

# Harvard Business Review

## 哈佛商业评论



战略

区块链真相

区块链范式下的风险控制

区块链+云平台未来商业新规

区块链在共享经济中的作用



# 关于区块链 你不得不知的真相

《哈佛商业评论》出品

# 哈佛商业评论

关于区块链，你不得不知的真相  
(《哈佛商业评论》增刊)

《哈佛商业评论》中文版 出品

# Harvard Business Review

哈佛商业评论



战略

区块链真相

区块链范式下的风险控制

区块链+云平台未来商业新规

区块链在共享经济中的作用



## 关于区块链 你不得不知的真相

《哈佛商业评论》出品



## 增刊：关于区块链，你不得不知的真相

---

[序言：区块链的真相](#)

[区块链真相](#)

[区块链范式下的风险控制](#)

[区块链+云平台未来商业新规](#)

[区块链改造电子健康档案的潜力](#)

[区块链在共享经济中的作用](#)

[区块链将会帮助证明“我是我”](#)

[版权页](#)

《哈佛商业评论》中文版 · 关于区块链，你不得不知的真相

编辑：王婷

## 区块链的真相

几乎每个人都听说过：区块链将彻底改造行业，重新定义公司和经济。什么是区块链？区块链是建立在互联网基础之上的P2P网络，于2008年10月首次应用于比特币的协议中。比特币是区块链技术的第一个应用案例。比特币是种虚拟货币系统；它将货币发行、所有权转让和交易确认去中心化。

如果说互联网TCP/IP协议让我们进入了信息自由传递的时代，那么区块链的创新将把我们带入信息的自由公证时代！区块链技术可以称得上是人类信用进化史上的重要里程碑，将会像互联网一样重构人类社会的生产和组织方式。

如果区块链得到普及，未来合同将嵌入数字编码并保存到透明、共享的数据库中，可防止数据被删除、篡改和修订。到那时，每份协议、每个流程、每项任务和每次付款，都会有一份可识别、验证、保存和分享的数字记录和签名。律师、代理人 and 银行家等中间人可能就不是必要的交易参与者了。个人、组织、机器和算法彼此之间的交易和互动将顺畅无阻。这就是区块链的巨大潜力。

我们看好区块链的潜力，但同样也担心它遭到捧杀。我们担心的不仅仅只是区块链存在的安全隐患，比如2014年某比特币交易平台的崩盘以及更近期的黑客攻击事件。在技术创新领域的研究经验告诉我们，只有消除在技术、政府管控、组织和社会等多方面的障碍，才有可能真正发生区块链革命。

实际上，区块链并非“颠覆性”技术，它不能用成本更低的解决方案颠覆传统商业模式，并迅速压倒在位企业。区块链是种“基础性”技术：它有为经济和社会体系创造新基础的潜力。虽然它的影响巨大，但要渗透到我们的经济和社会基础设施中，仍需数十年之久。随着技术和制度改革的浪潮势头渐猛，区块链的应用将稳健推进。

本期《哈佛商业评论·区块链的真相》精选6篇文章，从区块链的由来讲述到它的商业应用、前景及影响。



# 区块链真相

## THE TRUTH ABOUT BLOCKCHAIN

马尔科·扬西蒂（Marco Iansiti） 卡里姆·拉哈尼（Karim Lakhani）| 文

刘筱薇 | 译 齐菁 | 校 钮键军 | 编辑



充满了想象空间的区块链技术距离大规模商业应用，尚需几十年的时间。作者基于基础性技术占领高地的四象限模型：单一案例、本地化、取代和改革，分别给出了公司投资区块链业务的具体指导建议。

### 核心观点

#### 热点

我们都听说过区块链将彻底改革行业，但整个过程要比很多人声明的时间久。

#### 原因

区块链和TCP/IP（互联网的基础）一样，也是需要多方协调发展的基础性技术。区块链面临的技术、监管和社会方面的复杂性也是前所未有的。

#### 真相

TCP/IP的普及说明，区块链将走上一条我们可以预见的道路。虽然这段征程还很遥远，但公司提早做计划很有必要。



合同、交易及其记录是我们的经济、法律和政治体系中，起决定性作用的结构。它们保护资产并确定组织边界（organizational boundary），建立并核实身份和历史事件，影响不同国家、组织、社群和个人之间的互动，引导社会和管理行动。但这些关键工具以及衍生的官僚机构没能追赶上经济数字化的转型步伐，其笨拙程度如同在堵车高峰期追捕一辆F1赛车。在数字世界中，我们调整和维持行政管控的方式必须改变。

区块链有可能解决这一问题。它是比特币（bitcoin）和其他虚拟货币的核心技术，本身是一种开源分布式账本，能够高效记录买卖双方的交易，并保证这些记录是可查证且永久保存的。该账本也可以通过设置，自动发起交易。（见[《区块链的运作原理》](#)）

我们能够想象到，如果区块链得到普及，未来合同将嵌入数字编码并保存到透明、共享的数据库中，可防止数据被删除、篡改和修订。到那时，每份协议、每个流程、每项任务和每次付款，都会有一份可识别、验证、保存和分享的数字记录和签名。律师、代理人 and 银行家等中间人可能就不是必要的交易参与者了。个人、组织、机器和算法彼此之间的交易和互动将顺畅无阻。这就是区块链的巨大潜力。

几乎每个人都听说过这一说法：区块链将彻底改造行业，重新定义公司和经济。我们同样看好区块链的潜力，但也担心它遭到捧杀。我们担心的不仅仅只是区块链存在的安全隐患，比如2014年某比特币交易平台的崩盘以及更近期的黑客攻击事件。在技术创新领域的研究经验告诉我们，只有消除在技术、政府管控、组织和社会等多方面的障碍，才有可能真正发生区块链革命。若不清楚区块链将如何占领高地，贸然开始区块链创新就是个错误。

我们认为，真正由区块链引导的行业和政府改革，还要在很多年后才能实现。原因在于，区块链并非“颠覆性”技术，它不能用成本更低的解决方案颠覆传统商业模式，并迅速压倒在位企业。区块链是种“基础性”技术：它有为经济和社会体系创造新基础的潜力。虽然它的影响巨大，但要渗透到我们的经济和社会基础设施中，仍需数十年之久。随着技术和制度改革的浪潮势头渐猛，区块链的应用将稳健推进。我们将在本文中探讨这一洞见及其战略意义。

## 技术的普及模式

在部署区块链战略和投资之前，我们先回顾一下对技术普及的认识，特别是其他基础性技术的改革过程，比如分布式计算机网络技术。该技术出现在TCP/IP（即传输控制协



议/因特网互联协议）的推广过程中，为互联网的发展奠定了基础。

TCP/IP于1972年推出，最开始只在“单个案例”中得到普遍应用：TCP/IP是美国国防部研究员在阿帕网（ARPAnet，商用互联网的前身）上发送电子邮件的基础技术。TCP/IP出现之前，搭建电信网络架构的基础是“电路交换”（circuit switching），即通信双方或机器之间的连接必须提前建立，并在整个交换过程中都保持连接。为确保任意两个节点都能相互通信，电信服务提供商和设备制造商已经投资数十亿美元建立电信专线。

TCP/IP颠覆了电路交换模式。新协议通过将信息数字化并分成极小的组（每组都包含地址信息）来传递信息。各小组的信息发送到网络中后，可以采取任意路径到达接收端。位于网络边缘的智能发送和接收节点能够拆分并重组各组信息，同时解读编码数据。现在已经没有必要建设私用专线或大规模基础设施了。TCP/IP创建了一个开源共享的公共网络，没有任何中央机构或党派负责其维修和升级。

传统电信和计算机组织对TCP/IP抱怀疑态度。它们难以想象到稳定的数据、信息、声音和视频连接可以建立在新架构上，或者相关系统能够得到保护并大规模扩展。但在20世纪80年代末和90年代这段时间里，越来越多的公司开始使用TCP/IP，比如IT及互联网技术服务公司Sun、NeXT、惠普和硅图（Silicon Graphics）。这些公司应用TCP/IP，在一定程度上是为了在组织中创建本地化的专用网络。为实现这一目标，它们开发了多种构造块和工具，从而在电子邮件的应用基础上，进一步扩大了TCP/IP的使用范围，使之逐渐取代较为传统的本地网络技术和标准。组织在应用这些构造块和工具的过程中，发现生产率急剧提升。

万维网（World Wide Web）在20世纪90年代中期横空出世，使TCP/IP的公用范围迅速扩大。新兴技术公司很快涌现，建设“基础管道”——提供必要硬件、软件和服务，来连接现已开放的网络以及交换信息。网景通信公司（Netscape）将很多有助于开发普及互联网服务及应用软件的工具和部件商业化，包括浏览器、网页服务器等。Sun推动了Java和编程语言的开发。随着万维网中的信息急剧增多，引导用户寻找信息的搜索引擎Infoseek、Excite、AltaVista和雅虎应运而生。

“管道”的基础设施达到一定规模后，新一代公司就可以利用低成本的网络连接，积极创造能够取代既有公司的互联网服务。CNET公司开始发布网络新闻。亚马逊销售的书籍比任何一家书店都多。在线旅游中介Priceline和Expedia让飞机票订购更容易，并将整个购买流程的透明度提升到一个前所未有的高度。这些新兴公司能用较低成本连接大量客户，给报纸和实体零售商等传统企业带来了巨大压力。

新一代公司凭借几乎无所不在的互联网连接，创造了很多改革性的技术应用，彻底改

变了公司创造和捕捉价值的方式。新兴公司基于新的P2P架构而建，通过协调分布式用户网络获得价值。比如eBay用拍卖的形式改变了在线零售业；Napster改革了音乐行业；Skype重塑了通信业；谷歌利用用户自创的链接提供更多相关结果，是网页搜索的革新者。

归根结底，TCP/IP用了30多年时间，才走完所有阶段：单个案例、本地化、取代和改革，最终彻底革新整个经济。如今全球最有价值的上市公司中，超过半数拥有由互联网驱动、基于平台而建的商业模式。我们经济的基本根基已经改变。实体规模和独有的知识产权不再有不可撼动的优势；经济主导者更可能是那些起到“基础”作用的公司：它们积极组织、影响和协调社群、用户和组织组成的庞大网络。

区块链大幅降低了交易成本，如果得到广泛应用，还能改变整个经济。

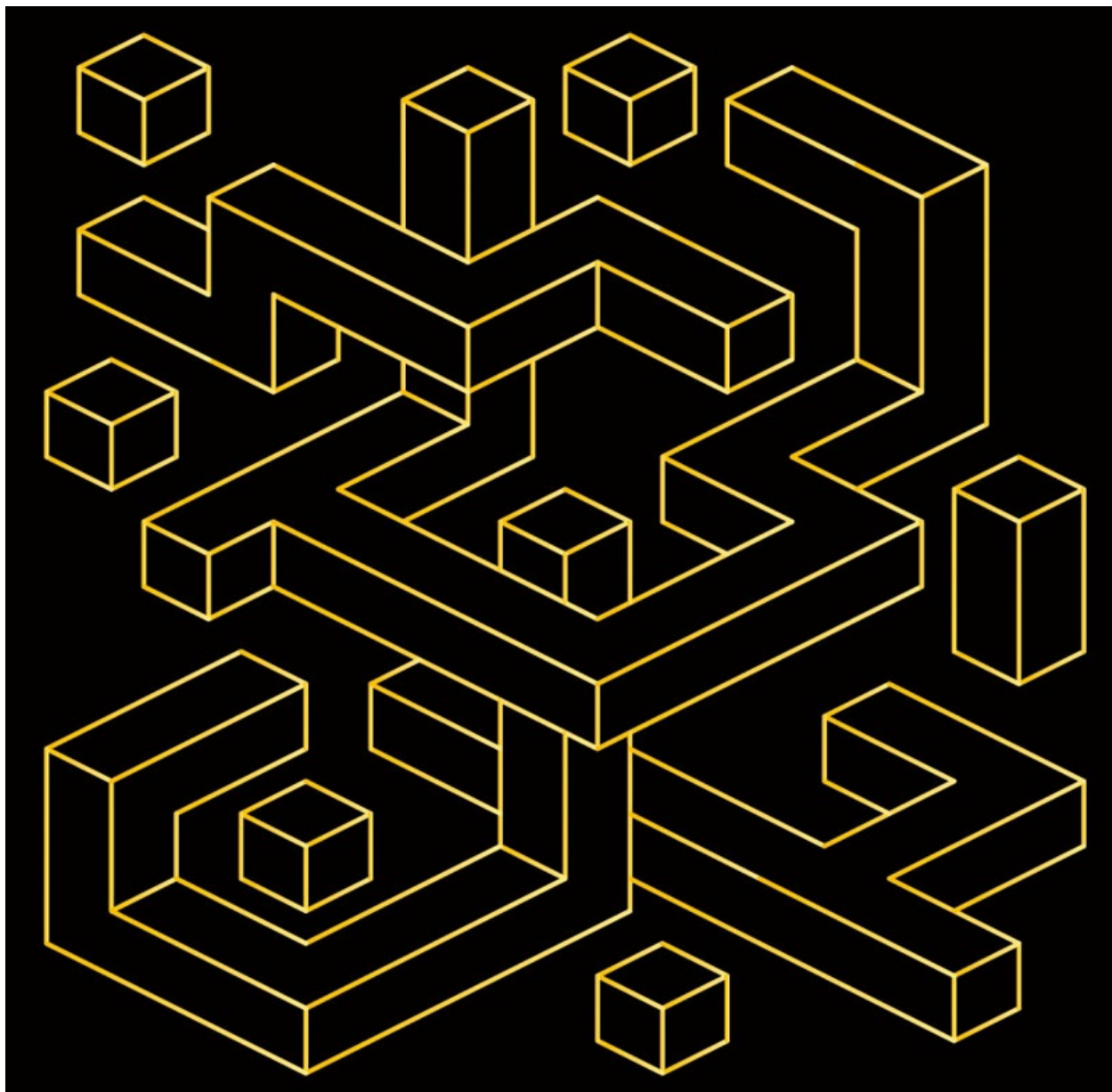
## 新架构

区块链是建立在互联网基础之上的P2P网络，于2008年10月首次应用于比特币的协议中。比特币是种虚拟货币系统；它将货币发行、所有权转让和交易确认去中心化。比特币是区块链技术的第一个应用案例。

区块链和TCP/IP之间的相似之处显而易见。电子邮件使信息双向发送成为可能，比特币则让金融双向交易成为可能。区块链的开发和维护是开源、分布式以及共享的，而TCP/IP也是如此。两者的核心软件都由一个来自世界各地的志愿者团队维护。此外，比特币和电子邮件都是从积极性很高但规模较小的社群中流行开来。

TCP/IP大幅压缩连接成本，释放了新的经济价值。同样，区块链也大幅降低了交易成本；它有潜力成为所有交易的记录系统。如果这一天到来，那么随着区块链衍生品影响力和控制力的扩大，整个经济都会再次经历巨大转型。

在现行商业模式下，持续记录交易往来是每家公司的核心职能。这些记录追踪过去的行动和表现，并指导未来计划的制定。记录不仅说明了组织内部的运营情况，也显示出组织的外部关系。每个组织都有自己的记录，而且不对外公开。很多组织没有记录所有活动的总账本；相反，这些记录都由内部各部门和职能掌管。但问题在于，将各个私有账本中的交易全部核对一遍要花很长时间，而且容易出错。



比如某次股票交易可以在几微秒内进行，往往不需要人工干预。但股权转让可能要用一周时间，因为交易双方无法看到彼此的账本，不能自动确认资产的实际所有权和转让权限。组织交换交易记录时需要一系列中间人，充当资产的担保人；账本也要逐个更新。

区块链系统中，账本在大量相同的数据库中复制，每个数据库都由一个利益相关方主管和维护。任意一份文件有改动的话，其他所有文件都会同时更新。同样，如果出现了新交易，交易资产和价值的记录就会出现在所有账本中，并且永久保存。没有必要请第三方中间人确认或转让所有权。在以区块链为基础的系统中进行股权交易，数秒内就可以完成转让，既安全，又有据可查。（臭名昭著的黑客袭击比特币交易事件并未凸显区块链本身

的弱点；相反，这些事件反映了连接不同区块链使用者的独立系统有严重漏洞。）

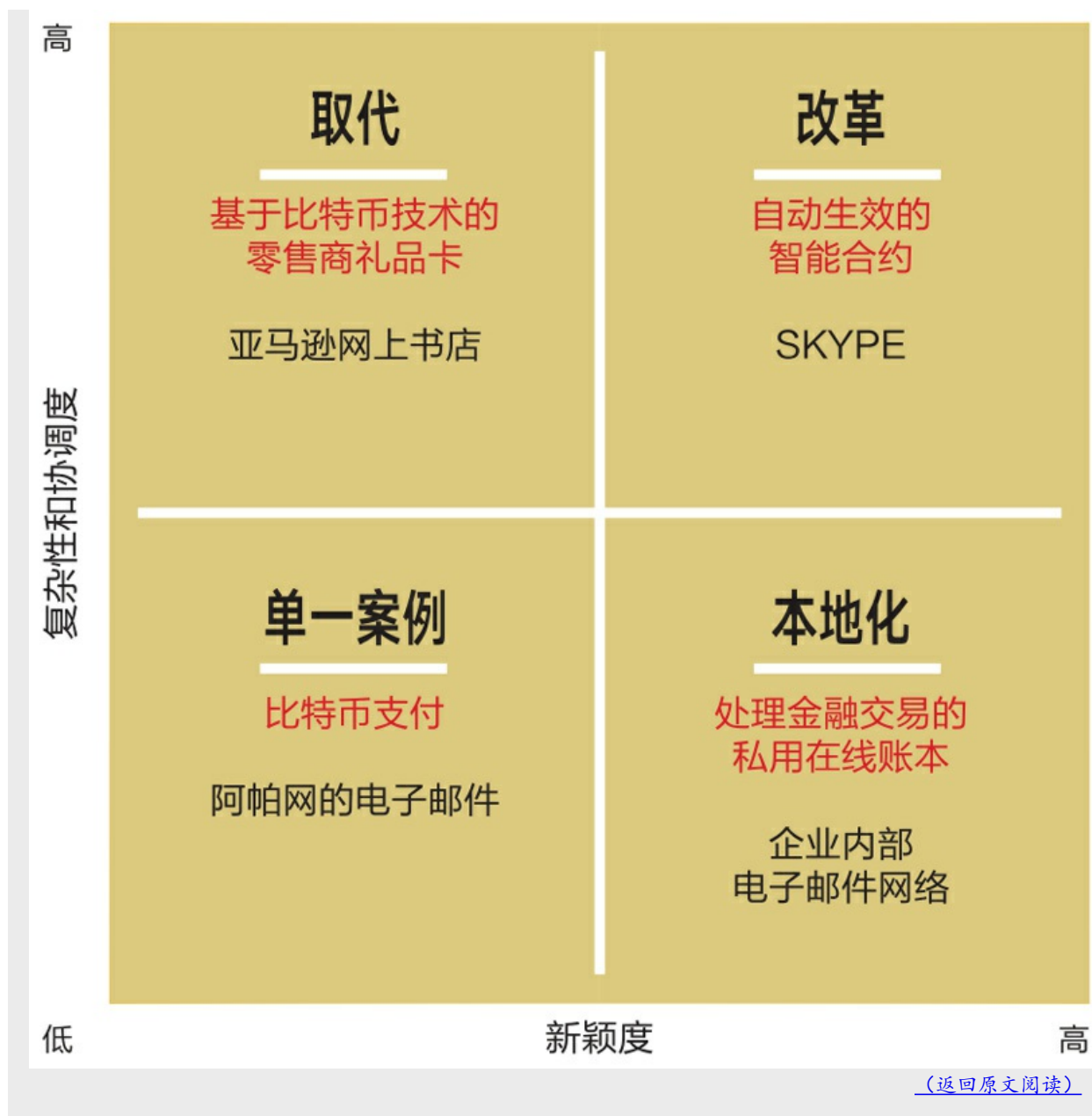
## 普及区块链的框架

如果说比特币好比早期的电子邮件，那么区块链是不是也要等很多年，才能充分发挥出其潜力？对这个问题，我们要给出一个不完全肯定的回答。我们无法准确预测区块链改革要用多长时间才能实现，但可以猜想，什么技术应用会最先受到欢迎，以及区块链的普及最终将以什么方式实现。

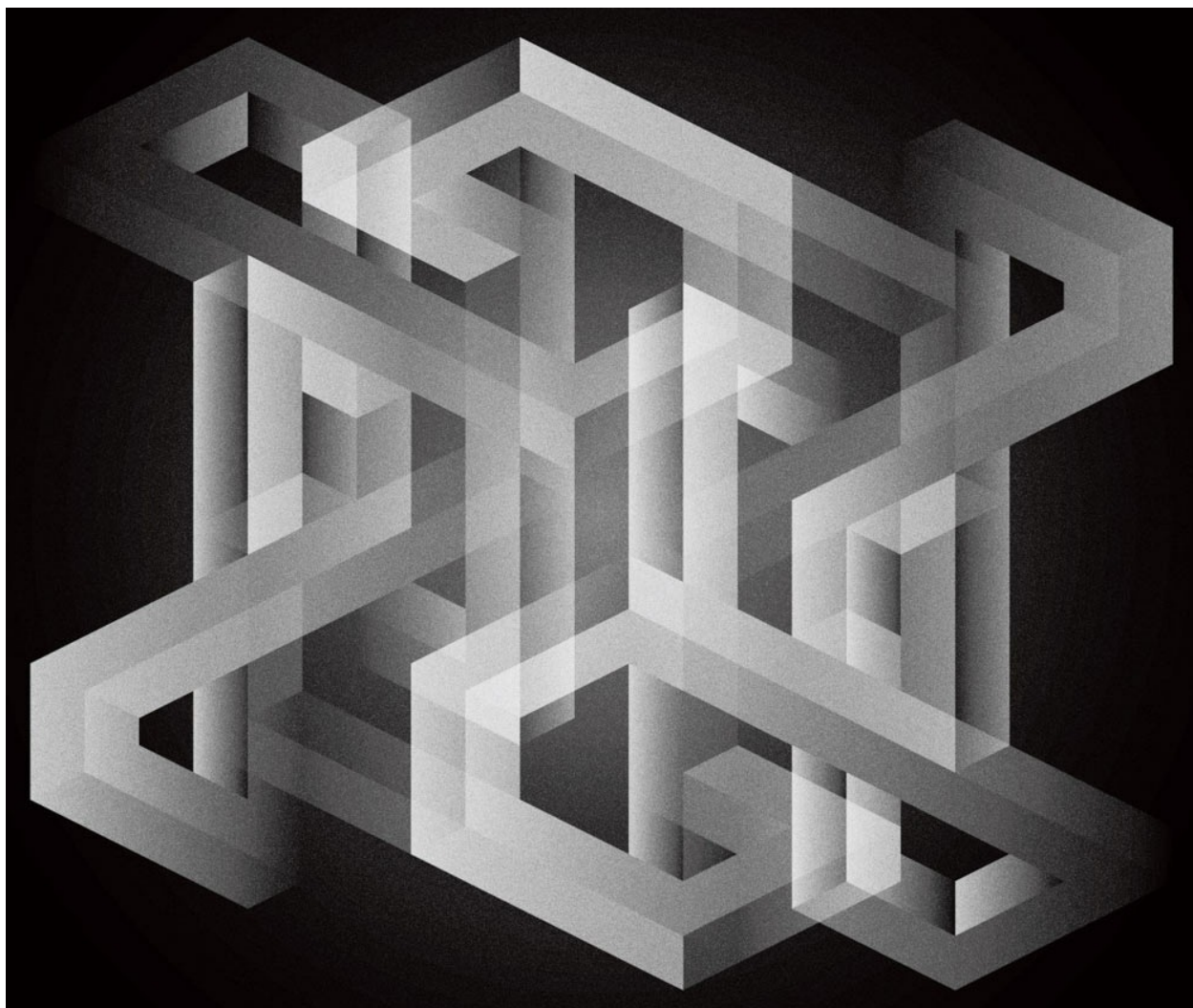
反观历史，我们认为有两大维度会影响到基础性技术及其商用案例的扩展和演进。第一个维度是新颖度，即技术应用相对于外界事物的新鲜程度。新颖度越高，开发人员就要花越多精力，确保用户了解到新技术能解决的问题。第二个维度是复杂性，或者说，技术应用要求的生态系统协调度——须合作利用新技术，产出价值的相关方数量和多样性的情况。举例来说，只有一个成员的社交网络基本上毫无用处；只有足够多的联系人登录后，建立这个社交网络才有意义。其他用户也要参与进来，这样所有参与者才能获得价值。区块链技术应用的运作也是如此。此外，随着这些新应用规模和影响力的扩大，其普及将需要重大机构性的改革。

### 基础性技术如何占领高地

基础性技术的普及一般分为四个阶段。定义不同阶段要考虑到两个因素：技术应用本身有多新颖，以及应用这些软件必需的协调工作有多复杂。新颖度和复杂性低的创新最先得到接受。新颖度和复杂性高的创新要用数十年时间才能演进，但这些创新能够改革经济。1972年首次在阿帕网中得到应用的TCP/IP技术，现在已经演进到了改革的阶段，但区块链的技术应用（红色字体）仍处在早期发展阶段。



我们建立的框架从以上两大关联性维度（contextual dimension）出发，划分出四个象限，将不同形式的创新划入不同象限。（见《[基础性技术如何占领高地](#)》）不同象限代表着技术发展的不同阶段。确定好某项区块链创新属于哪个象限，有助于高管认识到自己将面临什么样的挑战，合作和共识必须达到怎样的水平，以及需要哪些立法和监管措施。这一图表还显示出，促进创新的普及须建立哪些流程及基础设施。管理者可以用它评估区块链在各个行业的开发情况，并考查公司在建立区块链能力的战略投资。



单个案例。新颖度和协调度双低的技术应用属于第一象限；这些创新带来更有效，成本更低，定制化的解决方案。电子邮件是TCP/IP的单个应用案例（虽然其价值随用户数量增多而上涨），它是电话、传真和传统邮递的廉价替代品。比特币也属于这一象限。在其早期发展阶段，即使仅将比特币作为支付手段的用户，也不太可能即刻获取价值。（你可以将比特币视为一种电子邮件，只不过更为复杂，不仅传送信息，还传递实际价值。）2016年末，比特币交易的预测值为920亿美元。虽然这一数字和411万亿美元的全球支付款数相比，仅是个零头，但比特币发展迅猛，在即时支付、外币和资产交易等现行金融体系有局限性的领域中，重要性日益凸显。

#### 区块链的运作原理

以下是构成区块链基础的五大原则。



## 1 分布式数据库

区块链中的每一方都有权限查看整个数据库及其完整历史。数据和信息不由任何一方掌管。各方都可以直接确认交易伙伴的记录，根本不需要中间人。

## 2 P2P传输

通信可以直接在各点间进行，不必通过一个中央节点传送信息。每个节点都可以保存信息并向其他节点转发信息。

## 3 使用化名提高透明度

有权限登录系统的人能看到每次交易和交易价值数额。区块链中的每个节点或用户都有自己独特的地址（30多位的数字和字母组合）。用户可以选择保持匿名状态或向他人提供身份证明。交易发生在不同的区块链地址之间。

## 4 记录不可更改

一旦交易信息录入数据库中，账户得到更新，那么记录不能再被修改了，因为这些记录与之前的每一条交易信息都有联系（这也就是区块链中“链”字的来源）。区块链用了很多计算算法和方法，确保数据库中的记录是永久、按时间顺序的信息，而且能让网络中任何人都看到。

## 5 计算逻辑

数字化账本意味着区块链交易可以和计算逻辑捆绑在一起，而且是可以被编写的。所以用户可以设定算法和规则，自动发起节点间的交易。

[\(返回原文阅读\)](#)

本地化。构成第二象限的创新新颖度较高，但因为这类创新仅要求有限数量的用户创造即刻可得的价值，所以促进其普及并不是很困难。如果区块链采取和网络技术一样的路线进入企业，我们就可以预期，区块链创新以单一应用案例为基础，创建本地私有的网络，让多个组织通过一个分布式账本相互连接。

很多早期以区块链为基础的创新都出现在金融服务领域，而且一般在一些公司组成的小型网络中，所以对协调度的要求不太高。纳斯达克（Nasdaq）正在和区块链基础设施供应商之一Chain.com合作，提供处理和确认金融交易的技术。美国银行、摩根大通（JPMorgan）、纽约证券交易所、富达投资（Fidelity Investments）和标准渣打银行（Standard Chartered）正在测试区块链技术，试图让其代替基于纸张的手动交易处理流

程，并在贸易融资、外汇交易、跨境结算和证券结算等领域应用。加拿大银行正在测试一种名为CAD币（CAD-coin）的数字货币，用于跨行转账。我们预测，未来私有区块链会激增，在各行各业发挥特定作用。

取代。第三象限的创新建立在单个案例和本地化技术应用的基础之上，所以新颖度较低，但由于其公用范围和幅度更广，所需协调度很高。这些创新旨在取代整个商业模式，但也因此面临巨大障碍——它们需要更高的协调度，而且想要取代的流程可能已经很成熟，并在组织和机构中已根深蒂固。取代的案例包括加密数字货币

（cryptocurrency）。这是种健全的新货币系统，由简单的比特币支付技术演进而成。两者最大的不同是，加密数字货币要求进行货币交易的各方都要使用该系统，这给长期以来处理、监管此类交易的政府和机构带来了挑战。消费者也要改变自己的行为模式，并了解如何使用加密数字货币的新功能。

麻省理工学院（MIT）近期的实验让我们看到，数字货币系统面临的挑战。2014年，MIT比特币俱乐部为4494名MIT大学生每人免费提供价值100美元的比特币。有趣的是，30%的学生甚至都没有申请这笔钱，20%的申请者在数周之内就把比特币兑换成了现金。即便是颇懂技术的人，也要下很大工夫弄清比特币的使用方法和用处。

非营利组织Stellar算是改革力度最大的取代案例之一。该组织试图为从未使用过金融服务的人提供廉价的银行业务、小额资金支付和汇款服务。Stellar有自己的虚拟货币和微服务架构，还允许用户在自身系统内保存多种资产，包括其他币种的货币、电话时长、数字贷款。Stellar最开始主要面向非洲，特别是非洲的最大经济体尼日利亚。Stellar的服务在目标客户中得到广泛应用，其成本效益也有目共睹，但前景依然不确定，因为它对整个生态系统的协调度要求很高。尽管民众接受度已经证明了Stellar的可行性，但要成为标准银行业务，仍须政府调整政策，并说服中央银行和大型组织也使用Stellar的服务。完成这一目标，可能需要各方数年之久的协同努力。

改革。位于第四象限的是全新的技术应用。这些创新只要能成功，就可以改变经济、社会和政治体系的本质。这类创新要求协调多方的行动，并在标准和流程上与相应机构达成一致；其普及则要求社会、法律和政治方面出现重大改革。

“智能合约”（smart contracts）可能是现在最具改革性的区块链技术应用。只要交易符合合约条款要求，智能合约就可以实现自动支付和货币等其他资产的自动化转让。举例来说，某份智能合约能在货物签收后，立即给供应商支付应付款项。某公司可用区块链表明某特定货品已经签收；或者产品可能有GPS追踪功能，可以在区块链中自动更新地理位置，而这一功能反过来还能发起收款。我们已经看到一些自动生效型合同的早期实验，应

用的领域包括风险投资、银行业务和数字版权保护。

智能合约的前景一片大好。公司基于合同而建；从法人团队的组成到买家与供应商的关系，再到雇员关系，签订合同都必不可少。如果合同可以自动生成，那么传统企业结构、流程以及律师和会计等中间人将会发生什么变化？管理者又会受到什么影响？他们的职责会发生巨大改变。但我们现在为这一想法激动不已恐怕太早，要记住，智能合约得到广泛普及那天为时离我们还有数十年之久。没有众多机构或其他力量的支持，智能合约并不能彰显其作用。只有就如何设计、确认、实施和强制执行的问题上达到高度协调和明晰化，这类合同才能实现潜力。我们认为，肩负这些重责的机构要用很长时间才能完成转变。它们面临技术方面的严峻挑战，特别是安全挑战。

## 区块链投资指导

高管如何为所在组织布局区块链？我们制定的框架有助于公司抓住正确时机。

总体来看，最简单的方法是从位于单个案例象限的技术应用开始。这样做可以将风险降至最低，因为这些创新不新颖，而且对第三方的协调度基本没有要求。公司的策略之一是，让比特币成为一种支付机制。比特币的基础建设和市场已经成熟，应用虚拟货币会迫使多个职能部门（包括IT、财务、会计、销售和市场营销）锻造区块链能力。另一种低风险的方法是，将区块链当作内部数据库使用，保存多个应用软件的数据，比如实体和数字资产管理软件中的信息，内部交易记录和身份确认信息。有些公司为保持内部多个数据库信息一致，已经焦头烂额；对它们来说，引入区块链不失为一种极其有效的解决方案。测试单一案例的技术应用有助于组织开发必要新技能，为使用更先进的软件做准备。而随着区块链云服务（初创公司和亚马逊、微软这样的大型平台都提供此类服务）的出现，实验正变得越来越容易。

开发本地化的技术应用是公司自然而然会采取的第二步。我们看到，如今在私用区块链网络上的投资巨大，而相关项目似乎是为了在短期内取得成效。比如一些金融服务公司发现，它们和可靠的交易伙伴（数量有限）建立的私用区块链网络能够显著降低交易成本。

组织也可以利用本地化的应用软件，解决跨国交易中出现的特殊问题。比如公司已经开始利用区块链技术追踪复杂供应链中的产品。在钻石行业，区块链可以持续追踪宝石从挖掘到出售阶段的情况。现在这类实验的技术，应用起来已十分方便。

开发取代型技术应用需要严谨的计划，因为现有解决方案可能很难颠覆。改革方法之

一是，将精力集中在那些不要求终端用户做出太多改变的新产品，并保证用户得到更廉价，或更有吸引力的解决方案。要提升吸引力，取代型创新必须保证产品性能和传统解决方案同样优秀、完善，同时要方便整个生态系统采纳自身技术。第一资讯（First Data）首次尝试利用区块链技术发行礼品卡，这就算是一个考虑周全的替代方案。为消费者提供新型礼品卡的零售商能够利用区块链在账户内追踪现金流，避免了对外部刷卡服务提供商的依赖，从而大幅压缩每次交易的成本，并加强安全性。新的礼品卡还允许多个商家通过统一账本，互相之间转移欠款和交易能力。

改革型技术应用离我们还很远。但现在评估其潜力，并投资发展必要的基础设施仍有一定意义。一旦这些创新捆绑了不同于以往价值创造和捕捉方式的新商业模式，就能发挥出最大效能。虽然接纳新商业模式需要很大付出，但能够打开公司未来增长的大门。

举例来说，律师事务所未来必须改革，为实行智能合约铺路。它们要发展软件和区块链编程方面的新专业技能，可能还要反思现行的按小时付费模式，并考虑是否根据合同收取转账或托管的费用。这仅仅是两种可行方案，但不论高管采取哪种方法，都必须在做出改变前，确定自己了解并测试过新商业模式的效果。

改革型创新会最后成功，并将带来巨大价值。这些创新可能对两大领域影响深远：

1) 和过境检查等职能配套的大型公共身份系统；2) 算法驱动的决策，用来防止洗钱和进行涉及多方的复杂金融交易。我们认为，这些创新要用10年或更久的时间，才能被大众接受并得到广泛应用。

改革型创新也会催生有能力协调并管控新生态系统的平台级公司。这些公司是下一代的谷歌和Facebook。抓住这样的机遇需要有耐心。虽然现在就在这类创新上投入大额资金似乎为时过早，但建设必要的基础设施（工具和标准）仍是值得的。

**TCP/IP**不仅为区块链的普及提供了模版，还为其铺平了道路。**TCP/IP**现在无处不在，而区块链技术应用基于数字数据、计算机通信和基础设施而建。**TCP/IP**既降低了区块链创新的实验成本，也促进了新使用案例的迅速崛起。

高管可以利用我们总结的框架，确定建立区块链能力的第一步。他们必须确保员工了解区块链，开发上文提到的四个象限中适合自己的技术应用，同时投资区块链基础设施建设。

但考虑到投资期、不利于新技术普及的障碍和达到与**TCP/IP**同等接受程度的复杂性，高管还必须谨慎看待区块链实验的风险。显然，从小处做起是为成就更大梦想打好专业基础的好方法。但投资力度应取决于公司和所在行业的具体背景。金融服务公司早已开始启用区块链技术，但制造业还未行动。

不管你所在公司处在什么背景之下，区块链都可能影响到你。这一前景已经非常明朗；一切不过是时间问题。

### 延伸阅读

要想了解更多技术普及的信息，请登录[HBR.org](https://hbr.org)阅读以下文章。

《数字化的普遍性：连接、传感器和数据如何改革行业》

马尔科·扬西蒂和

卡里姆·拉哈尼

《将战略视为生态系统》

马尔科·扬西蒂和

罗伊·莱维恩

《正确的技术，错误的时间》

罗恩·安德纳和

拉胡尔·卡普尔



马尔科·扬西蒂是哈佛商学院David Sarnoff工商管理教席教授。卡里姆·拉哈尼是哈佛商学院工商管理教授，也是哈佛大学定量社会科学研究实验室的主要研究者。





# 区块链范式下的风险控制

保罗·塔斯卡（Paolo Tasca） 马西莫·莫里尼（Massimo Morini）| 文  
齐菁 | 译 刘筱薇 | 校 钮键军 | 编辑

马尔科·扬西蒂（Marco Iansiti） 卡里姆·拉哈尼（Karim Lakhani），《哈佛商业评论》中文版2017年1月，《区块链真相》一文

在技术创新领域的研究经验告诉我们，只有消除在技术、政府管控、组织和社会等多方面的障碍，才有可能真正发生区块链革命。若不清楚区块链将如何占领高地，贸然开始区块链创新就是个错误。

区块链技术，也被称作分布式记账技术（DLT），将我们带入从“信任人”到“信任机器”、从“中心化”到“去中心化”的新范式。区块链通过去中心化的、同级验证的、时间戳账本来确认匿名的身份和交易。每个人都能对账本进行核查验证，但它不受任何一方控制。基于区块链技术的商业活动有永恒性、自动性和透明共识三大特性。

这些技术特点可以帮助企业缓解商业风险，下面就来说说区块链可以帮助缓解哪些风险，以及如何缓解风险。

回答这一问题，我们借用罗伯特·卡普兰（Robert Kaplan）和安妮特·米凯什（Annette Mikes）在《差异化风险管理》（详见《哈佛商业评论》中文版2012年10月刊）中的框架，将其延伸至区块链领域来解释如何使用区块链来缓解可预防风险、战略风险和外部风险。可预防风险是内部风险，由日常操作流程故障和员工失误或不恰当行为引起，比如某个贿赂官员的员工或是某个流氓交易员。战略风险来自企业的战略投资，比如研发项目和金融企业的信用及市场风险。要想得到丰厚的回报，这些风险无法避免。最后，外部风险来自企业外部，不受企业控制。传统意义上它指的是自然、政治或者宏观经济灾难。最近，世界变得越来越互联且依赖于信息的流动，网络风险也被纳入外部风险之中。无论任何行业，外部信息流的打扰和内部信息安全遭到破坏，都是必须关注的关键风险。

## 消除可预防风险

对于流程、人和系统来说，区块链都是风险监控和评估“合适且合理”的方式。

在流程方面，许多日常流程有风险是因为数据存在丢失和被篡改的可能性。然而，智能合约和自动化流程可以减少日常流程中人的介入。例如，美国五角大楼已经通过密码加密来解决这一问题。他们使用时间保护系统，将重要文件（与某一国家相关的文件）打乱并定期在公共报纸上发布，以保证记录的永恒性。区块链正是可以达到这种效果，且不用购买《纽约时报》的专栏版面。更宏观来看，区块链其实是一种非等级式的全新管理流程，决策分布在网络各个端口而非像企业通常那样，集中在中心处理。

DAOs（分布式自治组织）使其扁平化、民主化，甚至可能颠覆传统的管理金字塔等级。在传统企业的决策流程中，决策由人做出。与此不同，DAOs中的决策按照一定规则自行生成，也就是有预先设定好、无法被收买、强行实施并且防篡改的规则代码置入智能合约中。拥有设计精良共识协议的区块链可以使许多流程去中心化，比如招标，使用区块链让贿赂招标官员的企图成为泡影，因为不存在一个专门负责的工作人员，一切流程都透明公开。这一优势既可以在优化单个企业内部流程时使用，更重要的是，它也可以让监管者或是企业联盟降低公共流程的风险，使整个群体受益。

如果流程中有人的介入，企业就须评估并监控其诚信度、公正性、名声、竞争力、能力和稳定性。对于员工和管理者在运营和完成工作任务时的业绩表现，区块链可以帮助收集并存储企业所需的信息。违反法律法规、内部政策和市场期待的商业道德的不当行为，可能导致欺诈、诈骗、欺诈性财产转让以及会计花招。对于以上各种形式的不当行为须先行发现，然后使其受到法律的制裁。使用区块链管理流程，可获得永久性的记录（即事后无法更改）。知晓匿名账号背后真实身份的管理者，就有可能最大程度精确了解谁在何时做了什么，并让员工为自己的行为负责，帮助企业预防员工和官员的不当行为，降低运营风险。这一分布式的风格也消除了对中间专业审计人员的需求。

实际上，集中型数据库或硬件的管理员承担着巨大的运营风险，增加了单方面控制和改变规则并成为单点故障（single point of failure，常用于IT领域，指单个点发生故障时会波及整个系统或者网络，从而导致整个系统或者网络的瘫痪——译者注）的风险。大型机构还面临匹配不同数据库信息的问题。因此，他们将不得不通过低效的手动过程来调查和修复“中断”问题，不仅花费时间和金钱，还增加了出错的可能性。公司内部和公司之间的公共区块链数据提取层可以降低错误率，并降低监控和修复数据库之间的协调“中断”的成本，因为他们共享一个“完美”的数据库可供衡量。此外，实时协调消除了异常检测中不当的延迟。

任何用于收集、存储和处理日常交易以及财务会计数据的操作信息系统都可以从使用区块链中受益。特别是，在硬加密的分布式账本中，例如公共/私人密钥基础设施，拥有

实时存储的永恒性、标准化和经过认证的交易记录的系统成为可能。在这种情况下，任何不记录债务的公司资产负债表或任何其他财务欺骗的不当行为将立即被检测到。区块链的透明度可以保证内部人员不太可能将公司资产从企业中转出。此外，会计花招成功的机会也会大幅下降，公司之间交易将变得更透明，发票对账更容易。投资者可以要求与任何其他“内部人”相同的访问权限，以便监控公司账目的交易（例如比对实时记录和季度报告）。

## 降低战略风险

与可预防风险不同，战略风险在一定程度上是不可避免的，因为其与企业业务活动相关。公司也会明确意识到，想要从其业务战略获取回报可能会遭遇的风险。区块链是一种多功能技术，它可以为不同目的，以不同方式实现。虽然区块链不能预防或阻止战略风险，但它应该能够降低风险实际发生的可能性，并提高公司缓解风险事件的能力（如果风险真的发生）。

金融风险。以此作为开始，显然是因为区块链最初被引入并应用于货币交易，随后吸引了银行和其他金融机构越来越多的兴趣。此外，卡普兰和米凯什认为金融领域的风险是最不可预测的和不断变化的。如今，金融风险不仅涉及金融公司。卡普兰和米凯什给出了一个关于信用风险的例子，一家IT服务公司通过监控客户的信用利差加速收取应收款项，如果利差超过了给定的阈值，则要求客户按进度分期付款。

只要此类交易通过区块链执行，这些风险管理行为就可以实现自动化。在一个有以数字合同编码的债务信息的共享分布式账本上，对于交易对手拖欠的债务数目，以及有多少抵押品可用，不会产生争议。而争议和延误是发生信贷事件时造成损失的重要原因。去中心化的共识和永久的实时数据让参与者在交易时间之前，有选择性地向另一交易对手显示可信数据，以提高其自身价值的确定性，从而降低风险和信用暴露。

区块链还能做到更多。智能合约可以使交易（一项服务或一次转账）与相应的支付同时执行，因为智能合约将控制交易的一方，直到相应的另一方完成支付。这将自动实现被称为“交付与付款”（一种规定付款必须在安全交付之前或同时完成的模式——译者注）的市场设计，智能合约甚至能够实现比这级别更高的保护。当事件发生大大增加交易对手违约的可能性时，智能合约可以自动将应收款从一方转移到另一方。这样的事件可能是可观察到的系列事件，如某一方错过了付款；或使用所谓的“oracle技术”及时探查到的风险，即可测量的外部事件，如信用利差达到阈值。这些保护契约可以成为双方交易都同意的智能合约的一部分，保护双方均免于违约风险。

合规。合规涉及广泛、不分领域。当然，金融是最受监管的领域之一。合规是有风险的，一旦不能根据行业法律法规、内部政策或规定的最佳实践行事时，可能触发法律处罚、财务没收和物质损失。合规也很昂贵，因其耗费大量资源，涉及公司内部多个职能部门，而且缺乏自动化和信息系统之间的整合，导致时间密集和效率低下。最后，合规还很复杂，须对法律法规的深入了解、高度专业化的分析师参与以及与企业领导层的长期接触。这一过程包括规划、评估、后续调查和报告几个步骤，以及与公司、审计员、会计师、市场监管者和国家当局多方沟通。

区块链有可能通过提高运营效率，为监管机构提供增强版执法工具和无缝自动合规解决方案来降低合规风险。在这个方面的应用可以用于如连续审计、企业税务申报和特定的行业报告中。公司和监管机构的传统平台将能够直接从区块链中输入和提取数据，这意味着公司和独立审计报告的数据可以直接部署并存储在区块链中，以供授权参与合规流程的人实时访问。区块链还能整合不同信息系统。在这方面，智能合约技术可以用来协调信息从审计报告到指定报告工具的移动，从而减少错误和重复工作的可能性。

虽然自动化合规已经列入许多公司和监管机构的议程，但其发展仍然存在一些障碍。首先，区块链缺乏对数据的分区访问。为了降低风险，外部用户应只访问对其合规性活动重要的数据。然而，当前的区块链解决方案授权仅提供对整体账本的访问，还无法提供分区访问的能力。在这方面，使用诸如零知识证明和安全多方计算技术的密钥设置可以防止公开任何敏感信息，同时允许其用于合规与规则。其次，自动化与合规的实时节奏相关。然而这可能导致新市场的扭曲，特别是在没有法律或监管先例的投资界。最后，该过程将需要与预先存在的传统平台的整合协作，以实现数据的传输和接收。但使用不同技术的参与方可能无法与区块链层进行交互。

## 缓解外部风险

外部风险由外部事件导致，企业无法控制和可靠预测，因此很难减少由其带来的损失。

版权侵犯。版权侵犯通常造成数十亿美元的损失，主要影响软件、音乐和视频行业。区块链是完全数据中立的，因此可以被用作所有权（作业历史）的注册，跟踪版权作品的所有权链条。想象这样一个案例，唱片公司签署了一份协议，承诺投入营销资金来宣传一位艺术家。在这种情况下，唱片公司面临着艺术家不会走红的风险，其营销资金也就打了水漂。此外，它还承担着被剽窃的风险。如果对音源和音乐视频版权的执行管理没有效果时，就会遭受此类损失。

在这一案例中，区块链能够完全消除侵权风险。目前，有几家公司正在利用这种区块链技术来验证内容的所有权。音乐可以在账本中以独特的ID和时间戳发布，这种方式高效且发布行为不可更改。这可以解决许多人通过流媒体、P2P文件共享等非法渠道毫无约束地下载、复制和修改数字内容的问题。每个记录的元数据都会被储存，信息的所有权和权限是永久且透明的，每个人都可查看和验证。它确保了透明度，使从艺术家、经理到唱片公司的所有参与者，都能够轻松、快速且可共享地访问数据，并因内容的使用获得报酬。

此外，基于区块链的版权和所有权验证系统有可能对更集中化的解决方案做出巨大改进，例如通常由第三方提供的不可否认服务。使用集中式不可否认服务的风险在于，如果服务下线，记录就可能完全丢失。即使企业尝试备份数据库和维护记录可用性，但失去了可信的第三方记录，企业记录的信任度无从考究。虽然在版权处理中，使用区块链仍然面临一些技术挑战，但这并不意味着这个思路本身行不通，版权可比比特的范围要广得多。Blockai、Pixsy、TinEye、Ascribe、Mediachain和Proof of Existence等公司有望在使用区块链技术注册和防止侵犯版权领域有所斩获。他们明白，对于艺术品、资料、手稿、照片和图像等原创作品的分类和存储来说，区块链这样的公开去中心化的账本是非常理想的，能够使其远离任何中央权威。

系统性风险。说到系统性风险，就不得不提及像2008年到2009年的金融危机之后的信贷紧缩这样的全球经济戏剧性衰退。对于大部分公司来说，那是一个无法预测也无法控制的外部事件。全球监管者重塑了金融世界，以避免类似的危机，其战略中很重要的一步是增强了中央对手方（CCP）的角色。CCP是在一项金融交易中插入交易双方中间的一个实体。在双方都同意进行交易之后，CCP就成为对任意买方的卖方和任意卖方的买方。在此过程中，CCP通过结网降低交易对手信用和流动性的风险暴露，减少了当一方违约时交易双方的直接接触的风险，但这么做的风险仍然集中。CCP的主要角色是：1.管理结算运行任务，降低结算风险；2.通过会员身份批准和实行保证金（最初的和变化的）监控个人的信用风险，提供透明的风险管理；3.处理违约方；4.监督市场上的系统风险。

在以区块链为基础管理的金融市场中，许多CCP的原则可能会被淘汰。可以设想的是，CCP的功能1和2将会被智能合约替代。DAOs的设计使交易双方发生关系，一旦植入在智能合约中的某些条款被触及，应收款项就能自动从一方转到另一方。CCP的功能3和4也可以被区块链技术提高，但它不太可能完全实现自动化，因为其对定向性程度和大型场景分析能力要求较高。相关区块链创业公司如Digital Asset Holding和D-Pactum正在与CCP展开合作，在不改变最近法律法规给予CCP的角色基础上，朝着分布式账本和智能合约的

方向重新设计他们的技术。这可能会发展成为增加金融系统复原力的根本性措施。在分布式账本上，可以设计出透明、标准化的交易流程，资本和保证金的相互关系可以自动发生，因此降低了中间管理者的风险负担。通过把各个参与方签订智能合约编码，管理危机事件的规则可以做到尽可能的确定性。

网络风险。这是我们要分析的最后一个外部风险，但并非最不重要。的确，对于网络风险或关键基础设施故障（如控制系统、能源、交通、电信和金融基础设施）相关风险的不理解或不重视，有可能对国家经济、多个经济部门和全球企业造成深远影响。进行风险评估和设置风险管理系统的责任现在落在了每个企业身上，但它们内部实践和流程千差万别，风险管理系统不成熟的小企业在这种情况下更易遭受网络攻击。

区块链是一种可行的解决方案吗？毫无疑问。数字货币的发展延伸了密码学的安全使用，并且创造了一种商业模式，针对网络攻击有了新型的复原力。在分布式账本上的一套完整系统可以提供比公司标准防火墙技术更高级别的网络安全。因为分布式账本是自动化的，并且由于信息共享的原则和共识协议的鲁棒性，账本历史是无所不在且无法更改的。因此在该系统中，高科技网络攻击可以在发生之前被阻止。

本文中我们关注的是因数字货币流行的技术区块链，而非数字货币本身。然而，在分析外部风险的最后，值得注意的是数字货币的出现第一次创造了一种与国家、跨国政府决策或是任何实体经济都不相关的流通货币。实际而言，数字货币价值的波动幅度巨大，但其方向和时间与市场不同，从而保持了与某国货币或股票市场非相关性。因此，比特币被称为“数字黄金”，和黄金一样，数字货币已被用作避险资产，限制宏观经济风险的影响。

总之，在深入挖掘区块链在风险管理方面的惊人效用之前，要明白区块链不是万能解药。它应该被看作是构建下一代风险管理基础设施的众多技术之一。



保罗·塔斯卡是伦敦大学学院区块链技术中心主任，前德国央行首席经济学家。马西莫·莫里尼是意大利联合圣保罗银行Banca IMI公司利率和信用模型总监。





# 区块链+云平台 未来商业新规

刘铮箏|文 时青靖|编辑

区块链的关键价值：

- 1.极大缩短多方交易结算的时间；
- 2.减少因中介产生的各种日常开支；
- 3.减少因篡改和共谋违法产生的风险和危害。

面临的最大问题：

仅靠技术宅的力量远远不够，必须有商业头脑的“伯乐”战略家来领导、研究这一或将重写商业和契约规则的技术。



如今“区块链”这一炙手可热的技术让IBM、英特尔、摩根大通、富国银行等科技巨头和金融机构纷纷慷慨解囊。为什么？如果你对这个名词依然感到陌生，那么不妨想一想比特币。区块链正是比特币等加密网络货币的“幕后奠基人”，目前能找到对它最明白的定义或许是：“通过端到端网络共享的分布式账簿”。这意味着该网络中的每一位参与者能共享账簿中的所有数据，如果要修改任何数据，须经所有参与者同意，而且所有修改都会被永久记录并留在账簿中。

区块链的关键价值有三：1.极大缩短多方交易结算的时间；2.减少因中介产生的各种日常开支；3.减少因篡改和共谋违法产生的风险和危害。区块链这三大价值蕴藏潜力无限，使其可能应用于任何行业。除了金融保险行业这些探索区块链应用的先锋之外，在供应链方面区块链也大有潜力可挖。试想，某飞机制造商如能利用区块链打造管理系统，就可保证计划、设计、组织、交付和维修每一环节所有的信息被忠实记录下来，并分享给所有供应商。同时飞机制造商还能利用区块链系统管理与供应链财务以及交易相关的所有步骤。现在这些步骤都是独立的，造成时间延误，生成了大量成本，中间产生错误的风险也

很高。有了区块链，任何数据无法随意被篡改；敏感信息得到有效监控；时间、成本和精度都将大幅改善，甚至可在几秒之内完成交易。

在过去20余年里，互联网为商业的方方面面带来变革，极大提高了组织和个人的效率，然而交易的基本机制始终没有改变，区块链带来的透明和效率，或将颠覆交易本质，也让很多互联网巨头看到了新契机。

互联网带来的网络效应与建立平台成本的降低，让平台经济大行其道，很多在位企业也纷纷跳上这条大船，精心管理平台成员带来的资源，不断扩展生态系统，力求最大化平台价值。IBM就是一例。在今年2月召开的IBM InterConnect创新应用大会上，这家百年老店宣布了一系列重大云平台战略转型举措，其中就包括对区块链的重点投入。由于区块链的技术开发尚处于萌芽阶段，利用IBM搭建的云平台Bluemix，对区块链感兴趣的开发者和公司无须巨额投入，就能在云端对区块链进行各种探索、实践和测试。

根据IBM院士、区块链业务副总裁Jerry Cuomo介绍，云是颠覆性的创新平台，能够加速开发并降低成本。尤其是结合公有云与私有云两者之长的混合云模式，将成为未来应用最广的云战略，企业无须重写编码，就能充分利用现有IT技术在云平台上创造新概念，为创新过程节约宝贵的时间和金钱。

今年2月，IBM与摩根大通和思科等企业一起加入了Linux 基金会的开源超级账簿项目（Hyperledger Project），并贡献了超过44000行代码投入开发开源区块链服务。该项目旨在探索的区块链的应用没有止于贸易贷款等金融体系，还包括体育游戏、假药侦测、连接物联网以及音乐出版等各行各业的可能性。

在比特币的例子中，任何人都可以参与“挖矿”过程，生成这类虚拟货币。但这种完全开放式的区块链并不适合区块链的商业应用。比如在金融服务业，法规以及数据隐私是大多数区块链应用的主要障碍。将区块链放在云端的安全性是很多公司的担忧之一。为解决这一忧虑，IBM倡导的“许可制区块链（permissioned blockchain）”，利用数字技术颁发许可邀请，在平台上实名添加区块链成员。这样做，能让区块链技术专注于法治行业、保障隐私和可追责性、注重保密和合规，顺应商业应用的需求。

区块链面临的最大问题是什么？从商业角度来看，就是不能仅仅把区块链当作一种技术。技术宅的力量还远远不够“拯救世界”，必须有商业头脑的“伯乐”战略家来领导、研究这一或将重写商业和契约规则的技术。但要是想提高区块链成功的几率，找到对的技术伙伴也不可或缺。



刘铮箏是《哈佛商业评论》中文版高级编译。



# 区块链改造电子健康档案的潜力

约翰·D·哈拉姆卡 安德鲁·李普曼 阿里尔·埃克布劳 | 文

如何和更多的利益相关者分享更多医疗数据，以实现更多目的，同时又确保数据完整和保护病患隐私，这是世界范围内各类卫生保健系统都面临的让人十分恼火的问题。

传统上，机构之间相互分享和操作医疗数据，一般遵循3个模式：推（push）、拉（pull）和看（view）（下面会有详细讨论），这三种模式都有其自身的优缺点。区块链提供了第四种模式，这种模式有能力确保，卫生保健机构可以安全地分享终身病历档案。

医疗信息的有效负载从一个机构被发往另一个机构，这种模式称为“推（push）”。在美国，有一种名为Direct的安全电邮标准，为发送者（如急诊室医师）和接收者（如个人基础保健医生）提供加密传输。尽管，在过去，卫生保健机构一直采用此模式，但是此模式有一个问题，即它预先假定正常运作的基础设施已经就绪，比如有一家为整个社区服务的电子设备供应商，同时业已制定了一套法律协议，允许数据的广泛分享。推模式是仅适用于两个涉事方的传输模式，不能有任何第三方。如果你最后又被转移至另一家医院，那么新的医院可能无法获取你的医疗数据，因为这些数据此前就已经推送至最初那家转诊医院了。从数据生成到数据使用那一刻，都没有办法担保数据的完整性，因为推模式一开始就假定了，发送系统能够生成准确的有效负载，而接收系统能够准确地摄取此有效负载，此间没有任何标准化的审计追踪。

一家卫生保健机构能够向另一家机构问询信息，此模式称为“拉（pull）”。比如，你的心脏病专家能够从你的初级保健医生那里获得信息。在拉模式中，所有的同意和许可都是非正式的、临时的，而且此间没有任何标准化的审计追踪。

一家机构能够查阅另一家机构档案里的数据，此模式称为“看（view）”。比如，一位外科医师在手术室中能看查阅你此前在紧急护理中心拍的X光片。此模式的安全体系是临时的，没有标准化的审计追踪，而且，未必会基于一段现存的患者-机构关系。

所有这些模式，技术上是可行的，但是围绕它们的政策需要受制于制度变化、地区实践、各州法律，以及美国全国范围内严格执行的隐私政策。

区块链则是一个完全不同的构造，提供普遍适用的加密工具，能够取保数据完整性和采用标准化审计，使数据访问的“契约”正式化。

区块链最初被构想为金融交易的账本。每一家金融机构都创建一份包含所有存取款记录的加密清单。区块链采用公钥（**public key**）加密技术，以创造一条只可增补（**append-only**）、永恒不变（**immutable**）、附带时间标记（**time-stamped**）的内容链。区块链的副本会分发到网络中每一个参与节点上。

如今，人们企图人工协调诊所、医院、实验室、制药厂和保险公司之间的医疗数据。这效果不佳，因为找不到一份统一所有涉事方数据的清单，或者一份表明数据访问次序的清单。我们或许知道所有开过的药，但是对于病患当前到底在服用何种药物，则可能无从知晓。再者，尽管比起以往，目前的数据标准进步很大，但是，每一份电子健康档案都采用了不同的工作流进行数据储存，因此，到底是谁在什么时候记录了什么，我们都无法弄清楚。

试想，如果每一份电子健康档案（**EHR**）都把有关药物、问题和过敏清单的信息更新，发送到一个信得过的、开源的、覆盖整个社区的账目中，这样，各个机构就能对医疗档案增减的内容有较为清晰的了解，能够进行审计。**EHR**不仅仅在单一数据库中显示数据，它能够在每一个受账目信任的数据库中显示数据。最后的结果十分优异，有关你的信息能够在整个社区中得到较为完美的协调，从数据生成那一刻到数据调用那一刻，都能保证数据的完整性，且不会有人为干涉。

我在MIT媒体实验室和以色列贝斯女执事医疗中心的同事，测试了该理念在药物方面的功效，证明了此模式确切可行。在我们的白皮书《关于区块链的案例研究》中，我们提议建立一个新颖的、去中心化的档案管理系统，利用区块链技术处理**EHR**。此系统我们命名为**MedRec**。

**MedRec**不会存储健康记录，或要求改变实践方法。实际上，**MedRec**在区块链上储存健康记录的数字签名并通知患者，而该患者最终控制该记录的去向。此标志确保了，一份不可改变的档案副本必须存在。此系统还把控制源从机构那儿，交还到病患手上，这样病患就能够掌握档案的管理了。一些病患也许不想要管理自己的数据，对于他们而言，我想，服务组织将会演化成病患的代表，负责管理他们的数据。此项目和理念面临一个挑战，即打造这样一个界面，能够让顾客认为此责任是可接受的。目前人们使用的大多数个体病患门户都有着累赘复杂的设计，催生了许多不必要的工作，而且，每一家机构都有不同的用户界面。日后部署的**MedRec**系统将拥有这样的用户界面：连接多家机构，简化病患与医疗记录的交互方式。

下一步，我们计划投入更多数据类型，招募更多数据贡献者，以及更多的数据使用者，从而增强**MedRec**试行项目。我们还将考虑现存区块链项目以外的革新的选择，比如



Silvio Micali's Algorand公共账目；和其他模式相比，此模式所需的计算能力要更低一些。

考虑在电子卫生保健档案中应用区块链的基本理论有两个方面。首先，其避免了在病患和档案之间再加入一个组织。对于数据而言，此不是什么新型的数据交换中心，或“保险箱”。区块链代表了一种去中心化的控制机制，在此机制下，所有人都是利益相关者，但是没有一个人能够独占这些信息。这是一次结构上的变革，概括了以往的医疗记录。第二，它充分考虑了含带时间标示的、可编程的账目。这无需为每一个位EHR拥有者设计定制功能，同时还能智能地管理档案访问。而且，此账本本来就包含了审计追踪。

我们所有人都可以希望这样一个结果：区块链能够继续在一家无私的、非营利的大学中发展，这样，此理念才能够在为了商业目的进行专门优化前，真正的成长起来。卫生保健用区块链还处于生命初期阶段，但是，和此前的模式相比，它更有可能以不那么累赘的方式，让安全数据交换标准化。（译言网网友ChaRIIEHeatHadJaNI|译）



约翰·D·哈拉姆卡医学博士，是以色列贝斯女执事医疗中心的首席信息主管。

安德鲁·李普曼是麻省理工学院媒体实验室的高级研究科学家。

阿里尔·埃克布劳是麻省理工学院媒体实验室的研究生。



# 共享经济时代，区块链能干吗？

普里马韦拉·德·菲莉比 | 文

**纵**观当今如谷歌、脸书、推特、优步和爱彼迎等互联网巨头的运作方式，你会发现他们都有一个共性，那就是在他们自己的平台上依靠用户的贡献来产生价值。20多年来，经济已经渐渐地从传统的集权公司脱离出来了。集权下的大公司常常因为拥有主导地位为大批被动型的消费者提供服务。如今，我们逐渐进入了一种新型的分权制组织，一些大公司通过聚集众多人的资源为更多积极的用户提供服务。这种转变标志着一种新的“非物质化的”公司诞生，这种公司不需要物质化的办公室、财产甚至员工。

在大多数情况下，这种模式是由大批的人去创造价值，而产生的价值不必再次平分给贡献价值的人，所有的利润全部由操作平台的公司所得。

最近出现了一种新的技术，它将改变这种不平衡的做法。数据区块链的产生为改变这种不平衡价值提供了方便，它采用一种安全、分散的方式运行，不需要中间人。

数据区块链最大的创新方面是，它能用安全和分散的方式运行软件。有了数据区块链，一些软件的应用程序便不再需要安装在集中的服务器上：他们可以在点对点的网络上运行，而不会被任何一方控制，这些基于区块链应用程序可以用来协调很多个体的操作，这些个体不需要第三方的帮助可以自我组织。区块链技术最终目的就是用安全和分散的方式让个体能整合他们日常的活动，直接与其他人进行互动。

如今已经有相当多的应用程序安装在区块链上，比如 Akasha、Steem.io 和 Synereo 等公司都是分布式社交网络平台，它们像 Facebook 一样没有中央平台。它们不是依靠集权型组织来管理网络，规定哪部分内容应该向公众开放（经常通过专门的计数法筛选哪些不能公布），而是通过一系列安装在区块链上以代码为基础的规则以非集中的形式将不同的对等团体的工作聚集起来，自我协调，唯一又独立。用户必须支付微量费用才可以在网络上发表信息，这些费用将用来支付给那些维护和运营网络的工作人员。发布者因为他的信息在网络上传播，也可能会得到那些费用（加上额外的报酬）和得到其他人积极的评价。

类似，OpenBazaar 公司也是一个分布式的市场，很像易趣网和亚马逊，但是它的操作不受任何中间商的影响。这一平台依靠区块链技术确保买家和卖家能彼此直接互动，不需要通过集权制的中间人。任何人都可以在此平台上免费注册发布产品，所有上网的用户能够看到。一旦有买家中意，建立在比特币区块链的第三方账户会要求三方中的两方（卖

方、买方和虚拟的第三方仲裁人）同意支付资金（也就是所谓的三方签名账户）。一旦买方支付完钱，卖方则负责发货，买家收到货物后便在第三方账户上支付资金。买家和卖家之间有一项事情确定系统需要第三方（如，一个随机选中的仲裁者）的加入来决定是否把钱给了卖家，或者是否把钱还给了买家。

也有一些分布式的拼车平台，如Lazooz和ArcadeCity，它们的操作形式有点像优步公司，但没有一个集中的操作方。这些平台仅仅通过安装在以区块链为基础的基础设施上的代码来进行管理，这种设计是把推动者和用户间进行点对点互动。这些平台依赖区块链来奖励对平台做出贡献的司机，他们使用特殊设计的令牌来代表平台上的份额。对平台作出贡献越多的推动者，他们将从这个平台得到更多的利润，在管理方面的影响也就越大。

所以一种新的组织形式出现的区块链技术不仅是“非物质化的”，而且还是“去中心化”的。这些公司可以没有总裁，CEO，甚至没有任何形式的等级制度，管理上都是在网上互动的个体在共同管理。同样更重要的是不会后传统模式下的“群众外包”的方式迷惑他们。在平台上运作的个体不会因为平台的成功而获利。区块链技术可以支持更多合作形式的群众外包，有时更倾向于“合作型平台”。用户在注册的平台上既是贡献者也是股东。由于没有中间人，产生的价值也会更公平地重新分配给创造价值的人。

随着新型的“合作化”产生的新机会，我们正慢慢进入真正的共享经济或者说合作经济，这种经济不会被一些大型中间商控制，它只会被个体管理，为个体服务。

你可能会说这没什么稀奇，以前我们不是曾听说过这样的承诺吗？互联网的发展不就是为了个体和小公司提供平台来对抗大公司的吗？是的，然而随着时间的推移，由于大公司组织并控制了我们的数字愿望，大部分的承诺和早期互联网的梦想已经消失殆尽。

如今，我们有了新的机会再次来实现这些承诺。区块链技术让用分布式的、自下而上的合作方式取代以前自上而下的等级公司成为可能。这种改变首先从财富分配方式开始，它可以使每个人能因为一个普通的物品合作创造价值，从而保证每个人都能因为他们的努力和贡献充分的得到报酬。

然而没有什么事情是想当然的。正如互联网一开始从一个高度分散的基础设施发展成了逐渐被几个网上的大公司操控的集中系统一样。在区块链这里也存在着最终会被大公司操控的风险。我们已经失去了我们可以利用的第一个互联网的机会。作为社会的一份子如果我们能在真正的共享经济概念下创造价值，那么我们所有人理应参与、体验这个新出现的技术，去探寻新的机会，同时部署大型、成功、全民参与的应用程序，以共同对抗区块链巨头的产生。（译言网网友阿丫丫|译 王婷|编校）

普里马韦拉·德·菲莉比是巴黎法国科学研究中心（CNRS）的固定研究员。她是哈佛大学法学院她是哈



佛大学法学院伯克曼互联网与社会中心的教师助理。



# 区块链将会帮助证明“我是我”

迈克尔·梅内里 | 文

“你是谁？”也许是世界上问得最多的问题了。在网站上、夜店里、机场中，或银行柜台前，所有人都希望我们能证明自己就是声称的那个人。

目前，世界范围内有24亿贫困人口，其中15亿已超过14岁，但是他们的回答仍然无法令权威机构满意。尽管他们肯定知道自己是谁，然而他们很多时候都无法享有财产所有权、自由迁移和社会保护，仅仅只是因为他们无法证明自己的身份。比起其他人，他们更容易成为腐败和犯罪的受害者，包括人口贩卖和奴隶。（联合国有远见地计划改变此情况，其出台了联合国可持续发展目标，第16个，和平、正义和强有力机构，旨在“于2030年前，为所有人提供合法身份，包括出生登记。”）

全球化和不断增长的人口带来巨大压力，使我们无法找到廉价高效的方案去证明身份。最近生物识别技术的发展，包括虹膜扫描、DNA分析和语音模式识别，对于固定我们的身份，可能会扮演重要角色，但是，身份不一定是一成不变的。我们的身份是我们过去行为的记录，而且它们随着时间不断改变。再者，我们的身份也取决于谁在进行身份识别工作。比如，税务局十有八九对你的成绩单不感兴趣，但是可能极度在意你成年后在国外度过的日子。

不论穷富，身份证明都是个问题。对于富人而言，反洗钱方面的法规、“了解你的客户”制度，和最终实益所有权都增加了法律和监管成本，让事情变得麻烦。在国际商会2016年所开展的全球贸易融资调查中，有90%的企业认为反洗钱是贸易最重要的障碍。

对于穷人而言，著名秘鲁经济学家Hernando de Soto（因其在非正规经济方面的贡献）观察得出：“缺乏完整的正轨产权制度，现代市场经济是不可想象的。”因此，缺乏正确的身份验证，现代市场经济是无法想象的，因为缺乏经过验证的财产权持有人。

尽管富人的麻烦和“无身份证明”穷人的日常性麻烦完全不一样，但是解决他们问题的方法可能是相同的：互通分布式账本（mutual distributed ledgers, MDLs），这是一项区块链技术。MDLs是不可改变的登记本，允许各群体在一个分布式计算器系统的网络中，去验证、记录和追踪交易。网络中的计算器遵循一套共有的协议，允许个体添加新交易信息和利用点对点结构发放这些信息。MDLs是跨组织的数据库，含带超级清晰的审核追踪。集中式数据库会自然地导致垄断，使得每个人不得不使用此数据库，但是MDLs是互

通的，即共有的，这意味着它们无法像自然式垄断一般被利用。我复制了一份账本，但是你不能收我钱，因为此账本的拥有人不是你。没有任何人拥有此账本。

在MDLs出现了20年后，人们大多会问这个问题：“那火爆的软件是什么？”自从比特币于2009年发布以来，答案很简单，且某种意义上说是不可靠的，那便是：加密货币。比特币自身也经历了大起大落。比特币社区所秉持自由主义“新货币”理念，和其高价格波动幅度，引发了较大的经济争议。比特币也同样搅动了社会上的争议，因为，有传闻说，不法分子使用比特币来进行毒品和枪支交易，这样的言论无疑引来执法机构的关注。不过，此种分散式加密货币以及其背后的MDL技术都有不错的成效，一些监管机构很不情愿地允许金融机构使用它。

目前，一项运用MDL技术的、更为根本的火爆应用正在兴起，这款应用能够安全地储存和传送含带数字签名的文件，并且进行审计跟踪。这些不可改变的文档交互网络在贸易金融、运输和保险业逐渐兴起，在这些行业中，人们都有一个大问题，那就是验证其他人和资产的身份。身份文件交换通常包含三方：（1）主体，即个体或资产，（2）认证者，通常是对文档进行公证的组织，例如政府机构、会计公司，或信用调查机构，以及（3）检查者，即审查机构，对主体开展“了解你的客户”或反洗钱（KYC/AML）行动。

MDLs通常分为两类：一类是内容账本，内含个人的加密文档，另一类是交易账本，内含加密密钥，能够访问一系列“密钥圈（key rings）”。这些密钥圈是一些文件夹，里面有身份、健康或学历等文档。主体能够准许身份验证人去在主体的密钥圈里放置已经进行了数字认证的文档。比如，一家法律公司或许会向主体提供含带数字签名的文档副本，供他们留着和使用。政府或许会给我们提供含带数字签名的驾照副本。认证人往后再也无法获取这些数据，但是检查者依赖这些可信的第三方机构认证过的数据，正如公证人给实体文档进行公证一样。

主体向检查者提供自己掌握的密钥，而检查者需使用智能合同，搭配这些密钥，进而检阅相关文件。智能合同是记录在MDL上的代码片段。此网络能够限制检查的数量，和安排时间，而且会为主体记录它们。根据已编写入MDL的权限框架，银行、保险公司或政府等第三方能够获得权限，访问这些文件。而商业认证机构，比如会计、律师或公证人可能会向检查机构提供保障服务（如保险有效期），收取一些费用。

引人注目的是，从2007年开始，爱沙尼亚便已利用区块链运作一项覆盖全国的数字身份计划。所有关于个体的政府数据都储存在一个分布式账本上，个体对此拥有控制权，且能够传送给他人。这个数字身份系统减少社会的文书工作，因为其采用的是数字签名技术。这项计划十分奏效，乃至欧洲其他地方的人也使用此计划来储存自己的个人数字签



名。

无论是高净值客户，亦或是低净值客户都指望找到合乎情理的、廉价的、通用全球的方式，去证明他们的身份，无论是用于支付、信用、政府记录，还是健康档案、学历。从理论上而言，MDL技术十分适用于不可改变的身份文档交互网络，而且已有许多项目旨在实现它们的潜力。赋权个体去储存、更新和管理自身的数据，包括行使他们“被遗忘”的权力，即取消他们的密钥，这看上去非常清晰。

在今天，证明你的身份非常昂贵。每一项身份文档的认证都需要花费大量时间，还涉及技术含量较低的文书工作。对于花了大价钱验证的身份文档，人们希望其有更多的用途。那么，其中一个方法就是增加使用数量。比如，在爱沙尼亚，银行意识到，账户权限既能够与国民身份证绑定，也能够和银行卡绑定。多用途身份证的发展会转而促进少数具有竞争力的全球体系的发展。

但这并不是万应灵药。围绕不可改变身份账目的终极问题是：对于人类而言，它最终会是生活必需品，还是变成负担？这样一种永远不丢失数据的账本，可能从根本上改变人们对待社会、隐私和安全的方式。官僚过失，譬如输错的名字，就能够得到解决，但是，这样的过失永不可能遗忘。行为会变，而且社会习俗也会随之而变。比如，当其他人看到我们自己有还未还清的罚款或过失行为时，我们可能会更能容忍他人的过去。或许，对于重要的事情如学历造假，我们会更严厉，而对于不那么重要的事情，如少数成绩较平庸的学科，我们则更加宽容。

想想永恒的遗产。如果我们的遗产是不能消除的，那么我们行动时会更为负责。比如，我们或许会选择使用智慧健康合同，一旦我们离世，合同就会把我们的健康数据捐赠给研究项目。如果我们的身份永恒的刻在不可改变的石头上，那么“请不要忘了我”可能成为更加经久不衰的曲子，余音绕梁，其影响远比我们想象的要持久。（译言网网友

ChaRIIEHeatHadJaNI|译 王婷|编校）



迈克尔·梅内里是Z/Yen Group的执行主席。Z/Yen从1995年开始，就已经从事MDLs方面的工作，创建了IDchainZ身份文档系统。他与伊恩·哈里斯合著《The Price of Fish: A New Approach to Wicked Economics and Better Decisions》一书，获得2012年的独立出版人金融、投资、经济学金奖。



---

## 哈佛商业评论 增刊：关于区块链，你不得不知的真相

### 《哈佛商业评论》出版集团

Harvard Business Review Group, [www.hbr.org](http://www.hbr.org)

总编辑 Editor-in-Chief

Adi Ignatius

### 《财经》·《哈佛商业评论》中文版

Harvard Business Review Chinese Edition, [hbrchina.org](http://hbrchina.org)

总编辑 Editor-in-Chief

王波明 Wang Boming

主管：中国证券市场研究设计中心

主办：中国证券市场研究设计中心

### 编辑委员会 Members of Editorial Board

戴小京 于颖 何刚 法满 靳丽萍 杨浪 齐馨

Dai Xiaojing, Yu Ying, He Gang, Fa Man, Jin Liping, Yang Lang, Qi Xin

---

主编 Editor

何刚 He Gang

副主编 Executive Editors

齐馨 Qi Xin 钮键军 Niu Jianjun

助理主编 Assistant Editors

李全伟 Li Quanwei 李剑 Li Jian

编辑总监 Editorial Director

李源 Li Yuan

高级编辑 Senior Editors

时青靖 Shi Qingjing 万艳 Wan Yan

高级编译 Senior Articles Editors

王晨 Wang Chen 刘铮铮 Liu Zhengzheng 刘筱薇 Liu Xiaowei

高级新媒体编辑 Senior Digital Editor

腾跃 Teng Yue

编译 Articles Editor

蒋荟蓉 Jiang Huirong  
撰稿 Writer  
廖琦菁 Liao Qijing  
新媒体编辑 Digital Editors  
齐菁 Qi Jing 周强 Zhou Qiang 王婷 Wang Ting  
驻上海高级编辑 Senior Editor (Shanghai)  
王晓红 Wendy Wang  
驻伦敦高级编辑 Senior Editor (London)  
牛文静 Niu Wenjing  
高级创意编辑 Senior Creative Designer  
崔晓晋 Cui Xiaojin  
特约设计师 Freelance Designer  
瞿中华 Qu Zhonghua  
流程编辑 Flow Editor  
苏然 Su Ran  
人事行政总监 HR Administration Director  
郝晶 Hao Jing  
总经理 General Manager  
刘霄 Liu Xiao  
执行总经理 Executive General Manager  
张瑾 Zhang Jin  
执行副总兼商业合作总监 Executive Vp & Director of Business Cooperation  
李一品 Yolanda Li  
执行副总经理兼品牌总监 Executive VP & Branding Director  
赵阁宁 Zhao Gening  
总经理助理 Assistant General Manager  
张菁 Zhang Jing  
发行总监 Distribution Director  
高云竹 Gao Yunzhu  
华东区市场部总经理 General Marketing Manager in East China  
杨志清 Yang Zhiqing  
华东区商业合作部总经理 General Manager of Business Cooperation Department of East China  
徐礼智 Damon Xu  
市场总监 Marketing Director  
王欢 Wang Huan  
副总监 Deputy Directors  
叶海虹 Ye Haihong 李淳 Li Chun  
高级经理 Senior Manager

刘浩宁 Liu Haoning  
高级品牌经理 Senior Branding Managers  
陈萌萌 Chen Mengmeng 张超 Zhang Chao  
王文睿 Lea Wang  
品牌经理 Branding Manager  
杨潇 Yang Xiao 杨逸雯 Yang Yiwen  
市场专员兼行政助理 Marketing Executive  
崔哲 Cui Zhe  
新媒体产品总监 Managing Product Director  
于慧媛 Yu Huiyuan 魏永 Wei Yong  
内容编辑 Editors  
姜维敏 Jiang Weimin 张亮惠 Zhang Lianghui  
贾苗苗 Jia Miaomiao 刘岩 Liu Yan  
高级开发工程师 Senior Development Engineers  
汪元豪 Wang Yuanhao  
开发工程师 Development Engineer  
庞超 Pang Chao 杨小 Yang Xiao  
邹志鹏 Zou Zhipeng 付常乐 Fu Changle  
产品经理 Product Manager  
初飞 Chu Fei  
设计主管 Design Director  
黄朝 Huang Chao  
设计师 Designers  
程爽 Cheng Shuang



#### 版权声明：

本刊主要内容是哈佛商业出版集团授权独家使用《哈佛商业评论》（Harvard Business Review, HBR）的简体中文版，其他内容来自《哈佛商业评论》中文版团队采写或编辑，未经许可，不得转载或摘抄。

Copyright Notice: Harvard Business School Publishing Corporation exclusively authorizes this publication as simplified Chinese Version of Harvard Business Review (Hereinafter referred to as HBR). Part of the content in this publication is created and edited by editorial team of HBRChina. All rights reserved. Without Consent, no part of this publication may be reproduced or transmitted in any form or by any means.

邮发代号 80-387

客户服务热线 400 009 0313

国内外统一刊号

ISSN1671-4725

CN11-4568

地址：北京市朝阳区朝外大街22号泛利大厦19层

编辑部联系电话：00-86-10-85657511

发行部联系电话：00-86-10-85650323

邮编：100020

广告部联系电话：00-86-10-85657236

电子信箱：hbrchinese@caijing.com.cn

## 版权信息

关于区块链，你不得不知的真相（《哈佛商业评论》增刊）

《哈佛商业评论》中文版 出品

©浙江出版集团数字传媒有限公司 2018

非经书面授权，不得在任何地区以任何方式反编译、翻印、仿制或节录本书文字或图表。

DNA-BN: ECFP-N00009848-20170330

制作：贺立川

出版：浙江出版集团数字传媒有限公司

浙江 杭州 体育场路347号

互联网出版许可证：新出网证（浙）字10号

电子邮箱：cb@bookdna.cn

网 址：www.bookdna.cn

BookDNA是浙江出版联合集团旗下电子书出版机构，为作者提供电子书出版服务。

如您发现本书内容错讹，敬请指正，以便新版修订。

©Zhejiang Publishing United Group Digital Media CO.,LTD,2017

No.347 Tiyuchang Road, Hangzhou 310006 P.R.C.

cb@bookdna.cn

www.bookdna.cn

# The End



浙江出版联合集团旗下电子书出版机构

<http://www.bookdna.cn>

新浪微博: [@BookDNA本唐在线出版](#)

微信公众号: 本唐在线出版



如您发现本书内容错讹, 敬请发送邮件至 [cb@bookdna.cn](mailto:cb@bookdna.cn) 指正。

成为作者，只需一步  
To be an author, just one click.

[BookDNA.cn](http://BookDNA.cn)