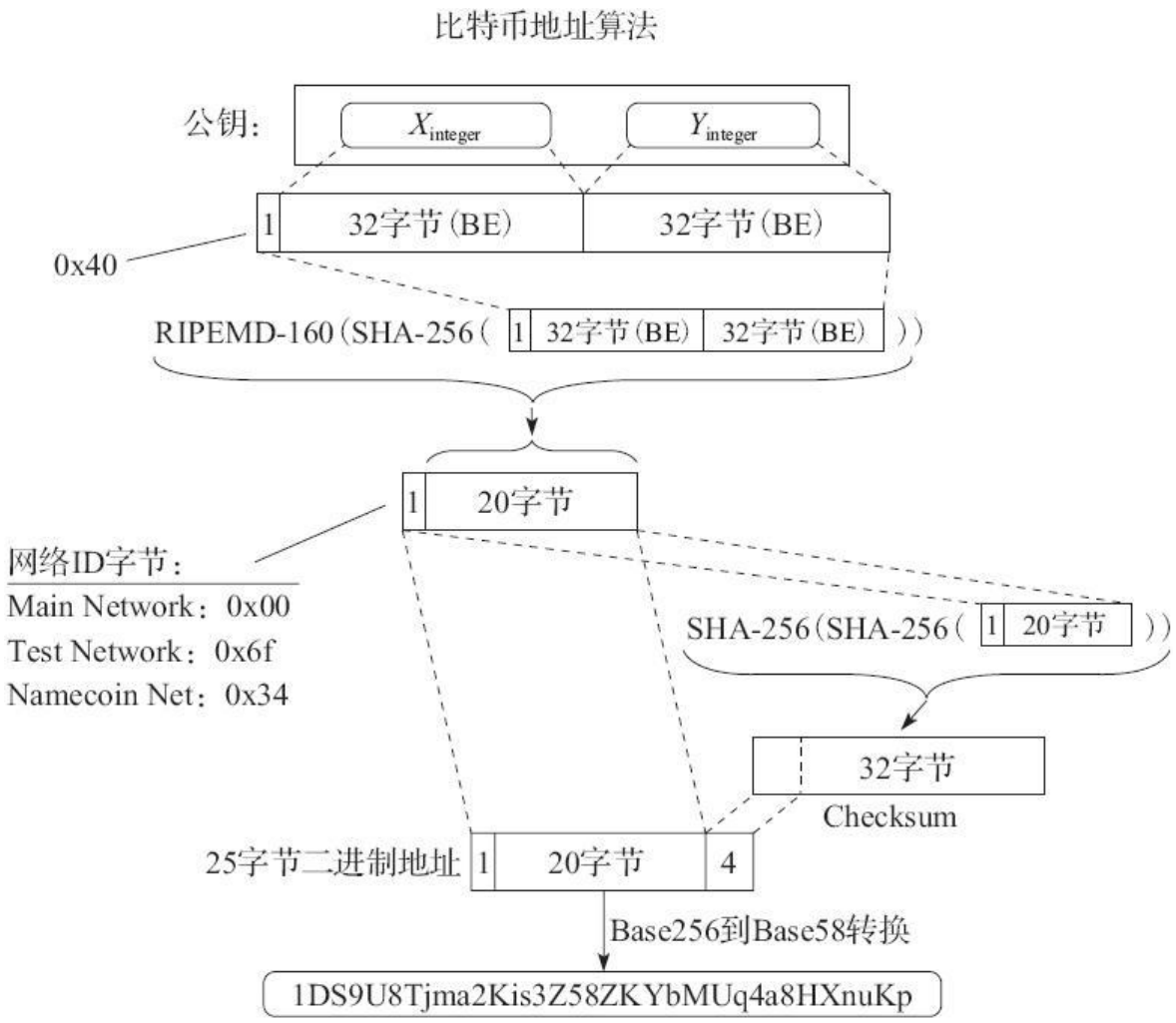
2）将公钥通过SHA-256哈希算法处理，得到32字节的哈希值。

3）对于得到的哈希值，通过RIPEMD-160算法来得到20字节的哈希值——Hash160。

4）把由版本号[2]+Hash160组成的21字节数据进行双次SHA-256哈希运算，得到的哈希值的前4字节作为校验和，放置在21字节数据的末尾。

5）对组成的25字节数组进行Base58编码，就可得到地址。

整个过程如下图所示。

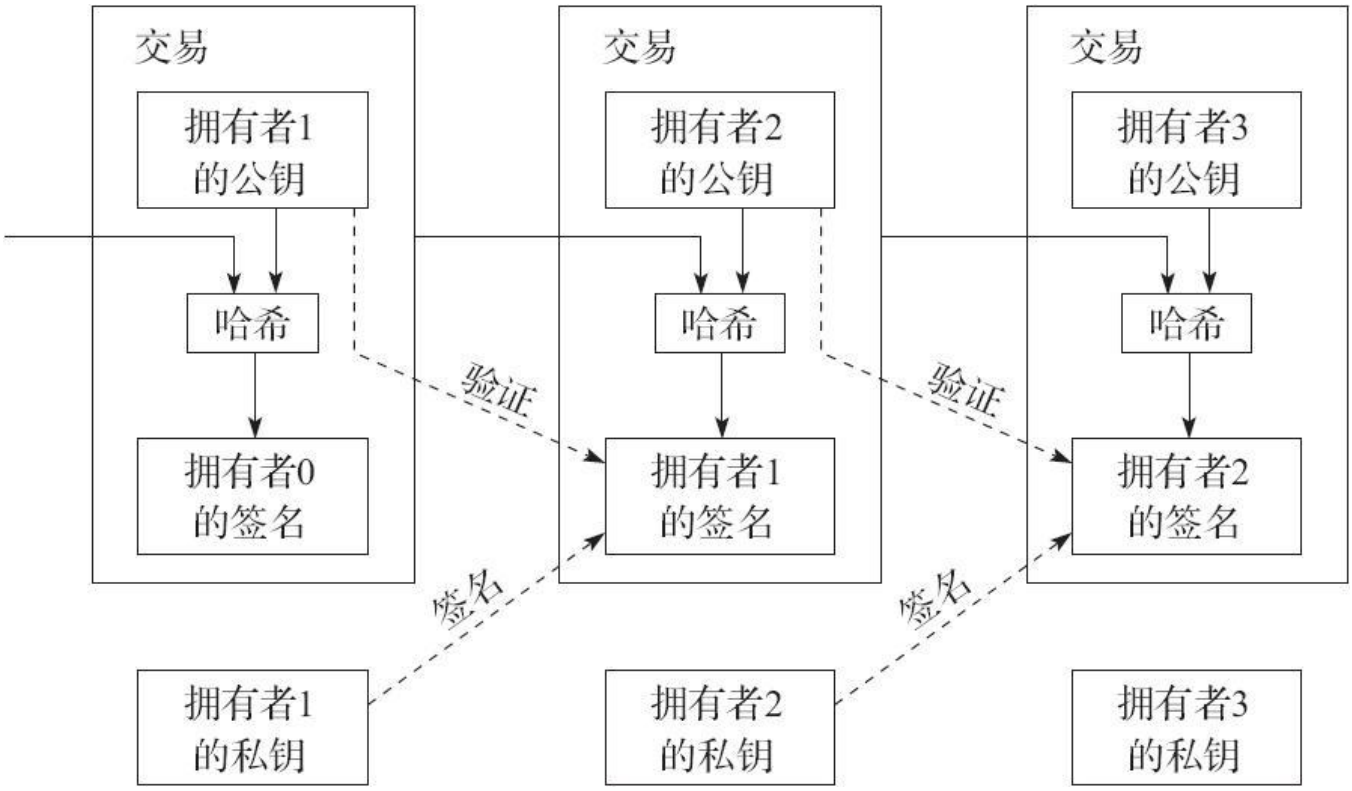


我们要花费一个地址上的资产，以构造一笔交易，同时使用与这个地址对应的私钥签名。而如果要将资产转移到某个地址上，只需要转账给它的公开地址即可。

交易

在中本聪的白皮书里，比特币被定义为一个链式的数字签名串。每一位电子货币的所有者通过这样的方式将它转移给下一位所有者：对前一个交易和下一位所有者的公钥签署一个数字签名，并将这个签名附加在交易的末尾。收款人通过验证签名，就可以验证电子货币的所有者链条。

交易的运作图如下。



这类交易体系的问题在于收款人很难校验之前的某位资产拥有者是否进行了双重支付（双花）。通常的解决方案是引入可信的第三方如银行来对每一笔交易进行检验，以防止双重支付。而如果想要排除第三方中介机构，那么交易信息就应当被公开，且需要整个系统内的所有参与者都有唯一公认的历史交易序列。收款人需要确保在交易期间系统内的绝大多数节点都认同该交易是首次出现[3]。

1.交易结构

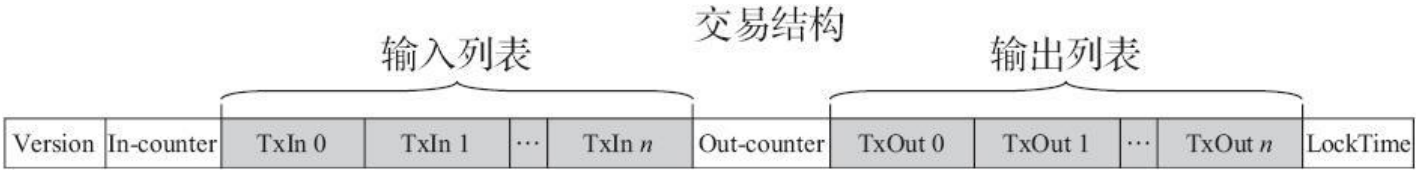
比特币的交易并不是通常意义上的一手交钱一手交货，而是转账。如果每一笔转账都需要构造一笔交易数据，那么显得比较笨拙。为了使得价值易于组合与分割，比特币的交易被设计为可以纳入多个输入和输出，即一笔交易可以转账给多个人。从生成到在网络中传播，再到通过工作量证明、整个网络节点验证，最终记录到比特币的区块链，这就是交易的整个生命周期。

交易的本质是一个包含交易发送方、接收方、资产转移等相关信息的数据结构，其数据结构如下表所示。

字段	描述	大小
版本（Version）	这笔交易参照的规则	4 字节
输入数量（In-counter）	交易输入（TxIn）列表的数量	1 ~ 9 字节
输入列表（Out-counter）	一个或多个交易输入	不定
输出数量（Lock time）	交易输出（TxOut）列表的数量	1 ~ 9 字节
输出列表	一个或多个交易输出	不定
锁定时间	锁定时间	4 字节

从整体结构来看，交易中的两个主要单元字段就是交易的输入与输出。输入标识着交易的发送方，输出标识着交易的接收方及对发送方的找零，交易的手续费则是输入的总和与输出的总和之差。由于所有的交易输入必然是前面某笔交易的输出，所以交易最核心的字段是交易的输出。

一笔交易的数据结构如下图所示。

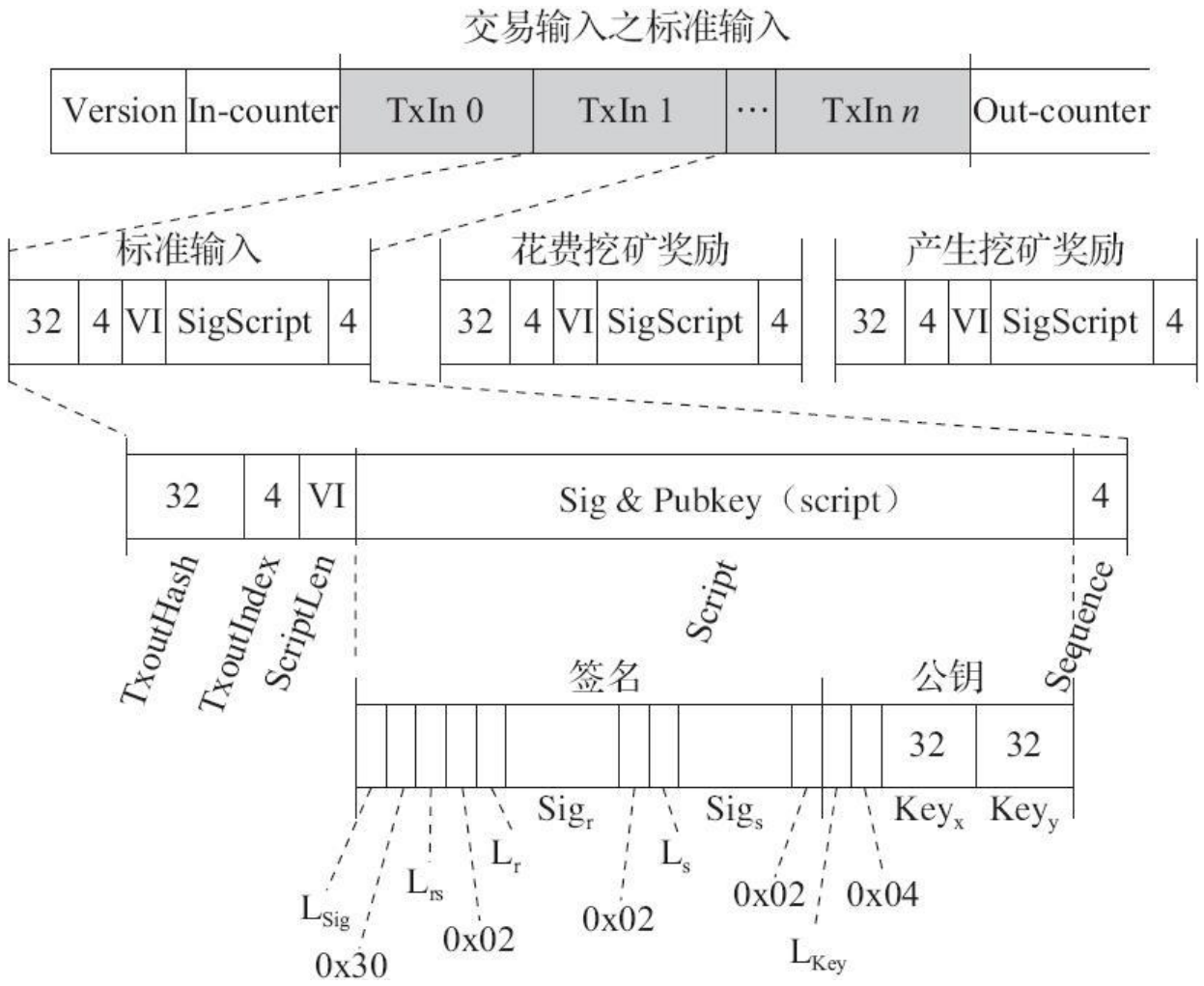


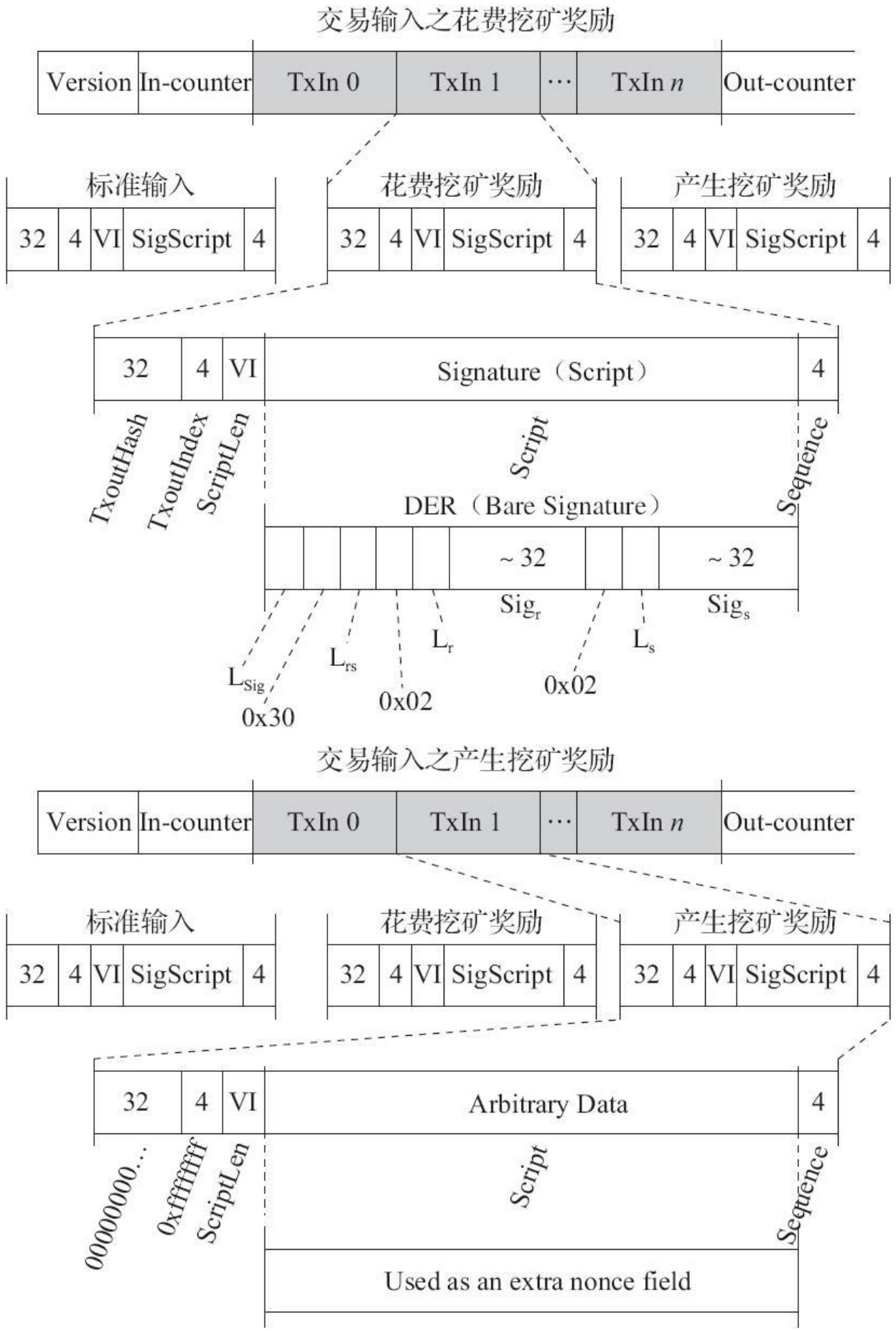
2.UTXO结构

UTXO（Unspent Transaction Outputs）是未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费的输出即为整个比特币网络的UTXO。

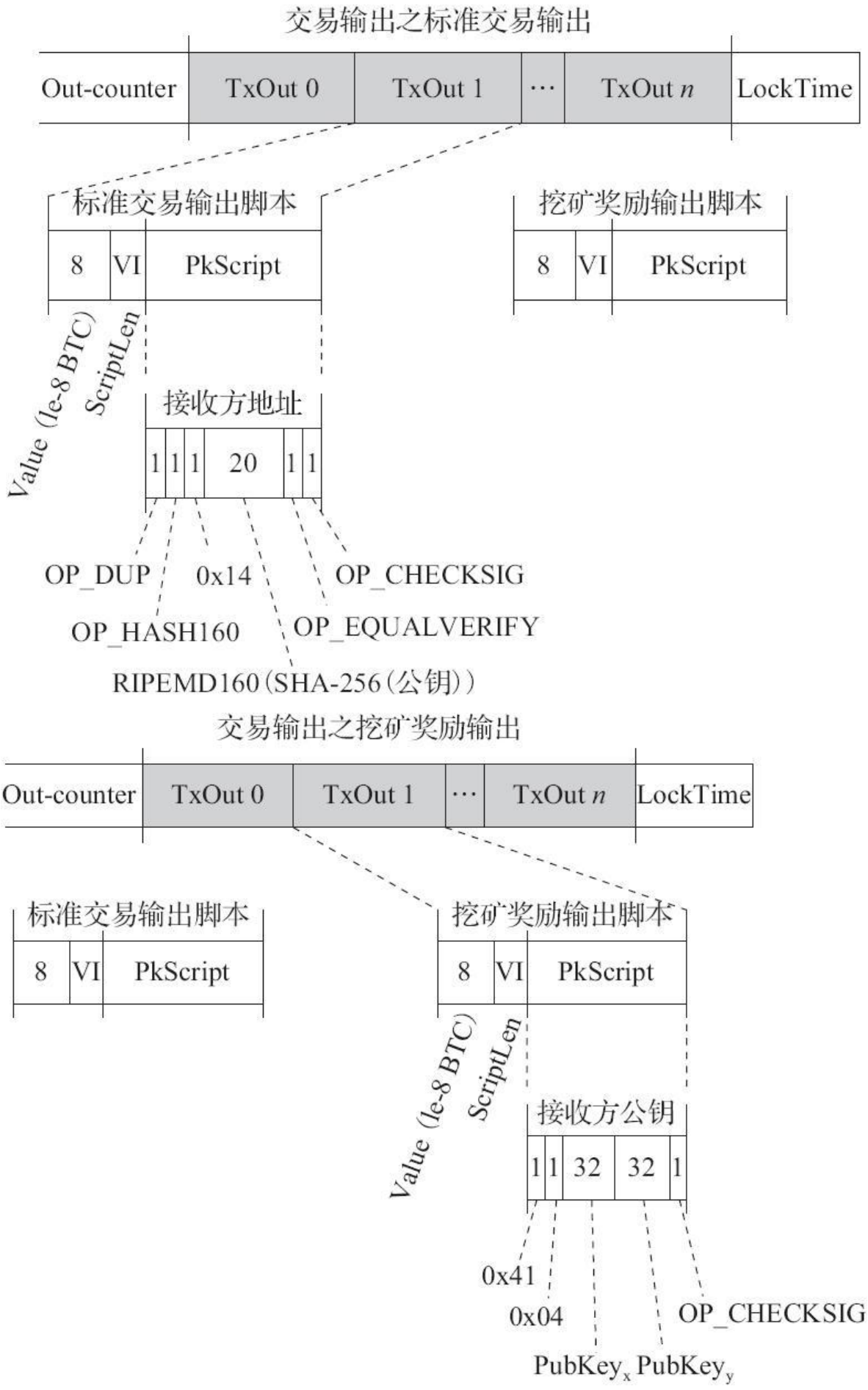
比特币规定每一笔新交易的输入必须是某笔交易未花费的输出，每一笔输入同时也需要上一笔输出所对应的私钥进行签名，并且每个比特币的节点都会存储当前整个区块链上的UTXO，整个网络上的节点通过UTXO及签名算法来验证新交易的合法性。

比特币的交易输入通常有3种，分别是标准输入（Standard TxIn）、花费挖矿奖励（Spend Coinbase TxOut）、产生挖矿奖励（Coinbase/Generation），下图分别描述了这3种交易输入的结构。





比特币的交易输出大致有两种，分别是标准交易输出（Standard TxOut）、挖矿奖励输出（Coinbase TxOut），下图分别描述了这两种交易输出的结构。



3.脚本

脚本是交易里另一个比较重要的技术。每一笔交易的每一项输出，严格意义上讲并不是指向一个地址，而是指向一个脚本。脚本类似于一套规则，它约束着接收方怎样才能花掉这个输出上锁定的资产。

交易的合法性验证也依赖于脚本。目前它依赖于两类脚本：锁定脚本与解锁脚本。锁定脚本是基于可变的模式，通过一段脚本语言来实现，位于交易的输出。解锁脚本与锁定脚本相对应，只有按锁定脚本的规则去解，才能花掉这个脚本上对应的资产，位于交易的输入。脚本语言可以表达出无数的条件变种。这也是比特币作为一种“可编程的货币”所拥有的特性。而解释该脚本是通过类似于编程领域里的“虚拟机”进行的，脚本分布地运行在比特币网络里的每一个节点上。

目前常用的比特币脚本主要分为两种，一种是普通的P2PKH类型（Pay-to-Public-Key-Hash），即支付给公钥的哈希值是地址，接收方只需要使用地址对应的私钥对该输出进行签名，即可花掉该输出。另一种是P2SH（Pay-to-Script-Hash），支付脚本的哈希值。拿多重签名来举例，它要求该输出要有N把私钥中的M把私钥（M≤N）同时签名才能花掉该资产，它类似于现实生活中需要多把钥匙才能同时打开的保险柜，只是更加灵活。

比如在比特币中，P2PKH的脚本规则如下：

```
pubkey script:
 op_dup op_hash160 <pubkeyhash> op_equalverify op_checksig
signature script:
 <sig><pubkey>
```

P2SH的脚本规则如下：

```
pubkey script:
 op_hash160 <hash160(
redeemscript)
> op_equal
signature script:
 <sig> [sig] [sig...] <redeemscript>
```

在上述的两种脚本规则里，Pubkey script代表着锁定脚本，Signature script代表着解锁脚本。以OP_开头的单词是相关的脚本命令，也是“虚拟机”所能解析的指令。这些命令规则根据Pubkey script的不同来进行划分，也决定着解锁脚本的规则。

比特币中的脚本机制相对简单，只是一个基于堆栈的、解释相关OP指令的引擎，能够解析的脚本规则并不是太多，不能实现很复杂的逻辑。但它为区块链可编程提供了一个原型，后续的一些可编程区块链项目其实是基于脚本的原理发展起来的，比如，以太坊就深入强化了脚本机制，该脚本机制不再只包括简单的OP指令，而是支持脚本语言，该脚本语言可以通过“虚拟机”去执行。以太坊实现了一个支持图灵完备脚本语言的区块链平台。

脚本机制对于区块链来说非常重要，它类似于区块链技术提供的一个扩展接口，任何人都可以基于这个接口去开发基于区块链技术的应用，比如智能合约的功能。脚本机制也让区块链技术作为一项底层协议成为可能。未来很多基于区块链的颠覆性应用，都可能是通过区块链的脚本语言来完成的。

区块

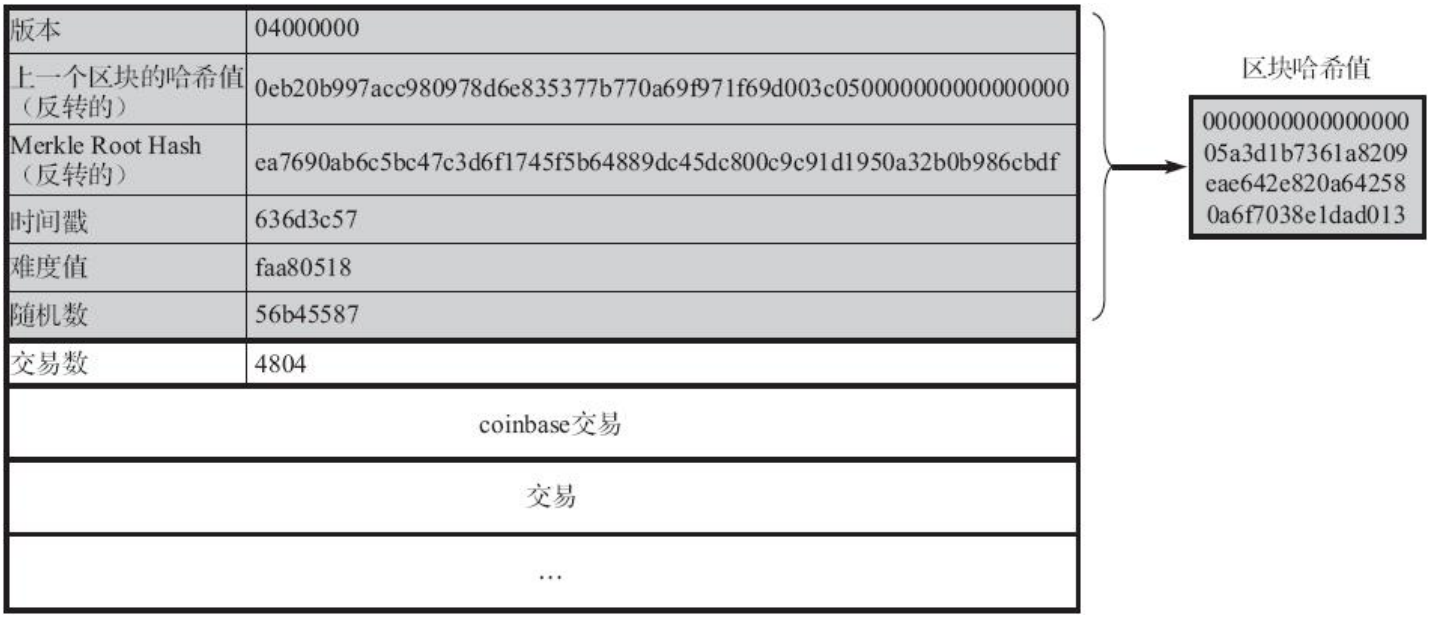
比特币网络中每个（挖矿）节点都基于已存在的最新区块生成下一个区块，同时将网络中未确认的合法交易包含进去。在完成工作量证明之后，将新的区块广播到全网，同时获得区块的奖励，这个过程就是将所有的交易打上时间戳标记的过程。由于只有最长链上的区块才能够获得奖励，这导致了所有的挖矿节点被利益驱使，形成唯一最长链的结果，从而达成记账系统共识的一致性，保证了整个体系的可靠与安全。而要了解这些过程，我们就必须先了解一下区块相关结构及区块链中所使用的相关技术与原理。

1.区块结构

比特币网络里合法的交易都会被打包成一个区块，包含到比特币的公开账本（区块链）里。区块由包含元数据的区块头和紧跟其后的交易列表组成。区块数据结构如下表所示[4]。

字段	描述	大小
魔术码	固定值 0xD9B4BEF9	4 字节
区块大小	用字节表示该段之后的区块大小	1 ~ 9 字节
区块头	包含 6 个字段	80 字节
交易数量	交易列表长度	1 ~ 9 字节
交易列表	记录到区块的交易信息列表中	不定

区块数据的核心示例结构如下图所示。



区块由区块头及该区块所包含的交易列表组成。区块头的大小为80字节，由4字节的版本、32字节的上一个区块的哈希值、32字节的Merkle Root Hash、4字节的时间戳（当前时间）、4字节的当前难度值、4字节的随机数等组成。区块所包含的交易列表则附加在区块头后面。比特币网络约定每个区块的第一笔交易是coinbase交易，这是一笔为了让矿工获得奖励及手续费的特殊交易。

2.Merkle Tree

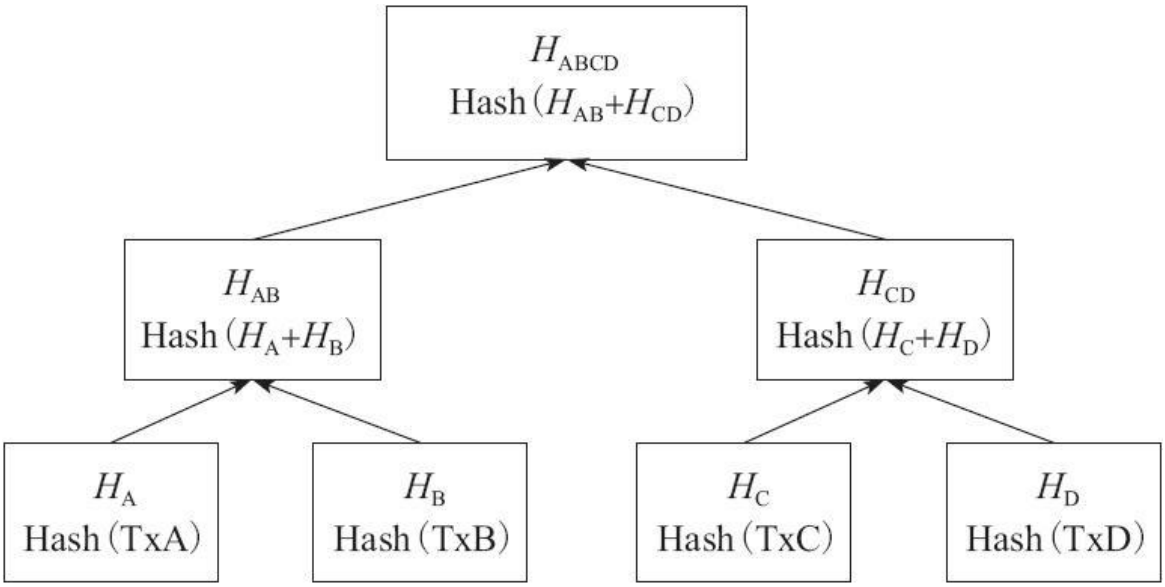
区块包含的所有交易首先都会通过Merkle Tree算法生成Merkle Root Hash并存储至区块头的数据结构里。Merkle Tree算法是用来同步数据一致性的算法，它基于一组哈希值列表构建成一个树，树的根哈希值作为原始数据列表的摘要。Merkle Tree具有以下特点：

1）数据结构是一个树，可以是二叉树，也可以是多叉树。

2）Merkle Tree的叶子节点的值是数据集合的单元数据或者单元数据的哈希值。

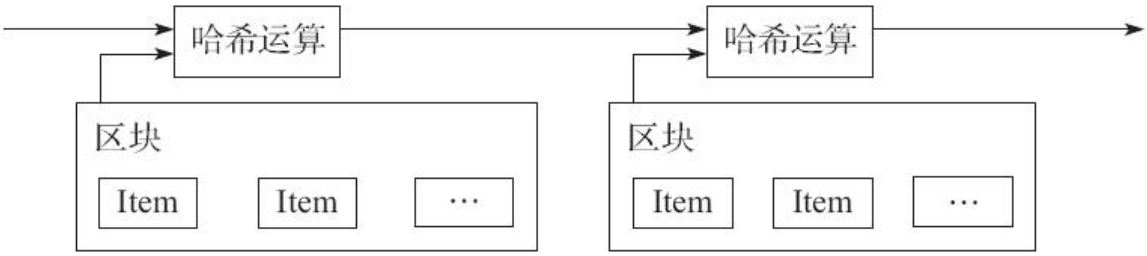
3）Merkle Tree的非叶子节点的值是所有叶子节点值的哈希值。

区块中所使用的Merkle Tree算法的原理如下图所示。



3.时间戳服务器

为了实现一个点对点的电子现金系统，中本聪提出了“时间戳服务器”方案。时间戳服务器对以区块形式存在的一组数据实施随机哈希处理，加上时间戳，并将该随机哈希值进行广播。显然，该时间戳能够证实特定数据于某特定时间是的确存在的，因为只有在该时刻存在了，才能获取相应的随机哈希值。每个时间戳应当将前一个时间戳纳入其随机哈希值中，每一个随后的时间戳都对之前的一个时间戳进行增强（Reinforcing），这样就形成了一个链条（Chain）。



网络

比特币采用了基于P2P（Peer to Peer）的网络架构。P2P是指位于同一网络中的每台计算机都是彼此公平、对等的，各个节点共同提供网络服务，不存在任何“特殊”（中心）节点。P2P网络通信本身并不是比特币独有的发明，在比特币之前就已经被应用于文件共享领域了。比特币被设计成一个点对点的数字现金系统，而P2P正好是这个理念的核心特征的反映，也是该特征的基石。抛开比特币客户端的钱包功能来看，运行在每一台机器上的比特币核心程序就是比特币P2P网络中的一个节点。每个节点之间互联，组成了比特币网络，保证了整个比特币系统的安全。

比特币网络的相关功能如下：

1）新交易广播到全网的节点，每个节点会收到交易消息。

2）每个（挖矿）节点将新交易收集到节点的内存，并组装成区块。

3）每个（挖矿）节点都尝试在自己的区块中找到一个具有足够难度的工作量证明。

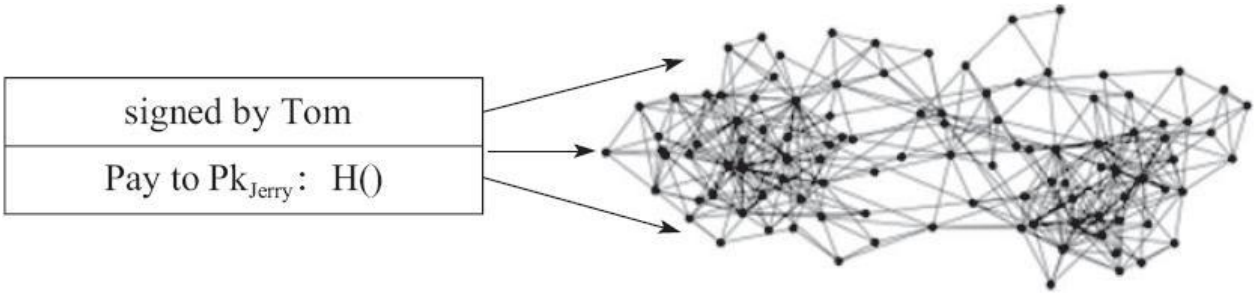
4）（挖矿）节点找到一个工作量证明，把有效的区块数据向全网进行广播。

5）当且仅当包含在该区块中的交易都是有效的，并验证其完成了工作量证明，其他节点才认同该区块的有效性。

6）其他（挖矿）节点表示接受该区块，并在该区块的末尾制造新的区块以延长整个区块的链条。

在比特币网络中，交易和区块信息的传播是通过洪水算法（Flooding Algorithm）进行的。简单地说，就是每一个收到信息的节点，

向与它相连的所有节点推送该信息。下一个收到信息的节点继续这个过程，信息很快就会像洪水一样覆盖全网络。可见，传播速度是呈指数增长的。通常在一两秒内，交易或者区块的信息就可以传遍全网。



广播交易内容　　通过洪水算法进行传播

节点始终都将最长的链条作为正确的链条，在它的基础上持续工作并延长它。如果有两个节点同时广播不同的基于上一个区块的新区块，那么其他节点在接收到该区块的时间先后上将存在差别。在此情形下，它们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条。该僵局的打破要等到下一个区块（工作量证明）被发现，当其中的一条链条被证实为是较长的一条时，在另一条分支链条上工作的（挖矿）节点将转换阵营，开始在较长的链条上工作。

所谓“新交易的广播”，实际上不需要抵达网络中的全部节点，只要交易信息能够抵达足够多的节点，它们将很快被整合进一个新的区块中。而区块的广播对被丢弃的信息进行容错处理。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了该区块，就会向较长链的节点发出下载该缺失区块的请求。

比特币网络中的矿工们不停地在最新的区块基础上构造下一个区块，通过算力竞争来争取记账权（将新区块写到比特币的区块链的机会），确认网络的转账交易，同时获取区块奖励。由于每一个区块都包含上一个区块的哈希值，通过这个前向的哈希值，区块以链条的形式进行相连，最终形成了由各个区块组成的记账系统——区块链。而确保这一切运转正常的正是我们接下来要讲的共识算法。

[1] 引自于https://bitcoin.org/bitcoin.pdf。

[2] 普通地址P2PKH 的版本默认值是0，P2SH 类型的地址版本默认值是5。

[3] 引用自https://bitcoin.org/bitcoin.pdf。

[4] 引用自https://en.bitcoin.it/wiki/Block。

共识算法

要想整个P2P网络维持一份相同的数据，同时保证每个参与者的公平性，整个体系的所有参与者必须要有统一的协议，也就是我们这里要讲的共识算法。比特币所有的节点都遵循统一的协议规范。协议规范（共识算法）由相关的共识规则组成，这些规则可以划分为两个大的核心：工作量证明与最长链机制。所有规则（共识）的最终体现就是比特币的最长链。共识算法的目的就是保证比特币不停地在最长链条上运转，从而保证整个记账系统的一致性和可靠性。

工作量证明

工作量证明（POW）可简单地理解为一份证明，用来确认你做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。比如现实生活中的毕业证、驾驶证等，也是通过检验结果的方式（通过相关的考试）取得证明。

1.起源

工作量证明系统（或者说协议、函数），是一种应对拒绝服务攻击和其他服务滥用的经济对策。它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间。这个概念由Cynthia Dwork和Moni Naor 1993年在学术论文中首次提出[1]。而工作量证明这个名词，则是在1999年Markus Jakobsson和Ari Juels的文章[2]中才被真正提出。

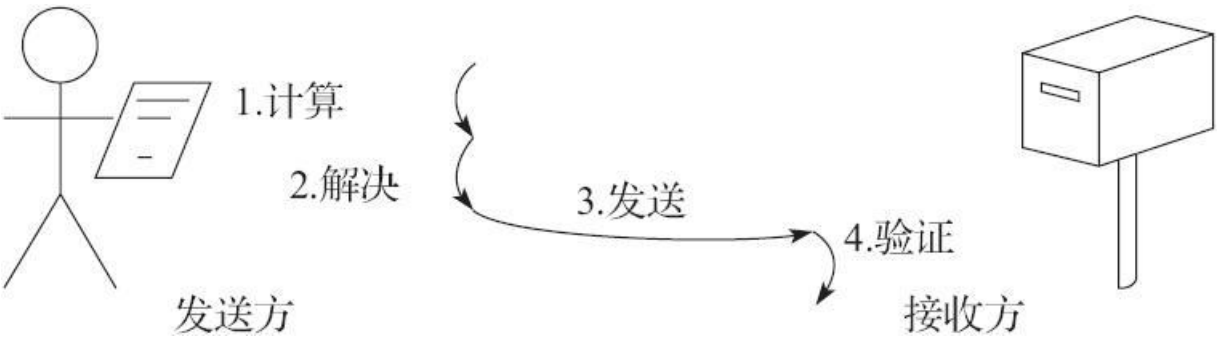
哈希现金[3]是一种工作量证明机制，它是亚当·贝克（Adam Back）在1997年发明的，用于抵抗邮件的拒绝服务攻击及垃圾邮件网关滥用。在比特币之前，哈希现金被用于垃圾邮件的过滤，也被微软用于Hotmail/Exchange/Outlook等产品中（微软使用一种与哈希现金不兼容的格式，并将之命名为电子邮戳）。

哈希现金也被哈尔·芬尼以可重复使用的工作量证明（RPOW）的形式用于一种比特币之前的加密货币实验中。另外，戴伟的B-money、尼克·萨博的比特金（Bit-Gold），这些比特币的先行者都是在哈希现金的框架下进行挖矿的。

2.工作量证明的基本原理

工作量证明系统的主要特征是客户端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查客户端是不是做了相应的工作。这种方案的一个核心特征是不对称性：工作对于请求方是适中的，对于验证方则是易于验证的。它与验证码不同，验证码的设计出发点是易于被人类解决而不易被计算机解决[4]。

下图表示的是工作量证明的流程。



举个例子[5]，给定一个基本的字符串“Hello，world！”，我们给出的工作量要求是，可以在这个字符串后面添加一个叫作nonce（随机数）的整数值，对变更后（添加nonce后）的字符串进行SHA-256哈希运算，如果得到的哈希结果（以十六进制的形式表示）是以“0000”开头的，则验证通过。为了达到这个工作量证明的目标。我们需要不停地递增nonce值，对得到的新字符串进行SHA-256哈希运算。按照这个规则，需要经过4251次计算，才能找到恰好前4位为0的哈希散列。

"Hello，world！0"=>1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

"Hello，world！1"=>e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

"Hello，world！2"=>ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7

...

"Hello，world！4248"=>6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965

"Hello，world！4249"=>c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6

"Hello，world！4250"=>0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

通过这个示例我们对工作量证明机制有了一个初步的理解。有的人会认为如果工作量证明只是这样一个过程，那是不是只需要记住nonce为4521使计算能通过验证就行了？当然不是的，这只是一个例子。

下面，我们将输入简单地变更为“Hello，world+整数值”，整数值取1~1000，也就是说，将输入变成一个由1000个值组成的数组：Hello，world！1；Hello，world！2；…；Hello，world！1000。然后对数组中的每一个输入依次进行上面例子中要求的工作量证明——找到前导为4个0的哈希散列。

由于哈希值伪随机的特性，根据概率论的相关知识容易算出，预期要进行2^{16}次尝试，才能得到4个前导为0的哈希散列。而统计一下刚才进行的1000次计算的实际结果会发现，进行计算的平均次数为66958次，十分接近2^{16}（65536）。在这个例子中，数学期望的计算次数就是要求的“工作量”，重复多次进行的工作量证明会是一个符合统计学规律的概率事件。

统计输入的字符串与得到对应目标结果实际使用的计算次数列表如下：

Hello，world！1=>42153

Hello，world！2=>2643

Hello，world！3=>32825

Hello，world！4=>250

Hello，world！5=>7300

...

Hello，world！995=>164819

Hello，world！996=>178486

Hello，world！997=>22798

Hello，world！998=>68868

Hello，world！999=>46821

比特币体系里的工作量证明机制与上述示例类似，但要比它更复杂一些。

3.比特币中的工作量证明

对于比特币网络中的任何一个节点，如果想生成一个新的区块并写入区块链，则必须解出比特币网络出的工作量证明的迷题。这道题的3个关键要素是工作量证明函数、区块及难度值。工作量证明函数是这道题的计算方法，区块决定了这道题的输入数据，难度值决定了解这道题所需要的计算量。

比特币网络中使用的工作量证明函数正是前文提及的SHA-256。已经讲过区块的数据结构，但并未具体描述区块的产生过程。区块其实就是在工作量证明环节产生的。矿工通过不停地构造区块数据，检验每次计算出的结果是不是满足工作量，从而判断该区块是不是符合网络难度。区块头即为比特币的工作量证明的输入数据。

难度值是矿工们挖矿的重要参考指标，它决定了矿工大约需要经过多少次哈希运算才能产生一个合法的区块。比特币的区块大约每10分钟生成一个，如果要在不同的全网算力条件下，新区块的产生都基本保持这个速率，难度值必须根据全网算力的变化进行调整。简单地说，难度值被设定在无论挖矿能力如何，新区块产生速率都保持在10分钟一个。

难度值的调整是在每个完整节点中独立自动发生的。每隔2016个区块，所有节点都会按统一的公式自动调整难度值，这个公式是由产生最新2016个区块的花费时长与期望时长（期望时长为20160分钟，即两周，是按每10分钟一个区块的产生速率计算出的总时长）比较得出的，根据实际时长与期望时长的比值，进行相应调整（或变难或变易）。也就是说，如果区块产生的速率比10分钟快，则增加难度，比10分钟慢，则降低难度。

这个公式可以总结为如下形式：

新难度值=旧难度值*（过去2016个区块花费时长/20160分钟）

工作量证明需要有一个目标值。比特币工作量证明的目标值（Target）的计算公式如下：

目标值=最大目标值/难度值

其中，最大目标值为一个恒定值：0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

目标值的大小与难度值成反比。比特币工作量证明的达成就是矿工计算出来的区块哈希值必须小于目标值。

我们也可以将比特币工作量证明的过程简单理解成，通过不停地变换区块头（即尝试不同的nonce值）并将其作为输入，进行SHA-256哈希运算，找出一个有特定格式的哈希值的过程（即要求有一定数量的前导0）。而要求的前导0的个数越多，难度越大。

可以把比特币矿工解这道工作量证明迷题的步骤大致归纳如下：

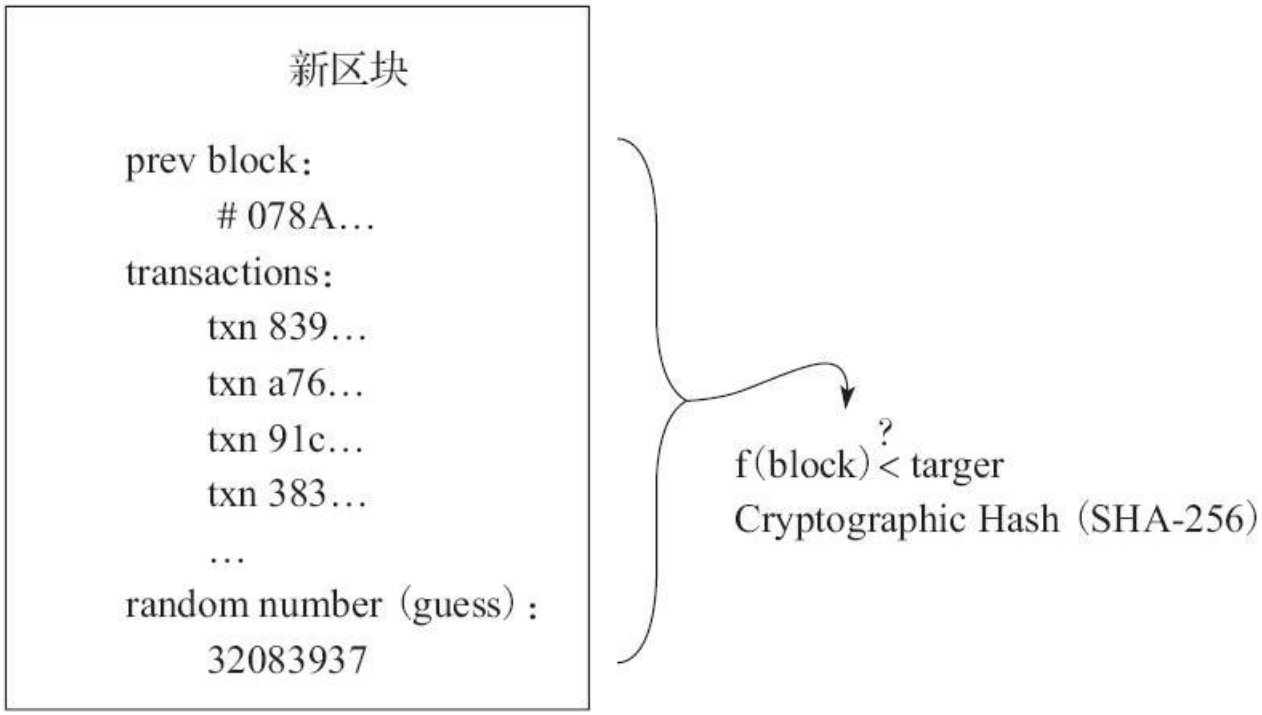
1）生成coinbase交易，并与其他所有准备打包进区块的交易组成交易列表，通过Merkle Tree算法生成Merkle Root Hash。

2）把Merkle Root Hash及其他相关字段组装成区块头，将区块头的80字节数据作为工作量证明的输入。

3）不停地变更区块头中的随机数（即nonce的数值），并对每次变更后的区块头做双重SHA-256运算（即SHA256（SHA256（Block_Header））），将结果值哈希反转并与当前网络的目标值对应的十进制字符串做对比，如果小于目标值，则解题成功，工作量证明完成。

该过程可以用下图表示：

区块迷题

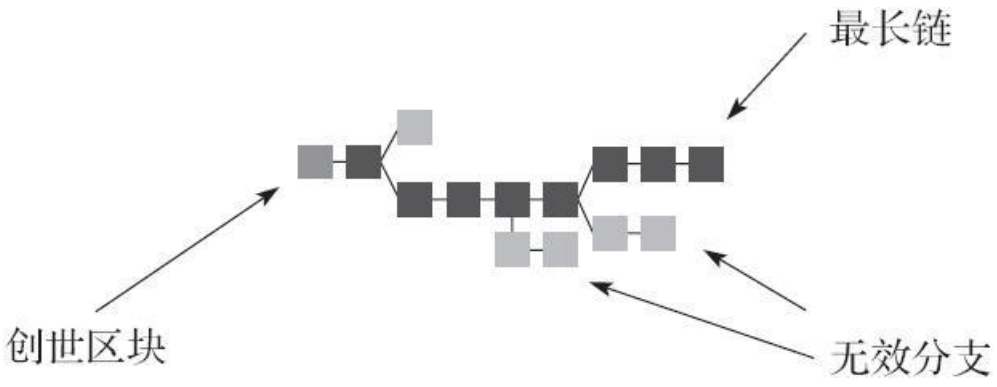


比特币的工作量证明，就是我们俗称“挖矿”所做的主要工作。理解工作量证明机制，将为我们进一步理解比特币区块链的共识机制奠定基础。

最长链机制

比特币网络要求所有节点都遵循一个协议（共识），所有保存到本地的区块链必须是被本地节点验证通过的最长链。由于区块链的每个区块必须引用它的前一个区块，所以最长链是最难推翻的。

理论上，矿工可以在任意区块的基础上开始计算下一个区块。但只有最长区块链上的区块才能获得系统的承认并得到挖矿奖励。打包区块获得的奖励在该区块上增加99个新区块（100个确认）之后才能使用。这是保证区块链不发生分裂的重要机制。



算力攻击

比特币在设计之初是为了实现一个点对点的电子现金系统，而这一系统的难题是如何避免双重支付问题。共识算法的目标就是降低双重支付的可能性。在中本聪的白皮书里针对设计的比特币体系做了一个数学推算，以验证整个比特币体系里发生双重支付的概率，这里引用相关原文，让大家来感受一下比特币区块链体系的安全性。

1.计算

设想如下场景：一个攻击者试图生成一条具有替代性的链，这条链的延长速度比诚实链的延长速度更快。即便这一目的达成了，也不意味着系统可以任攻击者为所欲为，比如凭空制造币或者拿走从来不属于他的币。节点不会接受一个无效的交易，而诚实节点永远不会接受包含无效交易的区块。攻击者唯一能尝试的是：改变一笔自己的交易，并尝试把钱从他最近的花费中拿回来。

诚实链和攻击链之间的竞赛具有二项随机漫步（Binomial Random Walk）的特点。成功事件意味着诚实链延长了一个区块，领先加1，失败事件意味着攻击链延长了一个区块，差距减1。

攻击者成功填补某一既定差距的概率类似于赌徒破产问题（Gambler's Ruin Problem）。假定一个赌徒拥有无限的透支信用，然后开始进行潜在次数为无穷的赌博，以试图填补自己的亏空，那么我们可以计算他补上亏空的概率，也就是该攻击链赶上诚实链的概率，如下所示[6]：

$$p = \text{诚实节点制造出下一个区块的概率}$$

$$q = \text{攻击者制造出下一个区块的概率}$$

$$q_z = \text{攻击者最终消弭了 } z \text{ 个区块的落后差距}$$

$$q_z = \begin{cases} 1, & p \leqslant q \\ \left(\frac{q}{p}\right)^z, & p > q \end{cases}$$

假定p>q，那么攻击成功的概率就随着攻击者要追上的区块数的增长而呈现指数下降。概率是攻击者的敌人，如果他最开始不能获得幸运的突破，那么随着他落后的越多，他成功的机会就会变得无限渺茫。

现在考虑一下，一个新交易的收款人需要等到多长时间，才能足够确信发款人已经不可能改变这笔交易了。假设付款人是一个攻击者，他希望收款人相信他已经付过款了，然后过一段时间将已支付的款项重新发回给自己。付款人希望就算届时收款人会察觉这一点，也已经于事无补。

对此，收款人生成一个新的密钥对，然后在交易签署前不久将公钥发送给付款人。这可以防止付款人预先准备好一个链，然后持续地对此区块进行运算，直到他的链幸运地超越了诚实链，然后立即执行支付。在此情形下，只要交易一发出，攻击者就开始悄悄地准备一条包含了该交易替代版本的平行链条。

收款人将等待交易出现在首个区块中，然后等到z个区块连接在其后。此时，他仍然不能确切地知道攻击者已经进展了多少个区块，但是假设诚实区块产生一个区块将耗费平均预期时间，那么攻击者的潜在进展就是一个泊松分布，分布的期望为

$$\lambda = z\frac{q}{p}$$

在此情形下，为了计算攻击者追赶上的概率，将攻击者取得进展区块数量的泊松分布的概率密度乘以在该数量下攻击者依然能够追赶上的概率：

$$\sum_{k=0}^{\infty}\frac{\lambda^{k}e^{-\lambda}}{k!}\cdot\begin{cases}\left(\frac{q}{p}\right)^{(z-k)}, & k\leqslant z\\ 1, & k>z\end{cases}$$

将其简化为如下形式，避免对无限数列求和：

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\cdot\left(1-\left(\frac{q}{p}\right)^{z-k}\right)$$

转化为C语言代码[7]：

```
#include double attackersuccessprobability(
double q,
 int z)

{
    double p = 1.0 - q;

    double lambda = z * (
q / p);

    double sum = 1.0;

    int i,
 k;

    for (
k = 0;
 k <= z;
 k++)

    {
        double poisson = exp(
-lambda);

        for (
i = 1;
 i <= k;
 i++)

            poisson *= lambda / i;

            sum -= poisson * (
1 - pow(
q / p,
 z - k));

    }
    return sum;

}
```

对其进行运算，可以得到如下的概率结果，发现概率对z值呈指数下降。

当q=0.1时：

z=0　p=1.0000000

z=1　p=0.2045873

z=2　p=0.0509779

z=3　p=0.0131722

z=4　p=0.0034552

z=5　p=0.0009137

z=6　p=0.0002428

z=7　p=0.0000647

z=8　p=0.0000173

z=9　p=0.0000046

z=10　p=0.0000012

当q=0.3时：

z=0　p=1.0000000

z=5　p=0.1773523

z=10　p=0.0416605

z=15　p=0.0101008

z=20　p=0.0024804

z=25　p=0.0006132

z=30　p=0.0001522

z=35　p=0.0000379

z=40　p=0.0000095

z=45　p=0.0000024

z=50　p=0.0000006

求解令p<0.1%的z值，具体如下。

为使p<0.001，则

q=0.10　z=5

q=0.15　z=8

q=0.20　z=11

q=0.25　z=15

q=0.30　z=24

q=0.35　z=41

q=0.40　z=89

q=0.45　z=340

计算结果表明，不管攻击者算力在整个网络的占比是多少，随着区块链里区块确认数增加，发生双重支付的概率就越来越低。只有当你的算力占比比较高的时候才有成功的可能，而这个其实又可以通过增加确认数来避免。如果支付方与接收方调整相应的参数作为交易的条件，比如规定N个确认才算交易完成，那么区块链的双花问题在这个体系下变得异常困难。

2.51%算力攻击

虽然比特币的体系在设计上已经大大降低了双重支付的可能，但没有绝对安全的系统。在攻击者拥有超过整个网络一半算力的情况下，就有能力推翻原有已经确认过的交易，使恶意的双花成为可能，业内形象地称之为51%算力攻击。攻击者掌握了全网51%的算力后，可以用这些算力来重新计算已经确认过的区块，使区块产生分叉，完成双花并获得利益。攻击者如果发动攻击，则能做到：

1）控制自己的交易，一笔发给接收者，另一笔发送给自己，让最终发给自己的交易成功而接收者的失效，欺骗接收者，实现双花成功。

2）阻止别人的交易被打包到区块，让交易不能确认。

3）阻止别人生成新的区块，获得区块奖励。

不能做的事情如下：

1）控制别人发送的交易。

2）阻止别人发送交易。

3）更改每个区块的奖励数量。

4）凭空产生币。

5）发送不属于他自己的币。

通过上述内容可很容易看出，攻击者实施51%算力攻击时唯一对自己有利的就是，完成对自己交易的双花，骗取交易接收方的利益。

而从经济学的角度去看这个攻击问题，攻击者通过攻击来获取利益，但这是需要成本的（算力成本），只有当攻击获取的收益大于成本，也大于他诚实工作所获取的收益时，攻击者才会自发动攻击的意图。假定的有理性的人，即为了获得更大收益而发起攻击的人，实际上是不会发动这样的攻击的。这样就产生了51%攻击的悖论，攻击者发起攻击要考虑自身利益，出于较高的成本，算力拥有者都会选择诚实的工作。

除了上述的攻击成本之外，攻击其实也依赖于社区的理性选择，这也让攻击的成功率很低。历史上，Ghash.io曾经出现过算力接近于51%的情形，造成了社区恐慌，矿工选择撤离，最终让Ghash.io的算力急剧下降。而国内4家矿池也曾出现整体算力

接近51%的情形。2015年，国内矿池联盟合作，而且并未遵守社区软分叉的协议，产生新版本号的区块，造成区块高度为36731~36736的相关区块不符合社区的协议。另外，其他矿池基于36731产生新版本的区块，而未选择在国内产生的新区块的链条上挖矿，此事件也同样引起社区的热议。最终，违背社区协议的国内几大矿池将所挖的区块作废，在遵从社区协议的链条上挖矿产生新版本号的新区块。历史上的诸多事件证明，除了共识算法，社区成员的理性选择，也同样是维护整个区块链体系安全的保障。

共识算法的探索

1.POW

POW使用的哈希算法原理上接近一个暴力破解的过程。随着比特币的发展及其市值的增加，市场上出现了ASIC矿机，它是专门针对比特币使用的SHA-256算法研发的，从而使系统总算力不断上升。算力的快速上涨既降低了挖矿过程的去中心化，又带来了越来越高的能源消耗。这种现象引发了社区的讨论。于是有新的竞争币尝试使用不同的用于工作量证明的哈希算法。

竞争币的鼻祖莱特币，除了修改了比特币的相关参数，最大的调整就是对共识算法的更改，将比特币工作量证明所使用的SHA-256哈希算法变更为Scrypt哈希算法，两者的不同在于，Scrypt哈希算法本身不适宜进行并行计算，因此制造专业的ASIC矿机比较困难。在实践中，随着莱特币市值的增加，人们也制造出了针对Scrypt的专业矿机。竞争币Darkcoin后续所使用X11算法，即让11种哈希算法串联起来作为工作量证明的哈希函数，以防止专业的ASIC芯片矿机。再到后来又有出现了专门针对矿池挖矿的算法SpreadX11，它的代表者则是竞争币Spreadcoin。

2.POS

POS（Proof Of Stake，权益证明）是一种不同于工作量证明的共识机制，它不通过竞争性的哈希计算，而是通过节点对所有权的证明来达成共识。有些人认为，随着区块奖励的减少，工作量证明机制最终会导致系统出现“公地悲剧”，而权益证明机制对矿工的激励机制，可以维持更好的系统安全。

真正将POS机制运用起来的数字货币是点点币（PPC，PPCoin）。这里首先要引入币龄这一概念，在比特币里，UTXO所位于区块的高度与当前最长链高度之间的差值决定着该笔Unspent币龄的大小，差值越大，代表着币龄越高。该Unspent的使用也就代表着币龄的消耗。在POS机制里，一笔交易可以消耗的币龄被视为POS的一种形式，POS指的是一种对货币所有权的证明。拥有币且币龄越高的节点拥有着产生新区块的权力。

3.小结

新共识算法的发明常常是源于对工作量证明能源消耗的优化及对专业矿机挖矿的抵制，很多人都在寻找任意节点（通过GPU或者是CPU，也就是一台计算机）都可以参与整个网络挖矿的方法。以太坊发明了自己的挖矿算法ethash来抵制专业芯片的矿机，同时宣称将会以POW+POS的机制来运行整个区块链网络。

另外，大量的私有链都尝试采用或发明了不同的共识算法。有限的去中心化，使得我们可以采用更为高效且低成本的共识算法。而类似于比特币区块链这样的公有链，由于需要达成所有节点完全平等、自由加入等特性的完全去中心化，相应的一定规模的资源消耗几乎是必然的。

[1] Dwork, Cynthia; Naor, Moni (1993).“ Pricing via Processing, Or,Combatting Junk Mail, Advances in Cryptology ”. CRYPTO ’92: Lecture Notes in Computer Science No. 740 (Springer): 139–147.

[2] Jakobsson, Markus; Juels, Ari (1999). “ Proofs of Work and Bread Pudding Protocols ”. Communications and Multimedia Security (Kluwer Academic Publishers): 258–272.

[3] 引用自https://en.wikipedia.org/wiki/Hashcash。

[4] 引用自https://en.wikipedia.org/wiki/Proof-of-work_system。

[5] 引用自https://en.bitcoin.it/wiki/Proof_of_work。

[6] W. Feller, An introduction to probability theory and its applications, 1957.

[7] 引用自https://bitcoin.org/bitcoin.pdf。

侧链技术

侧链

所谓“侧链”（又称楔入式侧链），是相对于主链而言的，是平行于主链的另一条区块链。它们通过“双向锚定”（Two-Way Pegging）来建立关联，实现主链与侧链之间价值的双向转移。可以在侧链上使用主链资产，并通过侧链来弥补主链功能的不足。虽然它们具有双向转移的能力，但它们是隔离的，即使侧链中的加密被破解（或恶意设计），所有的损害也都只限于侧链本身。

侧链作为主链新功能或新业务逻辑的“试验田”，一方面帮助主链试行、扩展新功能，另一方面随着各种主链本身无法具备的业务逻辑在侧链上实现，围绕主链可更进一步搭建起一个覆盖各种业务需求的产业生态圈。比如新的扩展可以支持无数资产类型，例如股票、债券、金融衍生品、真实和虚拟的世界货币，还能够实现智能合约、安全处理机制和真实世界财产注册。目前Blockstream以比特币区块链作为主链，正在做自己的侧链项目[1]。

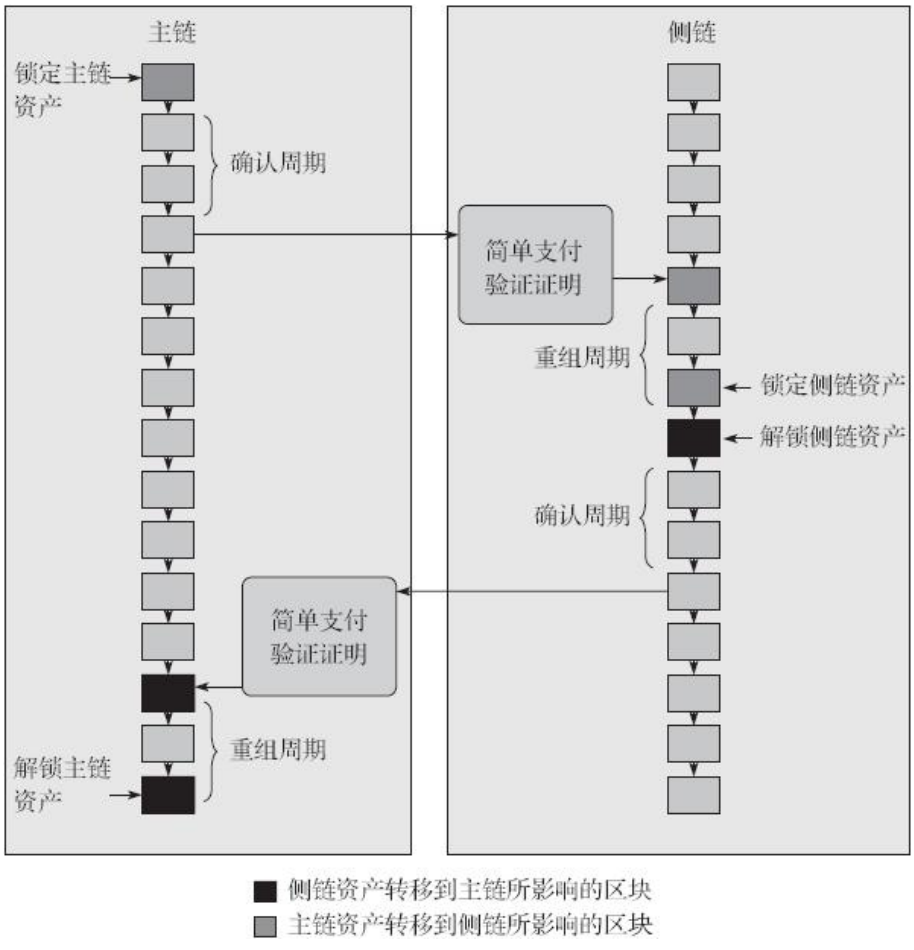
技术原理

侧链区块链使用的技术大体与主链相似，侧链技术的核心在于与主链之间建立起桥梁。这一技术又被形象地称为楔入，按楔入的实现方式，可将其划分为多种类型，这里主要了解双向楔入和联合楔入。

1.双向楔入

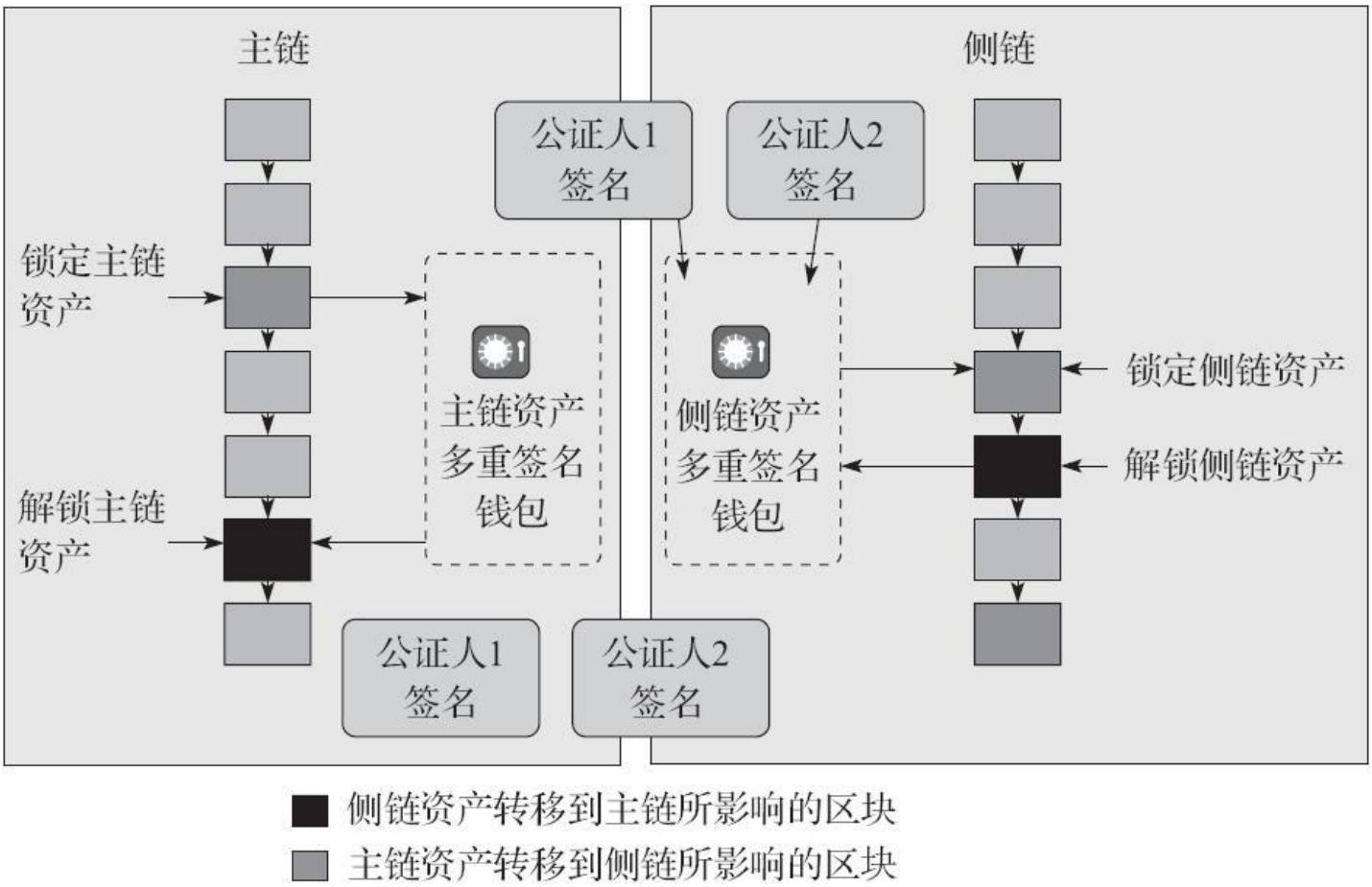
双向楔入是指将主链上的资产以一个固定的或者是确定的汇率在侧链间转入或输出的机制。它的核心机制其实是将一条链上的部分资产锁定，在侧链上生成或者是解锁一部分等价的资产。

双向楔入方式是需要主链与侧链都支持简单支付验证证明（Simplified Payment Verification proof，SPV），双方资产的转移是通过生成锁定的SPV输出来实现的，基于SPV协议的流程图如下。



2.联合楔入

另一种常被提及的楔入方式是联合楔入，它的机制类似于比特币多重签名，链上的资产转移到一个由多方公证人控制的多重签名地址，并由多方的控制权来锁定资产，进行资产的转移，其动作原理如下图所示。



[1] 引用自www.blockstream.com。

附录1　比特币：一种点对点的电子现金系统

中本聪　著

李志阔（网名：面神护法）　赵海涛　焦锋　译

satoshin@gmx.com

www.bitcoin.org

摘要

完全点对点的电子现金系统可以不通过金融机构，由一方直接发送在线支付给另一方。虽然数字签名为此提供了大部分解决方案，但是如果这个系统（电子现金系统）仍然需要可信的第三方来阻止双重花费（Double-Spending），那么它的价值就会大打折扣。本文提出了一种使用点对点网络的解决方案来应对双重花费。该（电子现金）网络通过对交易信息进行哈希运算，并将计算出的哈希值记录到一个不断延长的基于哈希运算工作量证明的链条上，从而为交易打上时间戳。除非重新完成工作量证明，否则链条上记录的信息不可被更改。最长的链条不仅可以证明（交易）事件发生序列，也可以证明该序列来自最大的CPU算力池。只要掌握大多数CPU算力的节点没有联合起来攻击网络，它们就将生成超过攻击者的最长的链。整个网络采用最简结构，信息得到了最大限度的广播，节点认同最长的工作量证明链条，可以随时离开和重新加入网络。

引言

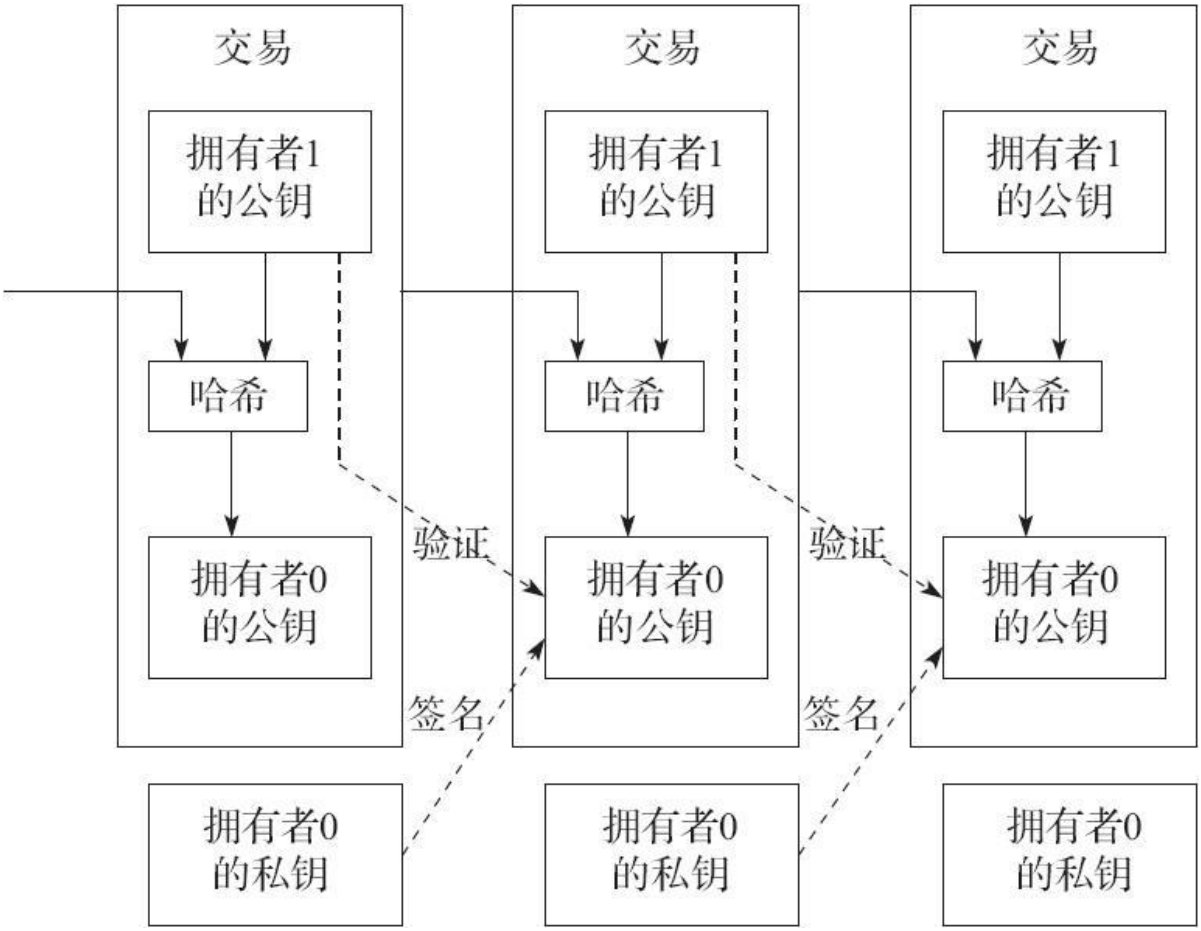
迄今为止，互联网上的贸易所涉及的电子支付几乎都需要金融机构作为可信的第三方来处理。尽管对绝大多数交易来说，这个系统的表现足够良好，但这种基于信用的模式（Trust Based Model）天生具有一些弱点。（提供信任的）金融机构不可避免地要调解争议，这导致无法实现完全不可逆的交易。调解成本增加了交易成本，限制了实际可行的最小交易额度，也减少了小额非正式交易发生的可能。有些服务是无法收回的，无法为这些服务提供不可逆支付的技术手段会（给我们）带来更多的成本。支付回滚的可能性增加了人们对信用的需求，（这导致）商家必须对他们的顾客保持谨慎，索取顾客更多的个人信息。尽管如此，商家仍然会将一定比例的（支付）欺诈列入不可避免的经营成本。虽然使用现金面对面交易可以避免这种成本以及支付过程的不确定性，但是目前在不需要可信第三方的前提下，还没有通过通信信道来完成支付的机制。

我们需要一个基于密码学验证而不是基于信任的电子支付系统，可以允许任意双方直接进行交易而不需要借助可信的第三方。如果交易回滚在计算上不可实现，就可以保护卖家免于支付欺诈，在此机制下，也很容易通过常规的第三方担保机制来保护买家利益。本文中，我们提出一种解决双重花费问题的方案：使用点对点的分布式时间戳服务，对发生的交易按时间顺序生成计算证明。只要由诚实节点控制的CPU算力总和大于由有合作关系的攻击节点控制的CPU算力总和，这个系统就是安全的。

交易

我们将电子货币定义为一串由数字签名组成的链条。每一位电子货币的所有者通过下面的方式将它转移给下一位所有者：对前一个交易和下一位所有者的公钥签署一个数字签名，并将这个签名附加在交易的末尾。收款人通过验证签名，就可以验证电子货币的所有者链条。

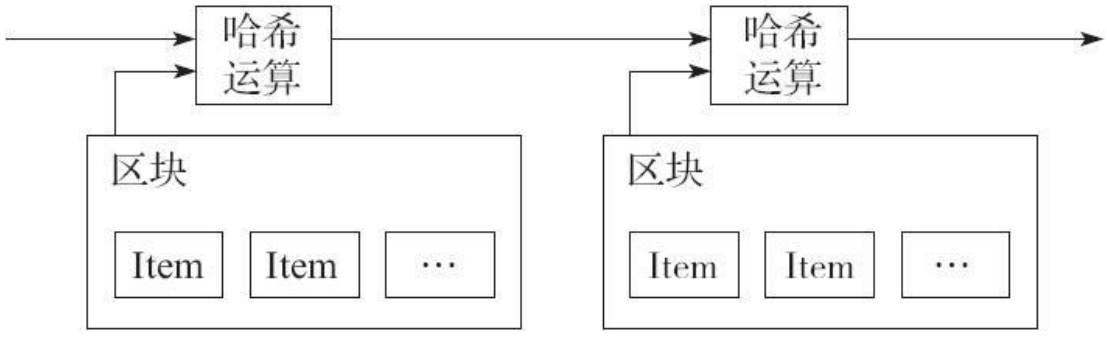
容易看出，通过这样的支付方式，收款人并不能确认链条上的某位所有者有没有进行过双重花费。对此最常见的解决方法是引入一个可信的第三方权威，以承担类似于“铸币厂”的职能：它会检验每一笔交易，以阻止双重花费的出现。每一笔交易完成之后，交易涉及的电子货币就必须回到“铸币厂”（销毁），同时发行等量的新币，只有“铸币厂”直接发行的新币才被相信不曾进行双重花费。这种解决方案的问题在于，整个货币系统的命运取决于运行“铸币厂”的公司，每一笔交易必须通过它们检验，就像经过银行检验一样。



还需要一种方法：让收款人可以知道前一位所有者没有签署过任何更早的交易（没有双重花费过）。为实现这个目标，我们只需要关注本交易之前发生的交易，而不需要关心之后的交易是否试图进行双重花费。只有知晓之前发生的所有交易，才能确认历史中的交易记录没有缺失。在基于铸币厂的模式中，铸币厂知晓所有的交易，决定哪一笔交易更早发生。为了在没有可信第三方的条件下实现这一点，交易必须被公开宣布（Publicly Announced）[1]，同时我们也需要这样的一个系统，所有参与者对他们接收到的交易的历史顺序能达成共识。收款人需要获得这样的证明：大部分节点都同意，在时间顺序上（链条上的）每一笔交易都是首次出现的。

时间戳服务器

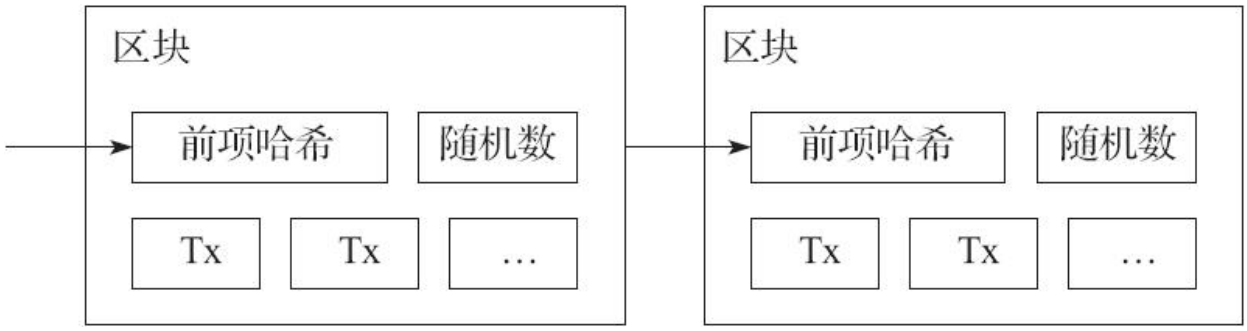
我们提出的解决方案始于时间戳服务器（Timestamp Server）。时间戳服务器通过对交易事件组成的区块进行哈希运算，从而为区块打上时间戳，并像通过报纸或者Usenet发帖一样，广播该哈希值 [2] [3] [4] [5]。通过获得哈希值的顺序，时间戳能证明特定数据在特定时间下是存在的。每个时间戳应当将前一个时间戳纳入其随机哈希值中，每一个随后的时间戳都对之前的一个时间戳进行增强，从而形成了一个链条。



工作量证明

为了在点对点的基础上构建分布式的时间戳服务，我们需要类似亚当·贝克（Adam Back）的哈希现金[6]的工作量证明系统，而不是报纸或者Usenet新闻组。在进行哈希运算时，工作量证明引入了对特定结果的哈希值的搜索，比如在SHA-256下，哈希值要求以一定数量的零开始。随着被要求的零的数目的变化，完成哈希运算的平均工作量数目是呈指数级变化的。通过简单的一次哈希运算就可以验证整个工作是否合格。

时间戳网络完成工作量证明的过程是：在区块中增加一项随机数，（变换该随机数）直到找到一个值，使区块的哈希值出现被要求数目的零。一旦CPU通过运算，完成了工作量证明，那么除非重新完成相当的工作量，这个区块就不能再被更改。之后随着新的区块被连接在该区块后面，改变这个区块所要完成的工作量也将包含重新计算所有新区块所需要的工作量。



工作量证明在少数服从多数时，解决了如何决定谁来代表多数的问题。如果“多数”是基于一个IP一票选出的，那么任何可以分配很多IP地址的人都可以破坏这个投票过程。而工作量证明在本质上是一个CPU投一票，最长链包含了最大的工作量证明投入，即为大多数决定的体现。如果大多数CPU算力被控制在诚实节点手中，诚实链条将延长地最快，超过所有的竞争性链条。想要改变一个过去的区块，攻击者必须重新完成该区块以及之后的所有区块的工作量证明，然后才能赶上和超过诚实节点的工作。

为了平衡硬件计算速度的提高和节点参与网络的兴趣的变化（造成的全网算力的起伏），工作量证明的难度通过一个变化的平均值来调整，其目标是每小时总是产生平均数量的区块。如果区块生成的速度太快，难度就会上升。

网络

运行该网络的步骤如下：

1）新交易向全网进行广播；

2）每个节点将接收到的新交易信息纳入一个区块；

3）每个节点为自己的区块寻找指定难度的工作量证明；

4）当一个节点找到了（要求的）工作量证明，它就将这个区块向全网广播；

5）只有当这个区块包含的所有交易都是合法的且之前不曾进行消费，其他节点才会接受这个区块；

6）其他节点表示接受这个区块的方法是：使用这个被接受的区块的哈希为前导哈希，在这个区块的基础上创造下一个区块。

节点总是认为最长链就是正确的链条，并持续在它的基础上工作以延长它。如果两个节点同时广播了不同版本的新区块，其他节点可能会首先接收到其中一个。在这种情况下，他们会在首先接收到的区块之上开始工作，但是也会保留另一个区块，以防另一个链条会变成最长链。当一个区块的工作量证明被找到，其中一个分支变得更长时，这种平行状态才会被打破；在另一条分支上计算的节点将会切换到更长的链上来。

新交易的广播不必到达每一个节点。只要到达了一定量的节点，它们在不久之后就会被打包进一个区块中。区块广播同样也可以耐受信息的丢失。如果一个节点没有接收到某区块，那么它在接收到下一个区块时会发现自己丢失了区块，并请求下载丢失

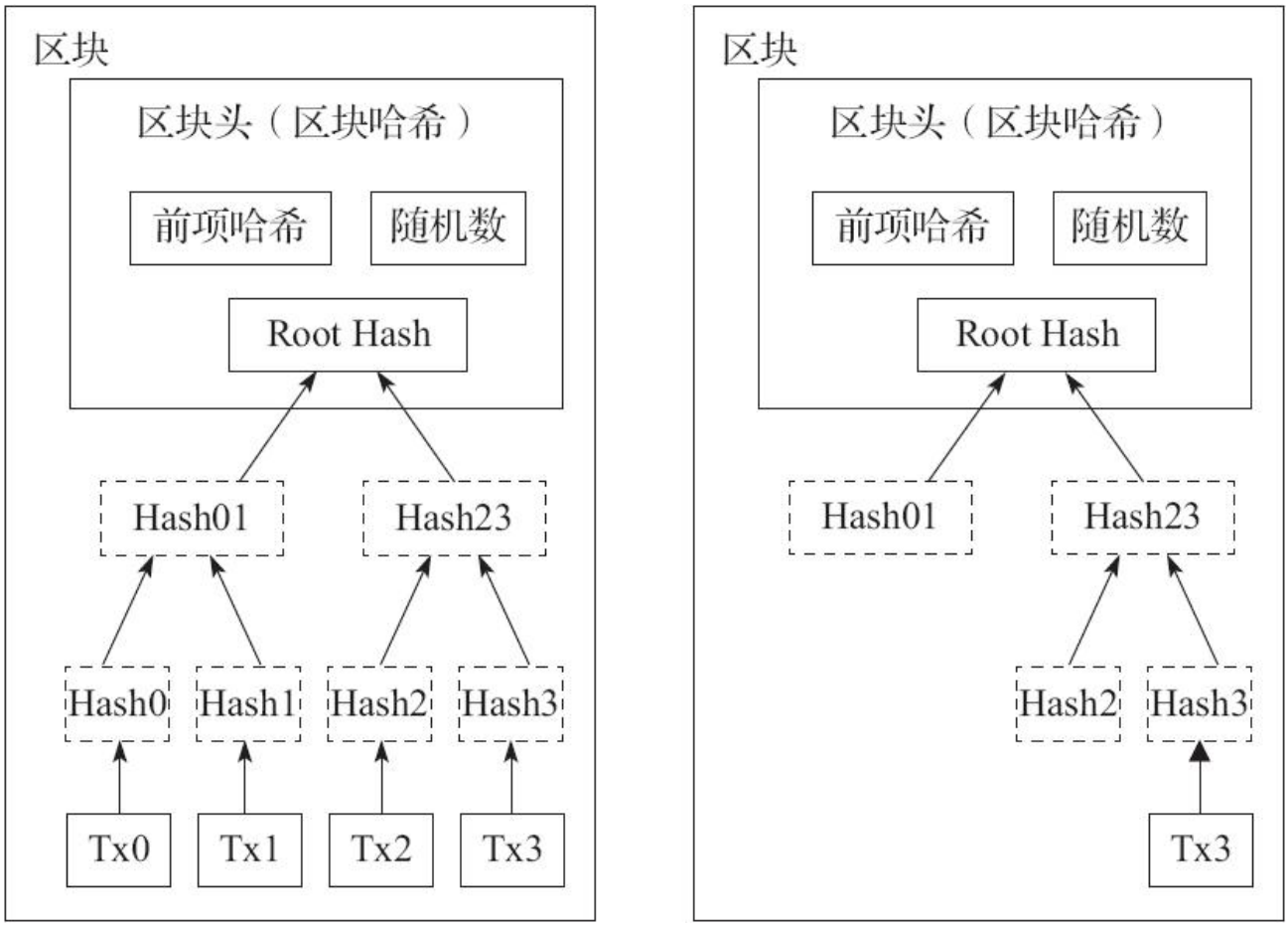
的区块。

激励

我们约定，区块里的第一笔交易是一笔特殊交易，该交易产生由区块创造者拥有的新币，这增加了对节点支持网络的激励。由于并没有中央权威来负责币的发行，这种激励方式也提供了在流通中，电子货币最初分布的分配方案。稳定的新币固定数量的增加类似于金矿消耗资源（挖矿）并将黄金添加到流通领域中。在我们的方案中，所消耗的资源是CPU时间和电力。

激励的另一个来源是交易费（Transaction Fee）。如果交易的输出值小于交易的输入值，它们的差值就是交易费。交易费被添加到包含该交易的区块的奖励内。一旦数量被设定的币（2100万）完全进入流通，激励来源就可以完全转化为交易费，整个电子货币系统会实现完全的零通胀。

激励机制有助于鼓励节点保持诚实。如果一个贪婪的攻击者能够控制比所有诚实节点更多的CPU算力，他将面临选择：是将已经付出的花费通过攻击拿回来，还是使用自己的算力诚实地工作以生成新币。他应该能发现，按照规则行事是更有利可图的，这些规则会使他获得比其他人更多的新币，而不是破坏整个系统，降低自己财富的有效性。



回收硬盘空间

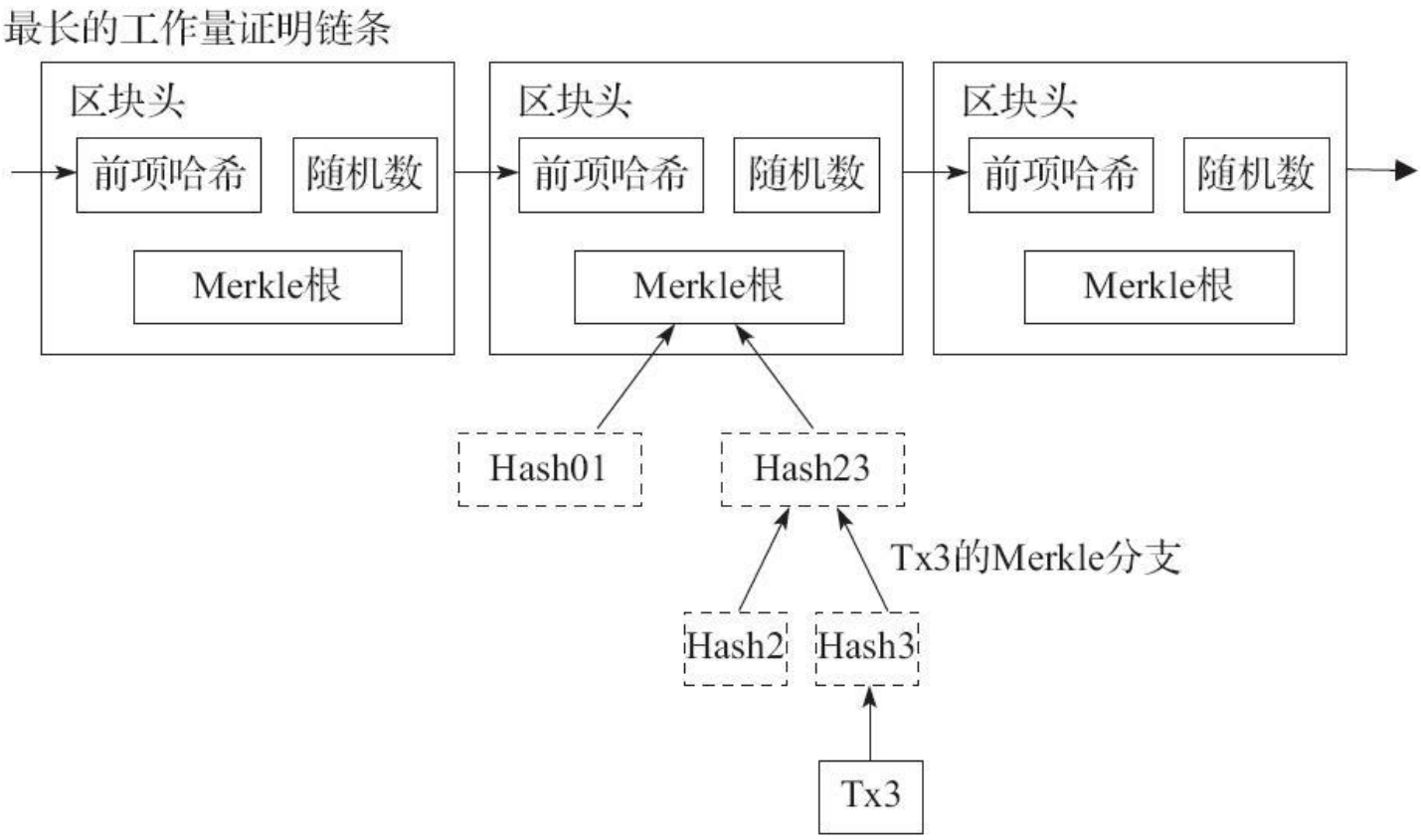
一旦最近的交易被纳入足够多的区块之中，就可以丢弃它之前的交易数据，以节省硬盘空间。为实现这一点同时又不损害区块的哈希数据，交易信息在哈希运算时，被构建成一种Merkle树 [7] 的形态，只有Merkle根被包含在区块哈希之中。通过将该树的分支清除，就能将老区块压缩。内部的哈希值是不必保存的。

不包含交易信息的区块头大小约为80字节。如果我们假设区块每十分钟生成一个区块，那么一年产生的区块头数据为4.2MB（80字节*6*24*365=4.2MB）。2008年常见的计算机操作系统的内存为2GB，摩尔定律预测，计算机内存每年的增长约为1.2GB。因此，即便区块头必须被保存在内存中，存储也不会成为一个问题。

简化支付确认

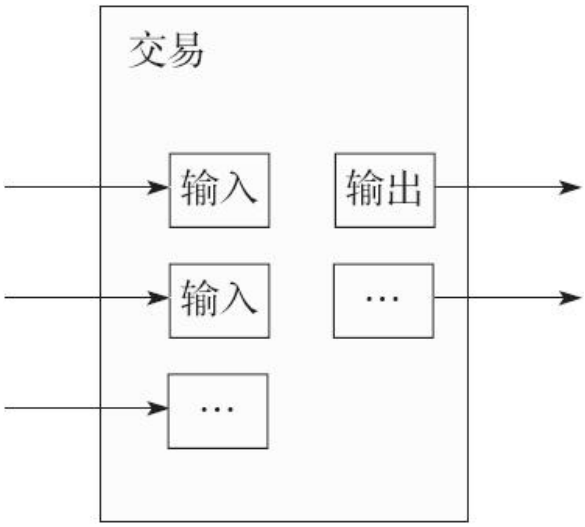
在不运行全网络节点的情况下，确认支付也是可能的。通过不停地向网络节点发起询问，用户可以确认最长的链条，只要保存最长的工作量证明链条的区块头数据副本，并且获得将待确认交易连接到相应区块的Merkle树分支，而尽管用户自身无法确认交易，但是通过将交易连接在链条的某个位置，就可以看到网络节点接受了这个交易，并且随着这个交易之后区块的累加，他能进一步确认网络接受了这个交易。

只要诚实节点控制着网络，这种确认方式就是有效的，但是当网络被攻击者控制时，这种方法就变得脆弱。全功能网络节点可以自行确认交易，如果攻击者控制网络，简化的交易确认方法就可能被攻击者编造的交易欺骗。对抗这种情况的一种策略是，可以从全功能网络节点处收听它们发现无效区块时发出的警告信息，鼓励用户去下载被警告区块和交易的完整信息，以明确不一致是否发生。接受频繁支付的商业机构可能仍会希望运行自己的节点，以达到更独立的安全性和更快的确认。



价值的组合与分割

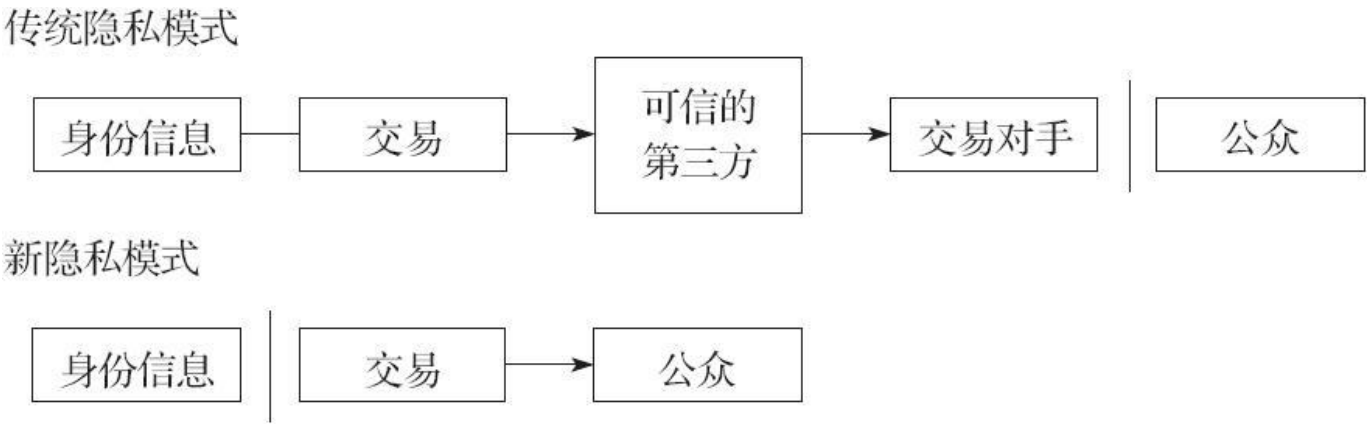
尽管逐一地对电子货币进行处理也是可能的，但是为转移中的每一分钱做独立的交易显然不明智。为了允许价值的组合与分割，交易可以包含多个输入与输出。通常，要么是由前面的较大的交易构成单一的输入，要么是由前面的几次小额交易合并为并行输入。输出最多有两类，一类用于支付；而如果存在找零，另一类输出则是返回给支付者的找零。



需要指出的是，当一笔交易会依赖之前的多笔交易，而被依赖的这些交易又会依赖更多之前的交易时，不会产生任何问题。因为这个机制永远不用去提取交易历史完全的独立副本。

隐私

传统的银行模式通过可信的第三方和限制获取相关当事方的信息，实现一定程度的隐私性。而将所有交易公开宣布的必要性排除了上述方法实现的可能。但是在这一过程中还是可以获得隐私性的：保持公钥的匿名性。公众可以看到一些人将一些钱送给了另一些人，但是却没有信息表示这些交易与哪些人有联系。这与股票交易所发布信息的隐私性是类似的，被公布的信息包括股票交易的时间与大小，“交易”是记录在案且可查询的，却没有表明交易者的身份信息。



作为一个额外的预防措施，每次交易应该使用新的密钥对，以确保密钥对不会与某个使用者联系起来。但是由于并行输入的存在，一些联系的发生依然是不可避免的，因为并行输入会告诉别人这些币属于同一个所有者。其中的风险在于，如果一个秘钥的所有者被泄露了，属于同一个所有者的其他交易也可能被泄露。

计算

设想如下场景：一个攻击者试图生成一条具有替代性的链，这条链的延长速度比诚实链的延长速度更快。即便这一目的达成了，也不意味着系统可以任攻击者为所欲为，比如凭空制造币或者拿走从来不属于他的币。节点不会接受一个无效的交易，而诚实节点永远不会接受包含无效交易的区块。攻击者唯一能尝试的是：改变一笔自己的交易，并尝试把钱从他最近的花费中拿回来。

诚实链和攻击链之间的竞赛具有二项随机漫步的特点。成功事件意味着诚实链延长了一个区块，领先+1；失败事件则意味着攻击链延长了一个区块，差距-1。

攻击者成功填补某一既定差距的概率类似于赌徒破产问题。假定一个赌徒拥有无限的透支信用，然后开始进行潜在次数为无穷的赌博，以试图填补自己的亏空，那么我们可以计算他补上亏空的概率，也就是该攻击链赶上诚实链的概率，如下所示[8]：

$$p = \text{诚实节点制造出下一个区块的概率}$$
$$q = \text{攻击者制造出下一个区块的概率}$$
$$q_z = \text{攻击者最终消弭了}z\text{个区块的落后差距}$$

$$q_z = \begin{cases} 1, & p \leqslant q \\ \left(\frac{q}{p}\right)^z, & p > q \end{cases}$$

假定p>q，那么攻击成功的概率就随着攻击者要追上的区块数的增长而呈现指数下降。概率是攻击者的敌人，如果他最开始不能获得幸运的突破，那么随着他落后的越多，他成功的机会就会变得无限渺茫。

现在考虑一下，一个新交易的收款人需要等到多长时间，才能足够确信发款人已经不可能改变这笔交易了。假设付款人是一个攻击者，他希望收款人相信他已经付过款了，然后过一段时间将已支付的款项重新发回给自己。付款人希望就算届时收款人会察觉这一点，也已经于事无补。

对此，收款人生成一个新的密钥对，然后在交易签署前不久将公钥发送给付款人。这可以防止付款人预先准备好一个链，然后持续地对此区块进行运算，直到他的链幸运地超越了诚实链，然后立即执行支付。在此情形下，只要交易一发出，攻击者就开始悄悄地准备一条包含了该交易替代版本的平行链条。

收款人将等待交易出现在首个区块中，然后等到z个区块连接在其后。此时，他仍然不能确切地知道攻击者已经进展了多少个区块，但是假设诚实区块产生一个区块将耗费平均预期时间，那么攻击者的潜在进展就是一个泊松分布，分布的期望为

$$\lambda = z\frac{q}{p}$$

在此情形下，为了计算攻击者追赶上的概率，将攻击者取得进展区块数量的泊松分布的概率密度乘以在该数量下攻击者依然能够追赶上的概率。

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{(z-k)}, & k \leqslant z \\ 1, & k > z \end{cases}$$

将其简化为如下形式，避免对无限数列求和：

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

转化为C语言代码[9]：

```
#include double attackersuccessprobability(
double q,
 int z)
```

```
{
    double p = 1.0 - q;

    double lambda = z * (
q / p);

    double sum = 1.0;

    int i,
 k;

    for (
k = 0;
 k <= z;
 k++)

    {
        double poisson = exp(
-lambda);

        for (
i = 1;
 i <= k;
 i++)

            poisson *= lambda / i;

            sum -= poisson * (
1 - pow(
q / p,
 z - k));

    }
    return sum;

}
```

对其进行运算，可以得到如下的概率结果，发现概率对z值呈指数下降。

当q=0.1时

z=0　p=1.0000000

z=1　p=0.2045873

z=2　p=0.0509779

z=3　p=0.0131722

z=4　p=0.0034552

z=5　p=0.0009137

z=6　p=0.0002428

z=7　p=0.0000647

z=8　p=0.0000173

z=9　p=0.0000046

z=10　p=0.0000012

当q=0.3时

z=0　p=1.0000000

z=5　p=0.1773523

z=10　p=0.0416605

z=15　p=0.0101008

z=20　p=0.0024804

z=25　p=0.0006132

z=30　p=0.0001522

z=35　p=0.0000379

z=40　p=0.0000095

z=45　p=0.0000024

z=50　p=0.0000006

求解令p<0.1%的z值，具体如下。

为使p<0.001，则

q=0.10　z=5

q=0.15　z=8

q=0.20　z=11

q=0.25　z=15

q=0.30　z=24

q=0.35　z=41

q=0.40　z=89

q=0.45　z=340

结论

我们在此提出了一种不依赖信任的电子交易系统。首先讨论了源自数字签名的常见的电子货币框架，这种架构提供了强有力的所有权控制，但是不足以防止双重花费。为了解决这个问题，我们提出了一种采用工作量证明机制的点对点网络，以记录公开的历史交易信息。只要诚实的节点能够控制大多数的CPU计算能力，就能使攻击者在事实上难以改变这些交易记录。该网络的强健之处在于它简洁的非结构化设计。节点之间的工作大部分是相互独立的，只需要很少的协作。由于信息只需要最大努力地传播自身，而无任何特定的流动路径要求，所以节点不需要验证身份。节点可以随时离开网络或加入网络，只需要下载工作量证明链条，并将其作为节点离开网络的时间内系统所发生的事件的证明。节点通过自己的CPU算力进行投票，以延长合法区块的链条反映对合法区块的接受，或以拒绝在无效区块之后延长链条反映对无效区块的拒绝。

在这个共识机制里面，所需的任何规则和激励措施都可以用本共识机制来执行。

[1] 戴伟，a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help，引自于http://www.weidai.com/bmoney.txt, 1998。

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, Design of a secure timestamping service with minimal trust requirements,, In 20th Symposium on Information Theory in the Benelux, May 1999。

[3] S. Haber, W.S. Stornetta, How to timestamp a digital document, In Journal of Cryptology, vol 3, No.2, p 99-111, 1991。

[4] D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital timestamping, In Sequences II: Methods in Communication, Security and Computer Science, p 329-334, 1993。

[5] S. Haber, W.S. Stornetta, Secure names for bit-strings, In Proceedings of the 4th ACM Conference on Computer and Communications Security, p 28-35,April 1997. on Computer and Communications Security, p 28-35, April 1997。

[6] A. Back, Hashcash–a denial of service counter-measure，引用自http://www.hashcash.org/papers/hashcash.pdf, 2002。

[7] R.C. Merkle, Protocols for public key cryptosystems, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, P 122-133,April 1980.

[8] W. Feller, An introduction to probability theory and its applications, 1957。

[9] 引用自https://bitcoin.org/bitcoin.pdf。

附录2　以太坊：下一代智能合约和去中心化应用平台（选译）

以太坊基金会　著

李志阔（网名：面神护法）　赵海涛　焦锋　译

中本聪2009年发明的比特币经常被视作货币和通货领域内一次激进的发展，这种激进首先表现为一种没有资产担保或内生价值[1]，也没有中央发行者或控制者的数字资产。然而，在比特币这场实验里面，更重要的创新可能是其底层作为分布式共识实现机制的区块链技术，它一出现，便迅速吸引了人们的注意力。常常被人们提及的区块链技术的其他应用包括使用链上数字资产来代表定制货币和金融工具（彩色币[2]），某种基础物理硬件的所有权（智能资产[3]），如域名一样的没有可替代性的资产（域名币[4]），更复杂的应用包括数字资产直接被一段可以执行任意条款的代码控制（智能合约[5]），甚至还有基于区块链的“去中心化自治组织”（DAOs[6]）。以太坊的目标就是提供一个内置成熟的图灵完备语言的区块链，用这种语言可以创建“合约”，编码任意状态转换功能。以太坊将允许用户通过简单的几行代码实现逻辑，创建上面提到的所有系统，以及更多的我们尚未想到的新系统。

以太坊

以太坊的目标是创建一个可实现去中心化应用的替代性协议，并提供一种不同的权衡模式，这在很多去中心化应用的实践中是非常有用的。我们特别强调，时间快速发展的状态、简单稀有应用的安全性、不同应用有效地相互作用的能力都是很重要的。以太坊通过图灵完备编程语言的区块链来实现这一点。以太坊允许任何人编写智能合约和去中心化的应用，并允许在其中自定义所有权规则、交易格式和状态转换函数。要使用以太坊，对于一个准域名币的系统，只需要两行代码就可以完成，而其他的诸如货币和信誉系统，也可以用不到二十行代码完成。智能合约（包含价值且只有达成某些条件时才能打开的加密“箱子”）也可以在以太坊平台上创建，由于增加了图灵完备性（Turing-Completeness）、价值知晓（Value-Awareness）、区块链知晓（Blockchain-Awareness）和状态（State）等特点，以太坊所能提供的智能合约比比特币脚本提供的（智能合约）功能强大得多。

以太坊账户

在以太坊系统中，状态是由被称为“账户”（每个账户有一个20字节的地址）的对象和在两个账户之间转移价值与信息的状态转换构成的。以太坊的账户包含4个部分：

1）随机数，用于确定一笔交易只能被处理一次的计数器。

2）账户目前的以太币余额。

3）账户的合约代码（如果有的话）。

4）账户的存储（默认为空）。

以太币（Ether）是以太坊内部的主要加密燃料（Crypto-Fuel），用于支付交易费用。一般来说，以太坊有两种类型的账户：外部所有者账户（由私钥控制）和合约账户（由合约代码控制）。外部所有者账户没有代码，人们可以通过创建和签署一笔交易而从一个外部所有者账户发送消息；每当合约账户收到一条可以激活其内部代码的消息，就会允许它对内部存储进行读写，发送其他消息或者创建新的相应合约。

注意，以太坊中使用的“合约”不应该被看作某些应该被“完成”或者“遵守”的东西，它们更像是生活在以太坊执行环境内部的“自动代理人”，当被某条消息或者交易“拨动”时，他们总是执行某个特定的代码，对以太币余额和秘钥/价值存储直接控制，对账户的变化持续追踪。

交易和消息

交易

以太坊中使用的“交易”是指从外部所有者的账户签发包含消息的数据包。交易包括：

·消息的接收者。

·验证发送者的签名。

·从发送者到接收者转移的以太币的数量。

·一个可选的数据区。

·一个STARTGAS值，代表交易执行过程中被允许的计算步骤的最大值。

·一个GASPRICE值，发送者为每一步计算支付的费用。

前三步在任何加密货币体系中都是可预期的标准步骤。可选的数据区目前并没有任何默认功能，但是有这样的操作码，即允许合约引用这里的数据。

在以太坊抵抗拒绝服务攻击的模式中，STARTGAS和GASPRICE字段是关键的部分。为了防止代码中出现计算浪费，乃至出现意外或者恶意定义的无限循环，每个交易被要求设定一个代码执行过程可以使用的计算步骤的上限。计算的基本单位是“瓦斯”（gas），通常一步计算消耗1gas，但是有些计算由于更加复杂，或者增加了作为状态的一部分而必需存储的数据量，会消耗更多的瓦斯。每一个字节的交易数据也会消耗5gas。费用系统的初衷在于要求攻击者为他们消耗的资源支付相应的代价，比如计算能力、带宽、存储等。因此会带来更多网络消耗的交易也要支付大致相应的交易费（瓦斯）。

消息

交易可以向其他合约发送“消息”，消息是虚拟的，永远不会序列化，只存在于以太坊执行环境中。一则消息包括：

·消息的发送者（隐式的）。

·消息的接收者。

·与消息同时传递的以太币的数量。

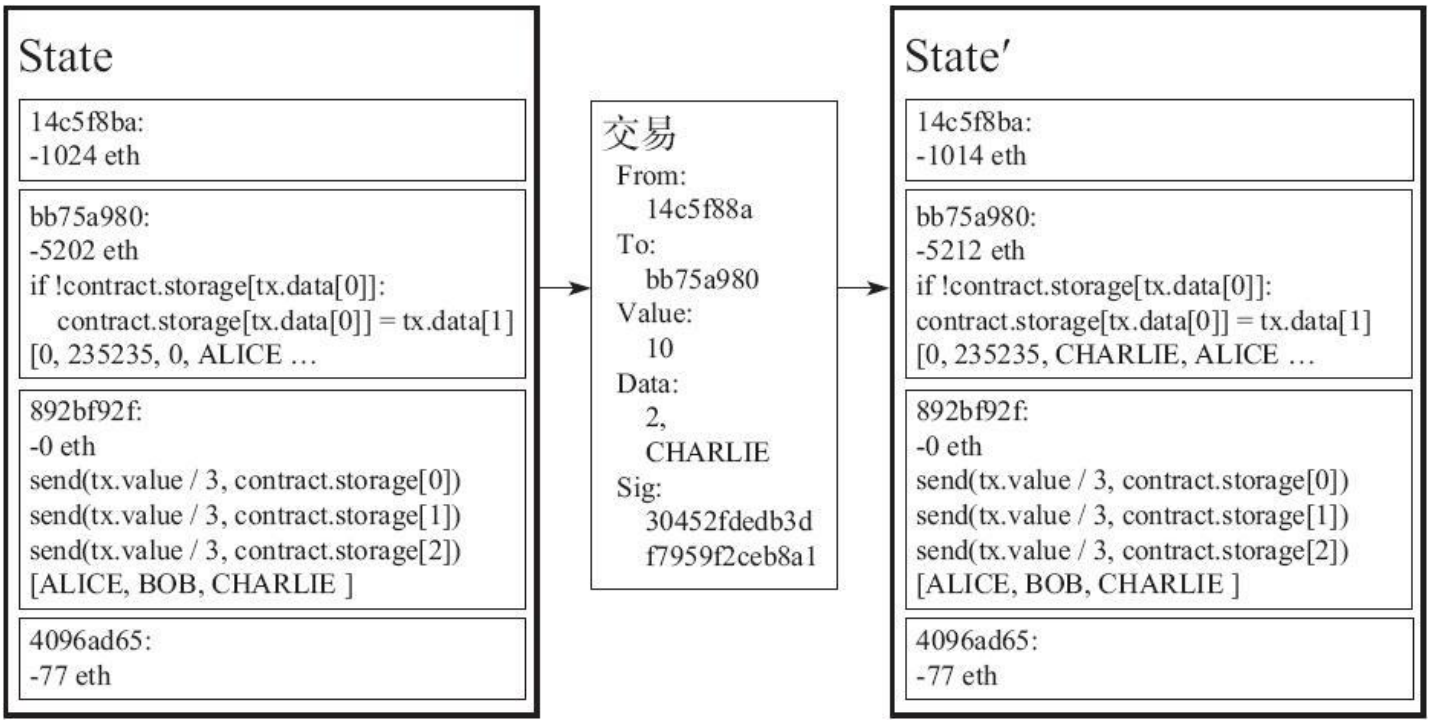
·一个可选的数据区。

·一个STARTGAS值。

基本上，除了消息是由一个合约而不是外部所有者账户发出之外，消息和交易类似。当一个合约执行“CALL”操作码的时候，消息产生，该操作码的功能就是生成和执行消息。像交易一样，消息可以使接受消息的合约执行自己的代码。因此合约可以和外部所有者的账户一样，与其他账户发生关系。

以太坊状态转换函数

以太坊的状态转换函数：APPLY（S，TX）->S'，可以定义如下：



1）检查交易格式是否正确（比如数值是否正确等）、签名是否有效、随机数是否与发送者账户的随机数匹配。如果不是，返回错误。

2）计算交易费用：fee=STARTGAS*GASPRICE，并从签名中确定发送者地址。从发送者的账户中减去交易费用，增加发送者的随机数。如果账户余额不足，返回错误。

3）初始值GAS=STARTGAS，按交易中的字节数减去一定量的瓦斯值。

4）将交易价值从发送者的账户转移到接收者账户。如果接收账户还不存在，则创建此账户。如果接收账户是一个合约，则运行该合约的代码，直到代码运行结束或者瓦斯用完。

5）如果因为发送者账户没有足够的钱或者代码执行耗尽瓦斯，从而导致价值转移失败，则恢复除了交易费之外的初始状态，交易费送至矿工账户。

6）如果没有失败，则将所有剩余的瓦斯归还给发送者，消耗掉的瓦斯作为交易费用发送给矿工。

例如，假设合约代码如下：

```
if !
self.storage[calldataload(
0)
]:
    self.storage[calldataload(
0)
] = calldataload(
32)
```

需要注意的是，在现实中，合约代码是用底层以太坊虚拟机（EVM）代码写成的。而为了清楚起见，上面的合约用的是高级语言Serpent语言写成的，它可以被编译成EVM代码。假设合约存储器在开始时是空的，交易发送值为10以太，瓦斯数为2000，瓦斯价格为0.001以太，整个数据大小为64字节。0~31字节代表号码2，32~63字节代表字符串CHARLIE。交易发送后，状态转换函数的处理过程如下。

1）检查交易是否有效、格式是否正确。

2）检查交易发送者是否至少有2000×0.001=2个以太币。如果有，从账户中减去2个以太币。

3）初始设定gas=2000，假设交易长为170字节，每字节的费用是5，减去850，所以还剩1150。

4）从发送者账户减去10个以太币，为合约账户增加10个以太币。

5）运行代码。在此案例中，运行代码很简单：它检查合约存储索引为2的位置是否已被使用，如果未被使用，将其值设为CHARLIE。假设这消耗187gas，于是剩余瓦斯为1150-187=963gas。

6）向发送者的账户增加963×0.001=0.963个以太币，返回最终状态。

如果交易的接收端没有任何合约，那么所有的交易费用就等于GASPRICE乘以交易的字节长度，与交易同时传递的消息数据与交易费用无关。

代码执行

以太坊合约使用的代码是低级的基于堆栈的字节码语言，被称为“以太坊虚拟机代码”或者“EVM代码”。代码由一系列的字节构成，每一字节代表一项操作。一般而言，代码执行的是重复操作构成的无限循环，程序计数器（初始值为零）随着每一次执行加1，直到代码执行完毕或者遇到错误，或者发现STOP/RETURN指令。操作可以访问3种存储数据的空间：

1）堆栈，一种后进先出的数据存储。

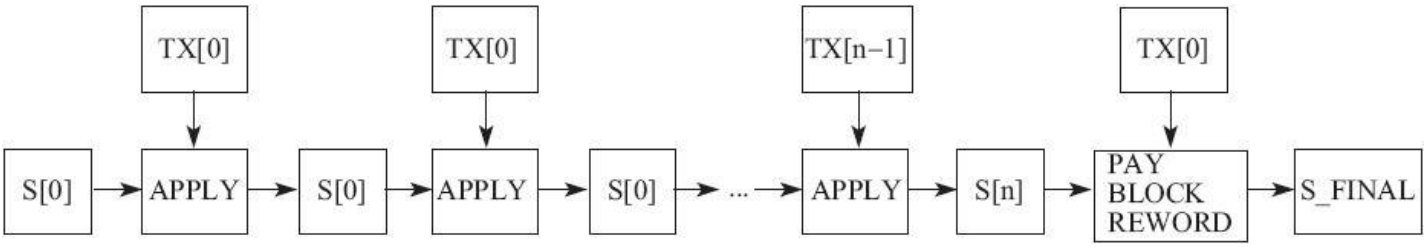
2）内存，可无限扩展的字节队列。

3）合约的长期存储，一个秘钥/数值的存储，不像计算结束后将重置的堆栈和内存，该空间的存储内容将长期保持。

代码可以像访问区块头数据一样，访问数值、发送者和接收到的消息数据，代码还可以返回数据的字节队列作为输出。

EVM代码的正式执行模型惊人的得简单。当以太坊虚拟机运行的时候，它的完整计算状态可以由元组（block_state，transaction，message，code，memory，stack，pc，gas）来定义，这里的block_state是包含所有账户余额和存储的全局状态。每轮执行开始时，通过调出代码的第pc（程序计数器）个字节，找到当前指令。在如何影响元组上，每个指令都有自己的定义。例如，ADD使两个元素出栈并将它们的和入栈，将gas减1并使pc加1，SSTORE使顶部的两个元素出栈并将第二个元素插入由第一个元素定义的合约存储位置，同样减少最多200的瓦斯值并将pc加1，虽然通过即时编译，有许多方法可以优化以太坊虚拟机的执行，但以太坊的基本功能可以用几百行代码来实现。

区块链和挖矿



虽然有一些不同，但以太坊的区块链在很多方面类似于比特币区块链。它们的区块链架构的主要不同在于，以太坊区块不仅包含交易记录还包括最近的状态，除此之外，以太坊区块链还包含区块序号和难度值。以太坊中的基本的区块确认算法如下：

1）检查区块引用的上一个区块是否存在和有效。

2）检查区块的时间戳是否大于引用的上一个区块，而且小于当前时间之后的15min。

3）检查区块序号、难度值、交易根，叔根和瓦斯限额（许多以太坊特有的底层概念）是否有效。

4）检查区块的工作量证明是否有效。

5）将S[0]作为上一个区块结束时的状态。

6）将TX作为区块的交易列表，设有n笔交易。对于属于0~n-1之间的任意一笔交易i，令S[i+1]=APPLY（S[i]，TX[i]）。如果任何一个过程发生错误，或者程序执行到此处所花费的瓦斯超过了GASLIMIT，则返回错误。

7）用S[n]给S_FINAL赋值，向矿工支付区块奖励。

8）检查S_FINAL状态的Merkle根是否与区块头提供的状态根一致。如果是，区块有效，如果不是，区块无效。

乍看起来，这一确认方法的效率似乎很低，因为它需要存储每个区块的所有状态，但是事实上以太坊的确认效率可以不低于比特币。原因是状态存储在树结构中，每经过一个区块后，只需要改变树结构的一小部分。因此，一般而言，两个相邻的区块的树结构绝大部分是相同的，因此存储一次数据，可以利用指针（即子树哈希）引用两次。一种被称为“帕特里夏树”（Patricia Tree）的树结构可以实现这一点，其中包括对Merkle树概念的修改，不仅允许改变节点，而且还可以插入和删除节点。另外，因为所有的状态信息是最后一个区块的一部分，所以不用存储全部的区块历史——如果这一策略可以应用到比特币系统中，则可以提供5~20倍的空间节省。

一个经常被问及的问题是，在物理硬件层面上，合约代码在哪里执行。简单的回答是，合约代码的执行过程是状态转换函数定义的一部分，是区块确认算法的一部分，所以如果一笔交易被加入到区块B中，那么这个交易引发的代码执行将会在所有目前和将来会下载与验证区块B的节点中进行。

计算和图灵完备

很重要的一点是，以太坊虚拟机是图灵完备的，这意味着EVM代码可以完成人们能想到的所有计算，包括无限循环。EVM允许两种形式的循环：首先，有一个JUMP指令，允许程序跳回到代码前面的某处，而JUMP1指令则可以实现有条件的跳转，允许类似下面的语句：while x<27：x=x*2。其次，合约可以调用其他的合约，潜在地允许通过递归实现循环。这自然带来一个问题：恶意用户可以通过使矿工和全节点进入无限循环而令用户不得不关机吗？这个问题出现的原因是：一般意义上，我们没有办法预知一个程序是否会结束（计算机科学中的停机问题（Halting Problem））。

正如前面所述，解决方案是为每一个交易设定计算步骤的最大数量，如果执行超过设定的步骤，则将交易恢复成原状但仍要支付费用。消息发送以同样的方式工作。为显示这一方案背后的动机，考虑下面的例子：

·攻击者创建了一个运行无限循环的合约，然后发送一个激活该循环的交易给矿工，矿工将处理交易，运行无限循环直到瓦斯耗尽。尽管瓦斯耗尽，交易半途停止，但交易依然是正确的（返回原状），并且矿工依然从攻击者那里得到了每一步计算的费用。

·攻击者创建一个非常长的无限循环，试图令矿工长时间计算，在计算结束前，若干区块已经产生，于是矿工无法收录交易以赚取费用。然而，攻击者需要发布一个STARTGAS值以限制可执行步数，因而矿工将提前知道该计算将耗费过多的步数。

·为减少风险，一个金融合约靠提取9个专用数据发布的中值来工作，攻击者接管了其中一个数据发布器，然后按可变地址调用机制将其更改为运行一个无限循环，试图令任何使用此金融合约的尝试都因瓦斯耗尽而中止。然而，该金融合约可以在消息里设置瓦斯限制以防范此类问题。

此外，图灵不完备甚至不是一个大的限制，在我们设想的所有合约例子中，至今只有一个需要循环，而且这一个循环也可以被26个重复的单行代码段代替。既然图灵完备会带来很多潜在的麻烦并且益处有限，为什么不简单地使用一种图灵不完备语言呢？事实上图灵不完备并非一个简洁的问题解决方案。为什么？请考虑下面的合约：

C0：call（C1）call（C1）

C1：call（C2）call（C2）

C2：call（C3）call（C3）

...

C49：call（C50）call（C50）

C50：（运行程序中的每一个步骤并在存储中记录发生的变化）

现在，发送一个交易给A，这样，在51个交易中，我们有了一个需要花费250步计算的合约，矿工可能会尝试通过为每一个合约设置一个最高可执行步数，并且针对递归调用其他合约的合约计算可能执行的步数，从而预先检测出这样的逻辑炸弹，但是这会使矿工禁用可以创建其他合约的合约（因为上面26个合约的创建和执行可以很容易地放入一个单独合约内）。另外一个问题是消息的地址字段是一个变量，所以通常来讲，几乎无法预知一个合约将要调用哪一个合约。于是，最终我们得到一个令人惊诧的结论：对图灵完备协议的管理很容易，而除非有相当的控制措施，图灵不完备时的管理惊人得困难——那为什么不让协议图灵完备呢？

[1] 引用自http://bitcoinmagazine.com/8640/an-exploration-of-intrinsic-value-whatit-is-why-bitcoin-doesnt-have-it-and-why-bitcoin-does-have-it/。
[2] 引用自https://docs.google.com/a/buterin.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit。
[3] 引用自https://en.bitcoin.it/wiki/Smart_Property。
[4] 引用自http://namecoin.org/。
[5] 引用自http://szabo.best.vwh.net/smart_contracts_idea.html。
[6] 引用自http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomouscorporation-part-i/。

后记

对话作者：区块链离我们还有多远

随着区块链的热度不断上升，我在不同时间接受了不同人的采访。每一次的访谈，同时也让我对区块链有了更深的理解。以下几节内容是从我的这些访谈中整理出来的，希望能对大家有帮助。

1.区块链的婴儿时代

记者： 最近区块链很热，那火币区块链研究中心最近在做哪方面的研究，或者比较看好哪方面的应用？

张健： 我们现在主要做的是区块链基础理论的研究及基础设施的构建，虽然我们也在应用层面做一些尝试，但目前来说，应用或者说应用层还不是这个阶段最大的机会。就像真正的互联网在形成之前，网络还是割裂的，还没有达到大范围的互联互通，基础协议及设施也不健全，不具备产生大规模商业应用的机会。所以我们主要还是做一些基础层面的研究，并尝试跟各个行业一起做一些基础层面的研究。

记者： 那你觉得当前区块链会在金融领域产生哪方面的影响？

张健： 最近这个概念很热，但金融领域有这样一个特点——变化没那么快，而且在区块链基础设施真正成熟之前，对于传统金融业现有的基础设施的替代性还没有那么强，金融业还没有充足的理由去依赖这样一个技术。所以说，目前存在的核心阻碍在于，由于区块链基础设施不够成熟，它给金融业带来的价值还没有那么大。我的观点是，随着区块链技术的演进与发展，它对于金融业的真正价值是提供了一个更大的想象空间。区块链可以从本质上提升金融业的效率，创造新的价值连接和商业模式，这是一个更为宏大的未来，而不仅仅是改造或替代现有的系统。

目前区块链技术在金融业的应用还处在探索阶段。有影响力的应用还没有诞生，大部分都处于理论研究及内部测试阶段。比较有影响力的探索就是R3CEV的银行联盟，现在已经有40多家国际顶级银行加入，以测试银行间的清算、结算网络。

另外，纳斯达克首次利用区块链技术完成和纪录了一项私人证券交易。德勤在近期已完成区块链技术与爱尔兰银行的系统相关技术融合的验模、验证。你会发现这类的探索越来越多，但这些都还处在非常早期的概念验证阶段。所以说，就当前而言，或者从短期来看，区块链对金融领域的影响会很有限。

记者： 那你认为区块链现处于概念宣扬阶段吗？

张健： 是的。区块链技术目前还处于概念宣扬阶段。区块链目前能解决什么问题？有没有什么不可替代性？未来到底会怎样？如果我们不谈未来谈现在的话，你会发现没有或者很少。就像很多技术的早期一样，最典型的是2000年前后的互联网泡沫，泡沫破灭后，你会发现互联网其实没那么神奇，不过尔尔，甚至连自身的商业化都有难度。并且早期的互联网也远没有到能影响、渗透各行业的地步。不过真正伟大的互联网公司的种子，也是在那时种下的。

当一种技术还没有达到可以爆发大规模商业应用的时候，特别是基础设施和普及程度都还很不成熟的时候，若基于很多很好的概念，认为大时代马上要到来，其实是有点早了。对于未来的预期你认为现在就能实现，这就是一种过热。

2.区块链的创业机会

记者： 您认为现在的区块链还处于婴儿时期，那么在婴儿阶段，属于创业公司的机会有多少？

张健： 我认为在整个大的行业中，属于创业公司的机会非常多。对于一项技术，特别是颠覆性技术而言，我们容易形成的误判是，高估短期影响，低估长期影响。用同样的道理去看创业机会，我认为，早期的机会远没有我们想象中那么多，而中后

期的机会却会远远超出我们的想象。

虽然区块链技术是一个比较新的东西，但它不是一个点的突破，而是一个面的突破，或者说是一种连线的技术，本身并不复杂，同时也利用了现有互联网的技术基础。因此，它不是一个超脱互联网层面的东西，它仍然是在现有互联网基础上构建的层级。所以从这个角度来讲，在互联网方面有很深积累的公司，或者在IT领域非常有经验的公司具有天然的优势。举个例子来说，银行系统用的大都是IOE的设施，如果现在要用一个区块链系统，那么银行怎么可能会让一个创业公司来担此如此重要的开发角色？所以，从短期来说，区块链创业公司对各个行业的影响较弱，针对私有链的建设等，也很难构建出什么大的平台。

从中长期来看，我认为这是一个非常巨大的机会，而且这个机会一定是新一代的公司能把握的。

记者： 目前已经有一些创业公司即将或已开始专注于区块链方面的创业，那你觉得如果要在未来胜出，最重要的是什么？

张健： 我认为最重要的是把握住时机。对于未来你是否能够在一个恰当的时间点切入并把握住正好属于你这个时间点的机会，除了能力之外，这还需要判断力、勇气、坚持，以及不可或缺的运气。

2000年左右，国内有一家叫8848的电子商务公司，它是当年互联网公司的翘楚之一，拿到过几千万美金的投资，一度声势很大，但最终没有成功。导致其失败的一个非常重要的客观原因是，除了互联网之外，其他和你配套的关键基础设施都没有——没有成熟的支付体系和物流体系。在网上卖东西，但没有便捷可靠的支付渠道，也没有高效的配送体系，用户体验非常差，怎么能够把这个做起来？它的规划是没有问题的，错的是那个属于你的成功阶段还没有到来。解决办法是坚持到那个阶段，或者也可以凭一己之力把整个基础设施构建完，让这个阶段提前到来。但事实上，这种大规模的基础设施构建往往不是一家公司就可以搞定的。这就是这一类新生事物发展成熟的规律，它需要依赖整个社会协作系统的建立，远不止是技术突破的问题。

精确地抓住时机是非常难的。那么从早晚来分析的话，如果做早了，只要方向对，还有坚持到爆发的可能；但如果做晚了，基本上你就和这个机会无缘了。正如你现在再去创建门户网站、再去创造BAT这样的平台，是没有任何机会的。因为属于那个时代最好的创业机会已经一去不复返了。

记者： 有些公司在区块链应用上已有落地，那你觉得如果要建立壁垒，主要应从技术层面还是商业层面入手？

张健： 我认为一定是技术层面与商业层面结合。如果你只是纯粹的商业模式，而不考虑互联网技术特征的话，商业模式不可能给出什么壁垒，可复制性非常高。而如果你仅仅认为这是一个技术问题，很大可能是，你做出的东西并没有市场。

回到现在，虽然现在很多公司对外宣布他们已经在区块链实际应用中有了落地，但我认为区块链技术在未来的应用将会超出你的想象，它将会是一个非常神奇、能带来无数惊喜的东西。所以我认为，在如此早的阶段，从应用角度看，早一点切入还是晚一点切入，并不会产生太大的差距。关键是能否构建你的壁垒。

目前所谓的一些落地应用，其实还没有用到区块链真正的价值。因为还没有一个构建得非常好的区块链基础设施，各种各样的资产还不能在此基础设施上很好地运转，完成转换和交易。所以，我的观点是：离互联越远，它的作用就越小，可替代性就越强。在这种情况下，它的概念性东西可能就会多一些，实际应用就会少一些。

比如企业内部可以做一个区块链，用于内部清算，那这能算是区块链吗？我个人认为这不是区块链，因为你没有连任何东西，你只是在连你自己。正如同你不能说把自己家里的3台计算机连起来就是互联网。内部的区块链系统只能算是数据库——分布式数据库。

因此，从目前来看，在大量基础设施还没搭建完善的情况下，想要在区块链应用领域做出一番事业，难度还是非常大的。

3.区块链离我们还有多远

记者： 从区块链技术的诞生到大规模的应用，你觉得还需要多长的时间？

张健： 目前离区块链大规模应用还有很大的距离，基础设施不够成熟是目前的核心问题。加快基础设施的建设很有必要。当区块链的基础设施成熟到能够方便地将各种形式的价值连接起来、并能够自由地和高效地传输的时候，基于区块链的应用将会体现出强大的价值，这时候区块链将得到更快的推广。

这是一个符合市场规律的自然发展过程，无论我们现在对于区块链应用有多么热切的期望，它还是会按照事物发展的客观规律从小到大，经历从不成熟到成熟再到繁荣的过程。

我认为大规模的爆发在未来一定会发生，那时区块链会建立起真正的优势。但预测未来是很难的，如果一定要预测的话，可以类比互联网从诞生到发展再到繁荣的过程。区块链目前的发展阶段相当于20世纪90年代中期互联网所处的阶段。由于科技的发展和普及速度是加速状态，所以我相信这个时间一定比互联网经历的时间要短。

大家谈之《区块链大革命》

2016年5月初，火币在巴比特论坛发起了一个征文活动[1]——区块链第一书：#我眼中的中本聪和区块链#。活动内容中提到“有独到见解、质量优秀的作品将有机会入选本书，并收录在“大家谈”章节印刷出版。”

征文活动获得了踊跃的投稿，其中一篇“区块链大革命”脱颖而出，它以独到的见解及流畅的文风，获得了一致好评。故笔者收录此文于结语，以飨读者。

区块链大革命

文/魏然

一、互联网&金融、信息&信任

该怎么判断一个人所处的行业呢？主要看“气质”！这并不完全是句玩笑话。我的朋友大多在互联网、金融或互联网金融行业工作，仅从气质上感受一下，便可以发现两者的价值取向截然不同。“码农”的标配是T恤和拖鞋，而“金融民工”都是西装革履。

为什么会这样呢？

这得从金融的本质谈起：金融是人们跨越时间、空间对价值进行交换的活动，而价值交换的前提是“信息”和“信任”。最原始的交换是以物易物，比如用一头羊换一只鸡，可是供需很难直接匹配，于是人们开始寻找贝壳、金银等作为价值交换的载体。再后来，由于金银等物质携带起来不够安全方便，纸币及银行应运而生，虽然纸币本身没有价值，但由可靠的银行为其背书，一张薄薄的纸也成了价值的载体。到了互联网时代，连纸都变得可有可无了，支付简化成单纯的“记账”行为。用刷卡、支付宝或Apple pay时，我们并没有付出任何实物，只是云端账本里的数字发生了变化。由此可见，金融的演进遵循3个逻辑：①金融创新来源于商业和技术创新；②信息不对称、分散风险等因素促使金融中介产生，但其物理形态不断演变，最终可能被数字取代；③金融创新的目的是覆盖更多的交易主体，更好地满足他们的需求。

而互联网的本质又是什么呢？最初，它只是信息的搬运工，我们可以通过互联网迅速将信息复制到全世界，但无法解决价值转移的问题。互联网所依托的TCP/IP协议不能实现信息确权，这让资产的交换变得很困难。比如，大家可以在网上随意下载mp3格式的歌曲，这使得唱片业受到很大的冲击。在互联网上，若连一首歌曲的产权都无法得到保护，那更不用提涉及更大价值的其他金融资产的转移了。

现在回到最初的问题，为什么金融民工都会穿得西装革履，但互联网巨头马克·扎克伯格却仍然穿着T恤拖鞋呢？

金融民工穿西服和银行的楼盖得金碧辉煌的原理是一致的，因为需要增加客户对中心化机构的信任。如果人们不相信银行的偿付能力，可能就会发生挤兑，从而导致银行破产；如果政府没有公信力，法币便会贬值如废纸。这种基于对单点的信任而建立起来的信用共识，逼迫金融中介去维护高大上的形象。

同时，按照金融演进的逻辑，传统的金融中介来源于线下商业活动，最初依赖抵押物来做典当式的借贷，后来随着数据技术的发展，开始尝试无抵押的消费贷款。然而，这种依靠资产抵押和收入状况来评估信用的模式，使富人、大企业比穷人、初创企业更容易获得融资支持。金融长期以来是偏向高端客户的服务业，这也是金融民工打扮得光鲜亮丽的原因。

互联网企业为什么会涉足金融呢？因为线上商业场景出现，在主战场上做起金融自然得心应手。其突出优势在于可以依靠线上数据来低成本地做信用评估。阿里、京东掌握了线上商城的交易数据，可以廉价地为小商户和个人进行信用画像，降低了服务门槛，满足了中低端客户的长尾需求。这可能是互联网企业更亲民的原因所在。

按这种说法，互联网企业不端、不装又劫富济贫的罗宾汉形象跃然纸上。然而，业内的各种乱象却击碎了我们乌托邦式的幻梦。当我们无法掌控自己的信用数据，而监管又不够给力时，互联网企业也可能依靠强大的信息掠夺能力建立起新的垄断，或变成跑路的P2P平台和贩卖虚假信息的“恶人”。

由此可见，单纯地利用互联网技术去除传统金融中心并不一定就是好事。传统中介和互联网公司在不同的领域有自己的比较优势，金融的完全去中介是不太可能也没有必要的，发展的趋势应是向开放的多中介和服务型的弱中心演变。

二、互联网革命之路——区块链

自诞生之日起，互联网便被寄予了美好愿望，我们期待代码将自由、平等的价值观变得程序化和可执行化。于是有人认为，如果互联网企业控制个人数据和信息入口形成新的垄断并取代旧的中心，便是在叛变“革命”，是人性最大的“恶”。

但我认为，这不仅是商业伦理问题，也是一个技术问题 。这些年来，信息互联网 赋予每个网民权力，每个人都可以成为信息的接收者和发出者，一篇微信文章可以拥有10万+的阅读量，一个公众号可以聚集成千上万的粉丝。阅读、点赞、留言都是一种公共参与。但由于信息未被确权，流动无据可查，许多罪恶都可以假自由之名而行，而且网络应用层的HTTP协议是中心化的，信息都集聚在公司手里，这可能造成了互联网巨头的原罪。

当市场失灵时，人们自然会想到依靠监管来维护互联网世界的规范，但依靠第三方监管来维护信息安全的效果也不尽如人意，过滤和审查信息的边界常常不由我们控制。要安全还是要自由，这是一个纠结的问题。

演变至今日，互联网必须要升级成对信息负责，给信息确权的信用互联网 ，而这个过程不能仅由政府、企业来完成，每个网民都应参与进来，一同决定互联网的前途。

在信用互联网上，每个节点都会成为信用公证员和监督者，而我们需要的是一套类似于互联网协议的制度安排，区块链便是应运而生的一种尝试。

2008年11月1日，一个自称中本聪的人在网络上发表了《比特币白皮书：一种点对点的电子现金系统》，在这篇报告里，中本聪阐述了他对比特币这一电子货币的构想，而区块链就是比特币的公共账本。

以区块链为基础，人们正在互联网上建立起一整套信用互联网治理机制 ，包括①工作量证明机制（如果要篡改区块链上的数据，需要拥有超过全网51%的算力，这会使得作伪的成本高于预期利益）；②互联网共识机制（无需甄别好坏，以共识来确保正确）；③智能合约机制（以可编译的程序代替合同，网络自动执行合约）；④互联网透明机制（账号全网公开而户名匿藏）；⑤密码学，非对称加密和公私钥等技术等。

依靠这些制度安排，区块链可以让参与者在不建立信任关系的情形下，通过一个统一的账本系统确保资金和信息安全 ，这项技术显然很合金融行业的胃口。利用区块链开源、透明的特性，参与者能够验证账本历史的真实性，这可以规避当前P2P借贷平台的跑路、欺诈等事件；而且，区块链交易被确认的过程就是清算、交收和审计的过程，可以提升效率。由于所有文件或资产都能够以代码的形式体现，智能合约及自动交易可以在区块链上实现。最后，区块链比单点中心的容错性高很多，具备安全性。除了金融领域外，区块链还是一个关于信任的底层协议，可以对社会生活的各个方面造成冲击 。根据梅兰妮·斯万的观点，区块链技术的发展可以分为三个阶段：1.0是货币（如比特币）；2.0是合约（如以太坊）；3.0是超越金融经济外，特别是在政府、文化、健康等领域的应用。

而在我的眼里，区块链最大的魅力倒不在于其改变世界运作规则的能量，而在于其延展我们个体自由的潜力。

三、区块链的人文和社会价值

中本聪是谁真的重要吗？在区块链世界的逻辑里，中心、权威、首创者、精神领袖都不应该成为关注的焦点。关注区块链

的人的动机各不相同，有想靠其投机赚钱的商人，也有金融从业人员与码农极客，还有自由主义者等热爱区块链背后所蕴含的意识形态的人。

信任，其实就是彼此相信对方不会做出伤害到我的欺诈和违约行为。信任的产生包含三个层面，一是对方没有欺诈的动机；二是对方有欺诈的动机却不敢或不愿真的去行动；三是对方不仅有动机，还真的做出欺诈行为，但由于各种原因，不会对我造成伤害。

传统的防止欺诈的方法针对这3个层面布局了一些制度设计。一是防心魔，即靠道德教化，不让你产生违约的动机；而是靠中心化强权，即不管是法律还是暴力，都在提升违约成本而阻止你开展行动；三是外部补偿，如买保险，由第三方补偿来规避风险。

但我们发现，这些制度设计都在一定程度上损害了个人的自由意志。我们得去遵守一些有局限性的“道德规范”，活在他人的评价体系里；我们要依赖第三方权威，否则无人帮我们申冤和规避风险。这依赖的是一种中心化的思维方式。

而区块链技术是对个体自由的极大伸展。个体不仅可以保留欺诈的动机，甚至可以真的采取欺诈行动，然而最后一道防火墙（区块链机制）可以消解节点的欺诈和违约对他人造成伤害的可能性 。

解除第三方权威是一件很刺激的事情，就像听到尼采说“上帝死了”一样令人激动。在19世纪，便有人说：“上帝是一个无用而且很花钱的假设，因此我们不需要他。”尽管没有了上帝，我们依旧要共同遵循某些规则，只是这些规则不再来源于“超验”的上帝，而是基于对科学和个人理性的共识。

摆脱对他人的信任而达成合作也是一件很刺激的事情，仿佛给“他人即地狱”的困境找到了出口。人在群体生活中为了达成共识必须主动（基于道德、同情等）或被动（迫于法律、暴力）地妥协。很多公共美德，如“诚信”“宽容”“互助”，本质上只是为了减少人们在交往中产生摩擦而进行的制度设计。个人不得不出让一部分自由意志来达成合作。

为了整体的“和谐”，我们都得戴上面具示人。有没有可能通过设计一个机制，让我们更真实地面对自己的“私心”和“杂念”，在交往中“少一点套路，多一点真诚”呢？

我认为是可能的，在“私心”方面，亚当·斯密假设每个人都只是最大限度地追求效用的“自私的人”，我们不需要伪装成“禁欲系”或无私奉献的“螺丝钉”。只要搭建了市场和价格机制这一基础协议，个体就有内生的动力来创造价值。我国的改革开放便是认同了市场这个“基础协议”的伟大尝试，事实证明“群集智慧”远远超过了“中心智慧”的财富创造能力。

这给了我们一个很大的启发，是不是只要能开发出另一套基础协议，便有可能解放人类的“杂念”——主观的道德判断（Moral Core），我们不必与他人达成价值判断上的共识，也不会伤害别人，更不妨碍整体的合作呢？有无可能不仅消解了第三方权威的背书，也不依赖海誓山盟或“人品”（一种基于口碑的信用凭证）而实现陌生人之间的合作呢？

有人可能会问，为什么要这样呢？听妈妈的话，做一个讲诚信的好人难道不是我们该做的吗？这也是一个很有趣的问题，因为这关系到“善”“恶”的标准究竟是什么，“诚信”是不是在任何情境下都是正确的，道德是绝对的还是相对的等哲学问题。

如果我们一辈子都待在一个小村庄里，这种道德哲学上的争论可能毫无价值。但在互联网将全球人类联系在一起，跨国跨种族跨文化交流成为常态的时代，我们会发现所谓的“道德”“习俗”甚至“法律”都有很大的时代与地域局限性，无法满足大规模的陌生人之间协作的要求。萨特在《存在主义是一种人道主义》中说，如果我们没有选择的自由，便不需为自己的行为负责，因为哪怕我做了恶，也不是出于我自由意志的选择，那么我何罪之有？必须首先保证人能真实地表达自己，有自由选择和行动的权利，他才能达致“善”或“恶”，否则他只是一个空壳式的道德模范罢了。因此，存在主义是一种人道主义，取消对个人价值判断的干涉是在恢复人的尊严。因此，在这种时代背景下，已经没有固定的“好”人的标准，尊重个性化和多元的价值观更为重要。

存在主义进一步说，人在为自己做出选择时，也为所有的其他人做出选择。比如我决定结婚，尽管这一决定只是根据我的处境和情感做出的，但我不仅在为自己承担责任（Commitment），而且表达了我对婚姻制度的认可，从而影响了他人。每个人都是一个节点，代表一个“主观性”，而世界便是“主观性”林立的分布式世界。区块链制度保证了每个节点都能平等地参与治理和表决，当每个人（Person）都成为具备表达和表决权的人（Man）时，由此组成的集合体（Collectivity）也开始富有人性。过去，在提到古雅典的城邦民主时常要强调其小国寡民的地理特点是实现直接民主的前提，而在科技高速发展的今天，我们完全有望突破物理条件的限制，将全世界的人接入网络社区实现民主投票和协同治理。

在传统经济学中，资源稀缺是基本假设，竞争并攫取资源所有权是主题。而如今，认知与资源盈余出现，合作并共享资源的使用权是大势所趋。而共享经济形态急需建立全球性的信用共识，因此我们寻找到人类文明最大的公约数——数学。区块链是一个对人性悲观却非常真诚的协议。既然没有办法逃避选择，不选择也是一种选择，人就必须为自己的存在和一切行为”承担责任“，与其信权威、信上帝、信他人，还不如信数学、信自己、信理性。

如果说市场机制这个基础协议解放了个体“私欲”，通过价格和竞争激发了每个节点创造财富的能动性，那么区块链机制这个基础协议便通过分布式的信用公证，使互不信任的节点进行大规模协作成为可能，这可以激发共享经济和协同治理的巨大潜能。可以运用区块链基础协议的领域从经济、金融向政治、社会拓展，比较突出的领域有共享经济、物联网、去中心化社会（DAS）、区块链婚姻认证（可用于有争议性的LGBT婚姻）等概念，这是一场正在发生的革命。

以婚姻为例，婚姻一般意味着双方通过合约绑定在一起，他们共享账户、地契，通过制定育儿、养老合约等确保未来安全地在一起。2015年10月，在美国佛罗里达的迪士尼乐园，全球第一例比特币婚姻被提交到区块链上，誓言被写入文本注释字段，并嵌入了0.1比特币的交易中，因此将永远记录在区块链账本里。区块链代替了政府的见证功能，在某种程度上更加公平和自由。

然而，我们也要注意到，区块链的算法信任只可以用于婚姻合约，却无法保证爱情的忠贞，比如对精神出轨的违约行为它是无能为力的。世界的实相是流动的事件，而不是静止的物件，一段关系的生灭常断，依赖不同的缘起条件，而人的心理活动（受、想、行、识）更是无常，想签订算法合约来维系情感关系本就是该破除的“我执”，能在分开之后说一句“爱过”已是仁至义尽。真实的情感交易也许从未发生，所以无法由他人为你见证、盖戳。互联网和人工智能的确给人类带来很多变革，但问世间情为何物，机器人如何能懂？

参考文献

［1］梅兰妮·斯万.区块链-新经济蓝图及导读［M］.韩锋，龚鸣，等译.北京：新星出版社，2015.

［2］秦谊.区块链冲击全球金融业［J］.当代金融家，2016.

［3］韩锋.未来区块链银行会是什么样［R］.“数字货币与区块链技术：前景、挑战与影响”主题论坛，2016.

［4］杨涛.从去中心化金融来看区块链［R］.全球共享金融100人论坛，2016.

［5］谢平，等.互联网金融报告2014——通往理性繁荣［OL］.http://business.sohu.com/20140425/n398824348.shtml.

［6］陈龙.互联网金融不会颠覆传统金融［R］.第二届互联网金融全球峰会，2015.

［7］保罗·萨特.存在主义是一种人道主义［M］.周煦良，汤永宽，译.上海：上海译文出版社，2005.

［8］刘保禧.林夕、填词与佛学［R］.林夕X爱情X佛学讨论会，2009.

[1] 引用自http://8btc.com/thread-32885-1-1.html。