

# 人工智能 时代

马兆林◎著

## 一本书读懂 区块链 金融

人类未来十年影响最大的黑科技

- 区块链的由来与发展
- 区块链背后的经济思想
- 区块链的技术原理与特征
- 区块链的应用前景

**对区块链的展望与畅想**  
引领读者走近了解并读懂区块链的世界



中国工信出版集团



人民邮电出版社  
POSTS & TELECOM PRESS

互联网+时代 企业管理实战系列

人工智能时代 一本书读懂区块链金融

马兆林◎著

人民邮电出版社

北京

图书在版编目 (CIP) 数据

人工智能时代, 一本书读懂区块链金融/马兆林著.--北京: 人民邮电出版社, 2017.4  
(互联网+时代企业管理实战系列)

ISBN 978-7-115-45029-6

I.①人... II.①马... III.①电子商务—支付方式—研究 IV.①F713.361.3

中国版本图书馆CIP数据核字 (2017) 第034681号

◆著 马兆林

责任编辑 赵娟

责任印制 彭志环

◆人民邮电出版社出版发行 北京市丰台区成寿寺路11号

邮编 100164 电子邮件 315@ptpress.com.cn

网址 <http://www.ptpress.com.cn>

北京隆昌伟业印刷有限公司印刷

◆开本: 700×1000 1/16

印张: 12 2017年4月第1版

字数: 176千字 2017年4月北京第1次印刷

定价: 49.80元

读者服务热线: (010)81055488 印装质量热线: (010)81055316

反盗版热线: (010)81055315

# 目录

[封面](#)

[扉页](#)

[版权信息](#)

[内容简介](#)

[前言](#)

[第一章 解密区块链，你所不知道的神秘区块链](#)

[自带比特币基因](#)

[区块链的3个进阶阶段](#)

[区块链的4种技术创新](#)

[区块链如何运作](#)

[区块链的技术挑战](#)

[区块链将颠覆我们的世界](#)

[第二章 人工智能时代，区块链带来金融科技的新蓝图](#)

[区块链重构金融业](#)

[互联网金融VS区块链金融](#)

[区块链助力共享金融的实现](#)

[区块链变革金融服务的基础设施](#)

[第三章 人工智能时代，区块链与金融大数据](#)

[“区块链+大数据”创造数据神话](#)

[大数据时代区块链再造信任体系](#)

[“区块链+大数据”破解传统风控难题](#)

[第四章 人工智能时代，区块链构建金融信用长城](#)

[从数字货币到信任社会](#)

[开启全新的金融信任时代](#)

[区块链技术构建金融信用生态圈](#)

[区块链构建银行业客户信用体系](#)

[第五章 人工智能时代，区块链金融的六大应用场景](#)

[数字货币](#)

[跨境支付与结算](#)

[数字票据](#)

[银行征信](#)

[有价证券交易](#)

[股权众筹](#)

[第六章 人工智能时代，区块链在数字金融资产中的应用](#)

[区块链在银行业的应用](#)

[区块链在保险业的应用](#)

[区块链在资产托管中的应用](#)

[区块链在信用借贷中的应用](#)

[第七章 人工智能时代，金融行业区块链的落地策略](#)

[各大金融机构争相逐鹿区块链](#)

[IBM与中国银联探索区块链技术落地应用](#)

[商业银行对区块链技术发展的应对策略](#)

[第八章 人工智能时代，金融业扛旗者走在区块链金融最前端](#)

[银行系：从担忧到拥抱](#)

[传统IT和新兴互联网企业：积极拥抱区块链](#)

[专项投资机构：翘首以盼](#)

## [第九章 人工智能时代，区块链让金融监管简单化、智能化](#)

[区块链技术对金融监管提出了新挑战](#)

[区块链改写P2P网贷监管格局](#)

[区块链让金融法制的执行走向智能化](#)

[区块链有效解决金融监管排斥问题](#)

## [第十章 区块链金融，金融创新的下一个风口](#)

[区块链成金融支付的下一个“爆破点”](#)

[区块链开启人工智能金融2.0时代](#)

[未来互联网金融环境基于区块链技术的蜕变](#)

[区块链加速实现普惠金融](#)

## 内容简介

本书从解读神秘区块链入手，详细阐述区块链与金融大数据之间千丝万缕的联系，逐渐引入区块链金融，深入介绍在当前的金融领域中，区块链如何构建金融信用长城，如何在金融的六大场景中和数字金融资产中应用，以及在金融行业中的落地策略，探讨金融业扛旗者如何走在区块链金融最前端，如何使得金融监管实现简单化，并且在最后画龙点睛地说明区块链是未来金融创新的下一个风口。

本书能够为金融机构、互联网金融企业以及互联网企业在区块链金融领域的开发提供一定的参考和借鉴，适合银行、保险、证券、资管、基金公司等金融机构管理人员，电商、贸易公司等互联网企业，关注本技术领域内投资的投资机构及投资人、准备进入区块链的技术人员，以及对区块链技术感兴趣的读者阅读。

## 前言

进入2015年，全球范围内掀起了一场投资金融科技的热潮，区块链受到了全球各界的追捧。2016年可以看作区块链元年，区块链已经成为人们茶余饭后的谈资，并且在各个领域中的应用也势不可当。然而，由于区块链技术最早诞生的产物是数字货币——比特币，是比特币的底层技术，是与比特币相生相伴的，因此，这就注定了区块链技术会最早给金融产业带来巨大变革。

当前，区块链已经受到了各界人士的广泛热议，既然区块链的发展如火如荼，尤其是在金融领域的影响最为深刻，那么究竟什么是区块链呢？相信对于绝大多数人来讲，较区块链，比特币更为人们熟知。而区块链是比特币的一项关键的底层技术，也是在比特币方面应用最为成功的新兴技术。区块链技术是点对点通信技术、分布式账本、共识机制、智能合约和加密技术的结合体。从本质上来讲，区块链是一种由不同的节点共同参与的分布式数据库，是一个开放式的总的公共账簿，具有不可篡改、不可伪造、公开透明、去中心化、去信任、安全可靠、匿名的特点。正是由于这些特点，使得作为比特币底层技术的区块链成为了“明星”，各个领域，尤其是传统金融机构更加希望借助区块链技术赶超互联网金融，由此将区块链作为一个新风口。

信用是金融活动的根基。具体到金融行业，区块链在金融业的所有场景中的应用都离不开“信用”这柄利器，区块链则可以有效解决金融活动中的信任问题。在传统模式下，金融领域进行一切活动都由作为信用机构的第三方来进行监管，包括证券发行与交易、资金托管、保险、信用借贷、跨境支付与清算等方面，而这些都是由于传统金融模式下的信息不对称造成的。这也正是长期以来信任问题难以有效解决的关键之处，也是公信力机构能够如雨后春笋般蓬勃发展的根本原因。如今，区块链给我们创造了一个可以用“共信力”来解决公信力问题的途径。

就当前金融业的发展情况来看，互联网科技和金融技术的进一步融合亟待加强。以金融领域的老牌军——银行来讲，就急需将自身业务逐渐实现数字化、智能化，从而更好地推动业务创新，以科学改进业务，以科技推动创新。区块链可以提供更好的解决方案，加快业务创新的速度和成效，进而更好地服务于客户。基于这一点，区块链可以更好地推动共享金融、普惠金融的实现。

也正是因为看到了区块链在推动金融创新发展的巨大优势，全球各个大中小型银行纷纷争相布局区块链，以期在激烈的市场竞争中拔得头筹，其中不乏全球知名大型银行，如花旗银行、国富银行、摩根大通银行、法国巴黎银行、加拿大帝国商业银行、德国商业银行、德意志银行以及我国的交通银行、平安银行、民生银行等，都纷纷加入R3区块链联盟。

同时，一些互联网排头军也积极与金融机构加强合作，在区块链应用方面进行了诸多创新。我国也不甘示弱，先后成立了中国分布式总账基础协议联盟、中国区块链研究联盟、金联盟，不少金融机构和互联网知名企业参与其中，互联网巨头BAT就是典型代表，通过积极拥抱区块链，与区块链擦出了不一样的“火花”。

虽然，当前区块链在各个领域中的应用处于初级的探索和实验研究阶段，但是各领域对区块链的应用热情十分高涨，金融领域更是如此。在2015年世界经济论坛上发布的一篇关于科技深入影响未来社会的报告中提到，58%的专家学者认为：“在2025年，10%的全球生产总值将来自于区块链技术的运用，而在今天区块链技术带来的生产总值占比仅为0.025%。”

互联网企业是基于互联网发展的，而区块链技术的本质就是价值互联网的核心，是区块链让传统的传递信息的互联网转变为了价值互联网，这是一种进化，也是一种创新。区

区块链技术出现之前，我们并不真正知道互联网将如何改变未来。区块链技术出现之后，我们才可以说，互联网将深刻改变现在，进而影响未来，推动人类社会向更公正、平等的美好时代前进。其中，当然包含金融业的未来。正如当初互联网的成长和发展一样，区块链当前仍在持续地寻找一个落地方式来证明自己是可行且具有强大能量的，可以改变工业、技术、金融，尤其推进人工智能时代的实现，为世界带来开创式变化。

未来已至，区块链金融的发展前景不可估量。相信本书能够为金融机构、互联网金融企业以及互联网企业在区块链金融领域的开发提供一定的参考和借鉴。



## 第一章 解密区块链，你所不知道的神秘区块链



当前，区块链在全球范围内异常火爆，越来越多的领域开始尝试通过区块链技术来发展自己的业务，提升市场竞争力。区块链正以加快交易并减少开支、降低欺诈风险等功能带来的高透明性、高安全性以及去中心化、不可篡改等优势，让全球各大领域，尤其是金融领域受益匪浅，也正因为如此，区块链荣耀加身，成为未来颠覆我们整个世界的创新性技术。

## 自带比特币基因

当前，区块链已经成为人们谈论的热点话题，在各个领域中的应用也有一种势不可当之势。尤其在金融领域，区块链受到了金融界人士的广泛热议。既然区块链的发展如火如荼，广泛影响各个领域，那么究竟什么是区块链呢？

要想说明区块链是什么，首先应当从比特币说起。这是因为，区块链脱胎于比特币，尽管很多人想绕过比特币直接谈区块链，但是如果深入了解区块链的历史，那么就不得不从比特币谈起。

### 比特币的诞生与发行

所谓比特币，就是一种P2P形式的数字货币。众所周知，2008年，出现了一场非常严峻的、全球性的金融危机，以雷曼兄弟的倒闭为开端，金融危机在美国逐渐达到高潮并且向全世界蔓延。

之后，比特币圈内的一个匿名者、一个爱收集火车模型的天才黑客——中本聪，受到了人们的关注。之所以如此，并不仅仅是因为他发明了比特币，而且还因为传言他拥有一笔类似尼伯龙根宝藏一样的海量比特币财富，以及其他诸多不为人所知的内容。在2008年年底，中本聪发表了一本关于他所研究的电子现金系统为内容的9页白皮书，名为《比特币白皮书：一种点对点的现金系统》。在2009年年初，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖掘出了比特币的第一个区块——创世区块，并且在当天的《泰晤士报》的头版——关于救助银行的新闻标题中写入创世区块，自此，创世区块的出现标志着比特币的诞生。

### 中本聪的《比特币白皮书：一种点对点的现金系统》论文简介

本文提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。虽然数字签名（Digital Signatures）部分解决了这个问题，但是如果仍然需要第三方的支持才能防止双重支付

（Double-Spending）的话，那么这种系统也就失去了存在的价值。我们（We）在此提出一种解决方案，使现金系统在点对点的环境下运行，并防止双重支付问题。该网络通过随机散列（Hashing）对全部交易加上时间戳（Timestamps），将它们合并入一个不断延伸的基于随机散列的工作量证明（Proof-of-work）的链条作为交易记录，除非重新完成全部的工作量证明，形成的交易记录将不可更改。最长的链条不仅将作为被观察到的事件序列（Sequence）的证明，而且被看作来自CPU计算能力最大的池（Pool）。只要大多数的CPU计算能力都没有打算合作起来对全网进行攻击，那么诚实的节点将会生成最长的、超过攻击者的链条。这个系统本身需要的基础设施非常少。信息尽最大努力在全网传播即可，节点（Nodes）可以随时离开和重新加入网络，并将最长的工作量证明链条作为在该节点离线期间发生的交易的证明。



事实上，早在2008年11月1日的深夜，中本聪就在一个讨论信息加密的邮件组中发表了一篇文章，用一种非常缜密的口吻描绘了一种几近完美的货币，但是，当时这篇文章发表之后，只能在像极客这样狭小的圈子里流传，却很少有大众的关注和问津。时至今日，随着比特币在全球范围内名声大噪，成为风靡全球的一个热词，并广泛流行和爆发于金融领域，这时候，才有越来越多的人参与到比特币势如破竹的发展与进化过程当中。[shu籍分享微信 whair004]

#### 知识拓展

##### 中本聪本尊乌龙事件

在发表完《比特币白皮书：一种点对点的现金系统》之后，出现了一则乌龙事件。中本聪就像人间蒸发一样在江湖中消失了。直至2014年年初，美国《新闻周刊》刊出寻找中本聪的文章，并声称已经找到了中本聪本尊，是一个脸颊瘦弱、表情黯淡、挺着大肚腩的、名为克雷格·赖特的人。此人符合比特币创始人的几乎所有的特征细节。

1.赖特概述了类似于比特币的设想。在2008年8月，赖特发表的一篇微博中提到自己想要发表一篇“加密货币的论文”并提到了“三重记账法”。“三重记账法”是金融密码学家伊恩·格里格于2005年发表的一篇类似于比特币设想的论文。

2.有力的比特币交易记录证据。在比特币发行之前，赖特和计算机取证分析员大卫·克里曼曾经共同探讨和写过一篇论文，其中谈到了“要不要让雇主买断自己现在的工龄，所得的钱去投资几百个计算机处理器来让自己的想法成真。”并且，还有一个克里曼（卒于2013年4月）为作者的PDF文档，在文档中，他同意掌管一个代号为“郁金香信托”的信托基金，其中存有110万单位的比特币。其中所有的信息，包括“百万比特币”“郁金香信托”，这些都与一笔在比特币的区块链上长期可见、被普遍认为是中本聪所有的神秘财产数量相当。只有中本聪本人才会拥有如此数量巨大的比特币。

类似于以上证明赖特就是中本聪本尊的细节特征还有很多，但是，赖特于2015年12月最后一次露面的时候，在Linux基金会的比特币开发者群组中发表了一封声明，其内容是这样的：

邮件标题：“Not this again（这次你们仍然没猜对）。”

正文：“I am not Craig Wright.We are all Satoshi.”（我不是克雷格·赖特。我们都是中本聪）。

这似乎看起来十分滑稽，但从赖特幽默的话语中可以肯定，赖特已经否定了自己是中本聪本尊，因此，中本聪本尊到底是谁，已经成为一个谜。

在当时比特币不断爆发的背景下，比特币的定价和发行是如何进行的呢？事实上，比

比特币完全没有一个主题，它的发行完全是由市场竞争机制来决定和完成的。虽然说任何人都可以“挖掘”到比特币，但是在这个“挖掘”的过程中必然要付出更多的时间、精力等成本。并且，要知道的是，比特币的“挖掘”系统不会受到任何人或者相关组织的控制，而是由众多的参与者通过利益互动来实现的。

中本聪发表的白皮书，让我们产生了两个方面问题的思考：

一方面，任何系统在运行的过程中都是需要运行成本的，比特币这种去中心化系统，更需要付出一定的成本；

另一方面，在未来，会不会出现一个共享机制让比特币变得更好，这也成为当前最大的疑问。

价格波动，时代造就

比特币从横空出世到渐入佳境，从无人问津到众人皆知，在其发展过程中，价格的波动也是每时每刻都存在的。对于价格的波动问题，也一直存在争议。当人们看过《十问比特币：3年翻25000倍》的标题之后，顿时觉得实在是不可思议，这样真的能实现吗？

比特币兑换美元的价格在2014年1月达到了峰值，为1120美元左右。通常情况下，对于“3年翻25000倍”这个问题的考虑，往往忽略了一个基本的数学常识：“如果一定要选用0作为除数的话，那么所获得的结果将会是无穷大的。”这么说的话，25000倍看上去也没有想象的那么离谱。这里，我们尝试用漫长的0值时期后非常早的一个点：中本聪依然频繁出现的2010年的某个点，以0.0619美元作为基准，做一下计算，得出的结果是18093倍，同样也是一个不小的数值。

2016年5月29日，比特币的兑换价格一度冲高到了599美元，24小时内涨幅达到了9.41%，为此有人惊呼：“比特币又回来了。”实际上自从2010年5月21日第一次“比特币—比萨”的公开交易兑换至今，比特币兑换美元的价格一直都是波动不止，暴涨暴跌已经是再正常不过的事情了，如图1-1所示。



图1-1 在加拿大Mt.Gox交易平台，比特币价格最高触及900美元后掉头狂泻至600美元

资料来源：[http://www.guancha.cn/Finance/2013\\_11\\_20\\_187046.shtml](http://www.guancha.cn/Finance/2013_11_20_187046.shtml)

## 知识拓展

### 第一次“比特币—比萨”

2010年5月21日，一名美国程序员用10000比特币购买了比萨饼的故事流传甚广，当时1个比特币的交易价格还不到1美分。这是比特币第一次在现实世界中作为支付工具使用。只不过换算成今天的价格，10000比特币足以购买一所豪华庄园，这个比萨也被戏称为“史上最贵比萨”。

2016年以来，银行领域对于区块链和数字货币给予了极大的重视，中国人民银行行长在接受财新传媒的采访中对于区块链和数字货币的相关问题给予了罕见的表态：“从历史

发展的趋势来看，货币从来都是伴随着技术进步、经济活动发展而演化的，从早期的实物货币、商品货币到后来的信用货币，都在适应人类商业社会发展的自然规律。作为上一代的货币，纸币技术含量低，从安全、成本等角度来看，被新技术、新产品取代是大势所趋。特别是随着互联网的发展，全球范围内支付方式都发生了巨大变化，数字货币发行、流通体系的建立，对于金融基础设施建设、推动经济物质增效升级，都是十分必要的。”从这段话中，我们看到，中国人民银行已经充分认识到当前数字货币的产生是时代发展的必然。

当前，金融领域的发展存在一些绊脚石，一方面，安全和信任主体缺失，使得金融信用体系严重受损；另一方面，纸币风险系数较大，容易带来经济损失。比特币则能够抛弃这两方面的缺憾，走得更远。比特币不但可以作为一种安全性更高的存储和转移法币价值的机制，还可以作为一种互联网协议上的价值操作方法，从而很好地保护使用者的资产利益，提供一种非常透明的执行机制，让所有的参与者都能够在记账上受到更加公平的对待。

回过头来，我们重温比特币的诞生历史，就会发现，比特币不仅仅是2008年金融危机泡沫中形成的产物，更重要的是整个金融时代的发展造就了比特币。

#### 比特币与区块链

从比特币受到争议到现在，已经经历了7年多的时间。在人类历史的长河中，很少有这样一种东西，人们对待它的态度能够表现得如此泾渭分明。比特币的支持者认为它能够改变甚至是颠覆世界，而反对者则认为比特币毫无价值可言。“币”仅仅从字面意思上就可以被看作一个具有金属属性的词，但是如果将其与具有虚拟化特点的“比特”联系起来，对于很多人是有一定的难度的。

事实上，比特币中重点强调的不是“币”，而是没有中心存储机构的“账本”概念。可以说“币”只是这个记账本上使用的记账单位。区块链是比特币的底层技术，本质上是一个去中心化的数据库，像是一个数据库账本，里边记载所有的交易记录。也可以认为区块链是一种去中心化、去信任的方式，通过集体来维护一个可靠的数据库方案。我们举个形象的类比，如果将区块链看作一个事务账本，那么一个区块就相当于账本中的每一页，区块中所承载的信息，就是这一页上记载的交易内容。

比特币这个属性本身就让很多人产生困惑，因为比特币本身就带有3个层面的含义，如图1-2所示。

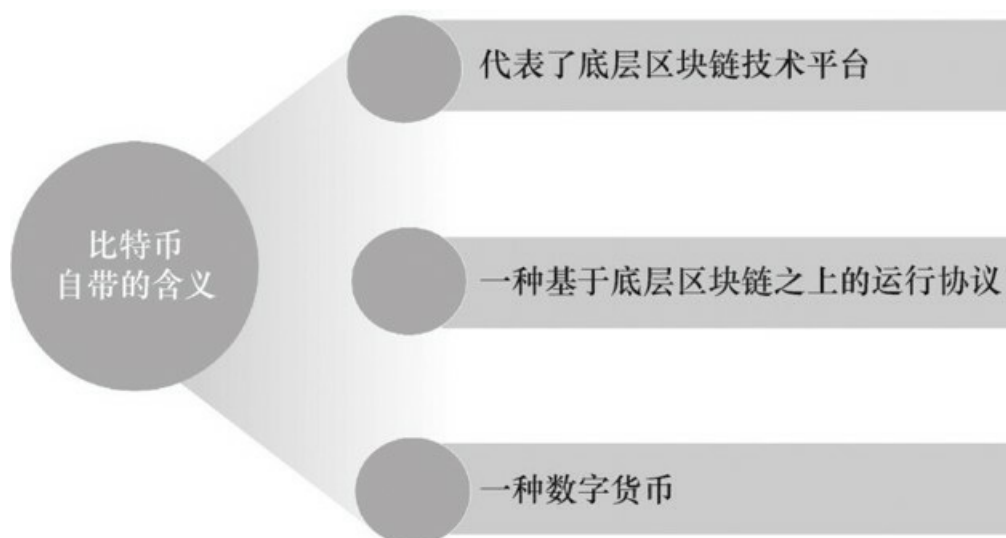


图1-2 比特币自带的含义

第一，比特币代表了底层区块链技术平台。

第二，比特币被认为是一种基于底层区块链之上的运行协议，基于这种协议，可以很好地描述资产是如何在区块链上进行转移的。

第三，比特币本身就是一种数字货币，比特币是最早出现的一种数字货币，同时也是当前规模最大的加密数字货币。

根据以上的关系剖析，我们发现很多人认为区块链是携带比特币的基因，实际上这样理解是有一定偏差的，区块链是比特币构成的一种底层技术，而区块链的产生是伴随着比特币的出现而出现的，因此，认为区块链自带比特币基因的说法其实是不准确的。

区块链本质上是一个去中心化的分布式账本数据库，是比特币的底层技术，是与比特币相生相伴的。区块链本身实际上是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。

每当有加密交易产生的时候，网络中就会有强大运算能力的矿工开始使用算法解密验证交易，并创造出新的区块来记录最新的交易记录信息。新的区块是按照时间顺序通过线性的方式对原有的区块链进行相接，从而达到补充和延伸、增长的目的。

但是，这个区块链账本与我们传统的账本是有一定区别的。不同点在于，区块链账本上的内容必须是唯一的，这样就导致记账是天然中心化的行为。在以往通信并不发达的时代，是如此，在当前信息化时代也是如此。然而，这种中心化的记账也存在一些非常明显的弱点：如果一个中心出现了问题，被篡改、被损坏，那么整个系统将会面临巨大的危机，严重的甚至会直接导致崩溃。

然而，通过复杂的公共钥匙和私人钥匙的设置，区块链网络将整个金融网络的所有交易账本实时广播，实时将交易记录分发到每一个客户端，同时还能保证每个参与者只能对自己的账单进行修改。虽然账单里还有别人的交易记录，但是仅仅可以看到别人交易的数值和相应的交易地址，在不借助其他技术手段的前提下根本没有办法得知交易者的身份信息，更无法更改账单记录。



过去，在网络中寻找最短路径以求最快发送到客户端



现在，发给每个人，每个人有秘钥才能打开

那么由谁来记账成为一个非常重要的问题。目前，就是谁的系统由谁来记账，比如，微信的账本就是由腾讯来记账，淘宝的账本就是由阿里在记账。但是在现在的区块链系统中，系统中的每个人都有机会参与到记账的行动中，如果在一定的时间内没有任何数据变动，系统中的每个人都可以参与进来进行记账，系统会在所有的参与者中做出评价，从而判断哪个参与者是记账记得最好、最快的人，就把他记录的内容写到账本上，并将这段时间里的账本内容发给其系统内的所有人进行备份。这样系统中的每个人都有了一本完整的账本。这种方式就是区块链技术。

单从技术角度来看，区块链可以看作一种数据库、一种分布式系统、一种网络底层协议。

### 1.数据库

区块链技术作为一种数据存储机制，必然也会具有数据机构发展的既定规律，同时它记录了网际间的所有交易信息，随时更新，让每个用户通过合法手段从中读取信息，写入信息，有效防止数据信息被篡改。

### 2.分布式系统

区块链技术在本质上就是分布式账本，因此，可以说区块链是一种分布式系统，它不放置在某一两个特定的服务器或安全节点上，而是分布式地存在于网络上所有的完整节点上，在每一个节点上保留信息备份。每一个参与者都是一个节点。

### 3.网络底层协议

区块链也是一种共识协议，基于这种协议，可以在其上开发出数目繁多的应用。这些应用在每一时刻都保存一条最长的、最具有权威的、共同认可的数据记录，并遵循共同认可的机制进行无需中间权威仲裁的、直接的、点对点的信息交互。



## 区块链的3个进阶阶段

最初的区块链仅仅指比特币的总账记录。这些账目记录了自2009年比特币网络运行以来产生的所有交易。然而这些总账并不是仅仅记录在某台服务器上，而是在所有的客户端都有一份相同的实时同步的备份。这个总账对于所有参与人来讲都是公开的，并且任何人都可以查阅、审核。

从应用角度方面来看，区块链就是一本安全的全球总账本，所有的可数字化的交易都是通过这个总账本来记录的。从数据的角度来看，区块链是不同的参与者在各个节点上的分布式数据库系统，具有不可篡改、不可伪造的特点。区块链根据其作用的不同可以分为基础层和应用层。其中基础层是一种类似互联网的TCP/IP协议，而应用层是基于该协议的应用。

应用层上，又可以套用梅兰妮斯万的观点将区块链细分为3个发展阶段：区块链1.0，可编程货币；区块链2.0，可编程金融；区块链3.0，可编程社会，如图1-3所示。

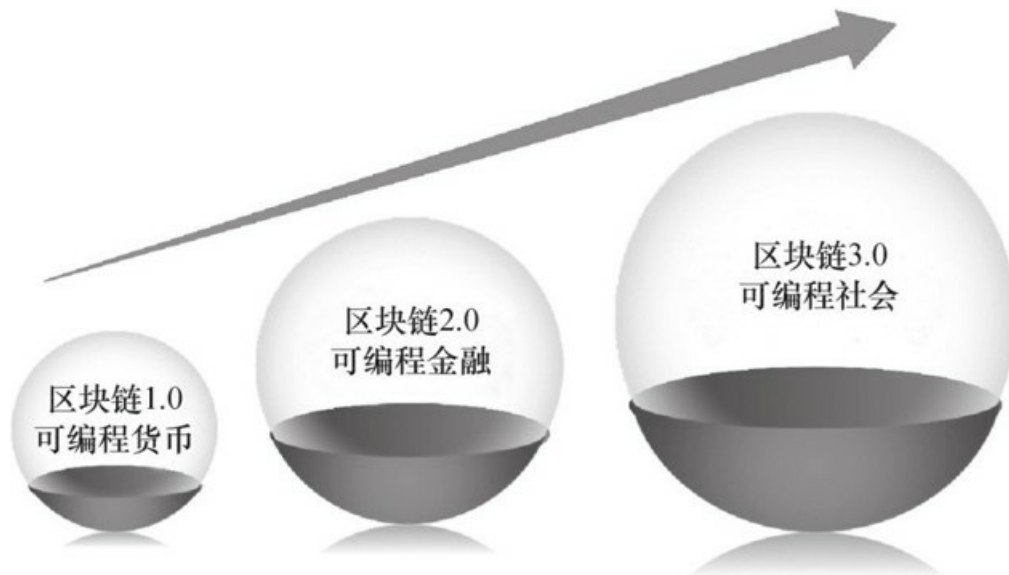


图1-3 区块链发展的3个阶段

### 区块链1.0，可编程货币

第一阶段是以可编程数字加密货币体系为主要特征的区块链1.0模式（图1-4）。在区块链1.0模式下，典型的应用就是比特币，主要解决的是货币支付手段的去中心化问题。主要内容包括以下几个方面。

#### 1.技术堆栈

从技术角度来讲，比特币有3层技术：区块链、协议和货币。

第一层区块链作为底层技术，是去中心化的、公开透明的交易记录记账，其数据库是由所有的网络节点共享的，并且由“矿工”进行更新，由全民进行监督，但是从根本上讲是没有人可以真正拥有和控制这个数据库的权利的。



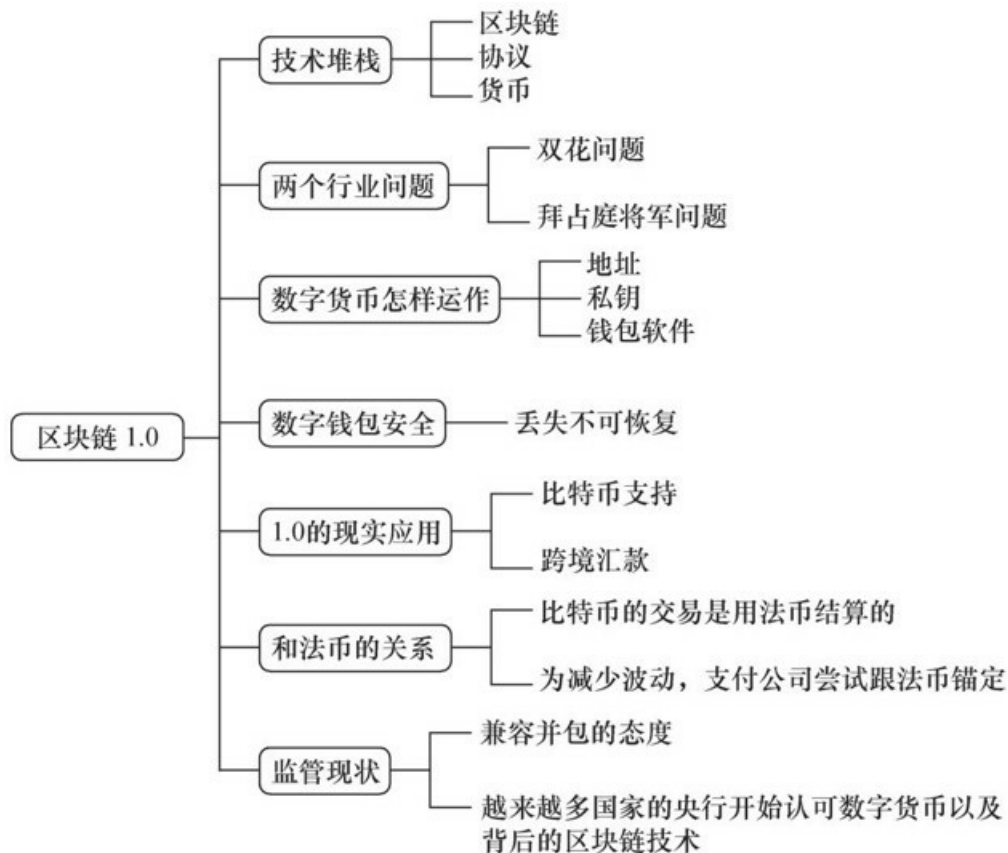


图1-4 区块链1.0

第二层是协议，即区块链上进行资金转账的软件系统。

第三层是货币本身，如比特币。

对所有的加密货币来讲，区块链、协议和货币这3个技术层是其通用结构，这就意味着每种加密货币都代表货币、协议和区块链3种技术的结合。并且，其区块链技术对于所有的加密货币来讲是可以实现共用的。

## 2.两个行业问题

### (1) 双花问题

在区块链技术还没有出现之前，数字货币和数字资产是可以复制的，并且可以无限复制，如果缺乏一个中心化的媒介，就很难确定甚至无法确定这笔资产是否已经被花掉了，所以需要依靠可信赖的第三方金融机构来解决这个问题，如银行、支付宝等。

如我有1个比特币，在两台机器上同时将其转给了甲和乙两个人，这时候系统如何才能判断这个比特币是甲还是乙花了呢？然而，通过银行、支付宝之类的第三方支付则可以通过其系统进行检测，并得知这1个比特币是否已经被甲和乙两人重复花掉。

区块链技术通常采用将点对点文件分享技术与公钥加密技术相结合的方式，区块链通过将点对点文件分享技术和公钥加密技术相结合，创造出了全新的数字金钱，这样就可以很好地解决“双花”问题。

### (2) “拜占庭将军”问题

知识拓展

“拜占庭将军”问题

拜占庭帝国派出了10支军队去攻打敌人。这个敌人虽然与拜占庭帝国相比是非常弱小的，但是也足以抵御5支拜占庭军队的同时袭击。基于某些原因，这10支军队不能集合在一起进行各个击破，必须分开包围敌人，并给敌人强烈的攻击。但是，派出的第一支军队在单独进攻之后，却根本无法取胜，除非结合至少6支军队同时袭击才能攻下敌国。于是，他们分散在敌国的四周，借助通信设备来相互协商进攻方向以及进攻时间。但是，值得一提的是，困扰这些拜占庭将军的问题是，他们并不能确定他们中间是否存在叛徒，因为叛徒很有可能会更改进攻方向和进攻时间。在这种情况下，拜占庭将军需要寻找一种分布式的协议来让他们能够远程协商，从而保证战斗力，更加团结紧密，这样才能赢得胜利。这就是著名的“拜占庭将军”问题。

“拜占庭将军”问题在于战场上多个将军之间并不会产生更进一步的信任，但是却需要建立某种沟通协调的机制。

回到区块链问题上来。区块链上每个记账页都被网络上的各个节点查看和验证，并不需要将其托管到一个中心化的机构，使用者根本不需要担心是否相信交易对手，而仅仅需要相信区块链网络就可以了，这就很好地解决了“拜占庭将军”的问题。

### 3. 数字货币运作的要素

数字货币的有效运作需要借助3个要素来完成。

#### (1) 地址

地址意味着别人能够将比特币发到你这里。

#### (2) 私钥

通过加密的方式将比特币发送给别人，这就好似送给别人一枚保险箱的钥匙。

#### (3) 钱包软件

即运行在电脑上的操作私钥管理的比特币软件。钱包软件可以保留区块链的副本，作为核查交易的去中心化体制的一部分。

### 4. 数字钱包的安全问题

数字货币当前存在一个严重的安全性问题，即一旦出现私钥丢失的情况，是无法重新找回的，并且对于普通的用户来讲，他们缺乏很好的保护私钥的能力，也正是由于这一点，使得比特币无法在大众中被普遍接纳。

### 5. 比特币1.0的实际应用

比特币已经是因特网的现金了，是一种数字付款系统，而且可能成为互联网货币，并以物联网关联机器的方式关联着金融。货币和付款成为比特币最明显的应用。有选择性的货币只有基于经济的论据才有实际意义。例如，减少了全球范围内的商业付款费用，从原来3%的费用到现在1%的费用，使得经济从中受益，这对于国际汇款的影响更大，因为此类交易手续费高达7%~30%。并且，这与等待转账相比，在电子钱包中使用者可以及时收账。比特币和它的模仿者可以为货币、交易和商业开辟出一条全新的道路。

区块链的核心功能就是直接在因特网连接的两个人之间发起并完成任何交易。使用代币，可以以去中心化、分散式、总体式的方式在个人之间分配并交易资源。当具备这一能力的时候，数字加密货币就可以变为一种开放的可编辑网络，为所有资源做去中心化交易，这种情况已经超越了货币和支付功能。

### 6. 监管现状

政府监管对于区块链产业的发展具有很重要的促进作用，同时也是决定区块链产业能否发展成为一个成熟的金融服务产业的重要因素之一。

比特币具有的去中心化的特点决定了其不能被某一国家或者团体所掌控，这对于某些本国货币强势的国家来讲是不能接受的：世界上最赚钱的事情就是印刷货币，经济强国可以通过印刷货币获得大量的财富，并且这是一个可以控制、牢牢掌握在自己手中的金融工具，所有的外交、军事、对外发展等活动都可以在某些情况下印证国家对于本国货币的地位提升的重要性。然而，比特币的出现给经济强国带来了诸多危机：比特币可以被世界上

任何一个人印刷出来，经济强国最可控的“生意”——印刷货币，就会受到比特币带来的有力挑战。未来，如果比特币能够成为主流货币，那么现有的货币体系将会发生重大的变革，经济强国再也无法倚仗自己的印钞机掠夺财富，从而导致其权威地位的下降，因此，对于某些国家来讲这是不可以接受的。

当前，全球各国对于比特币的看法不一：孟加拉国、玻利维亚、厄瓜多尔、冰岛、中国、吉尔吉斯斯坦、越南等国家正在实行纸质货币；部分欧洲国家，如加拿大、美国、瑞士、波兰等国家正在继续商讨比特币问题。

### （1）美国

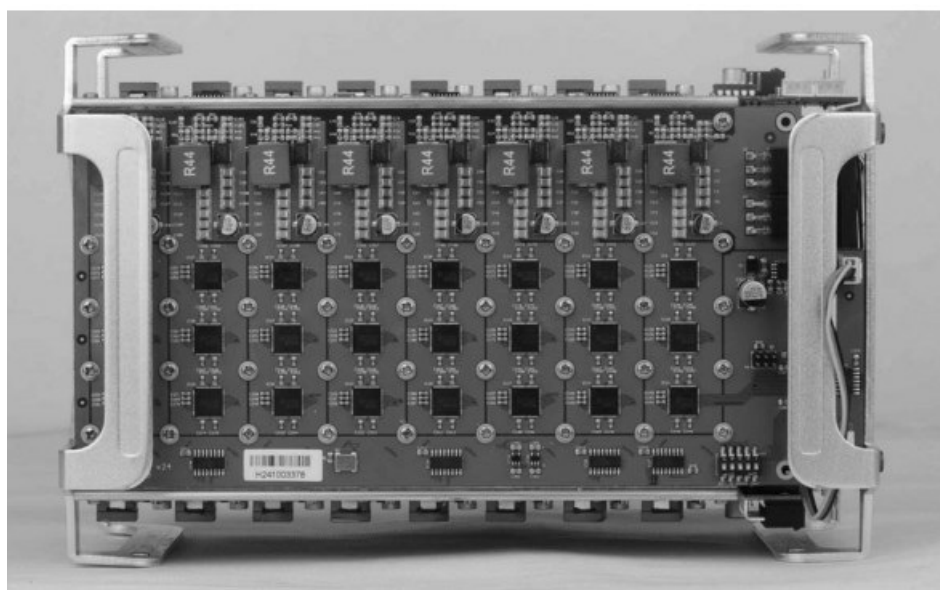
美国认为比特币是一种虚拟货币，不具备实体货币的全部属性和法定货币的地位。2014年年初，美国联邦税务局发布通告称比特币以及其他虚拟货币属于财产而不是货币，比特币的“挖矿”、买卖和使用行为均应适用相关税务规则，进行纳税申报。

美国摩根士丹利发布了最新报告，称：“Magister Advisor调查显示，2017年，美国金融机构预计将花费超过10亿美元在区块链项目的开发研究上，这将使其成为未来发展最快的企业软件技术市场之一。虽然区块链技术的价值已经得到了大部分金融行业的认可，对于银行来讲，区块链的应用也可以帮助其减少各种繁杂的运营成本。但是，区块链的开发研究和应用成本，以及其在未来发展的各种不稳定因素也可能使它变成一把双刃剑，对银行以及其他金融机构的竞争格局造成不可预测的影响。”

### 知识拓展

#### 比特币挖矿

自从2009年1月3日中本聪提出“比特币”概念以来，截至2015年年底，已经开采出了高达1500万个左右的比特币。与大多数货币不同的是，比特币不依靠特定的货币机构发行，而依据特定的算法，通过大量的计算而产生，人们把“利用计算机硬件资源计算比特币位置并获取比特币的过程”称为“比特币挖矿”。



### （2）中国

中国认为比特币不是由国家发行的，不具备法偿性和强制性等货币属性，并不是真正意义上的货币，不能且不应作为货币在市场上流通使用。

### （3）韩国

韩国拒绝承认比特币的货币地位，认为比特币不是真正的投资，不会对比特币征收资

本所得税，因为这将增加虚拟货币的合法性。

#### （4）荷兰

荷兰表示质疑比特币的存储保障能力，导致比特币的价格波动剧烈。

#### （5）加拿大

加拿大承认比特币的地位。

2013年12月，世界首个比特币ATM机在温哥华正式投入使用，这台ATM机被放在一个咖啡厅里。目前这台ATM机上的交易额已经取得了很好的成绩。由于受到不同州法律的监管约束，很多美国本土的比特币创业选择搬迁到加拿大进行。

#### （6）印度

印度继续关注比特币的发展，目前不会进行监管。

#### （7）法国

法国认为比特币交易是不会违法的，但是对于比特币的波动，监管机构告诫用户谨慎投资比特币。

#### 区块链2.0，可编程金融

随着技术的发展，区块链应用就会逐渐从1.0的应用慢慢拓展到其他金融领域，可以看到，区块链技术已经应用在股票、私募股权等这些所有与金融相关的领域，并开始解决现实中遇到的问题，我们可以将其统称为可编程金融。

第二个阶段是以可编程金融体系为主要特征的区块链2.0模式，可以理解为区块链技术在其他金融领域中的应用。该模式着眼于整个市场的去中心化，把任何资产变成数字化形态进行交易。

在讲到区块链2.0模式是实现可编程金融之前，我们不得不先讲一讲金融科技。金融科技在我国最早的定义为“促进科技开发、成果转化和高新技术产品发展的一系列金融工具、金融制度、金融政策和金融服务的系统性安排”。

金融业作为一个信息密集型行业，信息科学技术每发生一次全新的变革，都会深刻改变金融业的格局。事实上，在很早以前，金融业的发展就已经借助信息技术了，由脱机业务到联机业务，再到金融决策的信息化阶段，以及到现在互联网技术的应用阶段，都离不开信息技术。技术的不断发展本身就使得现代金融业出现了分工，使得互联网和相关软件技术在金融领域中逐渐渗透。近几年移动支付、众筹、P2P、区块链、量化投资、机器人投顾等新兴技术的发展更是推动了金融业的不断发展和创新，使得金融业进入一个全新时代。当前，从余额宝和各种宝宝们的互联网理财到P2P金融的百家争鸣，再到众筹的雨后春笋般快速成长，再到最近区块链和机器人投顾的萌芽与发展，如今的金融正在走向另一个高度。

如果说移动支付、众筹、P2P、量化投资[1]、机器人投顾[2]等新兴技术是金融科技发展的有效武器的话，那么区块链则是金融科技的核心武器。在过去，金融领域对于信息技术提出了很高的要求，需要其具有很高的可靠性。但是如今，金融领域对于透明性、可靠性和便捷性的要求越来越高，这个时候，区块链则能够成为金融业革新的重要武器。

区块链起源于比特币，是在创建比特币的过程中设计的一套分布式数据库技术。区块链本身就具有去中心化、高度透明化、不易被随意篡改、不可追溯的特点，这恰好是金融业需要的。可以说，区块链技术是互联网金融领域的重大技术创新，在对现有金融基础设施产生颠覆性破坏的同时，更带给金融领域神奇的新变化。

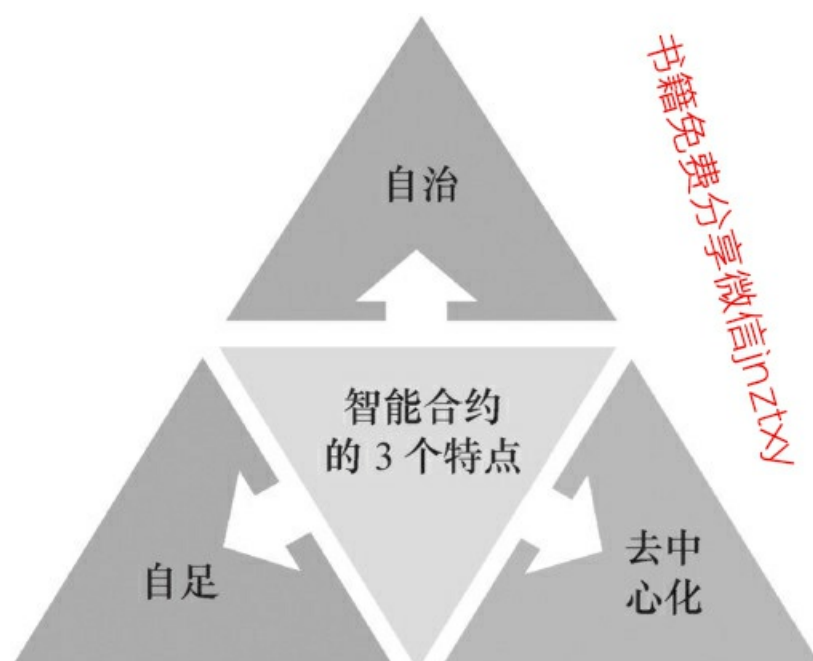
信任是金融领域能够持续发展的基础。在传统模式下，金融业为了获取和维护用户的信任，往往消耗大量的人力、物力、财力成本，还得依托于相关中介机构，包括托管机构、第三方支付平台、公证人、银行、交易所等，但最终收获的成果微乎其微。区块链技术在金融领域中的使用，借助于全新的加密认证技术和去中心化、共识机制去维护一个完整的、分布式的、不可篡改式的账本，可以让所有的参与者都能够在不需要建立任何信任

关系的基础上，就可以通过一个统一的账本系统确保资金和信息的安全。区块链借助分布式记账、P2P网络架构、基于计算机算法的协商一致的自治协议、安全的数据存储传输使用规则、可持续运行激励机制、开放式系统等保证金融业最大限度实现去中心化，确保这个系统对所有的用户，即参与者都是可信的，从而为交易各方的经济活动建立了更加具有信任特点的环境，这对金融机构来讲意义是十分重大的。

区块链技术的嵌入可以使得互联网金融的意义更加趋于深化，其中一个重要方面是通过程序化记录、储存、传递、分析信息数据，从而形成信用。这样对于传统的信用形成方式来讲，区块链能够省去大量的人力成本、中介成本，但是对于信息的记录而言则更加趋于完整化，具有不易篡改的特点。

除了以上特性以外，区块链之所以被称为颠覆性技术，其实主要是因为智能合约。智能合约实际上说明了区块链交易并不仅仅局限于买卖货币方面的交易，未来将会有更多的指令嵌入区块链当中。

传统合约是双方或者多方之间共同达成协议对于某件事情共同作出承诺，是做或者不做，从而换取某些一致协商的好处，并且任何一方都必须遵循和履行协议中的每个条款。而智能合约较传统合约来讲，具有3个特点：自治、自足和去中心化，如图1-5所示。



智能合约的双方或多方之间是建立在信任的基础上而共同达成的协议，因为智能合约是由代码定义的，并且也是由代码对合约各方进行约束，并强制执行合约内容的，智能合约就是利用程序算法替代人执行合同，因此可以说，在智能合约下，协议的执行完全是自动完成的，且外力是无法干预的。智能合约需要自动化的资产、过程、系统的组合与相互协调。合约包含3个要素，即要约、承诺和价值交换，并且有效定义了新的应用形式，这样就使得区块链从最初的货币体系逐渐向金融的其他领域进行深入拓展，这些领域包括股权众筹、证券交易等方面。当前，诸多传统金融机构也开始全面研究区块链技术，从而使传统金融的发展与区块链相结合，实现可持续性。

由此可见，区块链2.0阶段将会给金融服务业带来颠覆性变革。

区块链3.0，可编程社会

前面我们也讲到，区块链的本质就是一种关于信任的互联网协议。这也就意味着区块链是价值互联网的内核。区块链可以对每一个互联网中代表价值的信息进行产权确认、计

量以及存储，这样就可以更好地实现资产在区块链上的可追踪、控制和交易。加之互联网的核心是通过区块链来构建一个具有全球性特征的分布式记账系统，我们在前面也讲过分布式记账系统，它不仅可以记录金融业的交易历史，还几乎可以记录任何有价值的能够以代码形式进行表达的事物，如共享汽车的使用权、共享房屋的使用权、信号灯的状态、结婚证、账目记录、医疗过程、能源及投票等。因此，可以说，随着对区块链发展的进一步研究，可以将区块链技术的应用领域进行更大范围的拓展，包括审计公正、银行、医疗、物流等诸多领域，从而一步步推进到整个社会中去。届时，区块链的发展就进入3.0时代，即可编程社会的时代。

具体社会中各领域的应用如下。

### 1. 审计公正

区块链提供一个分布式机制可以锁定相关数据，从而使得数据可以被核查和独立审计。而在传统模式下，往往需要通过手工的方式来记录，又很难做到数据保护、同步更新和真实性几个方面。当进入电子化时代之后，电脑记录虽然比手工记录更加快速，但是记录内容仍容易被篡改，数据核查依旧是一个难以解决的问题。但是基于区块链协议构建的一层分布式的、匿名数据协议Factom协议可以有效解决这些问题。Factom协议维护了一个永久不可更改的、基于时间戳记录的区块链数据网络，从而有效降低了独立审计、管理真实记录、遵守政府监管条例的成本和难度。商业领域和政府部门可以充分利用简化数据管理与记录的流程，并解决数据记录的安全和符合监管的问题。

### 2. 代理投票

当前，使用最为广泛的投票机制是股东代理投票机制，这种机制的缺点就是程序繁杂。通常，资产管理人向代理投票经纪人发出投票指令，该指令会传递到投票分配者，然后再由投票分配者传递到托管人和子托管人手中。托管人会请求公证人对投票指令做公证，然后向登记方申请并完成记录，最后投票信息被汇总到公司负责人处。这个流程就是一个非标准化的流程，投票的信息存在不正确传递，甚至是丢失的风险。另外，由于托管人以及子托管人二者使用的传输系统和字符识别系统存在一定的差异，从而导致投票的追溯和确认变得非常困难。

借助于传统投票机制，荷兰一家研究机构针对代理投票做了一项专门的研究，研究结果表明，在荷兰使用代理投票系统的公司和企业中，能够确认自己代理投票结果的仅仅占到了31%。这样就给投票信息的正确传递以及追溯造成了极大的不便。

但是，借助于区块链技术，则效果完全不同，如图1-6所示。区块链技术可以优化股东代理投票流程。资产管理人首先需要下载投票软件，提交身份信息进行注册，即可直接提交投票。要注意的是，一旦投票结果在分布式数字化投票登记系统中成功提交，就不可对这些信息进行更改或撤销，同时基于区块链上数据的同步性，资产管理人可以借助区块链的这一特性对投票结果进行快速查询。基于区块链技术的股东代理投票流程与传统投票模式相比较，可以节省50%~60%的成本，除此以外，还可以使投票变得更加安全、高效、透明、便捷。

### 3. 医疗

医疗记录往往会存储一些与病人有关的保密性信息，然而这对于医疗来讲又是刚性需求，但是在现实当中往往这些保密性信息没有得到良好的高度保密，而是流于广告商以及黄牛手中。区块链技术的应用将彻底改善当前这种不良情况，为医疗信息的安全问题提供良好的解决方案。未来，病人将会拥有属于自己的独立区块链，通过多重签名的方式，防止医院在病人不知情的情况下将其私密信息泄露给他人。



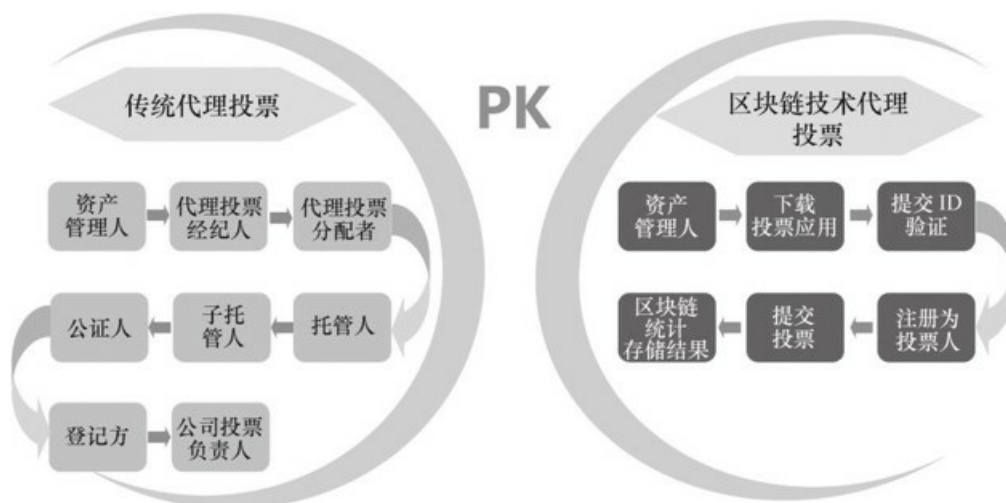


图1-6 传统代理投票流程PK区块链技术代理投票流程

#### 4.物流

2015年“双11”期间，淘宝销售额又一次创下了新高，即912.17亿元。但是，阿里巴巴董事局主席马云对于每年“双11”的短板问题，认为最重要的影响还是物流。确实，当前物流行业在享受各大电商狂欢节带来的巨大喜悦的同时，也承受着严重的包裹派送压力。许多物流快递配送站点在电商狂欢节期间所承受的压力比往常多出数倍以上，爆仓、丢件的事件频频发生。大多数的包裹是由电商企业用物流快递直接发送到消费者手中的，但是这样也会出现一个严重的问题，就是消费者的个人电话、地址等信息往往被泄露，进而被不良企业倒卖，所以物流行业的实名制政策亟待落实。区块链技术的出现将很好地解决实名制以及爆仓、丢件问题。

区块链技术还有一个非常重要的应用领域，那就是物流领域。借助区块链技术可以记录货物从发出到签收过程中的所有环节。通过创建共识网络，能够直接定位到快递在运输途中的任何一个出现问题的环节，也能够确保物流信息的可追踪性，从而有效避免快递出现爆仓、丢包、错领等现象的发生，也可以有效地促进物流实名制的快速落实。快递交接需要双方通过私钥签名，每个快递员或者快递站点都有自己的私钥，是否签收或者交付只需要在区块链中查一下就可以一目了然。如果收件人没有签收快件，快递员也没有办法伪造签名。另外基于区块链技术，还可以杜绝快递员通过伪造签名来逃避考核，以此来减少用户的投诉，如图1-7所示。

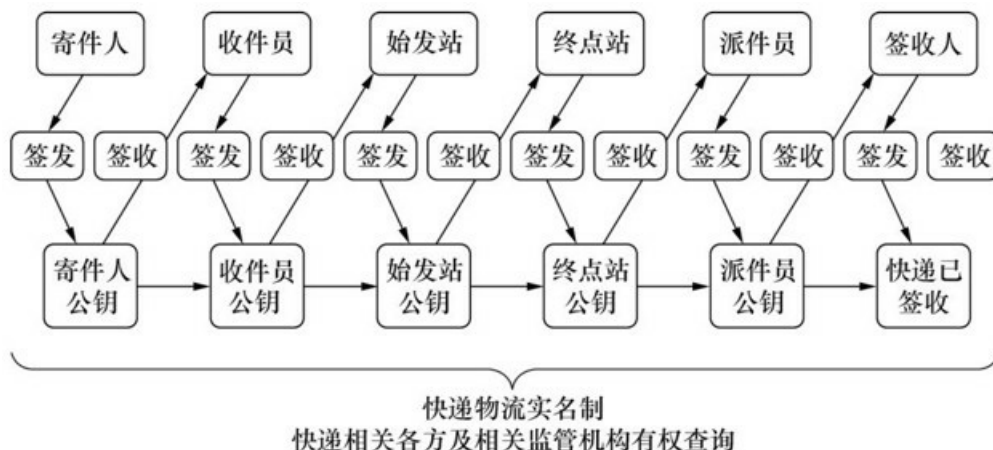


图1-7 区块链上的快递物流追踪

图片来源：复杂美区块链研究中心的《区块链项目白皮书》

书籍每日免费分享微信jnztxy朋友圈



## 区块链的4种技术创新

当前，随比特币的出现而出现的创新技术区块链，正成为全球政府、银行、科技巨头们所关注的对象。区块链本身是一种特殊的数据库技术，是基于密码学中的椭圆曲线数字签名算法（ECDSA）来实现去中心化的P2P系统设计，但是区块链的作用并不仅仅局限于比特币上。现代很多人使用区块链，并将其视为数据记录、数据库、数据库技术，这些都与比特币没有必然联系。因此，风靡世界的区块链技术已经在全球迅速发展起来，早已经从以往的密码学货币应用扩大到了政府、金融、货币、医疗、艺术、人工智能、能源环保等诸多领域。区块链技术已经成为当前又一世界级的创新。

从数据角度来看，区块链是一种分布式数据库，或者称为分布式共享总账，这里所谓的“分布式”不但意味着数据的分布式存储，同时也体现了数据的分布式记录，换句话说就是由系统中所有的参与者对数据记录的安全性进行维护和管理。简单地说，就是区块链能够实现全球数据信息的分布式记录、分布式存储。

第一，分布式记录，是由系统中的所有参与者共同记录，而并不是其中的一个个体或者一个中心化的机构去做记录。

第二，分布式存储，是在所有参与的节点中进行数据记录，而并不是集中存储在一个个体或者一个中心化的机构节点中。

从效果的角度来看，区块链可以生成一整套完整的记录时间先后的、不可随意更改的、可信任的数据库，在这套数据库中，所有的数据存储和记录都是去中心化的，并且数据的安全性能得到有力的保障。

总而言之，区块链作为一种全新的技术，脱胎于比特币的技术，提供一种去中心化的、无需信任积累的信用建立范式。在这种范式当中，任何互不了解的人都可以通过加入一个公开透明度数据库，通过点对点记账、数据传输、认证或是合约，而不需要借助任何一个中间方式来达成信用共识。这个透明公开的数据库中包含了过去所有的交易记录、历史数据以及其他相关信息，所有信息都是按照分布的方式进行存储，并且具有很强的透明化、可查性，并以密码学协议的方式，保证其不能非法篡改。

从以上这些方面，我们可以将区块链技术的创新分为以下4个方面，如图1-8所示。

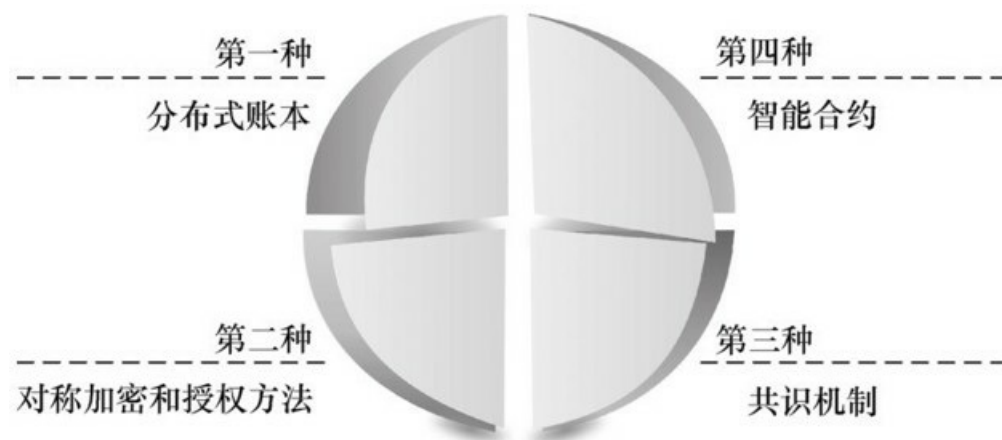


图1-8 区块链的4种技术创新

分布式账本

前边我们也讲到，区块链的本质是分布式账本，是一个可以在多个站点、不同地理位

置或者多个机构组成的网络里实现资产分享的数据库。换句话说，分布式账本由分布在不同地方的多个节点共同完成，并且每个阶段都记录了完整的账目，因此它们都可以参与监督交易的合法性。分布式账本其实也是区块链的一大颠覆性技术创新。诚然，在所有的经济活动中，进行记账、对账、分账的过程中都有区块链的应用。分布式账本可以通过广泛的应用场景去提高生产，并且有机会变革公共与私营服务的实现方式。

在分布式账本中所存储的往往是那些在金融或者法律基础上定义的实体或电子资产，因此账本中资产的安全性和准确性是有一定的访问限制的，只有通过公钥或者签名的方法才能获得账本的访问权和掌控权，即将公钥或者签名作为一种密码，对分布式账本的安全性和准确性进行保护和维护。

通常情况下，在一个网络里的参与者可以获得一个唯一的真实账本的副本，账本里一旦出现任何更改都会在账本的副本中反映出来，这种反映往往是非常迅速的，通常只需要几秒或者几分钟的时间。因此，对分布式账本进行随意篡改是极其困难的。只有在遵循网络中所达成的共识规则的基础上，账本中的记录才可以由一个人、一些人或者所有的参与者共同更改。也就是说，所有的参与者都可以共同为账本作证。

分布式账本有非常广泛的应用前景，如可以帮助政府征税、发放福利、发放护照、运行等级货物供应链等方面都可以用到分布式账本，这样可以从整体上确保政府记录和服务的正确性。

当前，英国国民健康保险制度（NHS）里已经应用到了分布式账本技术，通过改善和验证服务的送达以及根据精确的规则去安全地分享账户记录，并且在医疗保健系统方面也是非常具有发展潜力的。对于广大消费者来讲，可以根据每个消费者自身情况的不同，通过利用分布式账户这一技术，去控制其个人记录的访问权限，与此同时，还可以通过这一技术来得知其他机构对其记录的访问情况。

利用分布式账本可以解决当前改善基础设施过程中出现的效率极低、成本高居不下的问题。当前，导致市场基础设施成本高的原因主要有3个：交易费用、维护资本的费用和投保风险费用。要求承保的费用包括交易对手风险、本金风险等，这些费用都是非常昂贵的。其中还包括了中心化供应商管理风险的费用。降低结算时间成本，即达到及时结算，可以有效降低风险，分布式账本技术就是一种非常有效的降低结算时间的可行性技术。在某些情况下，特别是在有高水平的监管和成熟市场基础设施的地方，分布式账本技术更有可能形成一个新的架构，而不会完全取代当前的机构。[shu籍 分享 微信 whair004

总的来说，分布式记账与传统的记账方式的不同点在于，没有一个节点可以单独记录账目，而且避免了单一记账人被控制或者被贿赂而出现记假账的可能性。另外，记录账本的节点足够多，也避免了个别节点对账本的破坏。从理论上讲，只有所有的节点都对账本进行破坏，才能出现账目丢失的情况。也就是说，分布式账本技术从根本上保证了账目数据的安全性和准确性。

#### 对称加密和授权方法

在区块链上存储的交易信息是公开、透明的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问，从而保证了数据的安全以及个人隐私不受侵犯。

#### 知识拓展

##### 对称加密和非对称加密

对称加密，也叫私钥加密，是指加密和解密使用相同密钥的加密算法。有时也叫作传统密码算法，就是加密密钥能够从解密密钥中推算出来，同时解密密钥也可以从加密密钥中推算出来。但是，在大多数的对称算法中，加密密钥和解密密钥是相同的，所以也称这种加密算法为秘密密钥算法或者单密密钥算法。常见的对称加密有DES（Data Encryption Standard）、AES（Advanced Encryption Standard）、RC4、IDEA。

非对称加密，与对称加密的算法是有所不同的，非对称加密算法需要两个密钥，即公

开密钥和私有密钥，非对称加密算法在加密和解密过程使用了不同的密钥，非对称密钥也称为公钥加密，在密钥对中，其中一个密钥是对外公开的，所有人都可以获取，称为公钥；另外一个密钥是不公开的，称为私钥。

#### 共识机制

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已经超越了以往的数字货币。

比特币本身是由分布式网络系统生成的数字货币，其发行过程不依赖于特定的中心化货币发行机构，而依赖于分布式网络节点共同参与一种称为“工作量证明（Proof of Work, Po W）”的共识过程来完成交易的验证与记录。**Po W**的共识过程实际上就是俗称的“挖矿”，每个节点称为矿工，通常是各个节点贡献自己的计算资源来竞争解决同一个难度具有可动态变化和调整的数学问题，并成功解决该数学问题的矿工将获得区块链的记账权，同时当前时间段的所有比特币交易记

录被打包存储在一个新的区块中，并按照时间顺序将其连接到比特币链上。

区块链是比特币的底层技术，类似于一个数据库账本，由分布在不同区域的节点共同参与决策，并记载所有的交易记录，而这些决策规则的核心就是共识机制。

所谓共识机制就是用来决定按照哪个参与节点记账，以及确保交易完成的技术手段和机制。共识机制可以在区块链技术应用的过程中有效平衡效率与安全之间的关系。通常情况下，安全措施越复杂，则处理效率越差，如果想要提升处理效率，就必须降低安全措施的复杂程度。

从目前的情况来看，区块链技术的共识机制主要有：**Po W**（工作量证明机制）、**PoS**（股权证明机制）、**DPoS**（授权股权证明机制）和**Pool**（验证池机制），如图1-9所示。



图1-9 共识机制的4种类型

#### 1. Po W（Proof of Work，工作量证明机制）

所谓工作量证明机制，实际上就是获得货币量的多少取决于挖矿工作的成效，用户使用的计算机性能越好，则挖矿所获得的货币就越多，即根据工作量分配货币。

比特币挖矿就是通过参与或运算，计算出一个符合规则的随机数，即获得本次的记账权，同时发出本轮需要记录的数据，全网其他节点验证后，所有节点的参与人员一起存储该记录数据。系统用工作量证明机制来分发资产，以鼓励用户挖矿，从而保证网络的稳定性。当前，绝大多数的虚拟货币，如比特币、莱特币等都是基于Po W机制的虚拟货币。

Po W机制的优点是实现了完全的去中心化，节点自由进出。但同时也存在一些问题，一是当前比特币已经吸引了全球大部分的算力，使用Po W共识机制的区块链应用很难获得相同的算力，并以此来保障自身的安全；二是挖矿造成了严重的资源浪费；三是共识达成的周期较长。Po W机制虽然不太适合于商业应用，但是在太阳能的研究、宇宙智能探索方面具有很大的应用潜力。

## 2. Po S (Proof of Stake, 股权证明机制)

简单来讲，Po S机制实际上就是一个根据用户所持有的货币数量和时间来决定派发利息的制度。Po S机制中有一个叫作“币龄”的概念，每个币每天产生1币龄，如果用户持有币的数量达到了100个，并所持时间为30天，那么其拥有的币龄为3000。这时候，如果用户发现一个Po S区块，那么他的币龄就会被清空，用户每被清空365币龄，就会获得区块中0.05个币的利息（这里可以理解为年利率为5%）。由于币龄清空为零，没发现一个新区块，矿工的算力也归为零。

与Po W机制相比较，Po S机制是一种升级的共识机制，根据每个节点代币数量和时间比例降低挖矿难度，加快随机数的寻找速度。在实际运用中，Po S机制具有在一定程度上缩短共识达成时间的优点，同时也在安全性方面有了更大的保障，这对于大数据在金融领域中的应用具有十分巨大的作用。另外，Po S机制构建了区块链技术前沿运用的基础。其缺点是还需要挖矿，实际上并没有从根本上解决商业应用存在的痛点。

## 3. DPoS (授权股权证明机制)

DPoS机制是一种全新的保障加密货币网络安全的算法。它在尝试解决比特币采用的传统工作量证明机制，以及点点币和NXT所采用的股份证明机制的问题的同时，还能够通过实施科技式的民主以抵消中心化所带来的负面影响。简单来讲，其工作原理实际上类似于董事会投票，给持币者一把可以开启他们所持股份对应的表决权的钥匙，而不是给他们一把能够挖矿的铲子。

DPoS机制有很多优点，其中一点就是大幅缩减了参与验证和记账节点的数量，缩减了需要确认的需求，将使得交易速度在很大程度上得到提升，签署区块的任务将会托付给网络选出的可信之人。与Po W机制和Po S机制相比较，DPoS机制能够在单一区块中容纳更多笔交易，从而将加密货币技术提升到了一个更高的层次，使其能够与中心化的结算系统相媲美。

## 4. Pool (验证池机制)

Pool本身的意思就是联营、合伙经营，因此Pool机制就是一种基于传统的分布式一致性技术加数据验证机制。Pool机制是当前行业区块链使用最为广泛的共识机制。其优点在于不需要代币也同样可以照常工作，这极大地提升了验证速度，可以实现秒级共识验证，并且在提升验证速度的情况下还提升了验证的安全性，是适合多方参与的多中心商业模式。

总而言之，4种不同的机制适合应用于不同的场景，区块链共识机制的作用就是在效率与安全之间达成最佳的平衡。相信基于区块链技术的不断演化和发展，会有更多的技术和机制应用到我们的生活场景中。区块链在比特币中的应用为人们通向数字货币打开了一扇门，而从数字货币到数字金融最终达到数字社会的道路依然曲折坎坷，因此，区块链共识机制需要进行更多的完善和创新。

## 智能合约

我们都知道，自动售货机的使用方法是塞进钱去，它就会吐出你选择的商品。虽然我们看不到自动售货机的工作机制，但是一条不变的事实就是你不塞钱，它就不会吐东西。

出来。基于自动售货机的启发，一位名叫尼克·萨博（Nick Szabo）的计算机科学家提出了“智能合约”这个概念。在他看来，购买者塞入一定数量的货币，选择想要购买的商品，就在购买者与自动售货机之间形成了一种强制执行的合约。当购买者塞进钱币并选择商品，卖家通过对自动售货机进行内置设定逻辑就可以为购买者提供商品和找零，这就是在遵守合约。但是一旦塞入钱币，却没有吐出商品那么就严重违反了合约。

由自动售货机引出的“智能合约”的定义，即一个计算机程序，是一个任何人都可以使用的去中心化系统，是一套以数字形式定义的承诺，包括合约参与方可以在合约上执行这些承诺的协议。

智能合约的达成必须具备以下几个条件，如图1-10所示。

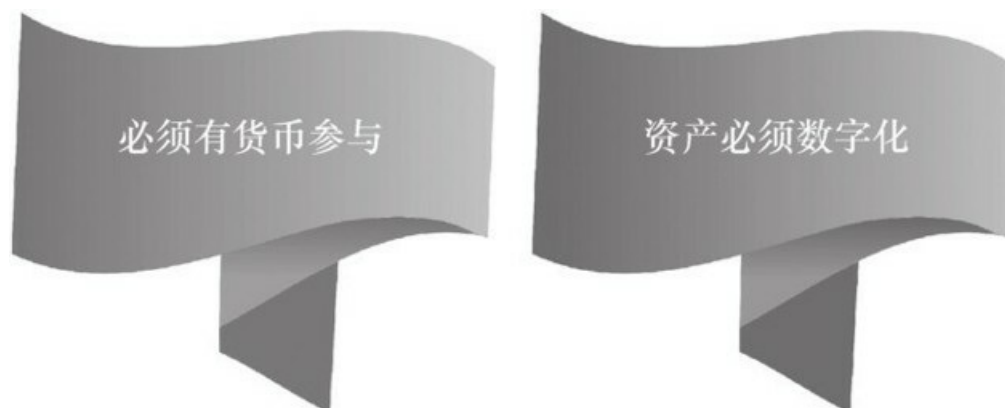


图1-10 达成智能合约需要的条件

#### 1.必须有货币参与

没有货币的交易是无法进行的，所以无论是使用法定货币还是使用加密数字货币，在交易中都是不可缺少的。

#### 2.资产必须数字化

如何能够将属于你的资产进行数字化呢？将你的房屋、汽车等进行数字化，就需要给其加一把密码锁。我们所开的汽车、居住的房子，其锁都属于物理锁，但是，设想一下，有一天，你的汽车和房屋只有通过持有密码学公钥的人才能打开，那么是不是为你资产的安全性提供了更多的保障呢？

在过去，合约的谈判、起草、签署、执行和跟踪是相互分离的，其成本高、效率低。但是通过区块链技术，合约不仅可以被植入整个交易过程中，还可以设置可执行的参数触发器，当具备不同条件时，系统自动跳转到相应流程，执行相应的指令，再反过来驱动新的合约的产生和执行。

智能合约是一段涉及资产和交易的代码，只有将其放在区块链上，才能有效防止出现“盗版”和“篡改”现象。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。

智能合约是一种全新的在参与者之间达成共识的方式。它的执行不依赖于任何参与者，而是自动执行的，违约情况几乎不会发生。智能合约将成为全区经济的基本构建，任何人都无需事先审查和承担高昂的预付成本，就可以使用这种方式来参与经济活动。

支付宝之所以受到广大商户和消费者的喜爱，关键点就在于它作为第三方金融机构，不会让交易双方之间出现买家付款、卖家却没发货的现象，而是需要买家事先将费用拨到支付宝，然后商家确认发货之后再把款从支付宝拨到卖家，这样就有效保障了交易双方的利益。支付宝这种工作机制实际上是与智能合约基本上一致的，其共同点就是基于信任而存在，使得工作效率更高，双方利益更具安全性。传统合同制定中，往往合同达成共识的各方会寻求类似支付宝这样的第三方信任机构来保证合约的正常运行，但是智能合约却移除了寻找对第三方信任机构的必要。

基于智能合约的不可篡改、无需寻找第三方信任机构等特点，人们对于智能合约充满了期待，但是智能合约的发展也存在一些现实的阻挠，主要体现在以下两个方面。

（1）目前基于区块链的资产数字化还远远不够。从内部依赖条件来讲，智能合约的应用是需要依赖于基于区块链的资产数字化的，但是，显而易见的是，当前基于区块链的资产数字化还远远没有实现，当前有的只是零星的尝试而已。因此，这对于智能合约的发展具有一定的阻碍性。

（2）智能合约是在去中心化的系统中自动执行的。如果仅仅智能合约的载体是去中心化的，这对于智能合约的发展是远远不够的。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，那么触发条件就容易出现不一致现象，这将会进一步影响智能合约作为一个去中心化系统的有效性。因此，智能合约的发展还需要依赖于事件或事实发生的去中心化，像去中心化预言机的出现就是一个典型。

从以上内容，我们发现，智能合约的应用并不是能够一蹴而就的，而是需要一个协作体系的建立与逐渐趋于成熟，才能一步步推动智能合约的不断发展。因此，可以说，智能合约虽然是区块链的创新技术之一，但是在大规模范围内实现成功落地还是需要一定的时间的。



## 区块链如何运作

区块链是支撑比特币的核心技术，但是其本身是一个完全独立的系统，可以说比特币是区块链技术的一个创新性应用。但是，区块链技术不仅仅局限于比特币的应用，它可以适用于任何形式的“货币”或“经济价值”。

区块链是一个具有“开放式”特点的自治账簿系统，按照复式记账方法记录了所有的交易数据，每一个单位的货币“从哪儿来”“到哪儿去”的全部详细历史数据。这里的“开放式”是指其存储的数据对于任何人来讲都是公开的、透明的，除了交易主体的隐私信息给予加密以外，任何人都可以查询其中的数据。所谓“自治”，就是指系统按照公开的算法、规则形成，在自动协商一致的机制基础上运行。区块链通过“开放”“自治”两个方面来保证记录在区块链上的每一笔交易都具有准确性和真实性。

### 区块链的记账方法

区块链从第一个“货币元”交易的发生开始到所有的交易进行记录，每笔交易都是按照复式记账的方式来完成的。由于任何一笔交易的借方和贷方的复式记账记录都是保存在一起的，因此每笔交易借与贷之间形成了会计关联关系，即一笔交易中的贷方总能够找到对应之前一笔交易的借方。通过这种方式就形成了一种复式记账的会计关联“链状”结构，这样就可以对每个“货币元”的详细档案记录下一个非常详细的描述：即基于复式记账的好处，可以从当前最新记录开始，采用倒推的方法逐级向过去追溯，就能得知每个“货币元”的过去的踪迹，能够得知其从哪里来，经历过哪些交易。这样，每个“货币元”的身世都非常明了，从而给识别和验证交易带来了非常大的好处，如图1-11 所示。

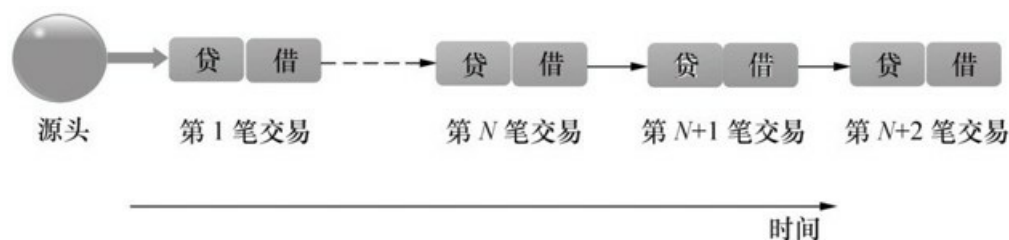


图1-11 复式记账的链状结构

甲要支付乙100“货币元”，乙就可以对甲的这100“货币元”的身世档案进行查询，乙追溯这100“货币元”的源头和出处，以及其交易记录，并且这100“货币元”最近的拥有者就是甲，对这100“货币元”的来龙去脉有更加清晰的了解之后，乙就可以放心接受甲提供的这笔钱了。如果乙在追溯过程中并没有找到这100“货币元”的源头和出处，就说明这100“货币元”不具备合法性，甲并不具备拥有这100“货币元”的资格，那么甲与乙之间的借贷关系就成为一种不合法关系，也因此使得借贷无法正常执行。只有那些可以追溯源头的“货币元”交易才可以被认为是合法的、可执行的。

那些被验证过的所有交易会被存储在区块链当中。显然，这样对每个“货币元”逐一追溯的话，整个“交易链”就会逐渐变得很长，按照以上的方法对每笔交易进行验证往往会耗费大量的时间，操作起来也比较烦琐。但是区块链就很好地解决了这个问题。

区块链采用了“分块”记录的方法，将发生在某一时间段内的交易打包成一个“区块”，每个“区块”与其前后向链接的区块按照时间顺序进行排序，每隔一段时间就会产生一个新的区块，将一个区块与其上个区块以及下个区块链接起来，就形成了“区块链”结构。这

样，我们可以将区块链看作一个不断增加页数的矩形账簿，每个区块可以看作一个账簿的一页，每页记录了一笔或多笔交易，每增加一个区块，则区块的堆高就增加一个梯度。

区块链借助Po W共识机制来确保只有合法的区块才能够添加进来。一旦一个区块通过了验证后链接到区块链中，就会被永久性地存储起来，任何时候都不会被任何外界因素所干扰、篡改。而每个区块链的合法性验证问题，包括对其中的所有交易的合法性验证以及区块之间数据关联性规则的验证。按照时间顺序将各个区块链接起来的方法实际上可以给人非常直观的感觉。这样就不必对每一笔交易记录进行全部验证，而仅仅是对其回溯的最近的某个区块进行验证即可。

另外，区块链采用分布式方式使得网络上连接的各个节点都保存了一份完整的账本副本，这些节点采用自治协议和规范，通过交叉审计和稽核，共同维护了区块链的完整性以及真实性。除了涉及交易各方的私密信息以外，区块链的数据信息对所有人都是公开的。任何人都可以通过公开的接口去查询区块链数据并且开发相关的应用。因此，可以说，区块链技术的应用使得账簿的真实性和完整性、合法性、公开性得到了很好的保障。

#### 区块链的运行机理

区块链的核心设计思想就是借助当前已有的成熟技术和条件，制定一个纯粹的、跨界的、具有信任特点的网络验证机制，在该机制的作用下，互联网经济变得更加简捷、容易。通常情况下是采用复式记账会计、Peer-to-Peer网络架构、基于机器算法的协商一致的自治协议、安全的数据存储传输使用规则、可持续运行的激励机制、开放式的系统来最大限度地“去中心化”，从而确保这个系统对任何用户都是“中性”和“可信”的，继而为交易各方的经济活动建立一个良好的信任环境。

具体来讲，区块链是如何运行的呢？区块链是建立在一个Peer-to-Peer网络架构基础上的自治系统，其运行体系主要包括以下几个部分，如图1-12所示。

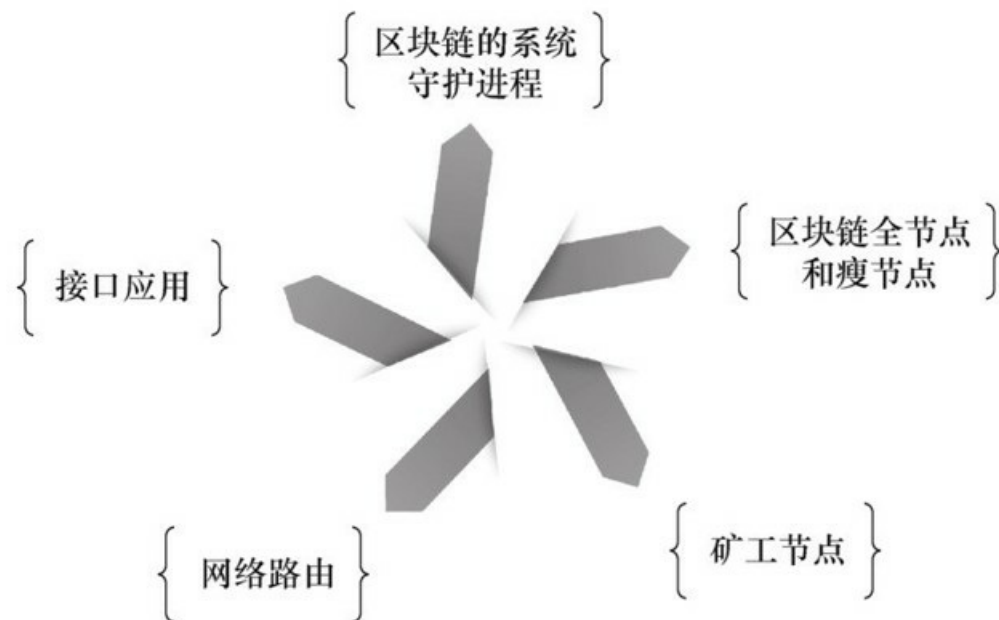


图1-12 区块链运行体系

#### 1.区块链的系统守护进程

区块链的系统守护进程是一种运行程序，该程序具有不断运行的特点，主要是用于处理服务需求。区块链的守护进程主要是驻存于网络中的区块链全节点的计算机中。

#### 2.区块链全节点和瘦节点

所谓区块链全节点就是在不需要外界指令的情况下能够自动执行验证任务。区块链节



点保持着完整的区块链并进行实时更新。瘦节点保存的仅仅是区块链的一个子集。

### 3. 矿工节点

矿工节点主要是采取竞争性规则来创建区块。这种竞争性规则就是谁能够率先解决一个PoW机制的问题，就意味着谁能够成功添加一个区块到区块链当中，并获得一定的奖励。

### 4. 网络路由

在每个区块链的网络中的节点上都嵌有一个专门接入网络、连接管理的系统，这就是网络路由。

### 5. 接口应用

区块链本质上是一种底层架构，它为上层应用提供多种接口，其中最常用的就是钱包，它是用户与区块链之间的应用接口。

当与网络连接的某一台服务器在运行区块链的系统守护进程的时候，就意味着一个区块链已经诞生了。通常由系统守护进程创建第一个区块。之后，区块链的全节点就开始逐渐扩张：一些节点计算机加入进来，并且按照Peer-to-Peer网络架构模式把这些节点一个个连接起来。这些全节点从网络中下载所需要的程序，并且将区块链上的所有数据都复制到本地。这种过程一直持续进行，直到全节点达到一定数量的时候，就产生了部分交易。紧随其后，矿工节点也陆陆续续加入进来。由于网络中已经有了“货币元”，因此，用户这时候就可以开始利用“货币元”进行交易了。在用户接口处会不断有新的交易请求信息发出来，而网络中的全节点会对这些新的交易请求信息进行监听，并且会对这些新交易中的“货币元”进行身世档案验证。但是，这时候经过验证的交易并不能直接存储到区块链上，而是需要与其相邻时间内产生的其他交易一起存储到新的区块后，这样才能保证该交易信息能够在区块链中永久保存。

除了最初的几个区块以外，其他的区块都是由矿工节点完成的。数量庞大的矿工每隔一段时间就会对新发生的交易进行自动采集，并将这些新采集来的交易以区块的形式进行打包。而区块链网络会将每一次新打包而来的区块进行设置，从而更好地保证区块链所记录的数据信息的准确性。当新的节点被加进来之后，全节点就会对网络中的其他节点下达通知，让其他节点的数据库进行实时更新。这样，区块链就按照时间顺序和交易的不断持续而逐渐增加。

## 区块链的技术挑战

2016年年初，中国人民银行举行数字货币研讨会之后，区块链的概念作为数字货币的关键技术进入了公众视野。也正是进入2016年后，区块链成为年度各大领域讨论的关键性话题。因为，虽然很多人对区块链并不是十分了解，但是该技术对于金融业、医疗行业、公证、通信领域等都有十分广泛的融合，区块链技术对这些领域的发展将产生不可估量的作用。但是，即便如此，区块链依然存在一些不可避免的技术挑战。

具体来讲，区块链面临的技术挑战主要体现在以下7个方面，如图1-13所示。

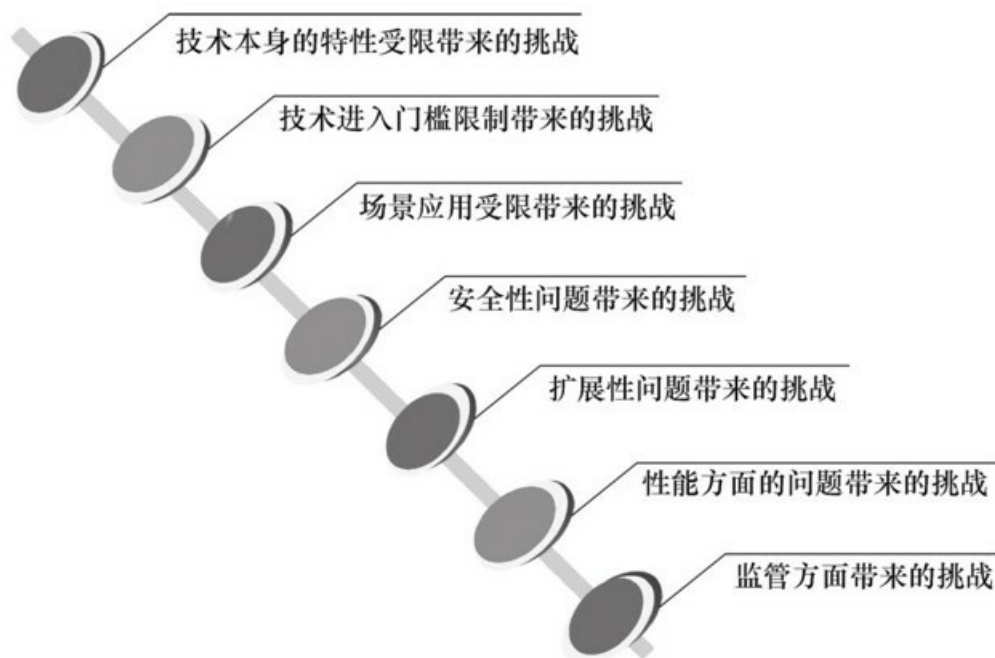


图1-13 区块链的技术挑战

### 1. 技术本身的特性受限带来的挑战

当前，很多人认为在所有行业中都可以找到区块链的踪迹，认为区块链是一个高度互联的、十分高大上的新型名词，但是根据当前的实际情况来看，区块链并没有非常成熟地应用在各个领域中，区块链在当前仅仅是处于婴幼儿时期，呈现一个比较原始的状态，这就好比是汽车出现之前的马车一样，虽然已经具备“车”的雏形，但是依然没有发展到更加成熟的阶段。之所以这么说，是因为区块链本身的交易速度是非常慢的，每秒钟的交易量是当前区块链在应用过程中所面临的一个重要的技术挑战。

### 2. 技术进入门槛限制带来的挑战

区块链技术本身就是一个非常复杂的技术，它涉及密码学、计算数学、人工智能等诸多跨学科、跨领域的一些前沿学科，一些普通的工程师是很难在短期内去完全掌握它的。要知道，对于一个新鲜的事物，往往是了解起来容易，真正掌握并将其应用的时候却发现很难。区块链亦是如此。

### 3. 场景应用受限带来的挑战

当前，很多在区块链方面研究的专业人士正在开发区块链的应用场景，一般可以将其应用场景分为虚拟货币类场景、记录公证类场景、智能合约场景、证券应用场景以及社会事务场景等，这些场景或多或少地涉及区块链的应用。但是换个角度来看，却与我们大众

生活的距离比较远，让人觉得区块链有点“高冷”，缺乏一些接地气的应用场景。因此，对于区块链技术的追捧，目前绝大部分是集中在一些高中端人群和企业中。基于区块链是以互联网协议为技术的，如果没有一个庞大的用户群作为发展基础的话，区块链在未来的发展前景将会受到极大的限制，将很难突破大众、主流市场。

余额宝是我们都熟悉的一个金融工具，但是，在余额宝创建之初，其发展是站在了阿里支付宝的“肩上”，从而使得普通用户规模能够快速增长。而区块链也应当借鉴余额宝的发展方式，这才是区块链发展并颠覆世界的真正起点。但是，就目前情况来看，区块链还没有找到合适的“肩膀”。

#### 4.安全性问题带来的挑战

从互联网角度来讲，在任何情况下，都不能够轻信一个系统是绝对安全的。区块链同样如此。尽管对于区块链系统的破坏需要攻击51%以上的节点，难度较高，但是这依然意味着区块链的安全性还有一定的漏洞，攻击者可以将攻击对象转换为攻击使用的个人，如侵入个人的钱包或者攻击相关平台等，因为用户与钱包之间的别名身份在匿名性上其实是相当弱的，加之比特币区块链交易具有公开、透明的特点，任何人可以通过观察区块链得出关于某事的结论。因此，区块链的安全问题也是一个巨大的挑战。

#### 5.扩展性问题带来的挑战

区块链本身是一个非常难以预测的系统，不论是其商业模式还是技术创新，当扩展到一定数量级的时候，由谁来承担责任就会成为一个难以解决的问题。

#### 6.性能方面的问题带来的挑战

数据在区块链上确权的问题实际上是由资源本身的特点所决定的。现实中竞争性资源可以放到区块链上进行交换；而数据型的、知识型产权，非竞争性资源反而不适合在区块链上边进行交换。[shu籍分享微信 whair004]

#### 7.监管方面带来的挑战

随着人们对区块链技术的关注越来越多，智能合约进入人们视野的频率也逐渐增加。简单来讲，区块链为智能合约提供了可执行的可信环境，即智能合约是区块链技术应用的一个拓展方向。但是2016年6月17日发生的一件轰动事件却给人们带来了警示。当天，黑客利用The DAO项目中的智能合约中存在的漏洞，劫持了高达360多万单位的以太币（合约6000万美元）。The DAO是一个基于以太坊的去中心化自治基金，是一个没有任何中心化的管理机构，由集体决策表决是否对某一区块链项目进行投资。这件黑客劫持以太币的案件让很多人对智能合约的安全性产生质疑，智能合约的声誉一下子跌到了低谷。但是从其发生的根本原因来看，实际上是因为当前还缺少一种能够在双方签署智能合约的过程中充当传统“律师”角色的介入者。

智能合约本身是一个不以人的意志为转移、进行自动执行的合约，并且一旦开始执行便会无法终止。因此，这个时候就需要由第三方角色对智能合约进行审查。随着智能合约应用范围变得更加广泛，对智能合约的创建和审查的需求也逐渐增加，由此诞生出新的行业。一旦有不法分子利用逻辑漏洞来破坏智能合约，产生破坏性影响，随之便会形成一些法律和监管方面的问题。当前，尤其是金融行业属于高监管行业，区块链技术应用于金融行业，将在全球范围内催生一个监管难题。因此，当前针对区块链技术结构，应当研发出更新的风险管控技术和应急措施，这也是区块链技术的一大挑战。

总而言之，区块链的发展前景是十分光明的，对于各领域发展的促进作用是不言而喻的，但是要想借助区块链技术快速推进各领域的持续快速发展，所面临的技术挑战依然是当前研究的重点方向以及亟待解决的重点。

## 区块链将颠覆我们的世界

2015年1月15日，全球首届区块链峰会“区块链—新经济蓝图”在上海茂悦酒店召开。该峰会吸引了来自海内外的近300位区块链领域的技术极客、创业精英、学术专家、投资人、金融机构代表以及监管决策者参会。在普及区块链技术概念的基础上，20余位演讲嘉宾分享了区块链在支付、互联网、供应链、证券交易、去中心化云存储、身份验证与管理、数字资产管理等方面的应用前景及案例。

资料来源：<http://www.8btc.com/blockchain-meeting>

我们可以从2015年在上海举行的这次主题为“区块链—新经济蓝图”区块链峰会中发现，实际上区块链作为一种先进的科学技术，已经强大到可以促进整个社会的基本发展，可以从经济、金融体系、政策上全面改善我们的生活，区块链正逐渐面向并进入我们生活中所涉及的方方面面，它是信息技术和数字化网络相结合的产物。可以说，当前，区块链正在改变为所能够想到的所有事情，在未来，将颠覆我们的整个世界，如图1-14所示。

### 1. 区块链对法治的影响

#### (1) 知识产权领域

区块链作为一种创新技术，也可以补充甚至取代当前现存的知识产权管理系统。例如，当前，我国的软件版权登记是需要去中国版权保护中心登记的，这是典型的中心化模式。但是如果将区块链技术应用于该领域，那么或许开发者手中的软件本身就可以成为登记证明。如果软件已发行的每一份拷贝也可以基于区块链技术，给予软件开发对软件更大的控制权，区块链这样的技术很可能会成为更加强有力的数字版权管理技术，到那个时候，区块链技术就可以将其应用场景扩展到对影视作品的版权和相关专利技术的有效保护方面。因此，基于区块链技术的知识产权将会在未来成为能够保证社会顺畅发展的一个巨大的转折点，届时，越来越多的经济活动将变得更加具有创新性。

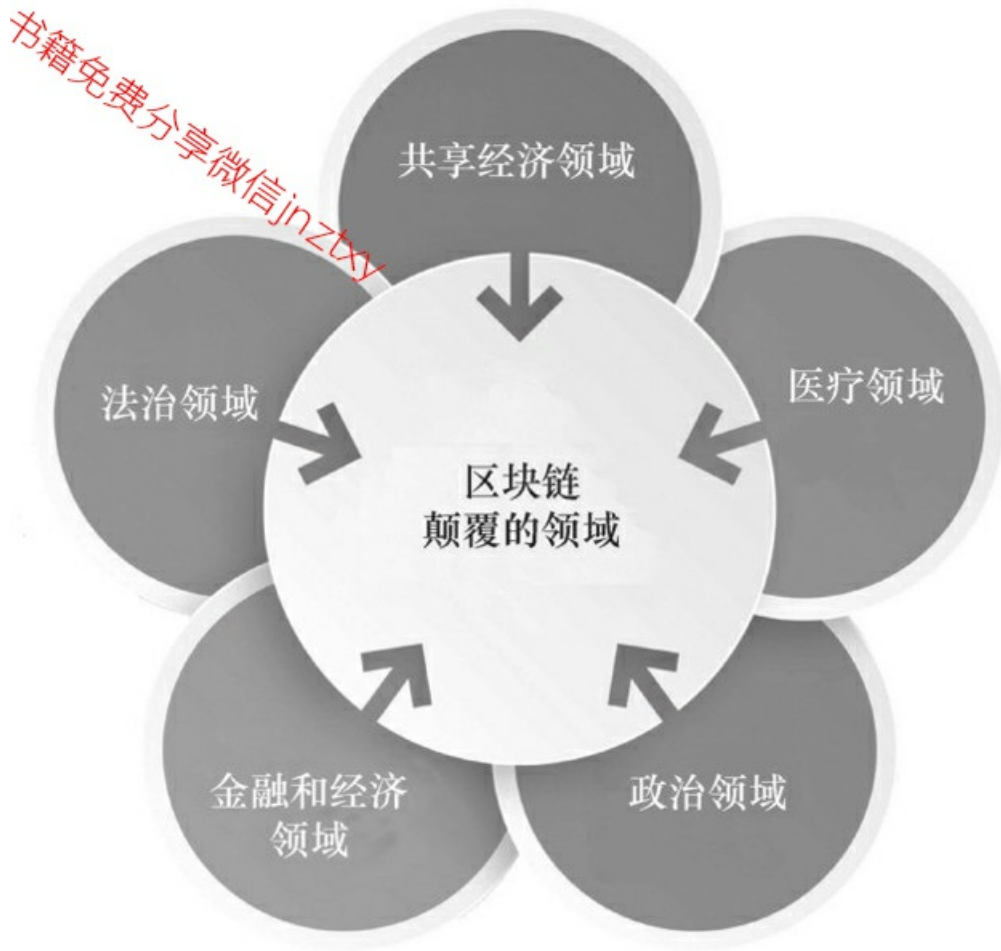


图1-14 区块链颠覆的领域

#### (2) 股权登记和证明领域

基于区块链本身具有确保数据真实性的特点，可以发现区块链有利于解决数据流通与追溯的问题，因此推断其具备优化当前法律规范的可能。例如，将区块链技术应用企业股东股权登记与证明之中。区块链能够在数据使用的过程中对其加以规范，并实现授权的精细化，防止数据滥用和违规使用的现象发生，能够确立数据使用的征信机制，实现数据的溯源。

#### (3) 个人信息使用和保护领域

区块链技术同样可以用于对个人信息使用和保护领域，这样就可以有效避免单一服务器所带来的风险，个人信息的安全性会得到显著提升，并且还可以提升用户本人对其自身信息的掌控度，包括其虚拟财产、邮箱、网络账号等。

#### (4) 合约领域

区块链在各行业的应用，同时也会催生新型的法律行为。传统的“代码法律”与区块链相结合，将打破原有的数字社会格局，并对其进行创新。在传统的现实社会中，法律往往借助合同来约束双方或多方当事人，合同是必须按照法律法规来撰写的。但是，在未来，法律可能不需要通过纸质合同来约束各方当事人，而是直接通过之前设置好的算法架构来实现，当法律成为一种代码，并借助于区块链技术加以实现，那么合同的功能将有更加宽广的拓展。

#### (5) 民事诉讼领域

当前，“互联网+”已经成为国家发展战略之一，受到诸多领域的热捧。民事诉讼为了



迎合这一发展战略，添加了“互联网+”的元素，例如，最新的《民事诉讼法》中新增了一个功能，就是“电子证据”，但是即便如此，在互联网上采集“电子证据”依然具有一定的难度。互联网上本身产生的数据就十分庞大且十分复杂，并且经过一定的技术处理，“电子证据”往往会出现失真情况。这个时候，借助于区块链的不可篡改的特点，可以有效缓解“电子证据”的失真现象。

## 2. 区块链对金融和经济的影响

区块链作为一项技术，率先应用的就是金融领域，并且给金融领域带来了巨大的变革，通过借助防篡改和高透明的特点将整个金融系统的成本降到了最低。证券市场是区块链应用的又一场景，证券市场和区块链之间具有很好的契合度，表现为传统的证券交易需要经过中央结算机构、银行、证券公司和交易所这四大机构进行协调之后，才能顺利完成交易活动，并且这种做法往往会造成效率低下、成本飙升的情况。正因为如此，使得强势的中介从中一跃而起，但却没有真正使金融投资者的权利得到有效保障，而区块链则可以独立完成一条龙式的服务。

奥纬咨询公司在2015年做了一份调查报告，该报告数据显示：“全球金融行业每年为交易清算付出的成本在650亿~800亿美元。”这一数字充分表明，传统证券交易的完成需要消耗的成本实在是很高。

针对这个问题，全球四大银行——瑞士银行、德意志银行、西班牙桑坦德银行和美国纽约梅隆银行已经开始联手开发新的电子货币，他们希望未来能够借助区块链技术完成清算交易，并且将这一模式定义为全球银行业的通用标准。并且，这四大银行还将与英国券商ICAP携手共同向全球各国央行推销该方案，并计划在2018年年初进行首次商业应用。

区块链技术，从本质上讲，就是一些算法的集合，借助于区块链的这些算法，可以不必像以前那样采用中央账簿的记账方式，而是直接通过使用网络将交易进行电子化确认。这些通过认证的对象就是机密货币，而比特币就是这些加密货币中的一种。金融机构在使用加密货币进行清算的时候，往往不需要等传统货币电汇到账，就可以直接使用电子货币，然而这些电子货币可以直接在央行处理转换成现金，之所以采用这种方式，关键在于它可以大大节省清算时间和金钱。当将这些存储在区块链中的电子货币转换成不同货币的时候，就可以即时应用于各种交易。

## 3. 区块链对政治的影响

区块链对世界的变革不仅仅体现在法律和金融、经济领域，对于政治、人道主义、社交、科学等领域也具有巨大的颠覆作用。区块链技术的应用，使得某些特殊团体可以处理现实中的诸多问题。例如，为了反抗压抑的政治体制，区块链技术可以用于制定一个去中心化的云端功能，这些功能可以由以前在司法权上受到限制的组织来管理，这种模式很显然对于像维基解密[3]这样的组织有很大的帮助，同时对那些保持中立政治立场的跨国组织也有帮助，像互联网标准群体ICANN [4]和DNS [5]服务。

## 4. 区块链影响医疗领域

区块链在医疗领域的应用主要是对患者的医疗记录进行保存，这一应用可以被看作区块链上的电子病历。如果把病历想象为一个账本，它由各个医院进行存储，但患者本人并不掌握，所以病人就没有办法获得自己的医疗记录和病史情况。这就好比银行记录的账目看不到过去的交易记录一样，会使病人在未来的就医过程中产生极大的困扰。但是基于区块链技术的个人医疗所记录的可用数据，不论是对未来的就诊还是对自我健康做科学、合理的规划，病人都可以对自己的真实病情有一个更好的掌握，而不是由某一医院或者第三方机构来掌握。另外，区块链技术应用于医疗行业，还可以对用户个人信息进行很好的隐私保护。

## 5. 区块链打造真正的共享经济

Uber、Airbnb和Lending Club等独角兽的一夜崛起，让共享经济火得一塌糊涂，几乎人人都在谈共享经济，人人都在实际发展中应用共享经济。但是2016年比共享经济更加

火爆的是比特币的底层技术——区块链。如果把区块链技术或者其采用的算法证明机制应用到共享经济中，就可以建成一个完全透明、无主、分散的共享平台和系统，即便在没有任何形式中介的情况下，依然能够保证各种交易方安全进行交易，这些交易方包括人、企业，甚至是 政府。

德国有一个名为Slock it的初创公司，突发奇想，利用区块链技术做一个智能锁，并将锁连接到互联网上，再通过区块链上的智能合约对其进行控制。然后，他们发给任何一个控制锁的人一把至多把钥匙，并且对私钥进行非常复杂的设定，包括什么时候启用智能锁、什么时候能开锁等。借助这种方式，共享经济能够实现去中心化，可以将任何能够被锁起来的東西进行租赁、分享、出售。这个新奇的概念很显然已经超出了常规的Airbnb用户服务的范畴，Slock通过这把智能锁对所有想要获得自己想要东西的人进行约束，只有支付一把私钥，才可以打开智能锁。当然，出租者也可以在用户走后随时更换私钥的定制，让整个体验更加方便、安全。同理，通过区块链技术设置的智能锁还可以进行自行车、密码柜的租赁等。

总而言之，无论政治、经济、人道主义还是法律系统、医疗行业等，抑或是我们前面提到的物流领域，都得益于比特币和区块链技术在传统基础上实现了重构。可以预见，在未来，区块链必将颠覆整个世界，打开未来的“金矿”也许就从区块链开始。

---

[1].量化投资：量化投资是指通过数量化方式及计算机程序化发出买卖指令，以获取稳定收益为目的的交易方式。在海外的發展已有30多年的历史，其投资业绩稳定，市场规模和份额不断扩大，得到了越来越多投资者认可。

[2].机器人投顾：机器人投顾又叫智能投顾，是量化交易、大数据、人工智能等多种技术的进一步结合和升级，它依托大数据和量化投资算法，让理财变得更简单、更智能。

[3].维基解密：是一个国际性非营利的媒体组织，专门公开来自匿名来源和网络泄露的文档。

[4].ICANN：互联网名称与数字地址分配机构，是一个非营利性的国际组织。

[5].DNS（域名系统）：因特网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便地访问互联网，而不用去记住能够被机器直接读取的IP数串。

## 第二章 人工智能时代，区块链带来金融科技的新蓝图



区块链技术被认为是继蒸汽机、电力、信息和互联网科技之后，目前最有潜力触发第五轮颠覆性革命浪潮的核心技术。仿佛一夜之间，“区块链技术”成了科技界和金融圈里最时髦的名词。放眼国内外，各领域的专家，尤其是金融人士，都对它青睐有加。作为比特币的底层技术，区块链不仅不像比特币那样饱受争议，还正在更大程度上被接受着、被扩展着。未来，人工智能时代，区块链必将给金融科技带来发展的新蓝图。

书籍每日免费分享微信jnztxy朋友圈



## 区块链重构金融业

比特币概念自2009年出现后，其底层区块链技术才从小众自由派密码学专家与电脑黑客的试验中走出来，逐渐成为开始吸引高科技公司、跨国金融机构和创投基金的投资新热土。

我们知道，区块链技术本身来自比特币，而比特币又是金融领域中的一个因子，因此，区块链最早接触以及应用最多的领域就是金融领域。当前，在传统的金融行业中，区块链涉足最多的就是银行、证券交易、P2P网贷、保险等环节，而诸如医疗、供应链、物联网、物流、游戏、公证、人工智能等领域，区块链的应用还仅仅处于初级或者概念设立的阶段。

区块链技术本质上是一个由所有参与方共同维护的去中心化的公共账本记录技术，是一种几乎不可更改的分布式数据库和账簿记录技术。它能够实现数据的分布式记录和存储，而并不是由统一的中心数据库处理，区块链技术更好地借助其去中心化的特点，从而保证账簿记录的交易时间先后顺序，保证账簿记录内容不被篡改，使得被保存的账簿内容具有可信性。由此可见，这种与账本记录有关的技术也是与金融关系最为密切的一个方面，更好地解决了金融领域最大的问题，即信任问题。可以说，区块链技术是人工智能时代实现金融领域可信性的理想技术。

虽然区块链目前还只是应用在基于比特币的虚拟货币领域，但是越来越多的权威金融机构在研究过程中发现，通过对区块链技术的进一步认识，区块链技术对传统金融的颠覆性影响，甚至可以说区块链技术为金融进入2.0模式打开了一条通道，尤其是对金融业的重构起到了超乎想象的作用。

具体来讲，区块链技术重构金融业主要表现为以下几个方面，如图2-1所示。

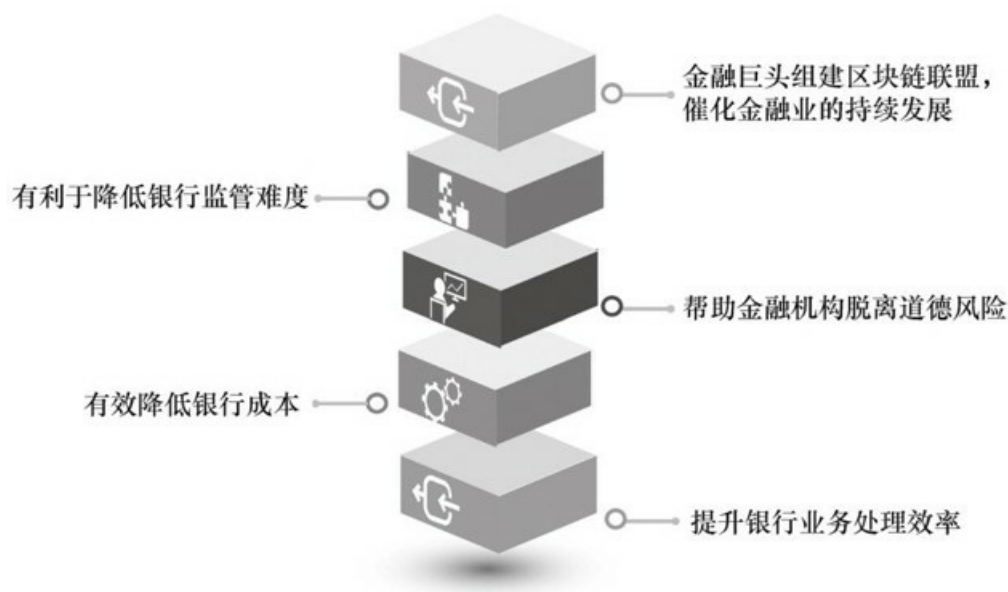


图2-1 区块链重构金融业的5个方面

### 1. 区块链提升银行业务处理效率

在当前货币交易模式中，银行履行了包括进行电子转账等第三方机构的职能，尤其是在当前全球化贸易环境下，银行在跨境交易的过程中出现的频率越来越高，并且必不可

少。但是，基于当前跨境计算耗时长、费用高等情况，尤其是不同国家采用不同计算程序，往往需要花费2~3天才能使资金到账，导致跨境支付的效率极为低下。区块链技术应用于跨行支付，就会使得这种情况发生很大的扭转。区块链作为第三方金融机构的中间环节，可以使得跨境支付的双方在交易结算的过程中通过点到点的方式快速且自动完成，使得结算速度大幅提升，并且还可以实现全天候支付、实时到账、提现便捷、无隐形成本。

麦肯锡区块链数据报告显示，从全球范围来看，区块链技术在B2B跨境支付与结算业务中的应用将可使每笔交易成本从原来的大约26美元下降为15美元。

## 2. 区块链有效降低银行成本

在当今的金融体系中，银行是一个典型的“中心化”代表。举个简单的例子，如银行花费大量的人力和财力去建造一个客户数据库，并且要经常去维护和管理、更新数据信息。目前，几乎所有的信用中介职能都是通过中心化的第三方服务来实现的，究其原因，在于金融的起源来自于信息不对称所带来的不信任性。从近代银行起源到现在的整个发展历程来看，金融业每发生一次巨变都是随着科技进步的演变而出现的。虽然中心化可以在一定程度上解决信息不对称的问题，但是随着系统规模的进一步扩大，一些弊端也随之产生，维护成本也逐渐增加。如果借助于区块链技术的“去中心化”，通过分布式记账与集体性数据维护，银行业的成本则会大幅削减。

西班牙最大的银行桑坦德银行发布了一份报告，其中有一条报告内容是这样的：“如果2020年左右全世界的银行内部都使用区块链技术，那么每年大概能够节省下来200亿美元。”

## 3. 区块链帮助金融机构脱离道德风险

任何科技创新与发展都离不开资金支持，因此，金融业是积极拥抱科技的先行者，没有金融业的大力支持，任何科技创新与发展都无法顺利进行，但是所有的科技进步都能够改进金融业的信用中介职能。基于银行票据交易是一项重要的常规业务，目前我国现有的汇票业务中，有70%都是通过纸质的形式完成的，但是在操作环节中处处需要人工参与，而且因为在该业务中往往会涉及较多中介参与以及人为介入，因此各个环节出现人工操作失误的可能性提升了很多，也使得票据市场出现了大量的违规操作或者客户欺诈的行为。2015年，我国国家商业银行在汇票业务中出现了信用风险。如果借助于区块链技术，这种问题吗迎刃而解，它使得人工参与业务的机会大幅减少，同时还可以将原来的纸质作业转化为数字化程序，从而有效降低了因人工失误而导致的失误。

麦肯锡通过对这方面进行研究，测算出区块链技术在供应链金融业务中的应用能够帮助银行在一年的时间里缩减风险成本11亿~16亿美元。

## 4. 区块链有利于降低银行监管难度

近几年，各大商业银行为了满足日趋严格的监管要求，不断投入人力与财力，并以此加强信用审核以及客户征信，从而防止反欺诈、反洗钱以及复杂金融衍生品过度交易引发的系统性风险。然而，如果银行建立起了自己的区块链，那么客户信息与交易记录就会较传统模式更加真实，而且还能够确保不被随意篡改，这样对于银行识别异常交易并防止欺诈行为的出现会有很大的帮助。另外，如果客户信息和交易记录能够实现自动化加密关联共享，那么银行之间就能够省去诸多重复性工作，银行也可以对共享的分布式账本内客户交易行为进行分析和检测，一旦发现异常，就会利用技术消除欺诈、洗钱等犯罪行为。

## 5. 金融巨头组建区块链联盟，催化金融业的持续发展

当前，全球金融正面临着巨大的成本压力，因此，急需借助金融科技来压低成本。当前全球金融业的现状：自2008金融危机以来，银行业的赢利状况一直没有持续好转，美国银行业也呈现疲软之态；欧洲银行也更是惨淡，在2015年出现了大面积亏损现象。因此，在这种盈利有减无增的持续恶化的环境下，以及整体金融业长期存在低息环境，使得收入无法实现持续向好，这也是金融领域出现大面积裁员、增加科技应用的直接原因，从而减少成本带来的巨大压力。区块链技术当前在金融领域中的应用只是一个初级阶段，并未达到成熟，但是科技与产业的密切结合将进一步加快区块链技术在金融领域的应用进程。可以预见，未来区块链技术必将成为金融领域各个企业之间争夺市场的主要工具。自2015年以来，全球各大金融机构已经开始着手组建区块链联盟组织，这或将成为区块链与金融业更加紧密结合的催化剂。

2016年年初，区块链与金融发展的头条消息就是微软宣布联手R3区块链联盟，并计划为各大银行和企业开发并测试一套全新的技术，进而将现有的老系统全部更换掉，以此来提高整个金融系统的工作效率。微软希望借助于Azure云服务让那些与它公共合作的伙伴能够逐渐扩大区块链服务的使用范围，并且希望这一转变能够更快实现。

R3CEV作为一家总部位于纽约的区块链创业公司，成立于2015年9月，其核心职能就是制定银行业区块链技术开发的行业标准，以及探讨实践用例，并建立银行业的区块链组织。至今，R3已经成功吸引了60多家巨头银行加入到R3区块链联盟，其中包括花旗银行、丹麦银行、德意志银行、高盛、汇丰银行、澳大利亚联邦银行、美国合众银行、加拿大皇家银行、法国巴黎银行等。目前，R3联盟已经完成了两轮金融机构的大规模参与的测试。值得一提的是，该联盟中所囊括的银行都是世界排名前50的银行。R3所倡导的区块链技术将很快在国际金融支付和清算领域中进行实际应用，而这一应用最先颠覆的将是当前金融领域中现有的支付系统。

区块链作为比特币的底层技术，已经率先迈进金融领域，并给金融领域的发展带来了极大的颠覆性作用，为未来人工智能时代的实现提供了极具前景性的创新。

## 互联网金融VS区块链金融

区块链是当下的热门话题，一些互联网创业企业项目如果不与区块链搭上关系，都感觉没有跟上时代潮流。因此，不少国内外金融机构、商业机构都在想方设法利用区块链技术在改进业务模式方面进行各种各样的尝试，而传统金融机构也在积极布局区块链，探索区块链技术可能的使用方式。区块链技术已经被视为下一代价值互联网的基本协议之一，对全球金融体系所带来的巨大影响是不容忽视的。

在互联网金融普及的今天，会不会进入一个全新的时代，即智能化的区块链金融时代？区块链金融的定义如何？区块链金融与互联网金融有什么差异呢？

### 互联网金融

随着人类科学技术的不断发展，互联网和金融之间已经产生了千丝万缕的联系，二者已经深度融合，已经不再是两个相互隔离的领域。互联网金融的概念也正是由此而生。随着互联网金融的不断实践和发展，逐渐成为我国金融界和IT界的热门话题，越来越多的人开始认可互联网金融，而互联网金融也给我们的生活带来极大的影响。在国外，金融科技（Fintech）已经成为了一个热点词汇，金融科技主要是指互联网企业或者高科技公司借助云计算、大数据、移动互联网等新兴技术来开展的低门槛金融服务。从表面上看，国外的金融科技和我国的互联网金融是不完全相同的，但是从本质上看，二者之间还是有一定的共同点的，即它们都是新的技术手段和传统金融的结合。从这一角度来讲，无论是国外还是国内，在互联网金融发展的方向方面还是一致的。

金融成为现代经济持续发展的基础和核心，当前，金融对各领域的影响已经超过了以往任何一个时期。互联网金融的兴起使得银行、证券、保险等之外的其他电子商务公司和IT企业也参与到互联网金融的创新过程中，从而诞生了更加丰富的互联网金融商业模式。金融业与非金融业之间的界限已经逐渐模糊。

互联网金融与传统金融相比，具有以下几个方面的特点，如图2-2所示。

#### 1.传统金融本质不变

互联网的出现给金融业带来的变化仅仅是形式和手段两方面的变化，而不是内涵或本质发生改变。互联网金融并不会改变金融的本质。

对于互联网不会改变金融本质来讲，我们举个简单的例子：以电子商务与传统生意之间的关系为例。电子商务并没有改变交易的本质，而是借助互联网打破信息不对称，提升了交易的效率，降低了交易成本。同样，互联网金融也是如此，改变的只是金融业发展的形式，从传统的线下金融活动连接到互联网上来完成，与传统金融活动相比，很大程度上提升了金融业的交易效率，而基于互联网“免费”的特点，降低了交易成本。

		互联网金融	区块链金融
不同点对比	金融本质是否变化	金融本质不变	对金融的空前颠覆与创新
	信息是否对称	信息不对称	信息对称
	中心化是否存在	中心化依然存在	去中心化
	成本是否高	成本相对较高	有效降低成本
	风险是否高	风险相对较高	有效降低风险
相同点对比	+ 金融	互联网金融和区块链金融都是新的技术手段和传统金融的结合	

图2-2 互联网金融PK区块链金融

互联网金融是新技术条件下金融手段的一种演化，并不会改变金融服务的内涵，主要表现为以下几点。

（1）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，并以此来服务实体经济。

（2）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。

（3）互联网金融不会改变金融风险。这里所指的金融风险包括市场风险、信用风险、流动性风险、操作风险、声誉风险、法律法规风险等。

## 2.信息不对称

这里所讲的信息实际上就是金融活动中所产生的知识差，这个差别包括信息的完整度和时间差。实际上，造成这种信息不对称的原因有两个方面：一方面是信息的传播渠道，另一方面是个体之间处理信息能力的差异。对于个体信息处理能力的差异往往是客观存在的，而随着信息传播渠道的不断进步，如互联网的不断普及，一直在降低信息不对称的程度。

金融存在的价值就是资金的融通。在金融领域，信息不对称是普遍存在的，如中央银行和商业银行之间的信息不对称、金融服务的参与各方之间存在的信息不对称等。很多时候，这些信息不对称会给违规企业或银行等带来非法行为的漏洞，进而造成道德风险，例如，金融机构借助自身信息优势违规经营、企业骗贷、银行惜贷等。信息不对称往往会导致金融秩序混乱，并且还会降低市场的运行效率，加大金融风险。

## 3.中心化结构依然存在

对于传统金融来讲，其典型的特点就是结构中心化，而互联网的出现推动了金融体系的重构，因此，在互联网时代，去中心化、去中介化成为一大趋势。但是，从当前的发展现状来讲，互联网金融的去中心化、去中介化还依然处于理论阶段，也就是说，在实践过程中依然缺乏能够实现去中心化的核心技术。这也就表明，当前互联网金融的理念和商业前景已经得到了大众的普遍接受，而在技术基础方面依然没有跟上理念的步伐。

基于当前的技术水平，金融业虽然在一定程度上摆脱了传统的中心化机构，实现了更高的信息透明度和效率，但是互联网金融服务的提供者由于受到技术的制约，使得去中心化没有完全实现。更严重的是，有一些所谓的互联网金融平台，不但没有完全实现去中心化，还缺乏传统中心化机构应有的信用保障和风控能力，进而导致尝试这些平台的消费者需要承担更大的风险。

在我国，P2P跑路事件频频发生，据权威机构调查数据显示，我国仅2015年就出现了660家跑路的平台，2016年1~2月就有约200家平台跑路。跑路现象往往让人深恶痛绝，与我国的跑路情况相比，起步更早的美国P2P网贷，却很少见到“卷款跑路”的现象。但是2016年5月，美国最大的P2P借贷平台Lending Club因为出现内部违规操作而让人震撼，其股价一周之内暴跌40%以上。这种因信用保障和风控能力缺失而导致的跑路现象，往往会给广大消费者带来非常惨重的损失。

## 区块链金融

传统金融在一定的科学技术基础上，呈现出更具有创新性的金融形态和模式，区块链的出现也为金融的发展带来了更加前沿的发展契机。“区块链+金融”是对金融领域的空前颠覆和创新。

区块链能够给金融业带来十分巨大的价值，主要体现在以下几个方面。

### 1.降低成本、提升效率

(1) 减少沟通成本。以证券交易为例，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，这样就会造成成本过高的结果。然而，区块链则可以通过多重签名等技术实现一条龙服务，并且可以共享信息，从而有效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) 缩短结算周期。区块链交易被确认的过程实际上就是清算、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。

### 2.降低风险

(1) 由于交易确认完成清算和结算，因此大大降低了交易对手的风险。

(2) 区块链使得交易过程数字化，并且进行了完整的记录，能够有效控制欺诈、手工输入过程中的人为因素导致的操作风险。

(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。

### 3.驱动新型商业模式的诞生

区块链技术的特点就是能够实现一些中心化模式下难以实现的商业模式。当前，在物联网产业，已经有相关机构提出要使用区块链技术去管理上百个物联网设备的身份、支付和维护任务。

### 4.推动去中心化

金融去中心化的动力来源于对技术的变革，去中心化可能会直接影响金融活动的规则，这种规则包含法律层面、商业文化、金融文化等各个方面。要知道，金融中介的出现遭遇去中心化，去中心化有效解决了金融信息的不对称性，以及搜寻成本、匹配效率、交易费用等方面的问题。区块链推动金融区中心化，使得金融业的全新信息匹配获得了实现的可能。

区块链金融的去中心化将会对金融业产生以下几个方面的影响：

(1) 区块链的去中心化技术应用于金融领域，可以提高资源配置的效率；

(2) 区块链的去中心化技术对实体经济有一定的影响，而且还会影响金融的发展方向，从而涌现出“小而美”的产业与企业形态，使得分散化、及时性、智能化、合作共赢的新型金融服务的落实变得更加有必要；

(3) 落实到制度层面，基于程序算法等，打造出一整套具有开放性、透明性的公共“游戏规则”。

区块链金融是传统金融互联网化、智能化的本质创新

金融机构存在的价值在于能够使人们在价值交换的时候能够降低成本，提高效率。对于价值互联网来讲，这是互联网技术发展的一个更高层阶段。2009年，区块链技术伴随比



特币的出现而出现，因此，可以认为2009年是价值互联网诞生的元年。当互联网技术逐渐发展升级到价值互联网阶段的时候，实际上是赋予了传统金融机构一个互联网工具，这样能够使得金融业企业内生的许多业务流程和应用场景实现了互联网化。简单来讲，就是传统金融企业要想真正实现“互联网+”，仅仅凭借学习电商或社交网络是远远不够的，因为传统金融企业实现“互联网+”仅仅属于信息互联网领域。如果想要传统机构真正实现互联网化，获得新生，关键在于利用价值互联网的工具来改善内生的业务流程，改善建立在金融体系上的应用场景，这样才能最终将其互联网化，这样的企业才能称为真正的互联网金融企业。因此，从这个层面上来讲，区块链就是传统金融机构实现向互联网金融企业转型的有效武器。换句话说，“区块链+金融”是传统金融实现互联网化的本质创新。

真正实现传统金融向互联网金融转型并不意味着仅仅开发几个APP就算实现了，而是看是否应用了区块链技术。这就表明，互联网金融是要建立在区块链技术的基础上，通过利用互联网技术而改变传统金融机构的核心生产系统。

当前，很多传统金融企业还没有真正与互联网接轨，互联网不仅可以改变金融的本质，还可以帮助金融更好地、自主地发挥其价值。金融的本质就是需要通过降低成本、提高效率而为广大人民提供金融交易服务。对于这一点，我们前边也讲过，区块链能够通过智能合约技术降低成本、提高效率，进而帮助人类社会更好地从事智能化的价值交换。因此，区块链技术则是金融本质的绝佳体现，只有区块链技术才能帮助金融更好地体现其本质和价值。

注意：

虽然区块链金融拥有很好的发展前景，但从目前的发展情况来看，区块链金融还存在一些“瓶颈”，主要表现为区块链金融技术在P2P领域中的操作和实践还存在着一定的难点。

（1）当前，区块链技术在金融领域中的应用还处于初级实验阶段，因此，对于区块链技术的完善性和市场应用效果还需要一段时间来检验。目前，已经有越来越多的互联网金融机构开始效仿传统银行保险机构，但也有不少相关机构对区块链金融业务依然保持观望态度。

（2）区块链技术是一种分布式记账的数据库系统，因此使得区块链本身不具备规模经济效应，尤其在区块链技术处理大规模运算以及实时性数据更新的过程中往往表现出极低的操作效率，这样就不一定能够满足P2P或供应链金融业务规模的扩张与交易数据的实时更新的需求。

（3）区块链技术具有信息内容不可篡改的特点，但是随着区块链技术的进一步发展，也不能完全排除有些黑客能够找到盗取或者篡改用户区块链数据的其他方法，这样势必会引发金融服务领域道德风险隐患。

（4）当前，区块链技术作为一项全新的技术，对广大用户来讲，还没有完全认识和真正理解区块链的真正内涵，以此，提升用户的认知度还需要一定的时间，从而导致区块链技术在金融领域中的推广成本提升，这也是不少互联网金融机构所顾虑的一个方面。

## 区块链助力共享金融的实现

2016年3月31日，“全球共享金融100人论坛·深圳春季峰会”在深圳成功召开，本次峰会的聚焦金融领域的关注重点——“风险防范与发展机遇：共享金融与区块链”问题。

2016年9月23日，在北京举办了一场题为“新规范·新科技·新发展——2016中国·北京互联网金融创新论坛暨《中国互联网金融发展报告（2016）》新书发布会”。该蓝皮书指出：区块链将有望主导共享金融，区块链金融可能是未来共享金融的高级形式。

无论是与“共享金融”有关的峰会还是论坛，实际上都表明当前共享金融已经成为推动金融业发展的重要动力。

在讨论共享金融之前，首先要讲的是共享经济。在过去，解决公平问题往往是靠平均分配来实现的，但是随着时代的变迁，平均分配已经不能让人信服，因此多劳多得成为解决公平问题的又一方式。但是，这种解决方式是建立在正经济的情况下实现的，如何在负经济的情况下依然实现公平公正呢？随着经济体制的不断变化与发展，原有的“平均分配”“多劳多得”已经不能适应新问题，因此，老套路理论也不能够解决新问题，创新则是必然的。共享经济就是一个很好的途径。因为共享经济从根本上、从准入层面解决大家共同参与并享受经济发展成果的机制。而金融作为经济的对应物，其深厚的根源一定是存在于经济制度中的。既然整个经济有向共享方向发展的要求，随之就有发展共享金融的需求。

### 何谓共享金融

“所谓共享金融，就是通过信息与网络时代的金融技术与制度创新，构建以资源、要素、功能、利益共享为特征的金融发展模式，努力实现金融资源更加有效、公平的配置，从而在促使现代金融均衡发展和彰显金融消费者主权的同时，更好地服务于经济社会的创新、协调、绿色、开放、共享型发展。”共享金融则重点强调和体现金融的个性和民主以及后工业时代和消费者主权社会对金融小而美的新要求，注重普惠金融、用户体验、各方共赢、利益共分、机制共担。

区块链为实现金融资源人人共享奠定基础

区块链为实现金融资源人人共享奠定了以下基础，如图2-3所示。

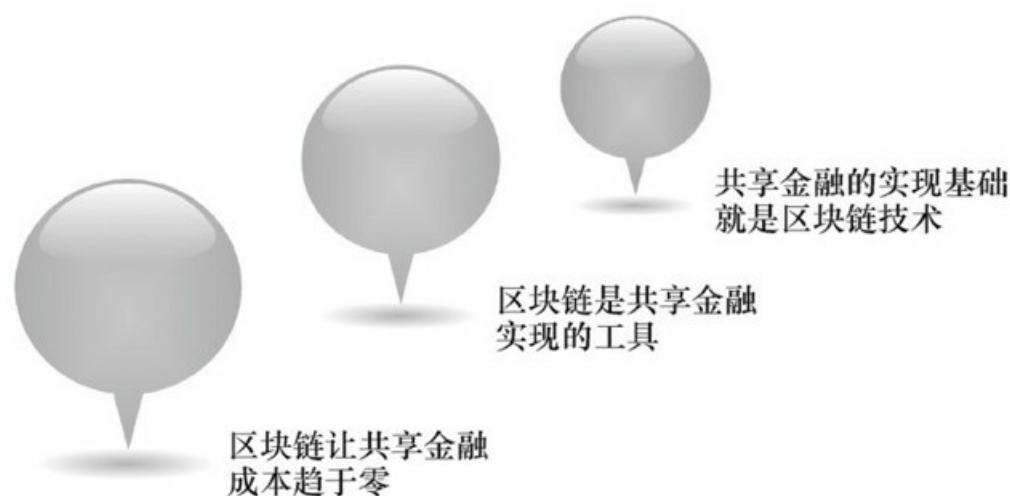


图2-3 区块链为实现金融资源人人共享奠定基础

### 1.共享金融的实现基础就是区块链技术

区块链作为互联网分布技术和金融制造相结合的新兴技术，比金融模式的发展要更进一步，在现有的制度和规则下，金融活动中的话语权掌握在中介机构手中，如银行、第三方支付机构等。金融的核心就是实现资金资源的合理分配，有效把控金融风险，因此，这就对金融中介提出了更高的要求，即必须专业化。互联网是一个能够实现金融中介电子化的工具，而在向电子化转变的过程中区块链技术能够对可能出现的风险进行有效控制。金融模式的实现使得业务操作模式中供需趋于相等，使得金融业有关的信任、信息、评级、金融技术等都能处于对称阶段，区块链凭借其去中心化的特点，为共享金融实现金融的人人共享奠定了坚实的基础。[shu籍 分 享 微 信 whair004]

## 2.区块链是共享金融实现的工具

在一定程度上，区块链可以看作一种实现共享金融的工具。有了区块链，才能够充分地揭示金融作为信息行业的本质。到目前为止，我国金融并没有有效、充分地展示其在信息行业的特征。其实金融本质上就是一个信息行业。之所以这么说，是因为有人对金融的利润来源进行过研究，发现90%的利润是从信息收集、分析、处理的过程中获得的。在过去，即便是产生了大量的数据信息，但是由于创新技术的匮乏，使得这些数据信息不可得、不可用。然而，在区块链技术基础上，这些数据变得可得且可用，可以通过收集金融交易过程中的数据信息来判断用户的信用度，以及给用户提供量身定做的金融产品和服务。另外，区块链、互联网在金融领域的应用，使得共享金融的成本大大降低，人人都可以共享金融资源，这样就出现了如众筹、网贷、保险、供应链金融之类的金融活动，让更多的人从享受共享金融服务的过程中获得实惠。

## 3.区块链让共享金融成本趋于零

共享金融可以让更多的人享受金融服务，不仅是因为互联网带来的便利，更是因为区块链本身就具有减少交易成本、提升交易效率的特点，甚至能够将成本降到趋于零。

金融服务无非就是满足广大用户3个方面的需求：投资、融资和支付。对传统金融而言，往往在这3个业务上设有较高的门槛，这是因为如果不设门槛或者低于这个门槛，金融机构就会赔钱。但如果借助区块链技术发展共享金融，那么这个难题则迎刃而解。区块链使得各个节点拥有权限的参与方通过多重签名的方式对相关的金融信息进行共享，减少额外的人工成本，并且有效提升整个业务的协作效率。

当前在投资、融资和支付领域，虽然基于区块链技术的共享金融才处于发展的初级阶段，但是值得肯定的是，共享金融已经成为金融领域的一种发展趋势，并且已经超乎预料地呈井喷式发展。有人预测，到2020年，共享金融将发展出更加丰富的生态圈并细分出巨量业务，总规模将达到万亿元；更有人大胆地预测，未来某一天，会有一大部分银行从金融领域消失，那些专业的金融机构也会消失大半，金融会依附于各种商业活动随时解决交易过程中所遇到的问题。总之，区块链技术深刻影响和变革了人们的生活，尤其是未来人工智能时代，金融领域必将在区块链的帮助下推动金融资源向着更加公正、公平的美好方向前进。

## 区块链变革金融服务的基础设施

2016年11月9~11日，广州举行的2016年世界经济论坛发布了一则联合研究报告，报告题目为“金融基础设施的未来：区块链重塑金融服务的大胆探索”，该报告中，分布式账本技术与流动性管理、合规性监管、内部及外部协调的关联获得了关注。

诚然，分布式账本技术凭借其透明性、不可篡改性、商业规则的自适应性，得以实现无中介的资产转移。这也正是区块链技术对于金融服务基础设施变革的原因，另外，这种变革还需要结合认知计算、人工智能和云技术之后的区块链技术才可以实现。具体来讲，区块链技术对金融服务基础设施的变革主要是审计的变革、资产确权的变革，如图2-4所示。

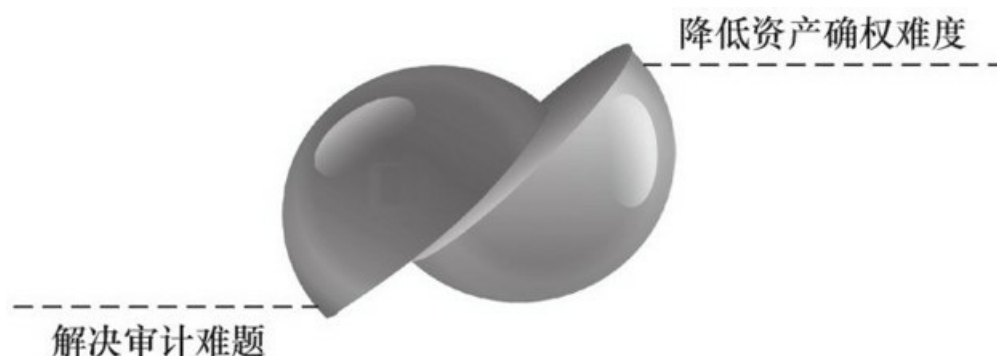


图2-4 区块链变革金融服务基础设施的两个方面

### 1. 区块链解决审计难题

通常情况下，审计员在进行年度审计和专项审计时，要进行很多必需的专业审计过程来确保所审企业的资金流动、交易往来的真实性，从而帮助审计员更好地出具对企业财务报表的审计意见，而这其中的很多过程都需要投入大量的人力、物力和财力，从而更好地保证审计结果的真实性。

区块链技术的应用使得这项业务变得更加轻松。如果企业与企业之间的资金往来、交易往来等能够真实无误、不可篡改且在全网上有时间戳记录，那么审计员的基础性工作将得到极大的减轻，同时更能保证审计的独立性。因此，区块链技术应用于审计行业，必将给审计行业带来更具价值和意义的变革。

任何经济活动都是建立在信任的基础之上的，维持客户的信任不仅要投入资金成本和时间成本，否则获得的效果往往并不显著。在现代经济社会中，信任缺失已经成为一个非常严峻的问题。基于信任缺乏的问题，要投入大量的资源来进行审计和记录核查，从而降低经济效率和投资回报率。诸多传统金融机构都已经逐渐发展成为维护金融领域信任的中介，如银行、托管机构、审计行业等。之所以需要借助如银行之类的传统金融机构来维护交易双方之间的信任关系，是因为金融活动或金融行业对信任的要求越来越高，需要专业人员的有效监管，才能保证金融活动的有序进行。

区块链作为一个基于信任的公开总账，可以将所有发生的交易记录在区块链上。区块链上的每个节点都可以将数据更新到网络，每个参与维护的节点都能通过复制获得一份完整的数据拷贝，这样就形成了一个去中心化的分布式数据库。在这个数据库中，区

区块链是利用数学方法在各方中建立起信任关系的，无需第三方参与，并且使得成本降到最低，接近于零成本。因此，基于这一点原因，区块链技术在当前发展未达到成熟阶段的情况下，应当以传统高成本的信任获取方式为切入点，而审计行业就是一个很好的入手点。

在有效完成审计工作的过程中，需要在两大准则下进行：一是会计准则；二是独立审计准则。通常情况下，一家企业在选择注册会计师的时候，决策权往往掌握在企业高管手中，注册会计师的选择以及聘请费用的多少和支付方式会对被审计企业的利益产生一定的影响。因此，如何在独立和有偿服务之间形成有效隔离，对于这一点，区块链可以提供非常切实可行的方案。

区块链上进行的所有交易参与方的个人信息都被同步记录在整个区块链上。而区块链网络上的任何节点都可以查询整个区块链上的数据记录。这样就可以帮助审计师在审计工作中审核被审计单位货币资金交易活动与其他企业交易往来业务合同以及费用的真实性，也降低了审计结论对于数据真实性依赖的风险。区块链的可靠性保证了经济活动交易记录的准确性，其透明性则大大解决了审计工作中需要大量人力物力去收集审计证据的难题，也在很大程度上降低了审计行业相应的成本。在当今的审计工作中，审计师需要发送银行询证函及企业询证函去证函被审企业银行账户资金余额以及交易合同或资金的真实性。在区块链技术的帮助下，所有数据均真实、可靠、透明地记录在区块链上，不但可以大幅降低函证的审计成本，节约了审计时间，更重要的是保证了审计的真实性，避免了第三方审计服务机构无法保持独立性。全球数万用户、事务所和监管机构共时记账，可以追溯，不可随意篡改，并且相关交易数据被区块链全部真实地记载下来，切实地提高了网络数据的可审计性。未来审计师可以实现基于网络和区块链的全球范围的审计。

当前，全球最知名的四大会计师事务所中，其中有三家，即德勤、普华永道、安永，都已经在区块链技术的研究和应用方面投入大量的人力和物力，以期进一步提升财务记账的透明度，从而更加高效、更低成本地进行审计。

事实上，早在2014年，德勤就建成了一家名为“Deloitte加密货币共同体”的集团，在全球12个国家中，大约分布着该集团的100名成员。目前德勤已经推出了一款名为Rubix的软件平台，在该平台上，用户可以基于区块链的基础设施创建各种相关应用，在Rubix平台上可以实现4个方面的利益：贸易合作伙伴关系、实时审计功能、土地登记功能和忠诚度点数。德勤公司内部则将工作重点放在通过一种隐秘的方法来自动解决审计处理中存在的问题上。德勤公司在开展审计工作的时候，由于被审计的企业的每笔交易都是在区块链上进行的，因此可以利用区块链设计出更好的解决方案，以此提升审计进度，并且使得审计成本更低，审计结论更加准确。

另外，基于区块链的真实性、实时性、不可篡改的特点，股东、银行、监管机构或者其他相关者都可以实时监控公司账本，从而减少欺诈和假账。区块链赋予的分布式据以及责任特性，使得提交真实、合法、完整会计资料的责任被直接分配到整个网络当中所有参与员工身上并共同行使，使得传统会计模型中的第三方机构检查系统的重要性逐渐弱化，企业借助区块链理财系统完全可以自己证明会计资料的真实性、可靠性和完整性。这样，从本质上讲，区块链可以满足股东等利益相关者对审计的公正性、有效性、准确性等多方面的需求，还可以弥补第三方设计机构在独立性、公正性、透明性、客观性等方面的不足，如图2-5所示。简言之，未来企业完全可以不需要第三方审计机构对其财务进行审计，借助于区块链技术可以更好地实现“自审计”。可以说，“自审计”时代的到来将成为人工智能时代的一道亮丽的风景线。





图2-5 区块链应用于审计行业具备的特点

## 2.区块链降低资产确权难度

资产确权是依照法律、政策的规定，经过向有关部门申报、权属调查、审核批准、登记注册、发放证书等登记规定程序，确认某一有形或无形的物体的使用权和所有权的隶属关系，这些权利包括资金、著作权、版权等。其在传统模式下是必须通过第三方权威机构按照法律相关规定予以明确的。然而，在生活当中往往会遇到诸多资产纠纷问题，这些问题往往给企业、个人等的生活带来极大的困扰，因此资产纠纷案件层出不穷，同时也给资产公证单位带来了极高的工作难度，具体表现在以下几个方面。

(1) 评估登记管理不完善，需要耗费较长时间。在我国，通常进行无形资产如专利权、著作权等做抵押登记的时候，需要一个半月的时间，其中公示需要10个工作日，等候1周之后，办理质押登记要再等15个工作日才能完成。

(2) 无形资产评估困难。无形资产在进行评估的时候，往往需要专业的评估机构，但是普遍缺少市场认可度。

(3) 无形资产流转处置困难。由于无形资产具有较强的专业性，因此，其价值确定也较为困难，变现渠道较为有限。

区块链的出现和在资产确权方面的应用，将有效解决资产纠纷问题，进而降低资产公证的难度。区块链应用与资产确权的过程中，你的资产无需相关证件来证明，因为会有很多人站出来为你背书。

当前，利用区块链技术解决资产确权问题的服务商不多，在国外有Proof of Existence (Po E)、Factom，在国内有安存。其中Po E和安存的出现，使得区块链技术可以用来证明某个文件、数字资产在某一特定的时间段内隶属于某人、某企业、某团体、某组织等，这实际上是为法律、合同带来了革命性改变。

而对于Factom而言，其存在的意义就在于创建更快、更便宜的方式来开发区块链商业级应用，从而更好地解决资产确权的问题。事实上，Factom走在了此方面的行业前沿，并已经开发出了第一个可供政府、金融等相关机构用于数据保存的区块链应用。通过在区块链上增加一个数据层协议，Factom实现了一个安全且不可逆的数据保存机制，仅仅需要一个“哈希”就可以安全可靠地保存百万级别的实时数据。Factom找到的方法使得每一条链都可以在不需要其他无关联的信息交互前提下进行验证，这样就可以最小化信息内容。Factom在区块产生的时间内，记录链条上的已有条目，而每一链条都是独立的。通过扫描这些记录，应用程序能够在链条上挑选出它们需要的内容，Factom用户只需要在他们感兴趣的链条上保持验证即可，从而对自己的资产进行确权。目前，Factom这种借助区块链进行资产确权的技术已经广泛应用于审计系统、医疗信息记录、供应链管理、投票系统、财



产契据、法律应用、金融系统当中。目前，Factom的总部设在美国，并已经在伦敦、北京、上海等地设立了分部。

### 第三章 人工智能时代，区块链与金融大数据



大数据和人工智能得到广泛应用，因此出现了区块链和Fintech等大火金融科技。然而，当前，无论是我们所谓的百度搜索数据，还是腾讯的社交数据，以及我们知道的阿里一些商户的数据，从严格意义上讲，其中的一些商业数据、金融数据是没有打通的，都是孤立的，这样对于个人的征信和各方面的使用意义甚微。区块链却是优于金融大数据，能够从根本上打破数据孤岛，实现真正的互联互通，这将为金融风控问题提供最佳的智能解决方案，也正是因此，使得当前区块链技术受到金融机构和资本市场的热捧。

## “区块链+大数据”创造数据神话

当前，大数据、云计算、人工智能已经成为各行各业发展以及提升市场竞争力的有效武器，因此，企业如何利用大数据创造价值成为各家企业所关注的重点。目前，各领域的企业都开始全方位寻求创新技术去挖掘和利用大数据，让海量数据为企业服务，大数据成为当前市场中备受青睐的创新科技。于是，区块链作为一种新型的分布式数据管理技术，凭借其巨大的魅力跃入人们的视野，受到越来越多企业的关注。区块链从最初在金融行业中的广泛应用，逐渐延伸到政府、医疗、零售行业，目前，已经一步步成为一个能够创造巨大价值的神话。

当前，全球都在对区块链在各领域的应用进行研究和探索。为了更好地使大数据应用于商业挑战，进一步推广大数据基础分析、商业环境下的大数据应用，推进大数据技术在企业实现转型中的创新能力和业务能力，提高大数据的新价值，基于具有公开性、透明性、真实性、准确性的特点，区块链技术已经延伸到越来越多的领域。将来区块链不仅有可能成为金融交易的基础设施，还与大数据之间在需求上有非常多的结合点，并创造出人工智能时代的数据神话。

现在，国内外对区块链、大数据都是非常重视的，也对两者在各领域的应用提出了一些要求。区块链技术具备以下四个特征：防篡改、可靠性、全网所有交易记录公开透明和去中心化分布式。区块链的本质就是建立信任、建立合约的一种方式。

而大数据则在具体应用过程中存在一些瓶颈问题，如图3-1所示。

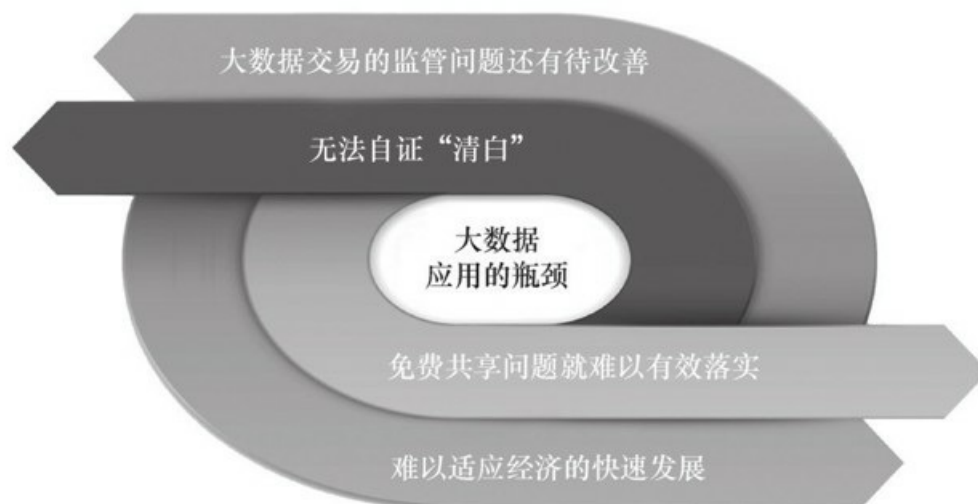


图3-1 大数据应用的瓶颈

### 1.难以适应经济的快速发展

大数据作为一项创新技术受到了国家政策的极大鼓励。大数据的核心技术就是处理和分析能力，并能够将数据搬到云端，进而在云端进行更大规模的处理，提升处理速度。但即便如此，对于提升经济发展速度来讲，依然是远远不够的，还并不足以支撑起一个新兴的行业的诞生。

### 2.免费共享问题就难以有效落实

数据本身就是一种非常高效的、推动企业发展和创新的资产，很多服务商和厂商都把大数据当成一种私有品，不愿意轻易拿出来与他人共享。因此，这就引出了大数据是私有还是公有资源的问题，以及到底谁拥有所有权、处置权、交易权，这个问题在短时间内是

无法解决的。

目前，我国大数据在各个领域中的应用速度是非常快的，通过将数据推上云端，建立基于数据共享的云端服务来进行实际应用。贵州提出建立“云上贵州”的计划，即未来所有的省内政务都在云上的系统中完成；湖北省正在建立全省政务系统的政务云，计划在2017年实现云上目标。但是，这些政务云仅仅是在公共政务领域实现开放、共享。政府通常会为了防止数据开放带来的个人隐私受到不法分子的侵犯以及商业机密的泄露的问题，而对数据共享在其他领域的实现问题上进行一定程度上的限制。企业，如互联网巨头BAT，往往把数据资源当成自己最重要的资产，因此，并不会轻易将自己的所有数据都开放出来。基于这些原因，数据的免费开放、共享、交易、流通，在具体落实的过程中，并没有想象得那么容易和简单。

### 3.无法自证“清白”

大数据在实际应用过程中，要有完善数据资产进行流通交易的环境，而大数据交易中心却无法对其所交易大数据的“清白”进行自我证明。

### 4.在法律法规的建设方面，大数据交易的监管问题还有待改善

大数据本身在监管方面存在着一定的难度，对整个数据流通的全过程缺乏一种全程跟踪的手段，有数据安全的保护、数据服务变现等方面的应用也存在很大的瓶颈。

区块链作为比特币的一种底层技术设施，也是在比特币方面应用最为成功的新兴技术。区块链的基础数据结构是存放数据的区块的，而区块之间则是通过哈希指针连接起来的。通过这样的设计，区块链成为基于各个节点共同参与的分布式对等网络，实现了分布式可信任的数据库架构，体现了其去中心化存储、数据不可篡改的特点。

随着区块链技术的发展从1.0到2.0再到3.0的过渡，区块链在各个领域中的应用将会变得更加广泛。在这样的背景下，大数据得到区块链的技术支持之后，将会创造出人工智能时代的数据神话，使得大数据能够发挥出更大的价值。主要体现在以下几个方面，如图3-2所示。



图3-2 “区块链+大数据”创造数据神话

#### 1.区块链让大数据放心地流动起来

区块链本身具有可信任、不可篡改的特点，使更多的数据被释放出来。

以区块链推进基因测序大数据的产生为例。区块链测序可以利用私钥限制访问权限，从而规避法律对个人获取基因数据的限制问题，并利用分布式计算资源、低成本完成基因测序服务。区块链的安全性让测序成为工业化解解决方案，实现了全球规模的测序，进而推进数据的海量增长。

## 2.区块链保证数据的安全性

数据分析的本质是实现数据价值。在进行数据分析的过程中，如何有效保护个人隐私问题以及防止核心数据泄露成为重要问题。

指纹数据分析应用和基因数据监测与分析手段的普及，会给很多人带来个人隐私安全危机，一旦个人健康数据和基因数据发生泄露，可能会导致非常严重的后果，如不法分子利用基因数据提取相关基因进行人体克隆等，将严重影响社会秩序。

区块链通过多签名私钥、加密技术、安全多方计算技术来有效防止基因数据泄露问题。使用数字签名的方式，使得只有授权人才能够对数据进行访问。数据是统一存储在去中心化的区块链上，即便没有对原始数据进行访问，同样可以对数据进行分析，这样不但可以保护数据的私密性，还可以让全球范围内指定的科研机构、医生共享，并将之作为全人类基础健康数据库进行研究，从而对全球人类的疑难疾病等的研究提供了极大的便利。

总而言之，大数据在各领域中应用发展到今天，虽然取得了众多令人振奋的成果，但是也面临极大的挑战和瓶颈。然而，区块链技术的出现，使得“区块链+大数据”产生了更大的应用价值，为大数据的应用带来了新思路和发展方向，使得其应用前景变得更加广阔。

## 大数据时代区块链再造信任体系

区块链技术本质上是一种特定的分布式存取数据技术，通过网络中各个节点中的参与者共同参与数据的计算和记录，并且相互验证数据信息的有效性。从这一层面来看，区块链技术也是一种特定的数据库技术。

当前，大数据的应用还处于基础阶段，当它一旦发展到区块链数据库阶段，就真正地进入了强信任背书的大数据时代。在这个时候，所有的数据“从哪里来”“要到那里去”“具有什么属性”等，与其身份有关的信息都将变得非常清楚、明确，任何人没有能力和必要去质疑其“清白”。

在我们生活中，任何一个举动都会产生大量数据，并且这些数据信息呈突飞猛进式增长。区块链技术不仅在金融支付领域有所应用，而且将会逐渐扩展到我们生活中的任何一个领域，如应用到去中心化的微博、微信、租房、打车等活动中。因为，区块链将可以让人类无地域限制、去信任的方式来进行大规模协作。然而，这一切都是建立在区块链具有信任特点的基础上的。可以说，区块链的出现为大数据时代重新构造了信任体系。

### 传统交易下的信任体系

人类文明的起源是从交易开始的。人与人之间、氏族与氏族之间、部落与部落之间、国家与国家之间，一切物质、知识、技能等的交易使得人类衣食住行的内涵得以丰富，从而构成了人类生存和发展的社会环境。在缺乏稳定的交易机制和环境的时候，交易将会受阻，同时也阻碍了人类社会进步的步伐。

交易的有效、持续进行，需要一定的信任机制和体系来维持的，或者用互联网的语言建立一个信任协议。然而，这个信任可以建立在双方的基础上，也可以是多方的，一个交易社会的建立是需要一个稳定信用体系来维持的。这个体系需要具备3个要素，即交易工具、交易记录和交易权威。

在几千年以前，人与人之间的交易工具往往是一些可以被广泛认可的特定物件，如贝壳、宝石，交易工具可以用来衡量商品的价值。每次交易的过程中都需要进行记录，可以凭借交易者的记忆或者通过结绳记事的方法来实现。一旦交易过程中出现争执，则由氏族、部落的领头人作为公平和公正的权威人进行调解。随着时间的推移，交易工具逐渐转为金属货币，交易记录逐渐采用纸质账本来完成，再后来记账方式就改为汇票，银行则成为权威机构。这时候，信任关系已经摆脱了原有的事物、区域以及特定的人物，而是变成了数字和账本，资本主义经济的运行有了自己加密并难以篡改的国际化信任协议体系。

[shu籍 分享 微信 whair004]

如今，每天有几千万亿元的资金流转推动全球经济的持续运行，因此也为几十亿的消费者和越来越多的企业提供信任交易体系。电子货币信用卡已经成为当前主要的交易工具，中央银行和政府成为垄断的交易权威，而天文数字般的交易账本则在计算机和计算云里完成记录。这就是当前我们生活的市场交易运作体系，也是当前保证交易安全的信任基础设施。

### 大数据、互联网革命与区块链下的信任体系创新

随着时代的变迁、科技的不断进步，大数据、互联网的出现成功颠覆了人类生活以及整个社会生态。一方面，互联网的出现降低了交易成本，提升了交易速度，同时也让交易不再受到时间和空间限制，实现即时的点对点联结，市场交易无论从深度还是广度上都有了无限扩大，从而突破了传统交易的边界。尤其是在金融领域，互联网金融以及金融科技的突飞猛进让传统金融的基础设施发生了颠覆性变化，从而使得金融服务体系实现了再造。另一方面，货币呈现多样化，支付方式也层出不穷，中央银行的独立性和权威性受到了威胁，集中的账本和数据体系被黑客攻击的事件层出不穷。尤其是金融数据支持设备和



网络协议的更新与金融创新 and 市场需求相比严重滞后，严重影响了金融业的发展，而传统的信任体系也岌岌可危。

信任体系再造包括交易工具、交易权威和交易记录三方面的再造。2009年，比特币成为一个全新的去中心化信用交易工具，更为重要的是区块链作为比特币的底层技术呈现在大众面前，并开始应用于除金融业之外的其他领域。

区块链之所以能够在很多领域被广泛应用，是因为区块链具有价值转移和信用转移的优势，这是一种“去信任”架构。在这个架构下，系统中的所有参与方即便非常陌生，也可以毫无顾忌地放心完成交易和协作，并且在这个架构下，基于不可篡改的特点，所有的参与节点实际上都是在对数据库进行维护，使得所有的数据都是精准的、真实的、可以被信任的。信任对于大数据来讲，往往是最为薄弱的一项。

简而言之，区块链建立了一个由无数独立且自主管理的计算机构成的账本网络，每一笔交易的发生都记录在案，任何第三方都可以对记录的数据内容进行验证，交易历史被记录在区块链体系中。基于分布式账本的加密方式，如果想对账本数据进行篡改，就需要对全网数据进行篡改才能实现，然而这样的结果势必造成巨大的更改成本。

区块链是一种建立在信任基础上的底层技术，用无数计算机的联网认证和纠错机制来建立公开的信任协议体系。这种信任协议体系下，取代了以往的政府、中央银行以及其他任何垄断机构的管理，在新的区块链技术的基础上再造了大数据时代的社会信任体系。

总之，在大数据时代，基于区块链的再造信任体系，无论是技术层面上的协议还是应用和监管层面上的场景实现再造，都是传统金融体系的重大创新。

## “区块链+大数据”破解传统风控难题

一直以来，风险控制都是金融领域的一个必不可少的环节。近年来，随着各种科学技术的不断出现，尤其是人工智能技术的出现，使得金融业的发展更加需要一种新兴技术有效把控金融风险，而大数据的出现一定程度上解决了风控问题。不过，大数据并不是十全十美，能够完全把握风控的，因为，当前依然存在着数据孤岛、数据低质和数据泄露等有效性不足方面的问题，也因此引发出了层出不穷的风险事件。因而，区块链技术的出现和应用，使得大数据和区块链很好地融合，并为风控领域带来创新性机遇。可以说，“区块链+大数据”人工智能时代实现破解传统风控的有力武器。

### 大数据风控模式

在我国的金融业中，信贷成为主要交易，并且其信贷市场规模在全球范围内位居第一。然而，信贷市场中往往潜藏着巨大的信用风险，因此风险控制在金融领域中起到了至关重要的作用。国家也在大力寻找更好的风控措施。在大数据出现之前，商业银行充当风控角色，这是当时最适合的风控模式。

传统的风控模式往往是以商业银行一直以来所沿用的以程控交换为主的风险管理系统。这种系统的优点是稳定性较强，但是在客户容纳体量方面却是有限的，且具有交易通信指令复杂的缺点，这就使得商业银行不能完全满足当前的投融资需求，尤其不能满足当前全国7000万家中小微企业的存贷款需求。这些需求已经远远超过了传统风控模式的承压范围，并且在欺诈检测和风险监管的系统容量上也已经与传统风控模式不相适用。这种现状下，创新就成为必然。随着数据处理需求的不断增加以及大数据技术的进一步发展，商业银行作为传统金融机构的代表，更是意识到数据资产的重要性，并逐步采用以IP网络为主的大数据风险控制系统代替了原有的程控交换系统。这是一种风控系统的创新，同时也体现出大数据在风控领域中应用的重要性。

2008年，随着大数据以每天平均2EB（即 $2 \times 10^{18}$ GB）的数量不断增长。如此庞大的数据却让以蚂蚁金服为代表的互联网金融企业看到了其中蕴含的巨大价值。这些金融机构开始借助大数据在风控领域进行创新，并且借助互联网平台打造出了诸如“蚂蚁大脑”“京东天机”等大数据风控系统。进入2013年，互联网金融得到了更加快速的发展，以P2P为代表的互联网金融企业层出不穷。但是随着P2P平台的不断出现，诸如跑路、停业、提现困难等方面的问题也随之而来，并且越来越凸显。尽管众多P2P平台都在极力宣扬自己的大数据风控系统有多么了不起，实际结果却往往事与愿违。由此表明，使用大数据进行风控，依然存在诸多不足，主要体现在以下几个方面，如图3-4所示。

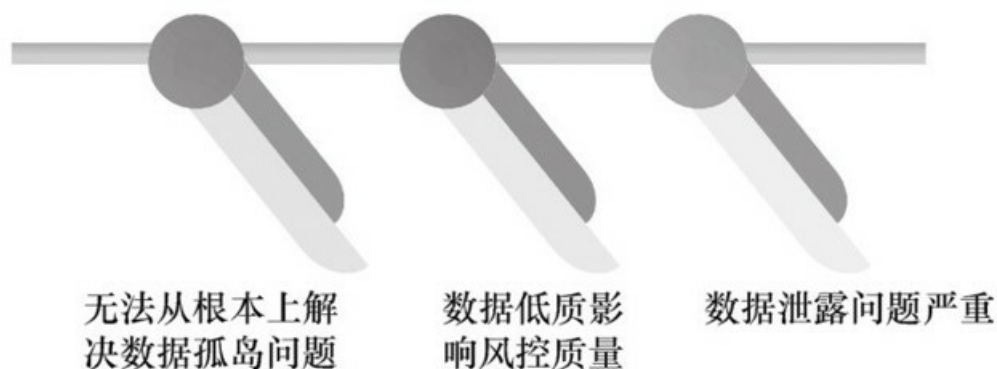


图3-4 大数据风控的3个不足之处

### 1.大数据无法从根本上解决数据孤岛问题

换句话说，就是没有从根本上解决数据的共享和开放问题。当前的现状是，在短期内，政府、银行、互联网企业、第三方征信公司之间是难以完全实现互联互通的，因此数据孤岛问题依然存在，这样就使得信息不对称、不透明问题严重，由此引发大量的风险和欺诈现象。

### 2.数据低质影响风控质量

在我们的生活中有诸多非结构化和半结构化数据，这些数据的特点就是实用性差，利用价值很低。以电商平台为例，每天电商平台上会产生数量巨大的数据信息，但是电商平台上往往会出现一些不良操作，如刷单等，就使得产生的数据出现了失真的情况。对于这些数据，其收集和利用的意义和价值就大打折扣，甚至毫无意义和价值。因此，应用在风控问题上，自然也就没有任何风控质量可言。

### 3.数据泄露问题严重

当前数据泄露事件经常出现，虽然政府监管条例出台很多，但是诸多不法分子钻法律法规的空子，导致数据泄露问题不断发生，因此国家监管力度仍需进一步提升。

### “区块链+大数据”突破大数据风控弊端

区块链作为一个去中心化的分布式数据库的出现，凭借其自身的去中心化、开放自治、匿名不可篡改的数据结构特性获得了全球的广泛关注，并且基于这些特点，使得应用场景更加广泛，如最初的数字货币、证券交易结算、会计审计等诸多金融领域的应用，以及政府、医疗等公共领域的应用。可以说，区块链打破了大数据难以解决的诸多技术壁垒。并且，重要的是，区块链的出现也有效解决了大数据风控的一些弊端，即大数据没有办法对自己的“身份”即数据源进行澄清，而区块链技术应用与大数据风控体系，可以有效解决大数据的孤岛、数据低质、数据泄露等数据源问题。

数据库的信息传递效率和维护成本直接影响大数据风控的有效性。仅仅从数据的层面上来讲，区块链是一个由所有参与者共同记录的信息，并且是由所有参与记录的节点共同存储的且不可篡改的数据库。在这个区块链数据库中，每一个节点都拥有整个数据库的完整副本，并且当某一节点要对数据库的数据进行变更时，是需要向区块链网络广播这些数据，从而便于其他节点对数据进行验证和审核。只有全网所有的节点都完成共同验证和认可之后，被更改的数据才能被认为是有效的。这样，区块链构建的数据库在大数据风控方面的有效性才能真正提高，如图3-5所示。



图3-5 “区块链+大数据”突破大数据风控弊端

### 1.解决数据孤岛问题

区块链具有去中心化、开放性等特点，使得大数据风控的数据孤岛问题得到有效解决，使得信息公开透明地传递到所有金融市场参与者。监管部门作为金融市场中的秩序维护者，可以利用区块链技术中全部数据链条对可能出现的风险问题进行预测和分析，并及时发现和预防这些风险问题，从而更好地维护金融市场有序运行。可见，区块链去中心化的特征可以消除大数据风控的信息孤岛，通过信息共享完善风控模式。

客户甲分别向银行A和银行B申请了100万元的房屋抵押贷款，实际上其房屋的价值也就只有100万元。如果银行A和银行B两者都加入了区块链，就可以对客户甲的交易行为和风险系数一目了然，这样能够有效避免房贷总额超过抵押值。不但如此，监管部门虽不是交易的参与方，但是依然可以加入区块链，对区块链上任何一个节点的交易行为进行实时监控，有效防止风险事件发生。

## **2.改善大数据风控中数据质量不佳的问题**

区块链分布式数据库可以改善大数据风控中数据质量不佳的问题，有效解决数据格式多样化、数据形式碎片化、有效数据缺失和数据内容不完整的问题。在区块链中，每个节点共同记录和存储交易的数据信息，每个节点都可以参与数据的检查并为数据的“身份”进行验证，这样就保证了数据的真实性。另外，去中心化决定了区块链上的数据是不可以随意更改的，这样就有效降低了数据更改的可能性。因此，可以说区块链技术使得数据更具公开性、安全性，从源头上提高了数据质量，增强了数据的检验能力。

## **3.防范数据泄露**

区块链作为一个去中心化的数据库，任何节点对数据的操作都会被其他节点发现，从而有效提升了对数据泄露的监控。并且，区块链中的各个节点的关键身份信息是通过私钥的形式才能获得的，而私钥仅仅是信息的拥有者才能知道，即便是其他信息被泄露了，但是如果私钥没有泄露，那么那些被泄露的信息也无法与节点身份进行匹配，这样，这些泄露的信息也就失去了利用价值。黑客发起的来自数据库外部的攻击，只有掌握了超过50%的计算力才能攻破区块链。并且，区块链上的节点越多，则需要的计算力也就越大，当节点的数量达到一定规模的时候，黑客进行一次攻击的成本之高，完全是得不偿失。这样一来，通过区块链技术对信息存储进行加密，就保证了数据的安全性，防范了大数据风控中可能出现的数据泄露的问题。因此，“区块链+大数据”是人工智能时代突破大数据风控中存在弊端、有效提升金融业风控能力的最佳模式。

## 第四章 人工智能时代，区块链构建金融信用长城



众所周知，金融经营的核心价值在于信用，可以说没有信用就没有金融，就没有经营风险创造利润的机会，也就不能在不同的时间和地点配置资源，最终也不能加速价值的流通。区块链的去中心化、去信任特点构建了去中心化的信用，因此，从理论上讲，这种基于区块链的信用长城的构建，是非常符合当前进入人工智能时代全球金融市场进化的趋势的。



## 从数字货币到信任社会

货币是人类社会进行任何交易都必不可少的一部分，随着科技的进步，货币的形式也变得更加丰富多彩，自从2009年中本聪创立比特币以来，社会中出现了多种类型的数字货币，而这些数字货币的运行都是基于公有区块链的。

随着互联网、云计算、区块链技术的不断发展，在全球支付方式发生巨大变化的背景下，未来货币的形式将更加多元化和智能化。以比特币为代表的数字货币的出现，表明货币类型的创新有更大的想象空间。2014年欧洲银行管理局对数字货币是这样定义的：“虚拟货币是价值的一种数字表达，它不是由中央银行或某个公共权威机构发行，也不一定与某一发行货币相挂钩，但被自然人或法人接受用于支付手段，可以进行电子化转移、储藏或交易。”“数字货币”已经不再仅仅是一个概念，还正逐渐成为一种需求。

区块链本质上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。因此，可以说，区块链与比特币即数字货币之间的关系：即数字货币是记账的表征，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。

这样解释看似比较烦琐，换一种简单的方式来定义区块链与数字货币之间的关系，就是将所有持有数字货币的人的账户信息、数字货币交易信息等，在世界上所有的电脑中都进行备份。因为无处不在，所以只要你打开任何一台联网电脑，就可以在里边发现你的信息。这样无论谁都无法对数字货币交易信息进行造假、篡改，更无法赖账。正是因为有这样一个特征，区块链技术给人们的生活带来了更多的信任感。

用区块链去做数字货币，给人们带来信任感，只是区块链应用功能中很小的一部分，那么如何才能通过区块链技术将信任带到寻常百姓家，实现全社会的信任呢？

区块链技术往往给人一种高冷的感觉，也许普通百姓人家对于区块链的真正内涵是很难了解和掌握的，但是专业领域的研究者、区块链技术极客以及资本炒家往往对区块链技术非常关心。

当前，我们所处的社会是一个高度中心化的社会，因此，为了证明所谓的信用，我们付出了太多的代价，由于与对方之间互不信任，因此我们建立了银行作为金钱的集中管理者；建设了支付宝作为完成网上卖家与买家之间交易的第三方中介；我们用P2P平台去筹集所需要的资金，来完成想要完成的项目。我们依赖的所有的这些中介，都是因为不相信我们对面的另一个陌生人，并且认为只有通过第三方机构才能保证脆弱的信任能够不被打破，因此，我们会通过第三方机构来完成更多的资金支付过程。

当前是一个共享经济时代，知名的共享平台有很多，包括房屋共享（Airbnb、小猪短租）、车辆共享（Uber、滴滴打车）和知识共享（网易教育）等。试想一下，在没有这些共享平台提供信任的基础上，谁会将自己的汽车、房屋、电脑等私有物品随便租给别人使用呢？在并不信任的前提下，谁能想象一旦将这些私有物品租给别人会发生什么情况呢？

区块链技术可以凭借其不可造假和篡改的特点，实现全社会的信用重拾。试想一下，当你每天所产生的行为都被大数据记录在册，被存储在区块链上的某个节点上，无法篡改、无法造假，那么任何人都可以用区块链来描述你的数字画像，借助区块链的评分来确定你的信誉度。一旦这个体系建立起来之后，大量的中介将会失去了其原本的价值，这时候，我们与所有陌生人建立信任关系也就不再是一件难事了。因为如果有人想要修改一个基于区块链的信用记录，那么他所要做的就是需要在世界上每个人的手机、电脑、i Pad



中进行修改，甚至所有的智能设备，这是根本无法做到的。

由于当前人与人之间的信任关系并没有完全建立起来，因此我们的共享经济目前仅仅能够停留在借助第三方共享平台来租借别人的房屋、别人的汽车，或者将自己的房屋、汽车出租给他人。一旦个人的信用由区块链技术验证，我们的生活将比现在的共享经济更加便捷、简单，也必将发生质的飞跃，如图4-1所示。



图4-1 区块链使生活发生质的飞跃

### 1.基于互联网的欺诈现象有所改观

区块链技术与普通人的日常生活是息息相关的。随着互联网技术的普及，人们的日常生活也随之进入了数字化时代。在这个数字化时代，互联网虽然给人们带来了生活的便利，却依然无法避免篡改等安全方面的问题。这也就意味着，互联网虽然优点有很多，但是却无法解决网络信任问题。而区块链则可以很好地解决这种基于互联网的欺诈现象，当每个人都在互联网上成为一个被区块链进行过画像描述的人，那么你的所有记录都将被记录，如任何信用污点，这样，谁也不会为了一时的名利铤而走险。

### 2.建立真正信用的共享社会

每个人周围都会或多或少地闲置着各种资源，这些资源在我们的日常生活中很少用到，包括房屋、汽车、知识、技能、资金等，不但占用了大量的空间，还没有将其应有的价值和意义体现出来。如果区块链能构建起人与人之间的信用，那么，无需共享平台的帮助，人人都可以将自己的闲置资源通过出租或出借的方式将其共享出去，从而将社会上的一切闲置资源充分利用起来，以最低的成本，实现资源使用率的最大化。如果任由这些资源搁置在一旁，那么也是一种极大的资源浪费。

可以说，区块链的出现不仅仅带来了数字货币，还为我们带来了一个真正信用的时代，从数字货币到信用社会，我们的生活变得更加透明化、便捷化、简单化，真正实现了去中心化的万物互联。

## 开启全新的金融信任时代

2016年，区块链成为继大数据、工业4.0之后的又一科技金融领域的热词，并且代表了科技的新前沿，各大商业机构、专家学者对于区块链领域都给予了极大的关注。2016年7月30~31日，在上海举办的“2016互联网金融外滩峰会”上，区块链被誉为“信任的机器”，使得区块链在金融领域的应用成为热点话题。

当前，许多金融界的领袖都在探讨未来金融发展的新方向，并对其在未来人工智能时代的发展进行预测，而其中最常被提及的就是区块链技术对金融业的影响。目前，区块链技术已经在金融领域发生了变革性的转变，但是其在金融领域应用的意义并不仅限于此，同时，区块链技术也开启了全新的金融信任时代，这也为金融行业的发展带来巨大的变革。

作为比特币的底层技术的区块链技术，如今，已经跳出了比特币的圈子，在金融领域大放异彩。当前，金融领域的信用问题虽然有诸多第三方平台来把控，但是依然没有得到彻底解决。然而，区块链本身就是一个通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案，连接相邻区块的链条本身就可以对相邻的区块进行相互验证，另外，再加上其数据的透明、公开性，让区块链技术自带信用属性。

利用区块链技术的属性可以对金融基础设施进行集中化处理，也可以对传统的中间性质的机构，包括银行、支付宝等进行信用去中间化，还可以借助于区块链技术的安全性更好地规避金融风险，这都归功于区块链技术的信用价值得到了极佳的体现。

以股权众筹为例。传统的股权众筹是借助众筹平台来完成众筹项目的，这种方法不但效率低下，而且投资者获得的回报也比较小。如果利用区块链技术，则情况大不一样了。基于区块链的股权众筹，得益于区块链技术的去信任中间化，能够快速完成众筹项目，并且投资者所获得的回报也是相当丰厚的，这些回报也是能得到安全保障的。

实际上，并不是说金融领域的一切活动在区块链技术的作用下就可以不受监管，而是采取社会中的所有入共同监管，即社会共治的方式，以代替传统的通过第三方机构来证明你是谁，而由社会共同证明你是谁。也正是基于这一点，区块链可以以极低的成本就能够很好地解决金融活动中的信任问题。信用是一切金融活动运行的根基，所有金融活动的监管，包括产品登记、信息披露、资金托管，都是在解决信任问题的基础上完成的。信任问题一直以来都是一个难以解决的社会问题，为此，社会上诞生了诸多公信力机构。区块链技术则为金融领域创造了一个用“共信力”解决公信力问题的途径。

2016年对于区块链相关从业者来讲，是一个让人感到激动的年份。世界著名银行巴克莱银行于9月初和一家致力于金融领域带来分布式分类账技术的初创公司Wave进行了一个分布式分类账技术的真实试验，即一个现场的信用公证贸易执行和完成。这是对区块链技术的重要验证。而Wave自从成为巴克莱银行加速器计划的一部分之后，就一直在探索新的用例，这些用例概念所针对的地区是英国和南非。此次双方合作，在很大程度上为巴克莱提升了影响力。

更加准确地讲，Wave致力于文档和区块链技术的结合。传统贸易文档在使用的过程中很容易因为人为问题而出现错误，并且随着当前科学技术的进步，伪造贸易文档也已经不是难事，这样就会严重影响贸易文档的准确性。基于区块链技术的分布式分类账则能够有效解决该问题。分布式分类账技术能够大幅削减成本，这也是为何巴克莱银行选择和Wave合作的原因。银行在传递信息的过程中往往需要花费高昂的成本费用，并且在使用

旧的方式来完成终端到终端的贸易融资交易的过程中，往往需要花费几天的时间才能完成。如果采用基于区块链技术的分布式分类账技术，就可以有效缩减时间，通常可以缩短到几个小时。

如果说建立信任是防止欺诈的第一步的话，那么区块链信用特征将是金融实现信任时代的重要推动力。基于区块链的存在，任何人的信用度都可以在全网进行查实和验证，因为每个人的记录数据是不可更改的。在这个基础上，每个人都可以利用自己的区块链数据向全世界任何一家银行申请信用贷款，同时也可以凭借自己的区块链数据向全世界的任何陌生人申请信用借款，这时金融交易将不需要银行作为中介来实现，而是大众化的、智能化的金融，人人都可以借助区块链信用实现资金融通，从而开启一个全新的智能化金融信任时代。

## 区块链技术构建金融信用生态圈

金融是现代经济运行的核心内容，而金融的存在和正常运转则依赖于良好的社会信用。“信用”一词属于纯经济学范畴，主要体现为商业领域、金融领域和流通领域的赊销、信贷等交易行为中产生的一种相互信任的产生关系和社会关系。正如某位银行家所讲：“信用是银行的生存之本。”的确，一旦缺失金融信用，银行的发展和未来就是无稽之谈。

金融信用作为银行赖以生存的基础，一方面银行必须确保存款人是自由取款，另一方面需要贷款人确保按时、如数还本还息，二者缺一不可，才能保证银行实现可持续发展。如果贷款人未能恪守信用，那么银行最终也无法保证对存款人恪守信用。因此，金融信用本质上是企业信用和个人信用的整合。

但是，仅仅将企业和个人信用进行整合还是不够的，更需要建立起一种金融信用生态圈，才能从真正意义上保证金融业更好地发展。区块链技术则是一个很好的构建智能金融信用生态圈的武器。

### 1.构建金融信用生态圈应具备的特征（图4-2）



图4-2 金融信用生态圈的三大特征

#### （1）能够满足不断变化的用户需求

这些用户需求包括交易需求、支付需求、投融资方面的需求等。由于用户风险偏好和资产情况随时会发生变化，用户数量也处于动态变化的状态，因此，金融业所呈现的创新信用生态圈也必须是动态的，这样才能与客户的动态需求相匹配，才更能满足用户的动态需求。

#### （2）能够有效整合大量数据

在互联网技术不断发展的过程中，很多企业都建立了属于自己的信息系统，同时也获得了大量数据信息。但是行业内部、行业之间并没有在数据统计方面规范口径，并且数据相关性的整合也有所欠缺，这样就使得企业所产生的大量数据所包含的巨大价值很难被利用和体现出来。但是，在新的信用生态圈中，应当有这样一个整合者，可以将所有的零碎数据信息加以收集、分析、处理，并最终进行有效整合，形成一个系统的、完整的、有机的大数据库。

#### （3）信息安全需求日益增强

在当前互联网高度发展的今天，无论是个人还是企业，都对信息安全非常重视。随着信息系统建设规模的不断扩大，新的信用系统必须提供完备的信用安全功能，这是保证安全的需要，也是当前互联网高度发展的需求，只有这样才能在支持用户信息资源共享的同时，确保用户信息的安全存储和有效隔离。

如何才能建立起具有以上几个特点的金融信用生态圈呢？区块链就是这个问题的最好答案。[shu籍 分 享 微 信 whair004]

## 2.区块链建立金融信用生态圈

### （1）区块链动态记录交易信息、支付信息、投融资信息

区块链采用了“分块”记录的方法，将发生在某一时间段内的交易打包成一个“区块”，每个“区块”与其前后所链接的区块按照时间顺序进行排序，每隔一段时间就会产生一个新的区块，将一个区块与其上个区块以及下个区块链接起来，就形成了“区块链”结构。这样，我们可以发现，区块链的构成是一个动态的、实时的信息记录堆积的过程。这些实时记录的信息，往往能够反映不同时段客户的动态需求，有助于金融企业快速制定实时、动态响应用户需求的金融产品。

### （2）区块链数据可进行再开发利用

区块链是比特币的底层技术，本质上是一个去中心化的数据库，像是一个数据库账本，里边记载所有的交易记录，其本身就是一种对数据的整合过程，因此是能够满足金融信用生态圈构建需求的。

### （3）区块链确保信息不被篡改以及安全性

区块链借助Po W共识机制来确保只有合法的区块才能够添加进来。一旦一个区块通过了验证后链接到区块链中，就会被永久性地存储起来，任何时候都不会被任何外界因素所干扰、篡改。而每个区块链的合法性验证问题，包括对其中的所有交易的合法性验证以及区块之间数据关联性规则的验证。这样就确保了金融信用安全的提升。

2016年10月9日，在上海陆家嘴举办了一场以“拥抱创新、防范风险、健康发展”为主题的2016陆家嘴区块链金融高峰论坛，并且正式启动了“陆家嘴区块链金融发展联盟”。此次论坛重点内容在于“区块链+金融”，既是跨界，更是融合，是当前金融科技的重点发展内容。在会议上，浙江银行上海分行的行长顾青良表示：“现在商业银行均或多或少存在小微金融的业务发展瓶颈和小微贷款增长难的问题，一边是贷款难，一边是融资难，使用区块链技术及其商业模式，有助于商业银行解决小微金融的相关难题，提高信息对称性和安全性，降低经营成本和信用风险，进而改善获客模式和盈利模式。区块链金融技术也有助于上海创建良好的金融生态圈，解决中小企业融资难的问题。”

由此可见，区块链对于金融业的发展具有颠覆性影响，对于人工智能时代金融信用生态圈的建立具有重要意义和现实意义。



## 区块链构建银行业客户信用体系

据相关资料显示，目前美国和欧洲所有的大型金融机构中，都有10~20个区块链项目的内部开发和评估。硅谷投资机构Magister Advisors也对未来区块链在银行业的发展情况进行过预测，表示2017年银行将会在区块链技术上投资超过10亿美元。这些数字意味着全球货币形式正在或即将要经历一场巨大的变革，数字货币的发行，会为全球央行货币的供应、发行、监管等方面带来巨大的挑战。

区块链本身具有去中心化、去中介化、无需信任系统、不可篡改、加密安全、匿名等特点，这些在交易支付领域都是不可多得的优点。另外，区块链的这种无需信任的点到点模式，意味着商业银行原本作为重要的支付中介和信用中介的必要性已经大幅降低，在一定程度上削弱了传统商业银行在货币创造过程中原本应当发挥的作用，进而对其存款和信贷领域也产生了巨大的影响。

信用本身将会对社会资源的配置效率产生很大程度的影响力。银行作为当前经济社会中重要的金融中介，其社会信用体系中的经济功能主要包括两个方面：一方面，解决资金供给双方的信息不对称问题；另一方面，对金融交易中所遇到的信用风险问题进行有效把控。也正是基于此，使得银行能够获得相应的经济利益。一旦数字货币完全取代现金，那么传统意义上的银行网点也将失去了其存在的价值。然而，发行数字货币并完全取代现金还是需要一定的时间的，并且需要移动数字设备作为硬件支持，还需要解决数字身份证以及隐私保护等诸多问题才能真正实现。因此，银行业可以有足够的时间去探索应对信用风险的方法，如图4-3所示。

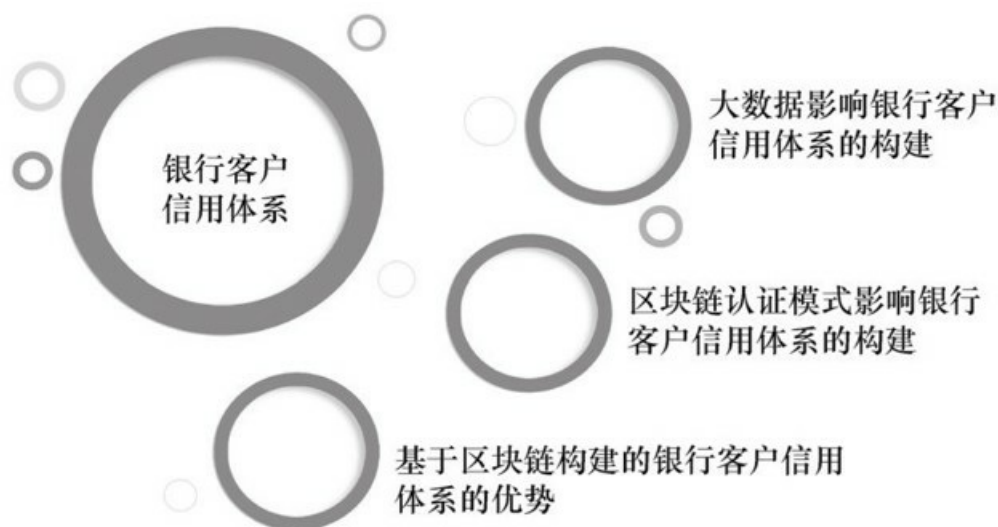


图4-3 区块链构建银行业客户信用体系

### 1. 大数据影响银行客户信用体系的构建

银行在构建客户信用体系的时候，采用的传统方式是通过实体机构对经济社会进行渗透，利用人工的方式来收集与客户相关的各种信息，并通过中心化系统处理数据从而实现对客户信用的评估。银行通过社会分工的组织形式解决金融市场中出现的信息不对称和信用风险管理等问题，这种传统模式可以更好地降低用于个体信用评估的成本。但是，这种



中心化集中处理的模式也存在一定的弊端，即在信息收集成本受限的情况下，银行对客户信用进行评估时所用的数据非常单一，主要是以结构化的经济数据为主，往往在获得客户评估结果时效率较差，并且得到的用户信用评估结果基于数据的原因主要是聚焦于正态用户，对于那些长尾用户的关注则显得极为缺乏。

不同的传统银行在进行信用评估的过程中所使用的数据往往涉及用户个体社会生活的方方面面，包括网络消费与交易、个体通信数据、交通地理归集、网络社区记录等。随着科技的不断进步，尤其是大数据的不断发展，使得数据成本大幅降低，并且个体生活也变得越来越趋于数字化，因此那些在过去没有被纳入银行客户数据的信息正受到征信评估的广泛重视。

与传统银行业通过现场调查等方式收集用户信息的方式相比较，大数据征信具有非常明显的成本优势。大数据已经突破了基本经济的数据范畴，从用户行为入手，作为数据收集的来源之一，在很大程度上为改善信息不对称提供了新的资源；大数据模式下个体数据具有容易收集和广泛性特点，具备了成本优势和信息基础以扩展覆盖到长尾客户的服务商；与现场调查和实验渠道获取数据的方式不同，通过对用户行为所产生的数据进行收集，所获得的数据实际上是“田野观察数据”，从某种意义上讲，是不受主观因素干扰和影响的。因此，银行业使用大数据进行客户信用评估已经成为了一种必然。

但是，在信息化时代，人们生活的方方面面都会产生海量数据，由于数据来源于传播具有一定的差异性，就造成了各种虚假、欺骗信息充斥期间，这就使得银行在进行客户信用评估的过程中遇到严重的干扰。数据信息泛滥以及数据的可操纵性，使得数据信任问题非常明显。海量数据的价值甄别将给银行带来巨大的成本代价，数据灾害也给银行客户信用评估带来严重的阻碍。

## **2.区块链认证模式影响银行客户信用体系的构建**

区块链从另一个方面进行定义是这样的，即是“一种密码学方法产生的动态编程数据块链，其本质是对数字世界中的数据与代码进行认证，从而使某类区块链协议的数据或代码被赋予了某种共识性信任。”区块链可以被用于解决数字化社会中数据与代码自身的可信任问题，从这个层面上讲，区块链技术可以改善大数据应用与银行客户信用评估过程中出现的成本高的问题。

区块链可以解决数字世界中的认证问题，因此对于传统的客户信用评估模式以及大数据信用评估模式来讲是一个巨大的颠覆和创新。针对信息构建中所表现出来的信息不对称问题，区块链技术重新定义了大数据在信用评估过程中的应用价值。扁平化数据的生成、数据资源共享，使得原本的信息不对称问题得以解决。另外，我们前面也讲过，区块链本身具有数据授权的优势，这样就保证了数据的不被篡改，同时也克服了大数据在应用过程中出现的隐私问题，使得大数据具有开放、共享、透明的特点。

通过对程序代码的认证，区块链技术将银行业在交易过程中出现的操作风险和信用风险评估与决策有效地融合在具体的执行过程中。在当前网络信息社会的扁平化、共享式特征下，信息社会的个体信用评估转变为基于技术与平台资源的分享式信用评估模式。区块链有效地解决了数字本身存在的信任问题，为信息社会的信用评估技术的使用奠定了基础，同时使得原来的个体信用权威中心面临重构。

当前，诸多具有信息技术和平台优势的组织和机构纷纷进入信用评估市场，试图在信用评估市场中占据核心领导地位。因此，在这种环境背景下，银行作为传统金融的老牌机构，更迫切地需要转型。借助区块链技术可以帮助银行快速实现客户信用体系的构建。

## **3.基于区块链构建的银行客户信用体系的优势**

区块链技术应用于银行客户信用体系的构建，具备以下几个方面的优势，如图4-4所示。

### **（1）改善征信成本**

区块链技术使得信任数据可以无限使用和分享，可以大幅减少海量数据的虚假问题，

从而使得数据收集、处理以及使用的时候能够有更好的便捷性，同时还会大范围地降低银行客户征信的数据处理成本和自动化运维成本。



图4-4 基于区块链构建的银行客户信用体系的优势

#### （2）拓展信用评估的覆盖范围，扩大客户群体规模

利用区块链技术还可以收集在传统模式下无法通过调查等方式顾及的所有客户群体的数据信息，同时可以针对特殊群体，即那些没有注册银行账户，但是能够与互联网接触的人群，对其展开信用评估，这样就可以很好地扩展信用产品服务的对象范围。

#### （3）改善信用产品管理成本

区块链可以使得信用的评估、定价、合约等能够自动执行与管理，无需额外的人工参与，这样就极大地降低了信用产品管理的成本，同时还能大幅提升银行的信用业务处理规模。

#### （4）提高信用创造能力

区块链下的信任代码技术，可以使信用产品的全部过程都具备动态编程的能力，这样就有效扩大了信用产品的创造空间。以“智能合约”为例，智能合约就可以适用于金融领域的任何场景。

## 第五章 人工智能时代，区块链金融的六大应用场景



区块链技术本身就是比特币的一种底层技术，也是一种全民参与记账的技术，可以被看作一个数据库大账本。从这些层面上来看，区块链注定与金融之间会产生千丝万缕的联系。根据麦肯锡分析，区块链技术对金融的影响最可能发生在支付以及交易银行、资本市场以及投资银行业务的主要应用场景，即数字货币、跨境支付与结算、票据与供应链金融业务、股权众筹、证券发行交易以及客户征信与反欺诈等六大应用场景。在人工智能时代，区块链技术在这六大场景中的应用必将开启金融发展的推动金融向更高阶段的发展。

## 数字货币

比特币作为一种数字货币，彻底颠覆了人类脑海中对于货币的概念。比特币以及其他数字货币的出现与发展，正逐渐改变人类使用货币的方式。从过去的物物交易到现在的物理货币交易再到以后的信用货币，这一发展历程是随人类的商业行为以及社会的不断发展而演进的。随着电子金融以及电子商务的不断崛起，伴随着人工智能的蓬勃发展，数字货币以安全、便利、交易成本低的优势，在基于网络的商业行为中应用，并将逐渐取代当前的物理货币，而成为流通的主流方式。正是由于比特币网络的崛起，使得区块链这种分布式账本技术在全球范围内得到了关注，并且在金融领域中开辟出更加广阔的应用天地。

具体来讲，基于区块链技术的数字货币包括以下几种类型，如图5-1所示。



图5-1 数字货币的类型

### 1. 社群数字“币”

社群数字“币”是以社群的认可度来做背书的。比特币作为数字货币的代表，是第一个去中心化的社群数字“币”。在比特币社区和许多比特币信仰者的支持下，比特币获得了价值支撑，同时也吸引了社群外的用户参与进来，进行交易与使用。这种比特币与各国的法定货币之间进行的大量等价兑换及流通，实际上意味着人们已经将比特币看作一种国际通行货币。

当前全球有大概1400家实体商户可以用比特币来进行交易支付，其中在欧洲有近600家，美国拥有400多家，在我国的北京、上海、广州等一线城市有20多家。

目前，在美国以比特币为代表的数字货币已经受到很大一部分市场的认可，不但消费者与商户在交易过程中使用比特币进行支付，还衍生出比特币的借记卡与ATM机等应用产品。另外，能够实现数字货币与法定货币进行等价交换的交易平台也诞生了。

美国知名的、最大的比特币交易平台Coinbase目前支持美金、欧元、英镑以及加拿大元与比特币之间的兑换。在我国也有交易平台OKCoin及火币，同样也支持人民币与比特币之间进行兑换。

比特币实现了几个方面的目标。

#### （1）制定规则

比特币通过区块链技术，借助数字算法和程序约定了发行总量以及发行方式。社群往往不像其他组织那样具有强有力的中心机构和行动能力，因此，社群中的利益和意见都是相对分散的，这种情况下，区块链技术通过加密算法形成的约定，制定了强制性的规则，

并且缔造了超出人为因素的信任纽带。

### （2）限定总量

社群数字“币”的总量和发行速度是被强制性设定的，这样使得早期的持有者因为社区的扩大、持有者人数的增加、社群内经济活动的增加，而得到越来越多的利益，从而数字货币又拥有了类似于股权的优点，使得社群形成一致的价值预期，产生了共同的内生经济动力。

### （3）匿名性

区块链本身具有匿名性、去中心化、开放透明的特点，区块链作为比特币的底层技术，使得比特币也带有这些基因，这样就很好地分散了法律风险和责任，也使得整个经济系统具有更高的风控能力。

目前，市场中具有交易和流通能力的社群数字“币”有上百种，统一社区内使用同一种货币，这样可以在经济利益上使社群内部形成一致的利益，并在社群内通过用户之间的交换、交易的形式来维持社群经济活动的持续进行。

## 2.企业虚拟“币”

当前，企业内部虚拟“币”的使用相对于社群数字“币”是比较落后的。企业内部存在的虚拟“币”的主要形式是游戏虚拟币、积分、Q币、储值卡等，但是这些数字货币往往和区块链技术形成真正的生态系统。当前，一些创业企业已经开始在这一领域进行大胆尝试，例如，Factom借助自己的软件服务，已经发行了可兑换的虚拟“币”；Bit Gold、Gold Pay两家企业也开始尝试基于黄金来发行自己的虚拟数字“币”。如果数字货币的发行能够有一定的规律可循，相信更多的企业会大踏步跨入数字虚拟“币”这一领域，届时，全球的企业会在数字虚拟“币”的连接下形成跨国生产和金融活动，实现全球企业之间的互联互通。

## 3.国家数字货币

2015年，厄瓜多尔率先推出了国家版数字货币，与其法定货币相比较，不但可以减少发行成本，还可以增加发行的便利性，更重要的是，也可以让偏远山区那些因银行资源匮乏而不具备享受金融服务的民众通过数字货币来实现商品的买卖交易，并且还能够进行水电费缴纳等。借助区块链分布式账本的概念，将交易记录记载于区块链上，这样更加方便管理。

厄瓜多尔并不是独例。其他许多国家也都在国家数字货币的可行性问题上进行深入探讨。目前，澳大利亚、俄罗斯、瑞典等国家正在探索数字货币的发行计划；2016年，我国央行也召开数字货币研讨会，对早日推行数字货币进行了深入的探讨。

当前，全球央行均认为数字货币能够替代事物现金，这样可以降低传统纸币的发行、流通成本，对于提高支付结算的便利性有极大的帮助。同时，数字货币的使用可以增加交易的透明度，在以下3个方面具有重要的作用。

### （1）防伪

国家希望通过数字货币提升交易的透明度，而区块链技术的应用正好可以满足国家的这一需求。区块链技术本身具有去中心化、开放透明的特点，这样，系统中的任何一个节点之间进行的数据交换都不必担心信用问题。区块链技术，使得数字货币体系中的所有规则都是透明的、开放的，所以国家可以利用数字货币防止像以往一样出现诈骗问题的发生。

### （2）减少洗钱、逃税漏税等犯罪行为

目前，分散的金融机构拥有多个内部账本，而未来区块链技术应用与国家数字货币，将为金融机构建立全国统一的账本，每笔交易都可追溯，任何逃税、漏税、洗钱等行为都会得到严格的监管，甚至可能实现在刷卡机上自动扣税。

### （3）自动化金融服务

区块链同时也是一种智能合约技术，这样就保证所有的金融服务都能在自动化、智能化的基础上实现，这样银行以往出现排队办理业务员的情况也将不复存在。

总之，基于区块链技术的数字货币将有效提升整个金融业的资金和信息安全，提升整个社会的能效性，对全球金融业的发展具有极大的推动作用。



## 跨境支付与结算

当前，跨境电商正处在风口期，各国对于进口食品、日用品、酒水饮料、婴幼儿奶粉等的需求推动了跨境电商的蓬勃发展。但是在为各国提供更多商机的同时，跨境支付也表现出众多痛点。具体来讲，这些痛点表现在以下几个方面。

其一，手续费极高、周转期漫长。目前，电汇成为解决跨境电商的直流支付方式，其汇款周期为3~5个工作日，除了中间银行收取一定数量的手续费之外，环球银行金融电讯协会也会通过其他系统进行电文交换收取较高的电讯费用。以我国为例，通过中国银行进行跨境汇款，会收取单笔150元的电讯费。

其二，跨境支付诈骗行为越来越严重，由此引发了跨境资金风险以及其他的法律商业风险。

其三，中间环节多。在现今的跨境交易的过程中，往往会找一个可信任的中介角色，当跨境汇款与结算的方式日趋复杂的时候，在付款人和收款人之间所依赖的第三方信任机构就显得尤为重要。

然而，区块链出现并应用于跨境支付与结算场景当中，摒弃了中转银行的角色，实现了点到点快速且成本低廉的跨境支付。具体来讲，区块链在跨境支付与结算场景中的应用优势主要体现在以下几个方面，如图5-2所示。

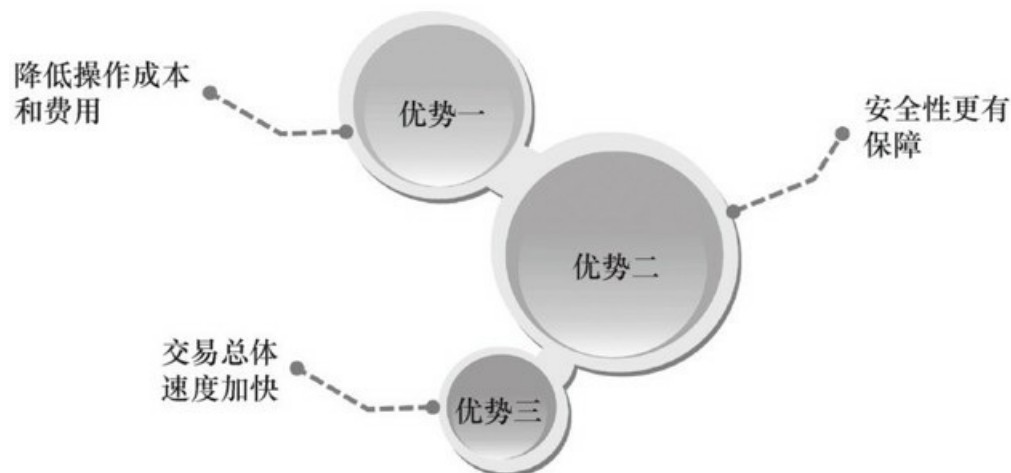


图5-2 区块链在跨境支付与结算场景中的应用优势

### 1.降低操作成本和费用

首先，区块链免除了中转银行这一环节，这就意味着免去了中间费用。

其次，因为不再需要与往来中转银行之间的银行业务关系，银行之间的竞争会加剧，给手续费和外汇业务利润带来压力，并导致总体成本降低。

最后，流程更加具有透明性。

麦肯锡相关数据预算显示：“从全球范围来看，区块链技术在B2B跨境支付与结算业务中的应用将使每笔交易成本从约26美元下降到15美元，其中约75%为中转银行支付的网络维护费用，25%为合规、差错调查以及外汇汇兑成本。”

### 2.安全性更有保障

区块链的分布式账本技术使得跨境支付与结算的安全性得到了更好的保障。

### 3.交易总体速度加快

在未来，银行与银行之间不再需要通过第三方，而是通过区块链技术打造的点对点支付方式，使得传统的中间环节可以省去，实现全天候实时支付与到账，提现便捷、快速，满足了跨境电商支付与结算的及时性和便捷性需求，从整体上提升了交易速度。

Ripple是美国旧金山的一家旨在利用类区块链技术概念来发展跨境支付和结算的新兴金融公司，Ripple建立了一个没有中央节点的分布式支付数字支付网络，采用分布式的身份认证技术，帮助全世界的中小银行，以低廉成本完成瞬间的跨国转账业务。这一业务是通过在全球统一网络金融传输协议取代传统环球同业银行金融电讯协会网络的跨境转账平台的基础上来实现的。Ripple的跨账本协议实际上是让所有参与协议的各方都能够看到相同的一个账本，通过Ripple的网络，银行客户可以实现点对点跨国支付与结算，整个过程中不需要中心组织参与管理，并且各国的货币都可以实现快捷支付与结算。另外，Ripple借助类区块链技术，使得传统模式下的中间环节和中间人都全部被砍掉，直接让小银行与小银行之间能够进行沟通，这对于小银行来讲的确是个福音。当前，Ripple已经与全球17个国家的银行展开合作，使得这些合作银行的费用大幅降低。以欧洲的一家名为“菲罗”的银行为例。在与Ripple合作之前，因为没有存款网点客户要在其进行开户并转余额的时候，就必须通过其他银行账户把余额转进去。但是在与Ripple合作之后，以前转账的手续费是每笔5欧元，现在则减少到0.49欧元，这样就相当于手续费降低了10倍。在之前需要2个工作日才能完成转账，如今可以实现瞬时到达。无论是对于银行还是客户来讲，这都带来了很好的体验感。

Ripple仅仅是利用区块链技术为众多银行等金融机构提供解决方案的典型代表。当前，Chain、Ethereum、IBM、Microsoft等知名企业也开始利用区块链技术发展跨境支付与结算业务。可以预测，在不久的将来，金融体系现有的传统交易模式将会被高效能、高安全性以及成本低廉的区块链技术所取代。

## 数字票据

票据本身是一种集支付和融资功能为一体的工具，近年来受到了银行和企业的极大青睐。当前票据市场已经成为货币市场中的重要组成部分，受到了金融机构的极大重视。票据业务为实体经济的发展提供了重要的支持作用，同时也推动了货币市场的进一步扩展，丰富了金融市场中的产品种类。因此，在某种意义上讲，票据已经成为整个经济发展的重要支柱之一。但是，从2015年年中开始，我国国内爆发了诸多票据业务的信用风暴。票据业务创造了大量流动性的同时，相关市场也滋生了大量违规操作或者出现了众多客户欺诈行为，陆续有多家商业银行的汇票业务事件集中爆发。

随着科技和经济的进一步发展，数字票据的概念随之产生。所谓数字票据，实际上不是一种实物票据，但也不单纯的是一种虚拟票据，它是借助于区块链技术，在现有票据属性、法律和市场的基础上诞生的一种新型票据展现形式。与现代的电子票据相比较，数字票据在技术架构上发生了很大的变化，但却同时拥有电子票据所拥有的优点和功能，在结合了区块链技术的基础上形成了一种更具安全性、智能性、便捷性，以及更具发展前景的票据形态。数字票据的出现给货币市场乃至整个金融领域的发展带来了另一番新天地，这也是进入人工智能时代的一种金融创新。

基于区块链技术的数字票据的优势

具体来讲，建立在区块链技术上的数字票据具有以下几个方面的优势，如图5-3所示。



图5-3 基于区块链技术的数字票据的优势

### 1. 系统搭建和数据存储越过中心服务器，同时也不需要中心级应用

这样将带来以下4个方面的优势。

- (1) 省去了中心应用和介入系统的开发成本。
- (2) 降低传统模式下系统的维护和优化成本，其中包括设备投入成本、数据备份成本、应急管理成本等。
- (3) 减少系统中心化带来的风险问题。这样就不会出现因为过于集中化而带来的服务器崩溃或者被黑客控制的问题。分布式数据库具有强大的容错功能，不会因为其中一个或几个节点的错误而影响所有参与各方的正常运转，更不会给数据的存储和交易更新带来任何影响。

(4) 减少了中心化模式下数据反复被记录和存储而产生的成本重复性浪费。各个参与者中记录的数据账本既可以看作是分账本，同时实际上也是总账本。

2. 使得任何交易都可以实现追踪和查询，对其中涉及商业秘密的内容进行屏蔽，起到保护隐私的作用

由于数字票据的数据具备完整性、透明性，以及可以通过时间戳获得可验证性的特点，使得任何交易都可以实现追踪和查询。这些数据不单单保存在某一个服务器或者某一个参与方的机器当中，还可以通过相应的技术对其中涉及商业秘密的内容进行屏蔽，从而达到保护隐私的目的。基于这一特点，呈现出以下几方面的优势。

(1) 通过所有参与方任何行为数据的记录和积累，形成信用分析和评估机制，这样就可以最大限度地降低违约后无人知悉的可能性，从而为信用环境的建立打下了良好的基础。

(2) 信息的可跟踪性可以更加便捷地实现历史数据信息的查阅，可以对票据的流转过程进行更好的控制，一旦发生纠纷，便可以使用相关权利进行自我保护。

(3) 对于票据交易以及其他票据产品中存在的风险进行有效把控，防止现有模式下重复质押或合作伙伴作案风险的出现。

3. 智能合约的形式使得数字票据的整个生命周期具备了一定的可编程性，即具备了限制性和可控性

这样给数字票据带来的优势体现在以下几个方面。

(1) 交易的控制方式表现出更加多元化的特点。例如，在实际交易过程中会存在数字票据代持的模式，那么，可以在交易一开始就将约定买回的日期通过代码的形式写在智能合约当中，等到到期时，再将票据自动完成赎回买断。这也就是所谓的“双买断”模式。

(2) 智能合约通过代码来实现的，在这种条件下，数字票据的交易就不需要再通过线下合同来作为强化执行，这样就很好地避免了执行过程中出现的违约现象。

基于区块链技术的数字票据的应用

基于这些优点，具体在数字票据的场景中的3个环节应用情景如下。

#### 1. 承兑环节

不同的企业在整个网络体系中所占据的节点是不同的，假如企业A需要为企业B开具票据，那么承兑人相当于对出具票据企业A进行第三方担保，这实际上与比特币的第三方记账十分类似，只是比特币争夺记账时比的是算力，而承兑环节则是通过建立一套完整的算法来完成承兑操作，并生成相应的数据区块。

在这一环节中，其突出的优点有以下3点。

(1) 与现有的承兑需要与中心的商业电汇系统进行数据交换和信息登记，实现了非中心化的出票过程。

(2) 省去了现有模式下企业需要到开户行开立企业网银的烦琐，这样就相当于省去了网银这个中介传输方。

(3) 通过记录数据块的时间戳解决了所有参与者对持票企业的信任问题。现有模式企业主要通过企业网银接入商业电汇系统，相当于将风险转移到了企业网银的信息安全上，一旦U盾丢失或被破解，将会带来巨大的隐患。如果借助区块链技术，则情况就大不一样了，每个点上的参与方都有自己的私钥，一旦丢失私钥或者被黑客破解，所产生的信息将在全网被公开，不法分子就无法作案了。

#### 2. 流转环节

该环节包含了企业间的流转、贴现、转贴现、再贴现、回购等一系列业务类型，如图5-4所示，这些业务类型以及交易中的要求和限制，举个简单的例子，比如在做回购业务的过程中，约定买入返售到期，可以通过编程的方式来实现。在流转环节中，可以参照比特币中的交易场景，卖出方公布公钥，买入方拿自己的私钥进行匹配，一旦匹配成功，则只需通过建立合适的规则来由第三方完成信息的记录并生成数据区块即可。



图5-4 数字票据流转环节的业务类型

这一环节中，突出的优点：

- (1) 省去了原来的中心化系统做信息流转；
- (2) 实现了卖方和买方之间点对点的交易，确保了价值传递的去中心化；
- (3) 通过智能合约和流转的可追溯性特点有效地避免了道德风险、操作风险和信用风险，从而保证了交易的公平性和真实性。

### 3.托收环节

在该环节，由于票据的到期日期在承兑时已经被写入代码当中，所以程序控制会在到期的时候由持票人向承兑人自动发出托收申请，等到托收完成后只需要按照一定的规则来由第三方完成信息的记录并生成数据区块即可。

该环节中，突出的优点表现为：

- (1) 价值交换直接完成，如果直接约资金清算挂钩，那么就不会存在托收预期的问题；
- (2) 通过代码控制，使得在托收的过程中不能同时进行其他操作，这样就确保了账实相符。

## 银行征信

信用一直以来都是影响社会经济资源配置效率的重要因素。银行作为经济社会中更具重要位置的金融中介，其在当前社会信用体系中所起到的核心作用主要体现在两个方面：一方面是解决资金供给双方的信息不对称问题；另一方面是对金融交易过程中出现的信用风险问题进行有效控制并进行定价。最后，再从这两个方面入手来获取相应的经济利益。然而，大数据的出现和突飞猛进的发展，使得越来越多的数据产生并推动了金融领域的发展，尤其是对于即将进入人工智能时代的银行来讲，更是为银行的信用评测提供了创新源泉。

区块链是指用密码学方法的动态编程数据块链，本质上是对数字世界中产生和存在的数据与代码进行认证，使得某类区块链协议的数据或代码被赋予了某类共识性信任。因此，利用区块链技术可以有效解决在数字化社会中存在的数据与代码的身份和信任问题，从而极大地提升银行客户信用体系构建的能力，对于银行征信将起到极大的操作风险和信用风险的把控作用。

基于这一点，可以说基于区块链技术的银行征信系统与金融业中其他机构的征信系统相比较具有极大的优势，具体从以下几个方面入手，如图5-5所示。



图5-5 区块链在银行征信系统的应用优势

### 1.形成信用客户传统资源

基于社会分工的原因，银行拥有了规模非常庞大的金融客户群，这个客户群体中所包含的客户属性几乎涵盖了整个经济社会的个体。对于银行来讲，个体银行账户数据是银行征信系统构建的重要数据，其中包含了用以判断客户信用风险的数据信息，因此，银行账户数据是银行征信体系构建必不可少的先天优势。另外，银行客户数据具有一定的历史性，在很大程度上是很难找到替代资源的，即便对于那些科技企业或者新兴的“互联网+”企业来讲也是无法做到数据追溯的。基于这两方面的竞争优势，银行应当对其自身所积累的大量数据资源进行保护，因而，区块链技术是非常不错的选择，通过区块链技术将银行所积累的海量数据进行认证，通过版权保护与主动授权的方式进行管理，逐步在当前互联网时代形成一个庞大的信用数据资源中心。

### 2.提升监管门槛与法律合规成本



当前，国家对社会征信方面的监管非常严格，提升了该领域的准入门槛，同时也提升了法律合规成本，然而银行作为金融领域中的传统经营机构，在这方面实际上是具有得天独厚的优势的，这对于那些企图进入信用评估领域的科技企业和互联网平台来讲，反而是非常不易实现的。

2014年，瑞士联合银行集团（UBS）支出了10亿美元用于信用风险的管控。另外，在2013—2015年，汇丰集团也采取了相应的措施，将原来法律合规部门的员工从2000多名增加到了7000多名。两家银行之所以这么做，并大幅提升监管成本，是因为可以通过这样的方式来提高交易安全性，并且保证交易更加符合法规要求。

### 3.培养专业人才

通常情况下，影响个人经济信用问题的因素是有很多的，不仅仅是因为个人经济状况而导致的，还包括个体行为、观念，甚至社会经济环境也会与个人的经济信用产生一定的关联。当前，即便是征信技术已经实现了跨行、跨领域，但是在信用评估和管理问题上依然在专业性方面有很高的要求，尤其是专业的特殊性往往是其他专业技术人员所难以把握的。这样就使得各种大批的专业性人才经过银行的专业性培养而成为银行征信系统管理的中流砥柱，这就使得那些科技企业望尘莫及。[shu籍分 享微 信 whair004]

### 4.反欺诈行为，防止金融犯罪

在过去几年，全球的商业银行为了满足日益严格的监管要求，所以选择加大力度投资信用审核以及客户征信，从而有效提升反欺诈行为的发生，进而减少金融犯罪的发生。区块链上记载的数据，包括客户数据信息和客户交易记录等，对于银行有效识别异常和防止诈骗行为的产生方面具有极大的帮助。基于区块链技术的信用特征，银行可以在辨别客户信用度的时候，将不良客户信息记录在区块链当中，这样，存储的客户数据信息和交易记录不但可以进行实时更新，还能够得到更好的保护。银行通过分析和监控共享的分布式账本内有关客户交易行为的异常情况来及时判断并消除欺诈行为。

Chainalysis作为瑞士一家专门打击利用数字货币洗钱和欺诈行为的初创公司，为银行设计了一款反欺诈监测系统。该系统的设计目的是帮助银行监测和分析其区块链上的异常交易行为，从而对交易过程中的不法行为进行有效控制，最终达到帮助银行实现反洗钱和反欺诈的目的。

书籍每日免费分享微信jnztxy朋友圈

## 有价证券交易

证券的发行与交易在操作过程中的流程是非常繁杂的，效率也相对低下。通常情况下，企业在发行证券之前，会事先找到一家券商公司与证券发行中介机构签订委托募集合同，再进行一系列的申请流程，最后才能寻求投资者认购。这样烦琐的流程需要很长的时间才能完成，通常需要3天的时间间隔。

基于这种状况，必须要寻求一种能够化繁为简，从根本上提升证券发行与交易效率的有效技术。使用区块链技术就是一种很好的解决方式。基于其本身所具备的特点，区块链技术使得金融交易市场中的所有参与方都能够平等地分享和使用数据信息，让交易流程更加公开化、透明化，从而极大地提升了交易的时效性。各方借助共享的网络来参与证券交易活动，使得原本在很大程度上依赖中介的传统交易模式才能完成的操作流程，进一步转化为分散的平面网络交易模式。这种基于区块链的交易模式在金融市场中呈现出明显优势，如图5-6所示。

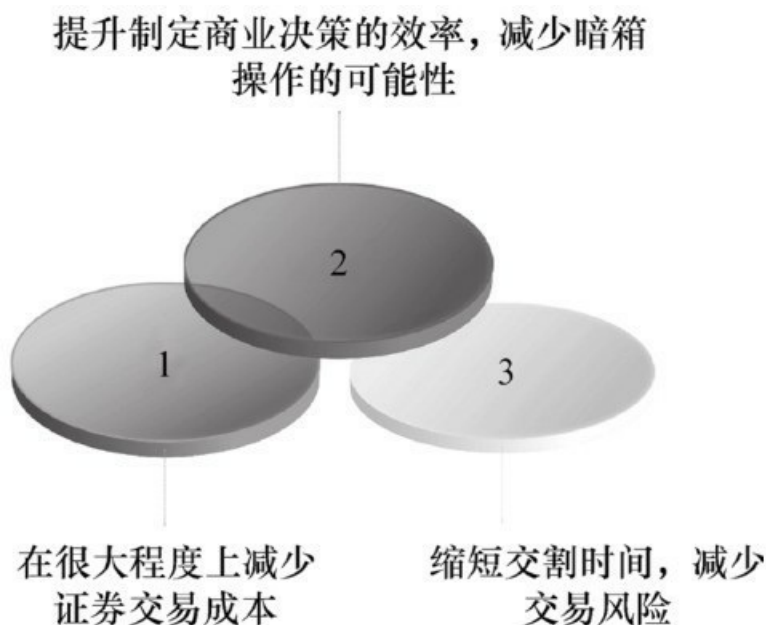


图5-6 区块链交易模式在金融市场中的应用优势

### 1.在很大程度上减少证券交易成本

能够在很大程度上减少证券交易成本，区块链技术的应用可以使得证券交易的流程变得更加简单、透明、快速、高效。

### 2.提升制定商业决策的效率，减少暗箱操作的可能性

利用区块链技术可以对交易双方或多方的身份、交易量等相关信息进行实时准确的记录，有利于证券发行者更加快速、清晰地了解股权结构，进而提升制定商业决策的效率；区块链的公开透明性以及可追溯的特点，使得证券交易过程中的电子记录能够减少暗箱操作以及内幕交易发生的可能性，更加有利于证券发行者和监管部门对于证券市场稳定性和安全性的维护。

### 3.缩短交割时间，减少交易风险

区块链技术在证券交易过程中的使用，使得以往的交易时间从原来的1~3天一下缩短到了10分钟，仅仅需要短短的10分钟就可以完成整个交割过程，减少了交易的风险，提高

了交易的效率和可控性。

基于区块链技术在证券交易场景中的使用较以往在效率方面有了很大的提升，使得越来越多的证券企业开始关注并进行了尝试，诸如美国全国证券交易协商会Nasdaq、芝加哥商品交易所、迪拜多种商品中心、德国、伦敦、日本、韩国等，我国以上海证券交易为首所组织的China Ledger联盟也在这方面有相关尝试。事实证明，大多都取得了很好的应用效果。

2015年10月，在拉斯维加斯举办的Money20/20大会上，美国加州一家帮助机构与企业定制部署区块链基础设施的全球世界知名初创公司Chain，与美国全国证券交易商协会Nasdaq，共同推出了私募股权市场交易平台Linq，该平台是通过区块链平台进行数字化证券产品管理的系统平台。对于股票交易者来讲，一方面，区块链可以帮助其在交易过程中打破传统的对纸笔或者电子表格等记录方式的依赖，减少交易过程中的人为差错，提高交易过程中交易记录的透明度和可追踪性；另一方面，对于股票发行公司来讲，Linq平台能够更好地管理股票数据，让Nasdaq在私募股权市场中为创业者和风险投资者提供了更好的服务。

2015年，澳大利亚证券交易所表示，将通过借助区块链技术设计一套全新的系统来取代以往的所有核心技术系统，以此来提升整体结算速度。美国区块链创业公司Digital Asset Holdings（DAH）已经筛选400家投标者并签订了有关这项计划的合同。DAH借助区块链技术研发的全新系统帮助所有的参与者在同一个数据库中进行实时的资产交易活动。在这个全新的系统中，所有的参与方都能够让数字资产在交易的双方之间进行转移，但是这个转移过程又不需要在任何中央机构的监督，因此，所表现出来的实时性是显而易见的，结算时间也从原来的两个工作日减少到了几分钟。

## 股权众筹

当前，国家提倡“大众创新，万众创业”，在这个时候，股权众筹成为众多投资者和创业者的机会，使其成为能够在当前竞争激烈的市场中能够站稳脚跟的基石。然而，区块链技术的出现以及在股权众筹场景中的应用，也为当前众多的创新人士在发展过程中提供了一个全新的视野。

### 1.区块链在股权众筹的发展领域具有极大优势

#### （1）公开透明、真实可信

所有的信息对于投资各方都是透明的，并且真实有效，而且信息记录是非常难以篡改和伪造的。

#### （2）促进股权流通和资源共享

股权转让以及股权登记更加具有安全性和便捷性，在众筹平台上所有的投资人和项目都可以实现共享。

### 2.区块链技术在股权众筹中的应用

#### （1）股权登记管理

区块链具有独特的身份账户体系，可以作为电子凭证。当前现有的非上市股权管理，往往需要经过人工处理纸质股权凭证、期权发放和可换票据。一旦股权变更变得频繁，则会使得股东名册维护变得更加烦琐，历史交易的维护和跟踪也会趋于困难。因为区块链技术具有将一切数字化的特点，因此可以使得股权登记变得更加安全和高效。区块链众筹股权登记借助于区块链账本的安全透明、不可随意更改、易跟踪的特点，从而保证股权变更历史更加精准记录。

#### （2）股权转让流通

区块链具有降低信用风险的作用。传统的OTC场外股权交易是建立在双方信用的基础上的，交易双方共同承担信用风险，需要建立双边信授之后才能进行接下来的交易活动，市场交易者的信用风险由交易平台集中承担。这样在区块链技术应用与股权转让流通之后，股权的所有权都被记录在区块链中，股权交易在获得所有者私钥签名之后才能验证通过。交易确认之后，股权的所有权记录在区块链中，从而保证交易双方的利益，如图5-7所示。

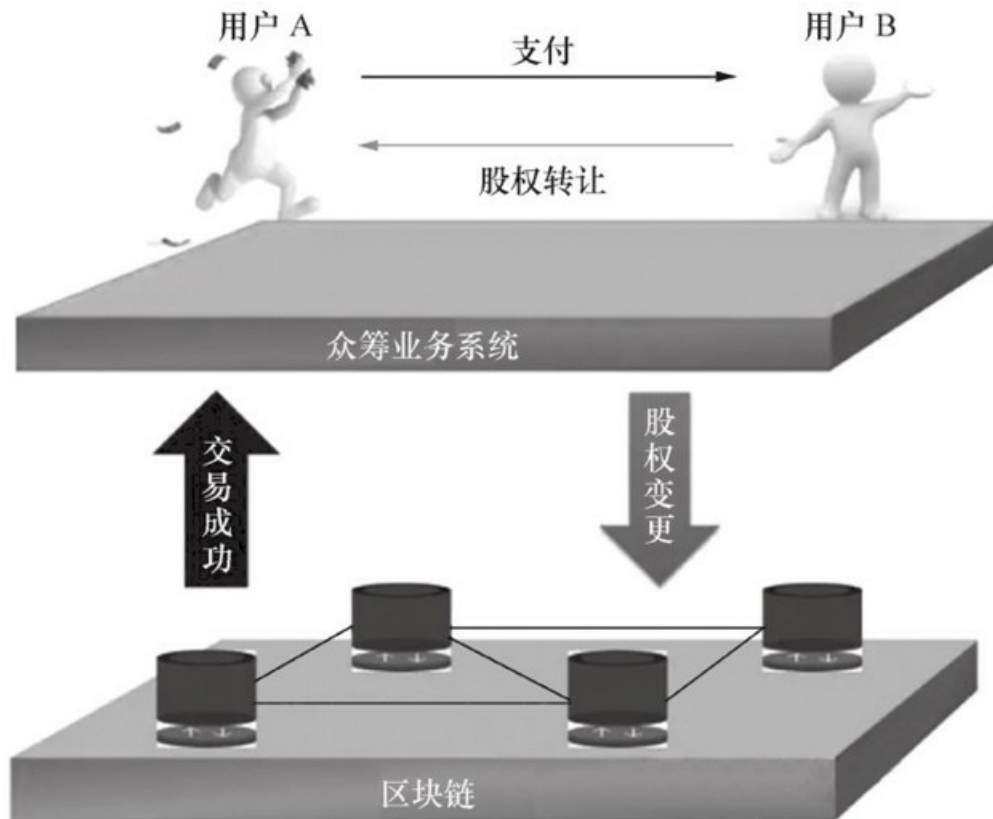


图5-7 股权转让流通

图片来源：《区块链，新经济蓝图及导读》

### （3）众筹合约

区块链具有确保合约履行不被篡改的特点。在股权众筹发起的时候，发起人、众筹平台、领投人、保荐人等都是需要签署众筹合约的，且签署的是同一份合约，约定各自承担的义务和责任。这份合约可以通过智能合约的形式存储在区块链当中，借助区块链技术来保证合约履行的合法性以及合约内容不被篡改。

假设根据合约的条件，众筹发起人发起了500万元的众筹，区块链底层首先产生第一个事务（TX1）：创建一个联名账户，从领投人的账户中拿出300万元打款到联名账户中，同时剩下的200万元生成借条，用于吸引跟投资人购买，在合约中共同签名的各方都可以共享和维护该联名账户；接下来再创建TX2（如果在规定的众筹时间内，200万元借条全部销售一空，则从联名账户中拨出500万元到发起人账户中）和TX3（如果此次众筹失败，则会跟踪联名账户的交易记录，将所有的投资资金全部退换给领投人和跟投资人）。TX1、TX2、TX3会被全部写入区块链当中，所有的众筹流程都基于区块链底层自动执行，不会受到任何人的干扰而出现被篡改现象，如图5-8所示。

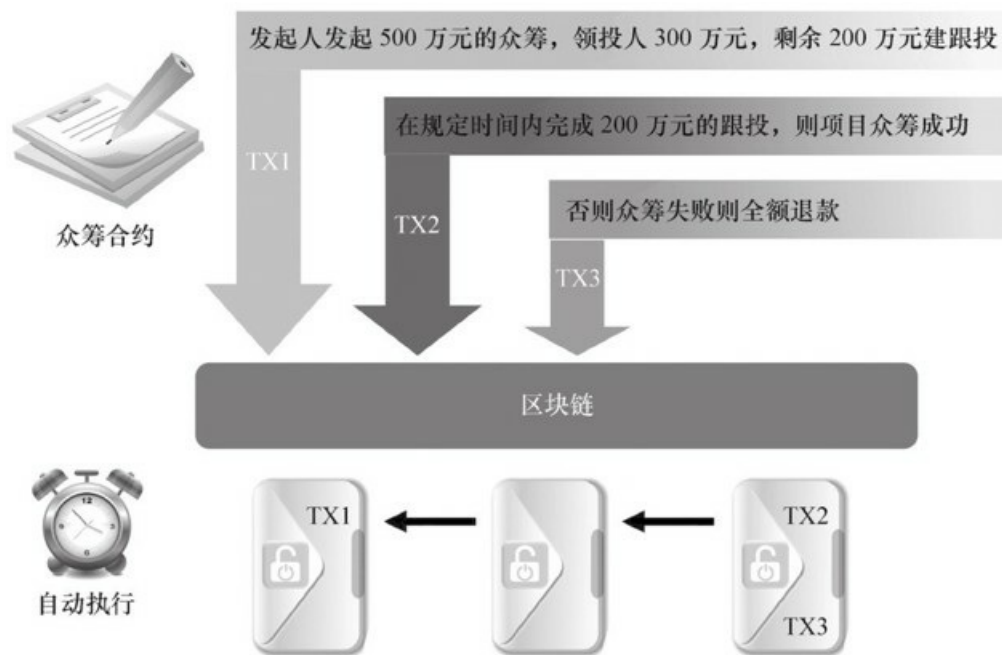


图5-8 众筹合约举例

#### （4）众筹联盟与数据共享

股权众筹业务本身与传统场内交易是有很区别的，股权交易业务活动并不是由一个或者少数几个统一的机构来组织实现的，而是需要很多独立经营的公司分别进行，这样就使得交易活动的各方都比较分散。而众筹联盟的作用就是将这些分散的参与者都聚集起来，从而形成一个联合的分布式交易中心。

但是，众筹联盟之间的存在的最大缺陷就是各方之间缺乏信任，信任是联盟能够持续下去的必要前提。区块链技术的出现以及应用于众筹联盟，则能够有效解决这个信任缺乏的问题。区块链技术本身就是一个去中心化的信用技术，因此在组建众筹联盟的过程中与其他技术相比较具有得天独厚的优势。区块链构建的信任是不以人的意志为转移的，即使彼此之间没有建立信任关系，依然可以保障系统和业务的顺利进行。每个众筹平台都是区块链上的一个节点，每个节点都有属于自己的私钥和公钥，在交易验证和记账的过程中大家都是参与者。不但如此，监管机构也同时可以称为区块链上的一个节点，从而使得各个联盟之间的活动能够实现透明化、公开化。

组建一个股权众筹联盟，首要的问题就是要将用户、项目以及股权的所有权进行共享。如果按照传统的方式来搭建众筹联盟，那么每个平台都有自己的独立数据库，就会使共享流程变得复杂化，不利于效率的提升。然而，区块链技术的应用能够使各个平台将其用户、众筹项目、股权凭证等全部映射到区块链上，所有信息对于各方都是可见的、透明的，从而使得共享流程变得更加简单化，能够实现数据的高效共享。



## 第六章 人工智能时代，区块链在数字金融资产中的应用



过去存取款要亲自去银行或分行，填写支票，现在我们可以足不出户，使用网上虚拟银行进行资金转账。在金融服务领域，比特币区块链技术的真正革命就是资产运转数字化、智能化，区块链要实现的是资产数字化以及这些数字化了的资产如何在整个经济环境中交易、处理和流动，而这将会真正改变金融服务运作的方式。这也是人工智能时代区块链应用与数字金融资产中的一项重要变革。

## 区块链在银行业的应用

当前，区块链概念在我国已经逐渐火热起来，凭借其去中心化、无需中心信任、不可篡改和加密安全的特点已经逐渐走入政府机构、金融领域以及诸多大型企业的视野。2016年10月18日，中国区块链技术和产业发展论坛成立大会暨首届开发者大会召开，会议中发布了《中国区块链技术和应用发展白皮书》，该《白皮书》对当前国内外区块链的发展现状和趋势进行了总结，并且分析了当前包含金融、供应链、智能制造、社会公益和教育就业等多个应用场景的技术应用，还特别指出了区块链的核心技术路径以及未来区块链技术标准化方向和进程。重要的是，该《白皮书》将金融作为区块链技术的第一个应用领域，分析其具体体现在支付、资管、证券、清算结算以及用户身份识别的细分场景。

目前，我国对于区块链的应用还处于探索阶段，各大商业银行也开始通过自身实验以及寻找合作伙伴的方式，把区块链技术作为继“互联网+”“大数据”“云计算”之后的又一全新工具来推动自身的发展，提升市场竞争力。

2016年1月，中国知名区块链企业Bit SE率先发布了首个基于区块链技术的真假校验平台，即Ve Chain平台。2016年3月，阳光保险用区块链技术作为底层技术架构推出“阳光贝”积分，成为国内第一家区块链积分的发行方、首家应用区块链技术的金融企业。

当前，国外金融机构对于区块链未来的应用前景非常看好，纷纷开始在区块链技术领域进行布局，并探讨区块链技术在银行、证券等领域的应用，其中应用板块包括支付结算、智能债券、财务审计等方面。

截至2016年11月，国富银行、花旗银行、法国巴黎银行、加拿大帝国商业银行、德国商业银行、德意志银行、摩根士丹利等全球60多家大型商业银行加入到了金融科技公司R3区块链计划当中，致力于金融领域区块链的开发和应用以及全球清算一体化行业标准的制定。2015年12月，美国证券交易委员会正式批准了在线零售商Overstock通过区块链技术在互联网发行股票的计划。纳斯达克在纳斯达克私人市场开启区块链技术在股票市场的应用测试。Smart Token Chain公司推出智能合约结算交易所，通过使用智能令牌和区块链技术将全球所有的银行和其他支付系统连接起来。一些银行也在区块链领域进行独立探索和尝试，如花旗银行试水“花旗币（Citicoín）”的加密货币；瑞银集团在伦敦成立了区块链金融研发实验室，探索区块链在支付结算等方面的应用。

具体来讲，银行对于用区块链技术的创新性应用过程中采取了以下几方面的措施，如图6-1所示。

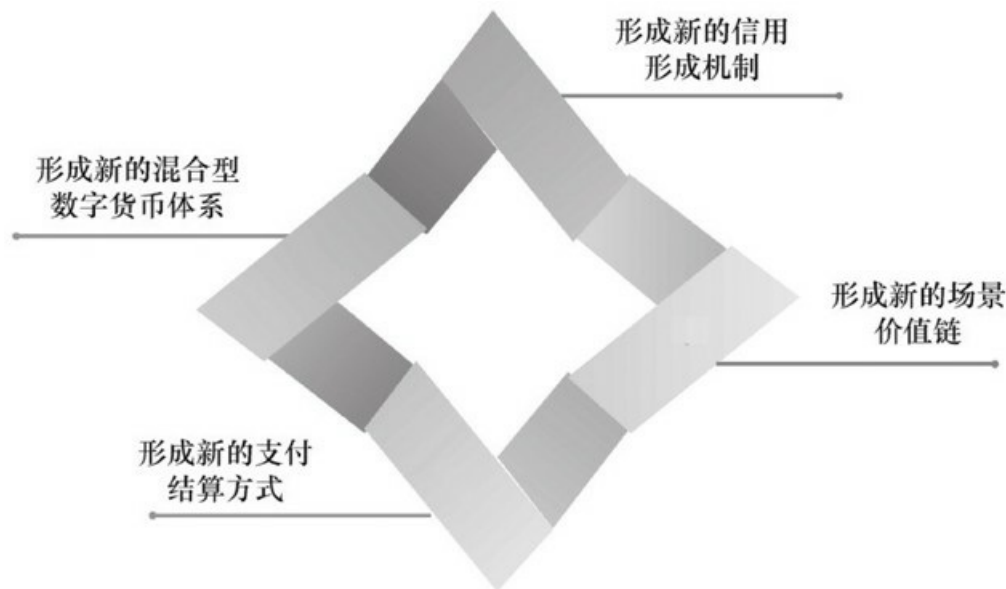


图6-1 银行实现区块链技术创新性应用的措施

### 1.形成新的混合型数字货币体系

区块链技术的出现，站在事实的基础上对数字货币的跨国界应用的可行性进行了验证，同时也证明了区块链技术可以实现信息共享和透明化。但是，如果站在国家主权的立场上来看，实现货币的国际化、构建一个新的国际化货币体系，在一定程度上还具有很大的困难。2013年，我国五部委联合发文防范比特币风险，并明确“比特币不具备货币属性，是一种虚拟的商品，不具有法偿性”这一特点。即便如此，数字货币依然在国际上的各大银行中受到重视。事实上，像比特币这类以区块链技术为基础的数字货币更可能是混合型的，其他发展前景可能会出现以下3种情况。

#### （1）混合型数字货币

由国家中央银行发行，这样无论其发行规模和汇率都是由国家统一掌控的，从而形成一个以法币为基础，以数字货币为补充的多元化货币体系。

#### （2）形成不同金融场景的虚拟货币

催生了虚拟金融的交易规则的流程，从而为实体经济的繁荣起到巨大的推动作用。当然，那些具有信誉度的银行推出了数字货币并创造了虚拟交易场景，则让消费者能够体验到更好的创新性服务。

#### （3）混合型数字货币

作为混合型数字货币，其产生的规则具有一定的可变性，并不以挖矿为基础的形式产生。

### 2.形成新的信用形成机制

信用体制一直以来都是银行发展的核心。在传统模式下，银行是通过相关管理机构来维护信用、管理风控的，信用评级技术根据用户不同性质进行分类，如小额信用贷款的授信技术等。在客户申请贷款的时候，银行需要查询与客户相关的各种征信数据信息。在查证环节中，信息的收集链条环节比较多，所涉及的范围比较广，但依然存在信息不完整、数据不准备等缺陷，同时还造成成本过高、决策程序冗长等问题，这样对银行高效完成业务操作具有极大的影响。

在大数据时代，各家企业往往采取多维度视角来挖掘和分析客户的行为特征，并以此分析客户的信用等级。例如，蚂蚁金服就是通过对淘宝、天猫用户的行为数据进行分析，从而判断用户的信用等级情况。虽然大数据可以对消费、小额贷款等进行批量授信，能够在一定程度上提升工作效率，使得数据信息具有一定的可靠性和较高的时效性，但是，这

仅仅是实现了传统金融的电子化，并没有使得信用创造的方式发生根本性变化。

区块链技术本身是通过去中心化的信用创造方式来进行信用创造的，其具有以下几个特点，如图6-2所示。

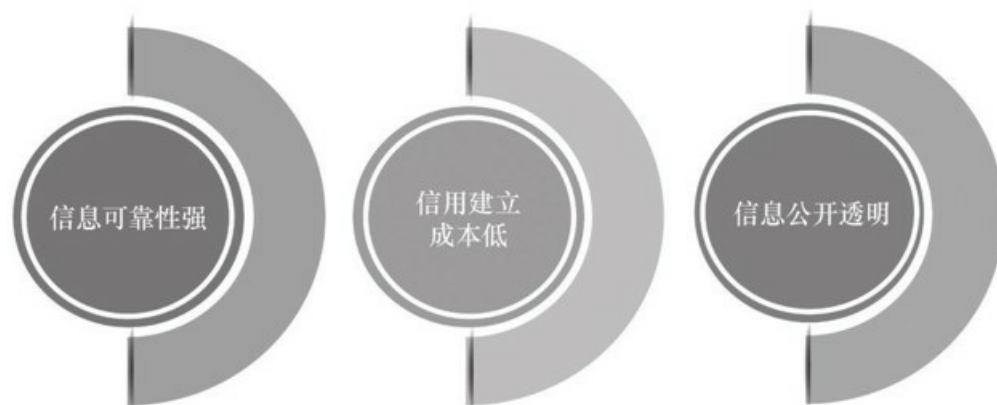


图6-2 银行借助区块链形成新的信用形成机制具有的优势

#### （1）信息可靠性强

基于去中心化的区块链技术，通过连接密码保证借款方信息数据的高度安全以及不能篡改的优点，使得每一个交易都能够实现程序化记录、存储、传递、核实、公开等，银行可以基于区块链的这些特点随时获得借款方的信用状况，并且其可靠性远远大于大数据风控，可以有效避免客户经理主观因素在客户信用等级评价中产生的偏离，同时也可以有效防范道德风险的发生。

#### （2）信用建立成本低

通过各个参与方全网记账的方式来建立信用，使得信任关系不依靠第三方中介机构就能保证数据信息的真实性，贷款人只需要调取区块链上相应的信息数据即可，这样就大大降低了信用建立的成本。

#### （3）信息公开透明

客户在贷款的过程中，其产生的所有数据信息只需借助程序算法就可以实现自动记录，并存储在数据块上，使得信息实现透明化、公开化，并且更具安全性，能够借助区块链技术获得更好地隐私保护。

### 3.形成新的场景价值链

互联网的突飞猛进以及对金融市场的极大冲击，使得传统的销售模式已经不再适应现代经济的运行需求。场景金融成为当前互联网金融发展的重要支柱，使得银行从传统的单一的厅堂营销服务场景融入更多的场景当中，比如网购场景、社交场景、旅游场景等，这样不但可以增强客户的体验满意度，还可以形成一个依托场景的金融生态圈。

区块链技术本身架构灵活，能够根据不同的应用场景、不同的客户需求、不同的客户结构以及不同的资金运转流程而创造相对独立的、能够进一步强化金融和实体经济相互融合的场景价值链。具体表现在以下几个方面：

（1）增加客户黏度和稳定性，使得金融交易更加依附于金融场景；

（2）客户在场景金融中的所有交易信息都被记录到区块链上，更具安全性；

（3）基于区块链这一“信任的机器”，场景客户的金融需求不再像以往一样依赖于第三方金融机构，甚至不再依赖于中心化大数据的支持，银行与客户之间比以往更具信任。

### 4.形成新的支付结算方式

虽然在当前的互联网时代，已经使得支付结算效率在很大程度上有所提升，但是在跨币种、跨国界、多种经济合约下，依然在多中心、多环节方面受到了限制，从而使得支付

结算的效率往往显得力不从心。

区块链技术的去中心化和点对点特征，能够减少中间环节、降低交易成本，在很大程度上提升交易效率。区块链在银行支付结算方面的应用，使得银行新城了一种全新的支付结算方式，具体表现在以下几个方面。

（1）基于区块链的点对点特征，使得点对点交易提升交易效率。交易的过程在本质上就是结算的过程。举一个简单的例子，用户在使用打车软件叫车，等到专车司机将其送到目的地并结账的时候，就不需要经过银行这样的中介机构来结算，而是直接通过数字货币的形式完成支付行为。

（2）传统模式下，跨界银行进行支付结算，往往需要借助SWIFT（基于脚本的编程语言）在全球各个银行、代理行之间进行冗长的交互，整个流程长、效率低、成本高。然而区块链技术应用在该场景当中，就使得所有交易被实时记录在全球共享的信息平台上，实现快捷、轻松交易。

（3）区块链是一种分布式数据存储模式，也可以说它是储存加密货币（如比特币）的交易记录的“公共账本”，因此其所提供加密的转账业务，能够让所有人都能得到准确的资金、财产或者其他资产账目记录，这样就可以有效提升支付结算的安全性。

总之，虽然当前对于区块链在银行业中的应用还处于探索和研究阶段，但是人们对于区块链技术的热情已经表现出来，并相信在未来人工智能时代，区块链在金融领域中的应用，尤其是在银行业的应用将会产生更加惊人的改革与创新，从而保证在金融领域的竞争模式下能够站稳脚跟。

## 区块链在保险业的应用

**未来场景1：**2026年，区块链技术在保险领域得到了广泛应用和认可，一家全球知名保险企业全部引入区块链技术，在分布在全球不同地域的20台高速计算机上进行数据备份，确保每位客户的信息不丢失、不遗漏……

**未来场景2：**2045年的一天，小郭去一家保险公司营业部续交当年的保险费。2016年他以期缴方式投保了一张30年的保单，今年是他续交保费的最后一年。但是业务员寻遍整个系统以及行业信息备份系统，却没有发现小郭的任何投保记录。29年来交纳的所有保费将近上百万元，面对当前情况正让小郭一筹莫展的时候，这家保险公司总裁授权从大洋彼岸的市区调取小郭的客户数据，小郭的保单得以成功找回，并且将最后一年的保费交纳完毕。

以上是我们所假设的未来场景，或许，在未来，并不需要10年或30年的时间，以上的一幕幕就可以成为现实。

无论哪个行业，都是将维护客户和最大化企业利益作为企业发展的战略目标。保险行业亦是如此。从互联网开始向金融领域渗透到现在，保险行业一直是一个慢节奏的行业，以目前的情况来看，传统保险业是通过一系列的人为操作所驱动的，即无论是从报价到投保申请、从承保到合规审核，还是从出单再到第一时间损失通知等，所涉及的每一个环节都离不开“人”的参与。这种情况就使得效率低下充斥了整个保险公司价值链的各个部分，与此同时也带来了一定的风险问题。也正因为如此，才有了区块链技术的用武之地，从而成为人工智能时代的一个创新性应用。

区块链本质上就是由一系列分布式账本组成，它的存在使得被信任交互与不可变审计跟踪的同时发生成为可能。这样，就使得区块链在保险行业中的应用能够产生以下几个方面的影响，如图6-3所示。

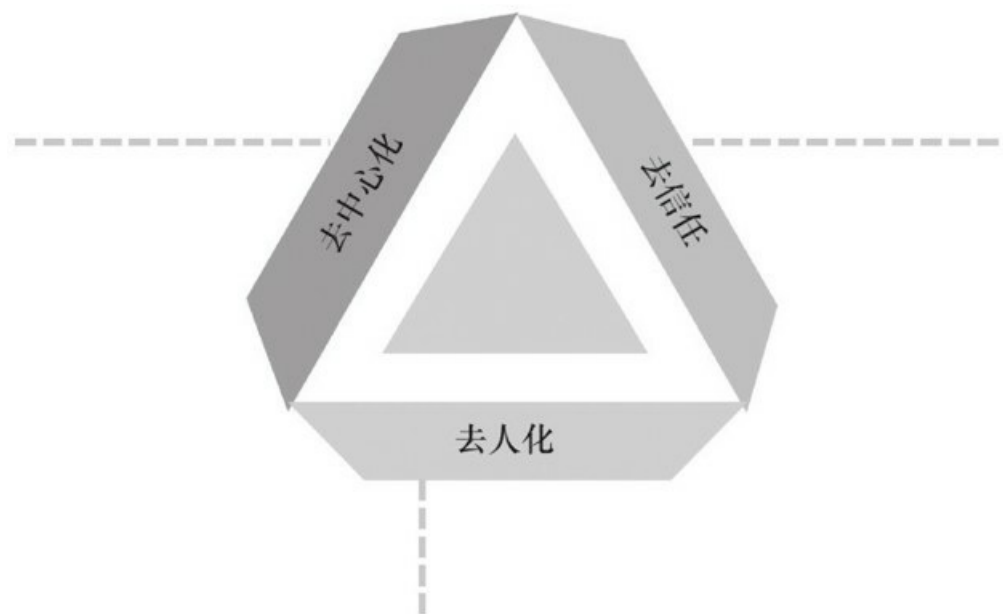


图6-3 区块链在保险行业中应用的影响

### 1. 去中心化

纵观历史，人类的发展和产业的形成一直以来都是通过逐步的中心化而实现的。保险



行业同样如此。保险公司实际上就是由政府 and 监管部门特许授权的风险转移集散中心，这些中心严重控制和影响着保险行业的运行情况和未来发展方向。长期以来，人们已经习惯于通过这些中心来完成有关保险的相关业务。

区块链具有去中心化的特点，区块链技术在保险业的应用，使得保险业也可以实现去中心化，由此不再需要银行这样的第三方中介结构，依然可以完成保险投保业务等，并且较传统保险业务效率更高、更具安全性。

## 2.去信任

当前，监管部门批准成立一家保险公司的时候，实际上已经为这家保险公司的所有业务贴上了一张基础信任标签。另外，保险公司为自己提升资本金、改善偿付能力，其目的同样也是提升自我信任标签的等级。除此之外，所有的广告宣传以及品牌推广，其最终的目的都是为了能够通过传播的方式来提升在民众中的信任感。由此可见，对于保险业来讲，信任可以说是其发展的核心。

区块链技术可以通过算法、密码、数据校验来确保金融交易的执行。区块链技术应用在保险行业，无论是买方还是卖方，都能够在无需基于诚信体系的背书和保证的基础上放心投保，完成交易。并且，基于区块链技术的使用，保险业的一切秩序的维护都通过算法、密码、代码的方式进行。

## 3.去人化

前边也提到，传统保险业中“人”的作用和影响非常突出，几乎每个环节都离不开“人”的操作，而区块链技术的应用将安全实现无人操作。这是因为基于区块链的智能合约技术，使得在履行保险业务的操作过程中，即便是没有投保人申请理赔，甚至是没有保险公司的批准理赔，只要有相关的理赔条件被触发，那么保单则自动为用户进行理赔，即实现智能理赔，并且在短时间内就完成理赔金额的支付操作。这样一来，大大地缩减了承保周期，而相关的承保产品也能够具备定制化的特点。整个过程中不再涉及任何人为操作，也避免了欺诈的产生。最终产生的结果就是降低了成本和风险，同时也降低了保费，为保险用户带来更加具有创新的革新体验。

乘客乘坐的航班出现延误情况时，就会触发原先通过区块链技术存储的一个智能航班延误险合同，再借助互联网的联通性能，就会使航班延误成为一个公开的记录，通过获取相关公开数据之后，系统就会将该事件判断为需要理赔的时间，从而自动并且及时地支付乘客理赔金。基于这种智能合约技术，使得所有的公开数据都不能随意被篡改，并且能够实现高效理赔，减少了理赔处理所需的成本，同时还提升了客户和保险公司双方的满意度。

在车险方面，主要为了帮助投保人覆盖因发生事故而产生的修车费用。通过区块链技术的存储的条件，当发生汽车事故的时候，通过互联网与汽车相连接，依据存储的条件，判断发生事故缘由之后，智能车险合约就被触发，进而进入理赔阶段。在智能合约里，理赔的修车主修地点也是被事先指定好的，这样可以很好地避开投保人自行选择昂贵的维修厂的可能，可以有效控制理赔费用的支出。

当然，除了航空意外险、车险以外，区块链的智能合约技术同时还可以用于汽车租赁险、旅游险、智能家庭财产险、农作物保险索赔、医疗保险索赔等诸多保险场景中。

总而言之，区块链技术已经成为当前传统保险业发展的转折点技术，未来人工智能时代，区块链技术可以帮助保险业更多地释放行业潜力，让保险业的发展能够“百尺竿头，更进一步”。

## 区块链在资产托管中的应用

当前，尤其是进入2016年以来，区块链凭借其分布式去中心化、不可篡改和加密安全的特点而受到越来越多人的关注，因此，2016年成为区块链技术的元年。正是如此，各行各业对于区块链在本行业中带来的巨大变革寄予了极大的期望，希望通过借助区块链技术加快实现自己企业的智能化步伐。

资产托管业实际上就是委托人接受托管人的资产委托，包括有形资产和无形资产两方面的委托，并对相关资产进行保管和保护。资产托管业务主要的步骤有签订托管合同、开立账户、估值核算、资金清算、投资监督、信息披露、对账等，其流程比较复杂，并在整个托管业务当中认为参与度极高。资产托管业务所面临的主要风险点包括法律风险、操作风险、声誉风险。面对资产托管所面临的诸多风险问题，不得不说，区块链技术的应用确实对资产托管产业链上的组织方式、交易方式、业务流程的变革提供了一项创新的技术支撑。

### 知识拓展

#### 资产托管业务

资产托管业务是指具备一定资格的商业银行作为托管人，依据有关法律法规，与委托人签订委托资产托管合同，安全保管委托投资的资产，并根据资产运作特点提供相应的投资清算、会计核算、资产估值、投资监督、信息披露、对账等金融服务的业务，履行托管人相关职责的业务。资产托管业务分为有形资产托管和无形资产托管两大部分。

有形资产是指那些具有实物形态的资产，包括固定资产和流动资产，如存货、对外投资、货币资产、应收账款等。

无形资产是指企业拥有或者控制的没有实物形态的可辨认非货币性资产，即没有物质实体的资产。无形资产有广义和狭义之分，广义的无形资产包括货币资金、金融资产、长期股权投资，以及那些具有某种法定权利或技术特性的资产，如专利权、商标权等。

银行托管业务的种类有很多，包括证券投资基金托管、委托资产托管、社保基金托管、企业年金托管、信托资产托管、农村社会保障基金托管、基本养老保险个人账户基金托管、补充医疗保险基金托管、收支账户托管、QFII（合格境外机构投资者）托管、贵重物品托管等。

虽然当前并没有明文规定不可以使用区块链技术解决资产托管业务中存在的诸多风险问题，但是，从资产托管业务本身来看，采用区块链技术，为实现资产托管合同上限、依照投资监督指标运行、对托管资产进行控制以及跟踪进行智能合约化，以及估值数据和凭证数据存储以及更新结构化和自动化提供了可能。从这一角度来看，区块链技术在资产托管业务中的应用，必将使得资产托管在安全、效率流程简化的问题上大有改善。

具体来讲，区块链在资产托管应用中的实施步骤如图6-4所示。

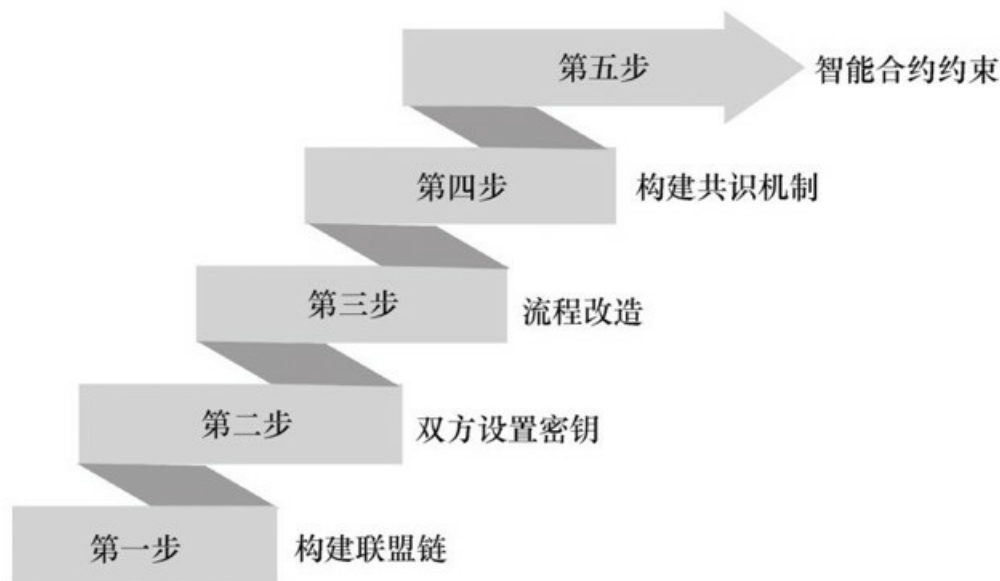


图6-4 区块链在资产托管应用中的实施步骤

#### 第一步，构建联盟链

由于客户类型相对固定的原因，再结合机构协同和业务流程交互的特点，因此在业务运营过程中资产托管客户与资产托管人之间的合作模型应当以联盟链为最佳。基于联盟链，托管行业或者管理人需要共同配合来构建区块链。

以资产证券化为例，纳斯达克交易所通过染色比的技术来实现资产的数字化，在功能分工上，专门设计了用于资产数字化的发行者节点，负责托管资产的发行。与此同时，该联盟链中的资产托管业务区块链中还引入了加密数字货币，可以实现从资产发布、交易、托管、流通到监督的全流程区块链化，最终实现资产和资金的可追溯。

#### 第二步，双方设置密钥

在资产托管业务中，涉及三类人，包括资产管理人、资产托管人、交易所或登记结算公司。基于托管业务，还包括监管信息报送和监管信息的查询两方面的工作，因此区块链节点类型就可以被分为资产管理人节点、资产托管类节点、交易所和登记结算公司节点、监管方节点，所有的这些节点都可以被看作区块链上的参与方。在数据安全问题，每类节点在交易发送过程中需要以接收方节点（即资产托管人）的公钥加密，并需要发送方节点（即资产托管客户）的私钥进行签名。[shu籍 分 享 微 信 whair004]

#### 第三步，流程改造

在进行业务流程改造的过程中，资产托管业务的各个流程中最为复杂的就是对托管产品的估值核算，并且会对托管产品会计科目和科目账进行实时更新。

#### 第四步，构建共识机制

资产托管业务在记账的时候，从业务的连续性考虑，资产托管业务区块链的区块依然产生于资产托管人的节点，但究竟是在哪个资产托管人节点产生区块，还需要依据当前的业务情况来制定和选择算法和共识机制。

#### 第五步，智能合约约束

在使用智能合约的时候，要综合考虑当前区块链技术的发展现状，同时还要考虑资产托管业务区块链的实时效率如何，并且根据业务需要进行区块链的技术改造。使用智能合约可以帮助委托人、管理人、托管人之间的合同或协议可以自动执行，同时还可以使交易和信息披露实现线上化、自动化、智能化。

版权作为一种无形的法定权利资产，当前也在区块链技术方面也具有非常光明的应用前景。2016年8月1日，国家版权交易中心联盟秘书长单位北京国际版权交易中心与北京太一云科技有限公司签署战略合作协议。双方签署合作协议的目的就是为了利用区块链技术来更好地保护著作人的权益。当前，版权问题依然非常严重，如确权难、盗版严重、公开性差等问题。区块链技术本身具有防篡改、不可逆、安全可靠、可信任、去中心化、分布式、公开透明的特点，区块链技术应用用于著作者确权场景中，可以很好地推动版权登记备案工作的进一步发展，将会给版权维护工作带来更具突破性的变革。

总而言之，区块链在资产托管方面的应用，将会给资产托管业务带来更加美好的智能化发展前景，这种基于区块链技术实现的人工智能化是以往任何时候都无法比拟的。

## 区块链在信用借贷中的应用

在金融体系中，对于借贷而言，最为重要的是对借款人的信用进行调查和评估，从而信用贷款业务的安全性，以及信贷企业的能够获利。因此，信用两个字对于借贷而言至关重要。

目前，除了银行借贷以外，诸如P2P借贷、小额贷款企业、提供贷款业务的担保企业、财务公司、金融租赁公司、典当公司、有借贷业务的保险公司，以及专门的贷款公司等如雨后天春笋般层出不穷。尤其是P2P借贷，作为互联网金融的重要组成部分，近年来呈现野蛮式增长。但是由于技术因素、管理能力、法制环境、信用环境等多方面的欠缺问题，P2P借贷的信用风险越来越突出。

显然，征信问题已经成为当前众多信贷机构开展业务重点关注的焦点。通常情况下，在贷款前，相关借贷公司都会预测贷款可能遭受的风险，评价借款人的还款意愿和能力，从而采取有效的防范措施，减少或避免信用风险。借款人的信用评价往往会通过其个人品德（是否诚实可靠）、资本（自有财产状况）、能力（未来按时偿还贷款的能力）、抵押品（审查抵押物的价值和变现的难易程度）、经营环境（是否对变动的环境具有适应性，能够保持经营的稳定性和持续性）、连续性（预测企业产品的生命周期和市场份额，以及企业的市场前景）等方面进行综合评估，如图6-5所示。但是目前，信用贷款业务的开展，主要是考虑借款人的自身债务偿还能力。

对贷款人进行信用调查分析是需要经过一系列的流程才能完成的，这个流程不但工作量大，而且存在信息不完整、数据不准确、使用效率低、易被恶意篡改等诸多问题。

但是，区块链技术在信用贷款业务中的应用，通过将其程序算法自动记录海量信息的方式，并且将它们存储在区块链网络的每一台计算上，使得这些信息更具透明化、公开化，这样就提高了信息的篡改难度，同时还在很大程度上降低了使用成本。各个借贷机构以加密的形式存储并共享客户在本机构的信用状况，这个时候，客户申请贷款就可以不像以往一样再到央行去申请征信查询，即实现了去中心化，借贷机构通过调取区块链的相应数据信息就可以快速完成全部的征信调查分析工作。



图6-5 借款人信用评价

此外，基于区块链的智能资产可以构建无需信用的借贷关系，在区块链上已经注册的数据资产能够通过私人密钥随时使用。借贷机构向借款人借出资金的时候，可以将智能资产作为抵押，再借助智能合约的约束来自动执行可以定位为抵押品的智能资产。当所有的贷款流程结束，即贷款全部还清之后，可以通过智能合约的条件自动解锁，这样就可以很好地化解可能存在的借贷双方之间产生的问题和争议。

2016年9月，微众银行和华瑞银行联合开发了一套区块链应用系统，该系统主要是应用于两家银行微粒贷联合贷款的结算和清算场景当中。微粒贷是微众银行的重点产品，这也是一种面向个人的消费贷款，目前已经获得了超过1000万的客户数量，并且已经发放了1000万笔贷款，发放金额也已经超过了1000亿元，并且目前已经拥有了超过20家的银行合作伙伴。按照传统的习惯，交易和资金的结算要分开进行，且数据信息的记录是通过对手来完成的，因此在各自交易完成之后，双方银行还需要投入大量的人力和物力来对账，从而确保账目的准确性。区块链技术的出现以及在实操中的应用，使得整个流程更加简洁化，将所有信息都记录在区块链网络上，就可以实现信息的透明化和公开化，从而达到无法篡改的目的，同时也保证了交易和清算的高效性。

未来，微众银行的合作银行还可以通过选择将部分信息写入区块链中，由微众银行提供统一标准的链上对账服务，以及统一的操作视图和交互接口，从而帮助合作银行能够更好地、更加高效地了解信贷以及资金交易情况，进行实时监控，很大程度上提升清算和结算效率。

当然，区块链这项技术同样可以应用于企业与企业之间、个人与个人之间的资金拆借



当中，尤其是陌生人之间的借贷方面，可以很好地解决信任问题，使得借贷业务能够更加高效地实现，为借贷双方建立更加友好的借贷环境，能更有效地降低借贷违约风险。

除了以上借贷场景，区块链技术还可以应用于数字企业债券领域。由发行人自主在区块链上注册，如果进行物品抵押或者借助第三方来进行担保，那么相关资产或担保也同样需要通过注册的方式来锁定，债券投资者通过各自端口接入自动发行体系进行认购，当发行人还本付息之后，可以通过智能合约中的条件进行自动解锁，这时候债券债务双方之间的关系就自动解除，这也是一种人工智能化的有效体现。

## 第七章 人工智能时代，金融行业区块链的落地策略



当前，越来越多的权威金融机构研究发现，区块链对金融的颠覆性影响不可低估，甚至可以说区块链将为传统金融开启一扇通往金融2.0模式，即人工智能化金融模式的大门。面对区块链技术的机遇与挑战，国际领先银行已经纷纷采取行动，根据自身特点采取不同应对策略，以此提升企业运营效率和收益。作为对金融业可能带来颠覆性影响的全新技术，区块链已经越来越清晰地出现在了人们面前。

## 各大金融机构争相逐鹿区块链

当前，全球范围内已经有多家金融机构开始逐鹿于区块链。银行作为金融领域中的老牌军，自然在所有行业中是对区块链最为热捧的行业。自从2015年区块链技术崛起，就不断有银行加入到区块链应用的探索行业。如今，区块链技术在银行领域的应用已经遍布全球五大洲，其中包含了全球最顶尖的银行，如美国花旗银行、英国汇丰银行、荷兰央行、摩根大通银行等。截至2016年11月，有60多家银行结成了R3区块链联盟，这又将区块链的应用推向了一个更高的阶段。

区块链技术在各大金融机构的布局策略主要包括3个方面。

### 1.参与区块链联盟，共同开发解决方案，建立行业标准

区块链技术在银行业中的应用当前还依然处于初级阶段。银行在当前一系列发展过程中，面临技术与模式的选择，存在监管合规以及应用模式等多方面的问题。在未来，无论是区块链金融科技公司，还是大型银行，抑或是监管机构，都将对银行业区块链的应用方面，包括应用方向和应用标准，产生极大的影响。其中监管将成为影响区块链技术应用的主导力量。基于这一点考虑，摩根大通银行以及高盛为代表的银行已经组建了以R3 CEV（纽约的区块链创业公司）为代表的全球银行联盟，二者希望通过从监管机构入手，提前参与并建立行业监管以及相应的技术标准，并以此来率先把握整个银行业发展的市场先机。

#### （1）R3 CEV联合全球领先银行，共同制定金融业区块链的应用标准

R3 CEV作为一个区块链创业公司，其主要创建的目的就是基于区块链技术建立符合国家监管要求以及金融业需要的分布式账本系统。2015年9月，R3 CEV与巴克莱、西班牙对外银行、摩根大通银行、澳大利亚联邦银行等9家银行共同成立了R3联盟，并自此开始投入到分布式账本的技术研发和应用探索领域。在同月底，还有13家银行加入该联盟，成为联盟中的意愿，包括美国银行、花旗银行、德意志银行、摩根士丹利银行等全球领先银行。R3联盟的建立被认为是一场区块链技术的革命性创新尝试。

#### （2）Hyperledger构建跨行业区块链联盟，致力于拓展不同行业的区块链应用

超级账本Hyperledger是Linux基金会于2015年发起的推进区块链技术和交易验证的开源项目，目前已经得到了30家大型公司的支持，包括思科、摩根大通银行、英特尔、富国银行、伦敦证券交易所、IBM、区块链公司DAH、R3、荷兰银行、埃森哲、芝加哥交易所集团等，成员分布比较广泛，这也正体现了金融与技术的多样性特点。正如Hyperledger官方网站所描述的那样，这一项目的目标就是发展一个跨行业的开放式标准以及开源代码开发库，允许企业创建自定义的分布式账本解决方案，以促进区块链技术在商业当中的应用。全球各大顶级金融机构给予的支持也体现了金融、技术机构对此次项目的认可。2015年12月计划成立该项目以来，超级账本项目已经收到来自多个企业的代码和技术，其中包括Blockstream、DAH、IBM、Ripple等，其他社区成员也在考虑如何最大限度地贡献自己的力量。Hyperledger项目是让成员共同合作，专注于开放的平台，以便满足将来不同行业各种用户的需求，简化业务流程。

#### （3）中国的China Ledger与国内11家商品交易所共同研发区块链技术在中国金融业中的应用

China Ledger（中国分布式总账基础协议联盟）2016年4月在万象区块链实验室的带领下成立，是由11个区域的商品交易所、产权交易所、金融资产交易所组成，并且由中国证监会所属的中国证券业协会互联网证券委员会担任项目顾问。China Ledger联盟的主要职责就是所有成员共同合作研究区块链技术，以中国当前的政策法规以及金融业独特的业务逻辑为依据，开发更加符合中国当前的政策、国家标准、业务逻辑、使用习惯的区块

链技术底层协议。

## 2.解决银行业务中的痛点

银行业务中使用区块链技术的目的就是为了解决当前核心业务的痛点。基于这一点，许多国际领先银行通过与金融科技公司建立合作关系，发展更多应用于银行核心业务的新技术。根据参与程度的高低，可以将银行与金融科技公司合作的模式分为多种类型，包括单纯参与项目合作、投入资金成为战略投资者、直接与科技公司合作成立合资公司等。不管是哪种类型，银行应用区块链技术的宗旨是不会改变的，即希望借助金融科技公司的技术，更加快速开发区块链技术的应用，从而更好地解决当前存在的业务痛点。

### (1) Visa与Chain为提升信用卡交易效率联手合作

就当前的实际情况来看，Visa在每秒钟内能够完成的交易笔数为65000，但是在与Chain研发的区块链技术相结合后，能将该数字提升两倍之多。区块链技术凭借其不可篡改的特点也能够很大程度上提升信用卡交易的安全性。Visa与Chain的合作，能够在未来的信用卡交易过程中更好地惠及更多的客户。

### (2) 星展、渣打银行共同与Ripple合作开发金融业务数字化应用

2015年，星展和渣打银行与世界上第一个开放的支付网络Ripple建立合作关系，并将区块链技术应用用于供应链金融业务，通过智能合约以及点到点跨境支付技术，使得业务流程实现自动化、智能化。与此同时，基于区块链技术的公开性、不可篡改性，使得供应链金融数字化流程应用更加趋于安全，可以大幅提升贸易交易的可能性，减少欺诈案件的发生，为银行节省数百万美元的风险损失。目前，这一策略正处于应用的尝试阶段。

### 3.成立区块链实验室，主动针对不同业务应用场景进行技术开发

当前诸多国际领先银行已经开始纷纷成立区块链实验室，希望通过该实验室来探索和预见区块链技术未来的应用场景。各金融机构除了在同业中建立联盟、与金融科技公司共同开发应用领域之外，还有许多金融机构成立了属于自己的区块链实验室，通过培养和收纳人才来成立属于自己的技术团队，从而快速进入实验性研究阶段。当前，UBS、花旗银行、德意志银行已经成立了自己的区块链实验室，针对不同的业务场景进行更加深入区块链技术应用的探索。

#### (1) UBS成立区块链实验室，致力于发展债券发行以及清算技术

2015年，UBS在伦敦成立了自己的区块链技术实验室，该实验室成立的目的是针对区块链应用于各种金融交易过程中的债券发行和清算，以便更好地提升交易速度和降低交易成本，提升运营效率。

#### (2) 花旗银行建立区块链实验室，以此来测试区块链在跨境支付方面的应用

作为全球银行来讲，花旗银行已经在创建区块链实验室方面成为了资深银行，聚焦于跨境支付领域的应用。在支付领域，花旗银行与电信运营商Safaricom达成合作，通过区块链技术实现手机点对点支付。

由此可见，不管各大金融机构在区块链领域如何布局，区块链为各个金融机构所带来的挑战已经激发了其他心动但未采取行动的银行的创新意识，这对于整个金融体系来讲都是一个极好的提升，对于推进金融领域快速进入人工智能化时代也具有重要的引导意义。

## IBM与中国银联探索区块链技术落地应用

2016年，金融行业谈论最多的就是区块链技术，去信任、去中心化的区块链如何在金融领域落地也成为重要的话题。目前，在互联网金融企业和银行之间相继爆出尝新硕果，“制造信任的机器”正在一步步打开未来世界的大门。

银行本身就是金融领域中的核心机构，信任机制是银行进行各种交易的核心保障，区块链技术伴随着比特币的出现而出现，比特币的底层技术区块链一直受到银行的关注，因此，应用区块链技术的各金融机构中，银行业首当其冲。

众所周知，当前，银行为了吸引客户以及维护客户的忠诚度，往往是采用银行卡购物获得积分的方式来实现的。从理论上讲，这种方式的确是一种行之有效的营销手段，网上的积分兑换商城中各种商品琳琅满目，客户只需将自己平时消费积攒的积分拿出来兑换即可。这种方式是获得客户青睐和一直保持使用特定银行卡的重要原因。但是，这种兑换方式存在一定的弊端，一方面，很多用户甚至不知道银行积分兑换业务的存在，另一方面积分奖励不能实现跨行兑换。对于如何让用户知道银行积分兑换业务的存在，其解决办法很简单，只要通过各种宣传就可以达到预期目的。但是实现跨行兑换则是一件比较棘手的事情。在这一点上，积分政策已经对兑换商品的权限进行了限制。这样又会导致许多客户获得的奖励积分不能很好地被利用起来，即便是客户知道银行卡积分可以用来兑换相关商品，但是又因为不能跨行兑换到自己最喜欢是商品而感到失落，势必给客户带来不佳的服务体验感。

如何设计出一个块金融机构的交换平台呢？使用传统技术来实现银行奖励积分系统的整合和共享会是一个非常严峻的挑战，因为系统和系统之间是存在一定的阻滞的，网络和网络之间是不可以连接的，而且作为一个中心化平台对接众多银行，做积分清算和结算显然是比较困难的。

针对这一问题，在2013年9月23日上海举办的区块链国际周上，IBM与中国银联电子支付研究院在区块链国际周活动上共同预演了如何通过使用区块链技术来完成跨行共享奖励积分的演示。通过演示，告诉消费者，只需要简单的几个步骤就可以非常轻松、快捷地完成操作，就可以实现跨行积分兑换，成功获得自己喜欢的礼品。

调查数据显示：“90%的用户不知道自己银行卡里有积分。”2015年的调查数据显示：“中国银行业银行积分卡价值超过400亿元人民币，但只有不到50%的积分最后被兑换。”如果银行能够投入积分的市场为400亿元人民币，假设其中5%的流量通过区块链技术构建跨金融机构来实现商品兑换，以从中赚取1%的手续费来算，那么这个区块链搭建的金融机构平台每年将可以赚上1亿元。

如果利用传统技术来实现银行积分奖励与商品兑换的整合和完善，那么这必然是一件极具挑战性的任务，并且会带来极高的成本。为了能够使这一问题得到很好的解决，同时为了银行客户能够获得更多的实惠，IBM中国研究院和中国银联电子支付研究院使用超级账本Hyperledger在IBM区块链上创建了一个全新的业务创新平台，打造出了一个激励积分交换的许可网络。

此次IBM与中国银联电子支付研究院的合作，不但解决了跨行积分兑换难的问题，同时还使用区块链技术将线上和线下渠道整合起来，这样，以后中国银联卡的所有持有人都可以去任意一家配备智能POS机的超市或者商场，轻松扫描一下，就可以快速完成奖励积分兑换商品的操作。未来，这种奖励积分跨区域兑换还将在其他领域中得到广泛应用和普及，如航班里程、手机话费、加油卡、餐饮等行业也可以实现跨店、跨区域参与自由兑换

和交换。[shu籍 分 享 微 信 whair004

当前，基于区块链技术的去信任特点，使得应用区块链技术的金融场景中的交易也更具信任。这将与其他使用区块链技术的类似创新一起，共同改变金融业的未来发展前景。为此，IBM中国研究院战略与业务拓展总监朱珉称：“区块链的平台是一个开放式的平台。一方面，积分的拥有者可以决定是否加入，何时加入。另一方面，银行作为积分发放者，也可以决定是否加入，何时加入。这个平台上的生态、环境应该被看成一种服务，相信有很多的积分发放者会主动参与到这个网络中，成为其中非常积极的一环，当我们把积分连通到全社会时，将有无限的业务创新可能，这就是区块链的含义。”

作为其下属的研究机构，中国银联电子支付研究院负责调研评估支付市场创新的前沿技术和模式，对支付产业发展趋势的核心技术和模型进行研究论证，以及对影响支付行业的前瞻性和基础性技术进行预演和分析。目前，银联电子支付研究院正在全面推动区块链、智能终端、大数据、可信执行环境等多项新技术在金融支付领域中的运用，以期加快进入人工智能时代。

目前，IBM正在迅速改善其自身的区块链咨询服务和能力，并积极与客户合作，探索和尝试如何能够将区块链技术用于更多的企业现实业务操作过程当中，堪称是一次创新的里程碑。基于这些探索和创新性尝试，我们看到IBM正在全面推动区块链技术的发展，从而使区块链的应用能够渗透到金融以外的其他领域，使得无限的业务创新成为可能，还将改变除金融以外的其他领域的未来。



## 商业银行对区块链技术发展的应对策略

2015年下半年以来，区块链技术迅速走红，成为全球市场中继互联网之后的又一新热点。进入2016年，区块链技术更是异常火热，诸多领域开始进入探索区块链技术应用的元年。可以说，区块链技术是一种还处于初级测试和探索阶段就能够获得各界科技大佬竞相关注和追捧的创新性技术，是一种被誉为人工智能时代将会颠覆传统金融模式的网络技术。

从本质上来看，区块链是一种交易协议，实际上就像是我们登录网站、收发邮件所遵循的网络协议一样，也是一种信息交互的协议，不同的是，区块链所交互的是资金变更的价值信息。区块链技术将给各个领域，尤其金融领域带来重大的颠覆性变革，将会改变以商业为代表的中心化的传统金融模式。

区块链对金融领域的影响

区块链技术将会给金融领域带来以下几个方面的影响，如图7-1所示。

### 1. 改变支付体系和架构

（1）区块链技术可以改变支付结算的底层基础设施和清算方式。假如通过央行建立区块链联盟，那么商业银行就可以借助区块链技术实现点对点支付，这样就可以很好地绕开当前的支付中心。

（2）清算组织的功能可能面临一定的挑战。在未来，商业银行极有可能会通过区块链技术实现点对点支付，这样清算组织的功能和存在的价值将会大打折扣。尤其是在跨境支付和清算领域，通过区块链技术可以省去那些没有必要的代理行环节，从而更好地进行点对点的对接，从而在很大程度上降低业务成本，同时还可以更好地提升支付和清算效率。

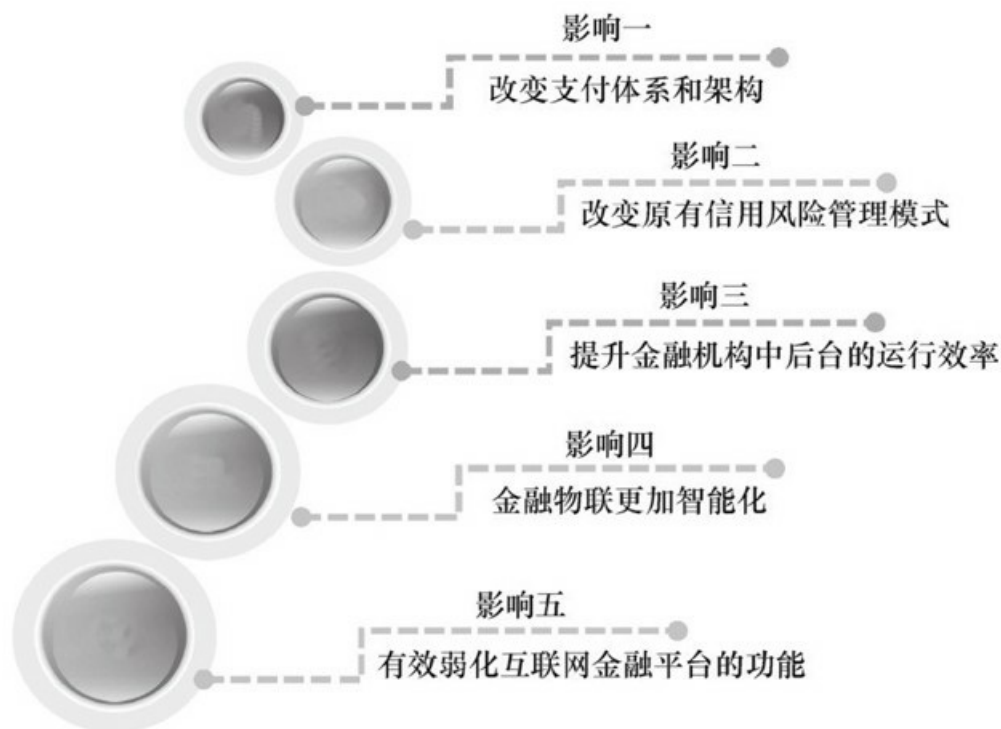


图7-1 区块链对金融领域的影响

(3) 大型区块链支付企业将会出现，这将改变现有的支付市场格局。大型的区块链支付企业可以给商业银行支付业务提供更加适合的基础设施支持服务，从而与现有的清算组织形成竞争关系，改变现有的支付市场格局。

银行最主要的职能之一就是完成支付业务。而区块链技术对于银行的支付体系和支付职能具有非常深远的影响。银行业在应用区块链技术之后，不但可以提升支付效率，降低业务成本，还可以对现有的体系和系统做出一个较大的调整，进而从更广、更深层次上涉及并改变的银行业务。

## 2.改变原有信用风险管理模式

区块链技术的不断发展，使得更多与征信相关的个人和企业的金融交易数据、商业交易数据等可以直接部署在区块链上。商业银行可以借助区块链技术完成征信工作，这样不但可以改变现有模式下信息的不完整性和数据的及时性，还可以使得运营成本大幅降低。

## 3.提升金融机构中后台的运行效率

(1) 区块链技术为中后台部门效率的提升提供了非常好的工具。

(2) 区块链技术可以有效缩短系统开发的周期，降低开发成本和运维成本。

## 4.金融物联更加智能化

区块链在金融领域中的应用和存在的价值在于，可以通过大量的智能设备之间建立低成本的相互直接沟通的桥梁，并且可以用去中心化的共识机制去提高系统的安全性和私密性。

## 5.有效弱化互联网金融平台的功能

区块链技术是一种去信任化、去中心化的机制，因此，区块链在金融领域中的应用势必会在一定程度上动摇第三方支付根基，从而使得第三支付的资金监管职能被区块链的智能合约所取代，从而实现合约的自动执行。也正是基于这些原因，使得作为互联网金融机构的第三方支付逐渐被边缘化，其功能也逐渐被弱化。

商业银行应当采取的应对策略

在区块链技术对金融领域的以上几个方面的影响下，各商业银行应当沉着应对，具体应当采取以下几个应对策略，如图7-2所示。

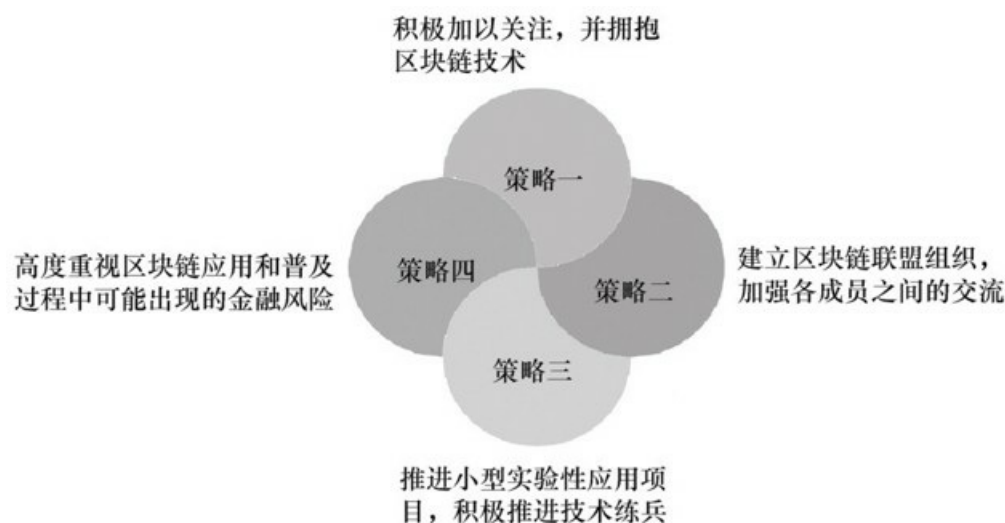


图7-2 商业银行应当采取的应对策略

## 1.积极加以关注，并拥抱区块链技术

当前区块链技术在金融领域中的应用处于初级的探索和研究阶段，这时候，商业银行可以包容的心态去接纳、研究、运用区块链技术，并且尽早占领技术积累和人才储备的战

略高地，成立专业团队去跟随当前趋势，推进区块链技术应用的探索，新技术的迅猛发展必将给商业银行的发展带来颠覆性变革。

我国各大银行等金融机构开始陆续拥抱区块链技术。2016年5月，平安银行成为首个中国成员加入到了R3联盟当中。2016年6月，香港友邦成功加入R3联盟。2016年9月，分别有中国外汇交易中心和招商银行正式加入R3联盟，成为我国区块链R3联盟的第三四位中国成员。2016年11月民生银行宣布正式加入R3区块链联盟。

## 2.建立区块链联盟组织，加强各成员之间的交流

当前，在国际上的重要区块链联盟组织主要就是R3 CEV，当前已经有60多家金融机构加入到该联盟当中，这些金融机构都是时下国际上最主要的商业银行成员，我国也有三家银行已经在2016年先后加入到了该联盟当中，成为其中的一员。因此，商业银行需要积极建立区块链联盟组织，加强各成员之间对于区块链技术应用的交流，并参与到国际银行、金融机构对区块链技术标准的制定和运用的计划当中。

R3于2015年9月成立了R3区块链联盟并积极发展Corda；全球区块链联盟委员会于2015年11月在迪拜成立；Liunx基金会则在2015年12月开始构建超分权而治的货币支持协议Hyper Ledger；日本于2016年4月成立了区块链联盟（BCCC）。中国的金融机构和金融技术公司当然也不甘落后。2016年5月31日，金融区块链合作联盟（深圳）成立大会在深圳五洲宾馆正式召开，标志着中国金融区块链合作深圳联盟的正式成立。

## 3.推进小型实验性应用项目，积极推进技术练兵

目前，相对于互联网金融企业以及其他金融机构对于区块链技术的高度重视，我国商业银行尤其是那些国有大型商业银行，还没有在产品和服务等金融创新领域中占有领导地位和领先优势。因此，应当创建相关实验室，推进小型实验性应用项目，积极推进技术练兵。

澳洲联邦银行对区块链技术的应用非常感兴趣，因此在很早就已经加入了R3 CEV区块链联盟，在悉尼创建了属于自己的实验室进行区块链技术应用方面的探索和研究，还举办过若干个全球性的区块链技术研讨会。2016年1月，澳洲联邦银行在香港又成立了一家实验室，充分看到了香港背靠中国大陆地区的有利位置的优势，并将希望能够把未来的创新重点放在区块链这样的互联网金融科技方面，显然，澳洲联邦银行的这一举措向我们证明，其在未来区块链技术于全球金融领域中的应用有着巨大的图谋。

## 4.高度重视区块链应用和普及过程中可能出现的金融风险

在区块链金融模式下，大量点对点的交易频繁进行的同时，必然会带来海量的网状数据信息，这时候，商业银行就需要改变传统的风险管控模式，在风险监管制度、数据处理水平、风险监控等方面做出及时调整，这样才能更好地控制区块链在应用和普及过程中可能会出现金融风险，从而降低资金损失。

截至2016年11月，全球10家来自R3区块链联盟的银行成员（包括西班牙对外银行、加拿大帝国商业银行、ING集团、意大利联合圣保罗银行、法国外贸银行、北欧联合银行、北美信托公司、法国兴业银行、瑞银、美国银行），成功进行了一个基于分布式账簿KYC（了解你的客户）登记系统的测试。在KYC系统中收集了大量企业和个人的身份信息，提供第三方身份认证服务。通过该系统可以有效防止现代银行发

生欺诈、腐败和洗钱行为。因此，基于KYC系统，商业银行等金融机构可以通过区块链共享交易各方的信息，将减少大量重复性工作，也为各家机构节省了大量的合规成本，同时还为商业银行在内的其他金融机构挖掘潜在的商业机会，以及有效识别金融风险，为金融机构的良性发展提供了很大的帮助。

## 第八章 人工智能时代，金融业扛旗者走在区块链金融最前端



从2015年9月9日~11日在大连举办的达沃斯论坛，到2016年17日~18日在上海举办的朗迪中国峰会，无疑，区块链技术俨然成为嘉宾分享、媒体报道的热点之一。事实上，从2015年下半年开始，各投资机构、传统金融机构、互联网金融机构以及互联网企业已经开始蠢蠢欲动，在区块链上投入大量的人力、物力。这一切都表明，金融资本永远走在行业的最前端，俨然成为了行业的扛旗者，它们将加速推进金融业向人工智能时代迈进的步伐。

## 银行系：从担忧到拥抱

2016年，金融领域谈论最多的无疑是金融科技这一热门词汇。一般情况下，人们认为金融科技可以分为3个部分：大数据挖掘、智能投顾和区块链应用。

大数据挖掘的意义和价值是众人认可的，因此，已经在各个领域中被广泛使用。尤其是金融领域，大数据挖掘已经被广泛应用到企业和个人征信以及风险控制领域，产生了“看得见、摸不着”的收益，因此，包括银行在内的各大银行机构纷纷跟进，或为之慷慨解囊，将大数据进行共享。

智能投顾在理论上看似是一个“万能科技”，适用于一切资产配置相关的领域，包括银行资管、金融市场、私人银行等诸多业务，但是国内任何投资的资产标的暂时数量有限，即便是那些券商都裹足不前，这样银行对于这一科技的应用保有观望态度也是情理之中的事情。

区块链是一项最耐人寻味的技术，虽然已经在诸多领域中获得了不少突破性进展，全球大银行也都在区块链方面进行全方位布局，但是在我国国内不少大型银行依然对该技术的出现和应用表示担忧，反而那些少数的中小银行（平安银行、微众银行等）却冲在了创新发展的最前端。

2016年上半年，互联网高科技领域中除了AR和VR之外，谈论最多、最炙手可热的另外一个新风口就是区块链技术。2015年，区块链成为美国创投中获得融资最高的板块，融资金额超过了10亿美元，诸如高盛集团、花旗银行、纳斯达克等都纷纷布局区块链，就连国内的三大巨头BAT也都纷纷试水。但是，值得一提的是，所有投资机构中，投资金额最多的却是传统银行，如花旗银行、摩根大通银行等银行巨头。

早在2004年金融科技正式进入金融领域以来，用户的理财和支付习惯已经彻底发生了改变，银行对于支付宝的出现以及造成客户的流失瞬间措手不及。之后，金融科技（Fin Tech）的兴起，又使得银行遭受到了暴击。在经过大数据挖掘、智能投顾的侵袭之后，银行还没有喘过气来，紧接着区块链的出现又让他们顿感惊慌，因为区块链技术作为一种分布式记账技术，基于其本身具有的不可篡改的特点，很好地解决了金融圈所面临的两个最大的难题：降低价值交换成本和降低信用成本。这样以往传统银行之间存在的清算复杂、数据存储复杂、跨境支付成本高昂等问题都能得到很好的解决。

但是即便如此，银行系还是心存担忧，并且未能将“心动”转化为行动，具体来讲，银行系所担忧的问题表现在以下几个方面，如图8-1所示。





图8-1 银行系担忧的问题

### 1.担心走错路

某银行的前行长曾经对于区块链的应用讲过一番颇具代表性的话：“我们对区块链的认识，与没有可能像前几年对互联网金融一样，再次陷入一种片面的误区，从而在发展的过程中，增加更多的、无谓的试错成本？”确实如此，对于任何新生事物，谁也不敢非常肯定地说只要投入就一定会有产出。但有一点是可以肯定的，如果不投入，就肯定不会有产出。

### 2.担心技术难

很多时候，银行过于强调技术的独立创新研发，但是结果却不尽如人意，开发出来的新技术往往不能与外部区块链技术公司之间展开合作。这也就意味着，需要在区块链技术相对成熟以及相关人才储备充足的情况下才能实现完美的独立研发。现实与理想之间往往存在很大的落差，也正是因为这一点，那些大型银行在迈向区块链应用的时候才显得畏手畏脚。

### 3.担心与政策、监管不同步

在区块链技术进入大众视野的初期，很多行业已经对区块链的应用优势表示极大的关注，但是在其应用前景不是非常明朗的情况下，国家对于区块链技术的应用和监管情况还不能给出明确的态度，这个时候对于银行系来讲，将区块链技术应用自身发展过程中是否会得到国家政策和监管的支持和允许还是模棱两可的。因此，在没有明确政策和监管信号的前提下，银行系还是会选择保守的犹豫和观望态度。

这也正是我国那些大型银行对自己未来前景所担忧的。事实上，无论国内还是国外的那些大型银行在区块链领域试水的初期都是心存担忧的，毕竟一项新技术的应用是需要进行更多的探索和研究、实验才能一步步取得成功的。

然而，在众多小型银行初步试水并取得一定成效的时候，全球银行逐渐从担忧转变观念，进而开始积极拥抱区块链技术，并寻找各种应对策略，像前文中讲到的：一方面，R3 CEV与巴克莱、西班牙对外银行、摩根大通银行、澳大利亚联邦银行等9家银行共同成立全球知名的金融区块链联盟R3，同时吸引了平安银行、招商银行、民生银行、花旗银行、美国银行、德意志银行、摩根士丹利银行等在内的60多家银行加入其中，也就是说，从内部发起革命；另一方面，积极落实研究试点、频频投资区块链创业公司，像CBW银行、纽约梅隆银行、巴莱克银行、瑞士联合银行、桑坦德银行、星展银行、西班牙对外银

行等，也就是说，从外部布置救兵。

**CBW银行：**堪萨斯州的CBW银行是一家有着一百多年历史的小型社区银行，该银行已经与数字货币公司Ripple Labs共同达成合作关系，并推出了实时支付系统ONE Card。拥有这样技术之后，CBW银行在同行业中更具竞争优势，可以更加快捷地实现实时结算，从而使得客户可以及时取回资金，为客户提供了非常满意的服务体验。

**巴克莱银行：**英国第二大银行巴克莱银行，在实施一个为期3个月的导师计划——“巴克莱加速器”之后，已经选出了三个区块链相关的初创公司，分别为Safello、Atlas Card、Blocktrace，之后这三家区块链初创公司纷纷加入巴克莱银行的金融科技孵化器中。在2016年6月，巴克莱银行与比特币交易所Safello共同达成协议，将在区块链技术如何加强金融服务业务方面进行更加深入的探索和研究。

事实上，银行系无论是从内部发起革命还是从外部布置救兵，都能够很好地说明它们已经逐渐开始从原来的担忧转向了对区块链的接受和拥抱，因为它们深谙生存之道：“与其被创新技术革命，不如提前自我革命。”

## 传统IT和新兴互联网企业：积极拥抱区块链

当前，区块链技术已经深入人心，也深刻影响着与生活息息相关的方方面面，尤其是在金融领域，区块链引无数银行竞折腰，就连国内三大互联网巨头BAT企业也对区块链技术的应用高度关注。作为我国大型企业中的领路人，阿里巴巴、百度、腾讯也以不一样的方式拥抱区块链，并根据自身独有的优势，全面吹响了布局区块链的集结号，争相在区块链应用方面拔得头筹。

在我国互联网的发展中，与最具重要推动作用的互联网三大巨头的支持和帮助是密不可分的。然而，在当前区块链技术进入热潮期的时候，BAT企业这三驾马车依然并驾齐驱地朝着区块链技术的创新性应用方向努力。虽然他们没有参与区块链的投资和产品研发，但是依然能够通过积极拥抱区块链，从而擦出不一样的“火花”，如图8-2所示。

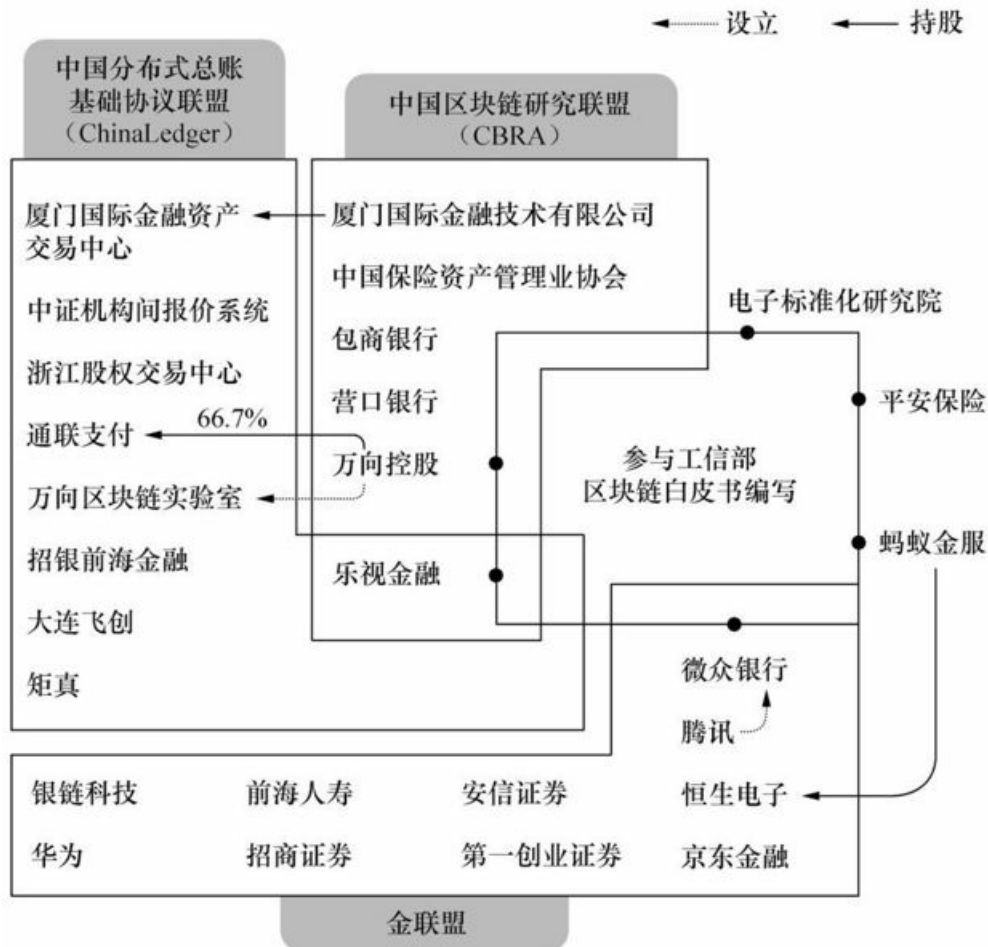


图8-2 传统IT和新兴互联网企业积极拥抱区块链

### 腾讯加入金融区块链联盟

区块链技术已然被越来越多的企业所关注，腾讯也不甘落后，积极参与区块链竞争。在2015年5月举办的贵阳大数据博览会上，马化腾曾强调“互联网+”也是一种连接的能力。那么作为“互联网+”时代连接器的区块链，腾讯自然也不会缺席。

因此，腾讯牵头发起并设立了微众银行，以期在探索区块链方面展开实践活动。2016年5月，微众银行在中国深圳参与并发起了中国三大区块链金融联盟中的金融区块链合作联盟，共集结了包括微众银行、平安银行、招银网络、恒生电子、银链科技、深圳市金融信息服务协会等在内的31家企业，其中发起单位有25家，此次参与联盟成员的还有华为、京东金融等几个大佬，会员中有70%是金融机构，30%是金融科技企业和互联网企业；6月又推出了基于腾讯云的联盟链云服务；9月底，在上海区块链国际周期间又与万向集团达成了合作协议。腾讯的这一连串举动充分表明，腾讯已经开始在默默布局区块链，如图8-3所示。



\* 注：图中所示联盟机构未包含联盟全体成员

图8-3 中国区块链三大联盟的参与机构

图片来源：http://it.sohu.com/20161117/n473445767.shtml

提到腾讯与互联网金融的渊源，不得不从2005年说起。2005年9月，财付通的成立标志着腾讯正式进军金融领域，到目前为止，腾讯作为互联网金融企业已经有十多年了。以往腾讯对于金融业的战略定位是“抢占渠道、流量入口，以合作的方式做大渠道好入口”。不得不说，这种打法是非常有利于充分发挥其传统资源优势的，但是缺点就是缺乏一以贯之的产品开发和真正的市场占有率。随着时间的一步步推移，腾讯金融的“全牌照”布局逐步实现，在建成金融生态闭环之后，腾讯金融又开始进行自身数据资源的挖掘以及应用场景的搭建工作。在互联网金融领域，腾讯布局的业务可以分为九大板块，分别为支付、贷款、理财、保险、证券、银行、基金、众筹、征信。

至于2016年腾讯开始加入金融区块链联盟的举措，是为了借区块链这条纽带，让与其相关的业务板块能够与区块链技术相结合，从而能够将其优势发挥得更好。

蚂蚁金服区块链技术与公益结合

在2016年7月9~10日举办的首届全球XIN公益大会上，阿里巴巴旗下的蚂蚁金服表示：“区块链技术即将上线，并会首先应用于支付宝的爱心捐赠平台。”这表明阿里巴巴将会把区块链技术应用用于公益事业。[shu籍 分 享 微 信 whair004]

基于区块链技术本身具有去信任、去中心化的特点，因此区块链可以应用于公益事业，从而保证公益的透明度和信任度。由于支付宝的爱心捐赠平台上，经常会出现几元到

几十元到上百元的捐助善款，因此当捐款进入公益账户中时，往往无法做到对款项的身份追踪。而蚂蚁金服推出的这一举措让每一笔款项的生命周期都能够很好地记录在区块链上，并且可以实现持续追溯，这样可以在未来对于慈善捐赠资金的走向和用户有更深入的了解。更重要的是能够在很大程度上提升服务效率、风险管控效率，让公益事业做得更好。

#### 百度战略投资Circle百度金融或成重心

百度作为一家依托中文搜索引擎起家的互联网企业，目前拥有着强大的入口和平台优势，并且具有举足轻重的科研能力，同时具有大数据、人工智能等国际先进的技术，并希望通过借助这些技术而更好地改变现在金融的整个流程和生产方式。

2016年6月22日，Circle在宣布获得由中国财团提供的6000万美元D轮投资的时候，其中的领投方式IDG，而跟投方就是百度以及其他机构，如中金甲子、光大投资管理公司、万向集团等众多行业巨头。本轮投资已经是Circle获得的第五轮投资。而Circle公司本身就是一家全球区块链技术公司，基于区块链技术做支付，尤其是社交支付对下一代互联网支付具有非常重要的意义。Circle通过借助区块链技术来快速进化支付方式，进而带动整个金融体系的变革，因此可以说Circle是基于区块链技术的支付应用，是一种面向未来金融形态的变革性支付方式。由此，我们对于百度作为跟投方的实际目的和意图就有了更加明确的了解。

百度之所以进行跟投，其原因就在于希望其旗下的支付工具百度钱包能够将区块链技术进一步延伸到百度生态体系内的各个应用场景中，这样就能够在未来的支付升级过程中进一步带动其整个生态体系的进一步提升。

虽然目前Circle进入中国尚需时日，百度未来的发展前景也有待静观，但是，百度的这一举动已经向我们表明心迹，同时也表达了百度对于布局区块链的决心。

## 专项投资机构：翘首以盼

2016年8月3日，在深圳前海深港青年梦工场举办的“2016世界青年创业论坛—区块链联盟分论坛”及“前海国际区块链生态联盟启动仪式”上，毫无疑问，区块链成为了一大亮点。“前海国际区块链生态联盟”的成立，代表了前海把区块链技术作为金融创新的战略高地来重点打造。在会上，各方专家对区块链未来的发展前景进行展望，“前海国际区块链生态联盟”的发起方深圳前海管理局也高瞻远瞩，支持区块链领域的中外著名金融机构、高科技公司、投资机构和孵化器等在区块链领域的投资和创新合作，进而引领打造“一带一路区块链”。

各国对于专项投资机构在区块链方面的资金投入是非常支持的，因为区块链技术形成的分布式结构，可以让用户更好地获取信息、参与交易和监督，这其中蕴含着无限商机。也正是基于此，越来越多的专项投资机构愿意花重金在区块链领域进行投资。

香港中文大学EMBA教授劳维信提供的数据信息显示：“在全球范围内，2009—2013年，投入到区块链初创项目的资金约为9300万美元；2014年至今，投到该领域初创项目的资金约为9.93亿美元，是此前的10倍左右。其中91%的资金是在2014年后投入的，60%的资金是在2015年后投入的。截至2016年9月，数字货币及公共区块链生态系统已经汇聚了17.9亿美元的投资。目前，美国已有800多家从事区块链相关领域的公司，在中国也有100到200家，平安银行已率先布局。”

资料来源：

<http://news.eastday.com/eastday/13news/auto/news/china/20160804/u7ai5899321.html>

短时间内就获得了如此惊人的投资金额，可见区块链技术在各个专项投资机构心中的价值是不可言喻的，同时也表现出专项投资机构对于区块链在未来的发展前景也是非常看好的，更希望能够通过在区块链这方面的投资而获得更高利润的价值回报。区块链技术为何能获得专项投资机构如此多的青睐呢？主要原因有以下几个方面，如图8-4所示。





图8-4 区块链技术获得专项投资机构青睐的原因

#### 1.财务交易不再中心化

区块链技术实际上是在科学领域中出现的一次根本性变革，从本质上看，推动了以比特币为代表的各类加密货币的发展。基于区块链技术，每项交易都是公开、透明的，这样世界上任何两个地方的人都可以完成资金支付，实际上与互联网的互联互通是类似的，不同的地方在于基于区块链的资金交易是没有中心化的概念的，彻底颠覆了互联网条件下原有的跨境支付的模式。

#### 2.小微企业不再需要银行

区块链技术可以说是对金融基础设施进行了一次颠覆性变革。从传统意义上讲，大型银行在美国垄断了金融交易，这对于那些小微企业来讲，在未来的求生道路上越来越艰难。而在我国，最早的金融机构是被传统银行所垄断的，互联网出现以后，支付宝、微信支付等异军突起，银行在金融领域中的主导地位逐渐开始趋于淡化。

#### 3.使用区块链进行跨境支付

区块链在跨境支付场景中的应用在前文中也详细阐述过。随着互联网技术的不断发展，一个个无障碍技术平台逐渐从本地市场向国外扩张，进而使其规模扩张呈现全球性特点。这样最终带来的结果就是，电子商务随之逐渐兴起，以阿里巴巴的支付宝和美国知名支付工具e Bay尤为突出。随着商业走向全球，区块链技术在跨境支付场景中的应用前景和机会也将增加更多。

#### 4.开发人员和投资人员正在投入区块链技术

区块链技术本身在聚集各类开发人员、技术人员的同时，也需要各种风险投资，从而保证区块链技术在其他领域中的应用能够更具安全性。

这些原因，带来了基于区块链技术的创业黄金时代。区块链技术也在登记、确权、智能管理等方面的应用进入探索阶段，从而吸引了越来越多的专项投资机构争相下赌注。

成立于1969年，从一个生产农业机械的小作坊起家的民营企业万向控股集团，是中国第一个为美国通用汽车公司提供零部件的OEM厂商（原始设备制造商），也是最早收购美国公司的中国民营企业之一。2016年7月31日上海举办的第六届上海新金融年会暨第三届互联网金融外滩峰会上，万向控股集团成立了一个5000万美元的VC基金专门用于投资区块链企业或项目。

这已经不是万向控股集团在区块链初创公司的第一次投资。万向控股集团其实在很早的时候就已经关注区块链技术的应用，并且是中国最早开始关注和布局区块链技术的大型企业之一。2015年9月，万向控股成立了区块链实验室，为了进一步推动区块链技术的发展，万向区块链实验室在2015年11月推出了每年约30万美元的名为“Block Grant X”的全球优秀区块链项目资助计划，并以此支持加密算法、共识机制、交易性能改进等区块链技术的基础性研究。截至2016年9月，万向控股集团已经在全球范围内向29家区块链初创公司进行了投资，投资规模高达2500万美元资金，如表8-1所示。

表8-1 全球知名区块链初创企业融资情况

企业	业务	时间	轮数	融资金额（美元）	本轮投资方
DAH	区块链初创公司	1月	A轮	6000万	高盛集团、IBM、荷兰银行、花旗银行
Gem	应用程序接口	1月	A轮	710万	Pelion创投、KEC Ventures等
Symbiont	智能证券交易平台	1月	A轮	700万	未透露
Blockstream	侧链	2月	A轮	5500万	安盛集团、Bigital Garage等
BitFlyer	比特币交易	4月	C轮	2700万	Venture Labo Investment、SBI投资
Bitfury	比特币挖掘	5月	D轮	3000万	中国信贷
Colu	虚拟货币	6月	A轮	960万	Spark Capital、Aleph、Digital Currency Group
MediaChain	元数据协议	6月	种子轮	150万	RRE Ventures、A16Z、USV
Circle	金融服务	6月	D轮	6000万	IDG、CICC Alpha等
MediaChain	数字版权保护	6月	天使轮	150万	Andreessen Horowitz、Union Square Ventures等
Quoine	加密货币相关业务	6月	B轮	2000万	未透露
Coinify	区块链交易公司	8月	A轮	400万	Seed Capital等
Ripple	区块链支付服务商	9月	B轮	5500万	A16Z、IDG等

虽然当前区块链技术还处于最原始的测试和试验阶段，但是像万向控股集团这样未雨绸缪、静待发令枪响起的专项投资机构已经纷纷开始行动，以期寻找更多的资源进行互动和碰撞，并伺机在时机成熟的时候一举爆发，从而为全面推进人工智能时代提供更大的动力。

## 第九章 人工智能时代，区块链让金融监管简单化、智能化



目前，经济社会的信用环境整体上看还比较薄弱，信用成本较高，基于区块链技术提出一套成本比较低的“信任解决方案”将从根本上解决信用问题，即通过去信任、公开透明化的特点让资金监管越来越简单，有效避免了反洗钱、反欺诈以及复杂金融衍生品过度交易引发的系统性风险问题，使得区块链金融的监管问题变得更加简单化、智能化。正是基于这一点，银行和金融监管部门对于区块链在金融领域中的应用给予了极高的重视。

书籍每日免费分享微信jnztxy朋友圈

## 区块链技术对金融监管提出了新挑战

当前，区块链金融成为金融界的热点话题，呈现出逐步取代互联网金融的风头。由于区块链技术本身具有不可篡改、公开透明、匿名性等特点，这就使得该技术在授信、清算、支付等金融领域有着非常广阔的应用前景。

各领域企业的发展，尤其是金融领域，对于成本和收益问题最为敏感，而“风险—收益”又是金融业恒久不变的中心。区块链在金融领域中的应用虽然还处于探索和研究阶段，但是区块链技术对金融监管所提出的新挑战却是不可忽视的。具体来讲，区块链技术在金融领域应用的过程中提出挑战主要表现在以下几个方面。

### 1.安全方面的问题

一直以来，安全问题都是信息化社会的“主旋律”。就像是云计算的概念提出和实际应用一样，虽然很多有关的个人信息数据已经被传输到了云端，但是，相信没有几个人愿意将自己的隐私信息在云端实现公开、共享。因此，人们对于区块链的应用所采取的态度依然是这样的。虽然区块链的自带特点就是安全、可靠、公开、透明，但是越是对其在实际场景中的应用深入探究，就越会发现，实际上，区块链技术的安全性还是存在一定的隐患的，这也正是制约区块链技术快速发展的重要原因。

区块链是一个分布式账本，是一种通过去中心化的方式集体维护的可靠数据库技术方案，比特币就是基于区块链技术存在的一种数字货币。数字货币将是未来无纸化货币时代的希望，将逐渐使得当前的纸币时代走向消亡。一旦基于区块链技术的数字货币成为国家法定货币之后，安全性就必须得到保障。

因此，可以说，安全问题是当前区块链在金融领域应用过程中所面临的重要问题之一。从安全分析的角度来看，区块链在金融领域中的应用面临着算法安全性、协议安全性、使用安全性、现实安全性和系统安全性等诸多方面的挑战，如图9-1所示。



图9-1 区块链对金融监管安全方面提出的新挑战

### （1）算法安全性

目前，区块链的算法是相对安全的。但是，我们不得不承认，未来随着数学、密码学和计算技术的不断发展，不法分子在破解算法、密码等方面的手段和技能也随之提高，这样就使得原本相对安全的区块链技术的安全性逐渐降低。

以“天河二号”的算力为例来说明。从“天河二号”当前的算力来看，产生比特币SHA256哈希算法的一个哈希碰撞就需要大约248年。但是随着量子计算机技术的不断发展，未来这种非对称加密算法具有一定的破解可能性，这也就是区块链技术在未来面临潜在安全威胁的原因。

### （2）协议安全性

基于PoW共识过程的区块链主要面临的是51%的攻击问题，这就意味着每个节点通过掌握全网超过51%的算力就能够成功篡改和伪造区块链数据。在最开始创建比特币系统的时候，51%的算力是基于数字货币中攻击者用更大代价的货币换取较小价值的比特币是不划算的角度来考虑的，原本是认为一般情况下攻击者是不会进行这种得不偿失的工作的，但是并不能排除攻击者会为了达到更加恶劣的意图而不惜付出更高的代价进而发生意料之外的攻击行为。因此，从这个角度来看，协议安全性问题依然存在。

### （3）使用安全性

区块链的一大特点就是无法轻易篡改、不可伪造，但是前提是能够保证私钥的安全性。私钥是用户生成并自主保管的，是没有第三方参与的。一旦发生私钥丢失的情况，便无法对账户中的资产进行任何操作。

#### （4）现实安全性

区块链是结合了大量密码学技术而形成的一种技术结合体，因此属于算法高度密集的工程，在现实中比较容易出现一些错误性问题。这种问题也曾经出现过，如NSA对RSA算法实现埋入缺陷，这样就能够轻松破解别人的加密信息。这种漏洞一旦出现，可以说区块链这座大厦的安全基础就会瞬间轰然倒塌，所有的金融交易过程中的参与者没有一个能够幸免于这场安全大厦倾覆所产生的恶果。

#### （5）系统安全性

在系统安全方面，主要是黑客利用上述安全漏洞为了达到攻击目的而给区块链的应用带来安全隐患。目前，黑客攻击已经对区块链系统的安全性造成非常严重的影响。

#### （6）隐私安全性

在传统模式下，数据是通过中心服务器来保存的，并且是通过系统运营方保护数据的隐私。但是在公有链中，由于没有中心化的运营方，每个参与者都拥有完整的数据备份，这也意味着公有链的数据库是透明的。比特币对隐私进行保护的措施是隔断交易地址和地址持有人真实身份的关联，以此来达到匿名的效果。虽然这种方式能够看到每一笔转账记录的发送方和接受方的地址，但是没有办法对应到现实世界中的具体某个人、某个企业等。对于比特币而言，这种方式或许就足够解决隐私安全问题了。但是如果当区块链需要承载更多的业务，例如，实名资产的时候，或者通过智能合约实现具体的借款合同的时候，这些信息如何更好地保存在区块链上，验证节点在不知道具体合同信息的情况下如何去更好地执行合同，这些问题就需要对同态加密、零知识证明等新型密码学方案在区块链问题上的应用进展给予更多的关注。

### 2.去中心化方面的问题

安全问题是区块链技术给金融监管提出的挑战以外，去中心化也是其中一个。虽然区块链以去中心化的方式维护数据库，这表面上看的确是对金融业的颠覆，而且还从根本上提升了效率、降低了成本，但是这种去中心化并不是意味着主体已经非常明确，因此，这也给金融监管的过程中带来一定的难度。

总之，面对区块链系统在安全方面和去中心化方面的挑战，监管者面临的任务更加艰巨，金融监管机构应当重新定义金融科技的监管方向，并且同步制定相应的法律法规与技术标准，从而加强监管、防范风险。



## 区块链改写P2P网贷监管格局

长期以来，P2P网贷不但是互联网金融领域中的热点和重点部分，同时也因为造假、坏账、跑路等一系列严重损害投资者利益的问题频频出现而成为一个备受争议的角色。2015年以来，强化互联网金融监管提上日程，各种监管政策出台。尤其是2016年8月17日，由中国银监会、工业和信息化部、公安部、国家互联网信息办公室制定了《网络借贷信息中介机构业务活动管理暂行办法》（简称“办法”）发布实施，对“信息中介的法律界定、备案制、实名制、双负责监管体制、负面清单、三方担保、三方存管、小额为主、信息披露、募集期、相关义务、过渡期”等方面都出了相关监管措施，这一“办法”的出台，被称为“史上最严监管新规”，同时也标志着一以来野蛮生长的P2P将正式告别“裸奔”时代。

如果按照传统方式来让某一城市的数以千计的P2P企业解决《办法》落地问题的话，通常采用的方法就是让每家P2P企业将其平台上记录的交易数据全部上报给相关监管部门，然后经过监管部门投入的庞大人力资源对这些海量数据进行一一核对，或者遇到人手不足的情况时还会向第三方机构来寻求援助。

然而，区块链的出现并应用与P2P网贷监管中，将使得监管政策的落地不再是难事。区块链技术具有可追踪、不可篡改的特点，这样监管部门可以将所有P2P企业上报的海量数据记录在区块链上，并能够在浩瀚的数据中对异常交易进行快速识别，并作出相应的反应，这对P2P网贷的监管来讲是非常有利的。

### P2P发展之痛

当前，我国金融发展的整个大的市场环境造就了P2P网贷，使得传统的线下借贷逐渐转到了线上，并且发展势头异常迅猛，从而演变出了区别于国外的特色商业模式，不但有效提升了金融闲置资源配置的效率，同时还扩展了金融服务的包容性和可得性，有助于进一步提升我国普惠金融给广大民众带来的满意服务体验，是对我国金融服务缺陷的一种有益补充。

但是随着市场的急速扩张，各种问题也便随之而来，诸如e租宝、金鹿、红顶财富、e快钱、贷乐网、宜众贷等，这些理财平台轰然倒地的同时也给广大民众带来了一例例血的教训，并且剑锋直指网贷监管，让监管机构也对此现状给予了高度重视。

2016年9月，由第一网贷发布的《2016年9月份全国P2P网贷行业快报》中所提供的数据显示：“9月末中国P2P网贷风险预警系统的风险池预警平台3587家，占全国P2P网贷平台6186家的57.99%；其中问题平台2297家，占全国P2P网贷平台6186家的37.13%。”

截至2016年9月底，纳入中国P2P网贷指数统计的P2P网贷平台为4284家，这些平台基本反映了目前全国P2P网贷的全貌；未纳入指数、而作为观察统计的P2P网贷平台为882家；另外，还观察了其余的1020家P2P网贷平台。三者合计共6186家P2P网贷平台，创历史新高。

截至2016年9月底，中国P2P网贷指数在选择样本4284家P2P网贷平台中，涉及31个省、市，平台数量前三名是广东省（857家）、山东省（547家）、北京市（517家），三省的1921家P2P网贷平台，超过了全国总数的44%。”

不得不说，在市场快速膨胀的近几年里，P2P网贷中确实存在很多问题，如法律地位不清、个人征信系统不完善、行业自律规范缺乏，从而导致信用风险、经营风险、法律风险等频频爆发。

面对这些严峻的问题，监管机构也显得捉襟见肘：一方面银行要做P2P网贷业务，为了独立开发P2P网贷业务，就需要建立一整套系统来对接P2P，这样就必然引发成本增加的问题；另一方面，三方存管对银行收益的贡献并不算高，而一旦对接的P2P出现跑路的

情况，或者涉嫌非法集资等问题，银行还要为这些不良后果承担相应的声誉受损的风险。这样，银行也会对其中各个利弊问题做一个权衡，最终就选择采取一种观望的态度。

#### 区块链解决监管难题

区块链所建立的是一个信任机制，借助区块链技术，既可以实时将各个P2P平台上产生的数据记录到账户上，还可以很好地保护平台的隐私，为监管部门提供了一个可以实时检查的窗口。这在以往的监管系统中是很难做到的。这样一来，就可以使得以前P2P相关利益方的痛点逐渐转化为多方共赢的机制，如图9-2所示。

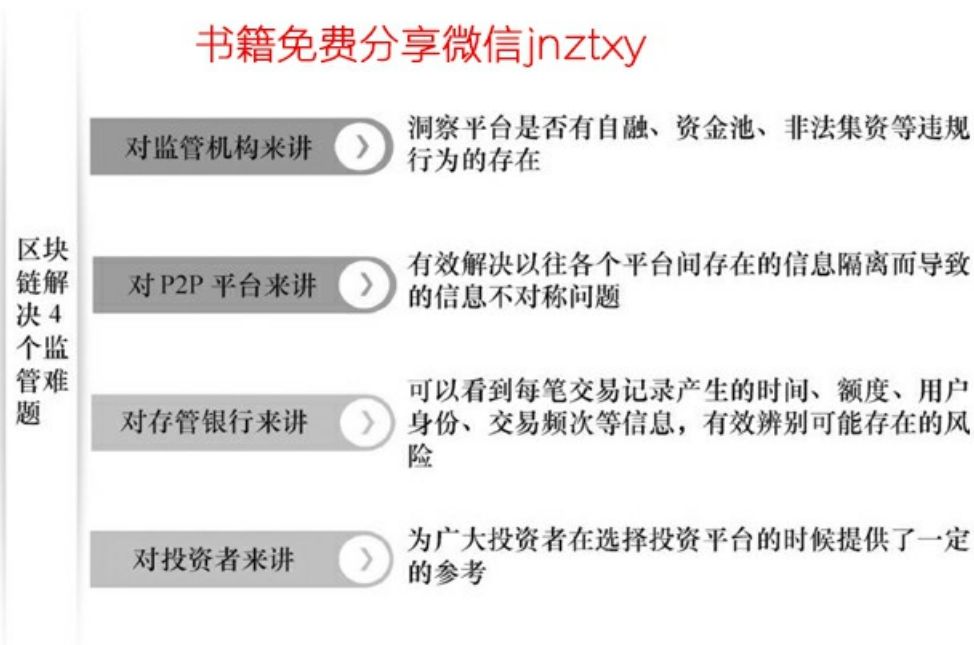


图9-2 区块链解决监管难题

#### 1.对监管机构来讲

可以通过监管节点实时了解到当前每家连接数据的P2P平台的经营状况，用区块链技术手段来洞察平台是否有自融、资金池、非法集资等违规行为的存在。

#### 2.对P2P平台来讲

如果某一位客户在多平台进行重复借贷，那么系统就会快速检测到并及时发出提醒，这样就有助于解决以往各个平台间存在的信息隔离而导致的信息不对称问题，并且还能够将更多的类似增值服务更好地挖掘出来，服务于各个P2P平台。

#### 3.对存管银行来讲

由于自身也是区块链监管系统中节点中的意愿，因此就无需再去开发单独的业务系统去与P2P平台对接，这样不但可以省去由此而产生的大量成本，还可以不用像以往合作的时候仅仅能够看到P2P平台上的每笔交易记录产生的时间、额度等相关信息，在存管银行获得授权之后，还能对交易双方的身份、交易频次等诸多核心信息进行查验，从而可以有效辨别其中可能存在的风险。在经过长时间的数据积累之后，存管银行可以通过数据分析，从中获知哪些P2P平台是优质平台，哪些是劣质平台，进而把优质P2P平台发展成为服务于中小微企业和个人的特殊柜台，进而将银行的理财资金等与其对接，实际上这样间接推动了普惠金融的发展。

#### 4.对投资者来讲

P2P平台敢于将自己的交易数据接入监管系统当中，其实也间接地证明对自己的平台安全的信心，这样做实际上也在无形中增加了平台在民众中的信用度，这也为广大投资者

在选择投资平台的时候提供了一定的参考。

北京阿尔山科技有限公司目前正在带领在区块链和开源软件方面的专业人才打造基于区块链随机数的网贷监管系统，借助传统金融风控和现代区块链技术的双重力量，按照企业级的规模和金融级的安全，对网贷监管系统部署进行设计。在设计过程中，把网络借贷企业、提供存管服务的商业银行、监管部门等三方的不同角色和功能都集中到同一个平台上进行操作，相关数据都放到区块链上，以便能够动态地记录各方的交易数据、反馈交易信息，并且可以根据需要和权限把控信息共享到各方。同时，通过加密技术，将网贷企业的一些敏感商业信息进行加密处理，在保证商业秘密不泄露的前提下，对存管银行和监管部门实现数据可视化、透明化、公开化，这样既方便了业务的正常开展，同时还能让监管部门实时发现监管风险。可以说，此次创新监管系统的打造，实际上无论对于作为信息科技手段的区块链的利用还是对于金融监管加强，都是一种全新的尝试，该系统的打造能够为P2P网贷的发展提供有力的支持和帮助。

基于区块链技术打造的全新监管系统应用于金融风险管控领域，是一种具备创新的、领先性的尝试，是金融监管机构实现对P2P网贷有序、高效监管的保障，也是改写P2P网贷监管格局的有效利器。

## 区块链让金融法制的执行走向智能化

法律是当前社会资源能够实现合理配置的有效机制，对社会经济的正常运行有直接的、重要的影响。一整套好的法制体系能够简化金融领域中金融供应链上各成员关系的复杂程度、节省交易成本，帮助金融供应链上各方能够更加安全、规范、有序地进行交易。

将区块链技术应用金融法制框架中，不但可以通过预设自动执行的智能合约，在约束并引导人们行为的时候引入其他相关技术，还可以依靠技术使信息更加透明化、数据更具可追踪性、交易更加安全、交易成本大大降低，从而实现法律法规和技术规则之间的协同作用，实现二者之间的相互补充，能够将法律和金融更好地融为一体，使得金融法制的执行走向智能化，迈进人工智能时代，如图9-3所示。



图9-3 区块链让金融法制的执行走向智能化

### 1.使金融领域法律约束实现低成本化和智能化

合同一直以来都是为了有效解决信任、透明度和执法问题的协议。区块链的智能合约技术实现了金融领域法律约束与执行的低成本化。智能合约与传统合约有很大的区别，它将分布式账本的加密算法、多方复制账本以及控制节点的权限等关键性程序结合起来，成为以计算机语言而非法律语言的方式记录交易条款合同内容，是一种承诺变现的自动化应用。它由计算机系统在条件出发时自动执行，排除了不必要的人工参与，很大程度上节省了签约成本、履行成本等，并且能够保证合同内容的高效执行，体现出的是一种无人化智能化法制机制。

### 2.对跨国金融犯罪进行智能管控

区块链技术本身具有分布式账本记录的特点，因此不但有利于金融交易信息的记录，同时还为金融监管部门提供了重要的证据线索。在区块链上存储的数据在任何时候都可以实现实时追踪和查询。这样就使得区块链技术在金融监管领域有更好的应用场景，特别是

用于金融刑事案件的查询。因为具有公开透明的特点，区块链技术可以用在打击跨国金融犯罪方面，如跨国洗钱等。目前，如果证据在其他国内，金融执法部门就会向国外执法请求援助，并依据国家法律条约、经过烦琐的程序，才能获得相应的证据，从而推动案件的进一步展开。因此，区块链技术作为全球范围内的数据账本，则可以快速、便捷、智能地实现证据的提取和使用，一旦激活犯罪条件，系统就自动限制资金流动，实现金融风险智能管控，在很大程度上提升跨国金融犯罪的执法效率。[shu籍 分 享 微 信 whair004

### **3.实现金融法律约束和执行的智能化**

智能合约使陌生人之间不需要具有公信力的第三方搭桥接线就可以直接达成交易，但是这并不是说无需律师和其他相关法律服务机构。智能合约丰富了传统的契约制度，而不是取代。律师和其他相关法律服务机构借助区块链技术编制高品质的智能合同，在谈判阶段无需人工参与，就可以自动帮助交易双方确定交易的所有方面，减少一对一谈判的风险和摩擦，弥补合同相关人员在交易信息和合同法律知识方面的不足，降低因合同条文内容的不完善和分歧而引发金融纠纷的可能性，以更好地实现合同的规范性、易用性、可操作性，更重要的是体现了金融法律约束和执行的智能化特点。

从以上几点可以看出，基于区块链技术下的智能合约在落实金融法制的执行问题上具有极大的优势，更加完善的智能合约设计，可以使得金融领域种的各种交易行为和法律实现一体化融合，从而使得各金融机构在智能化法制约束的基础上拥有更加广阔的发展前景。



## 区块链有效解决金融监管排斥问题

诚然，合规性已经成为银行和金融机构的获取成本的主要来源，因此去风险化和去银行化就成为确保与监管机构法规不冲突的一种简单方法，也正是因此受到了金融领域的推崇。在《贫穷国家的反洗钱法导致的意外后果》的报告中所讲的“一刀切”的去风险化的方法会导致不平衡的金融包容性，因为最穷的国家被认为是风险最高的地区，并且导致这些国家被认为是恐怖主义的发源地。在这里，没有明确证实自己身份的人就没有商业和个人信用，更不用说具备洗钱风险的认识，关闭这些人或企业的账户，对于金融监管来讲无异于治标不治本，并没有从根本上解决金融监管排斥问题。

同时，这种“一刀切”的做法也使得3个金融部门在金融监管方面受到了严重的影响，如图9-4所示。

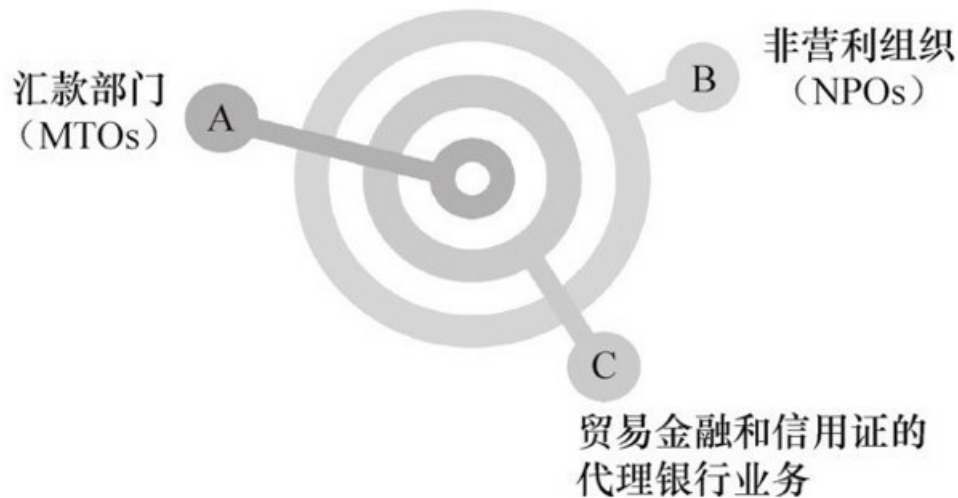


图9-4 “一刀切”的方法使金融监管受到严重影响的3个部门

### 1. 汇款部门 (MTOs)

汇款部门是金融机构，尤其是银行获取收益的很大一部分来源，因此在历史上被列为监管部门的危险业务。当前，从全球范围内来看，很大一部分汇款已经流向了高风险国家。这样，就在监管方面给汇款部门带来了严重的影响和制约。

2013年，将近1/3的美元汇款都流向了被反洗钱金融行动特别工作组（FATF）列入的高风险名单的国家或者非合作管辖区了。13%的资金流向了由巴塞尔协会洗钱风险指数测定的风险最高的25%的国家，6%的资金流向了外国资产控制办公室（OFAC）制裁程序所指定的国家。

### 2. 非营利组织 (NPOs)

非营利组织是受影响最大的部门，通常一些非营利性组织包括社会团体、基金会、慈善机构、寺院等，其捐助和帮助的来源主要是现金和匿名资金。事实上，在高风险地区的国家获得捐助是比较困难的，金融监管机构对于非营利组织的银行业务以及向目标国家发放捐助资金的处理过程是非常复杂的，因为这些地区大多数是贫穷且灾难比较多的地区，各种条件和设施比较简陋或者欠缺。

### 3. 贸易金融和信用证的代理银行业务



受影响的业务还包括贸易金融和信用证的代理银行业务。跨境支付也是银行的一项业务，就目前的业务量来看，国内外贸易往来频繁，使得跨境支付业务办理也相当频繁，同时交易量很大。跨境支付的业务中通常包括外汇、汇款和信用证等。一个国家在对方国家并没有相关分支机构，那么在对方国家进行金融活动时，往往是建立在一种合作关系的基础上实现的。如果一方违背合作章程行事，这就会在一定程度上造成了极大的跨境支付风险。也正是这种建立在合作伙伴关系基础上的跨境支付，使得监管部门在开展工作的時候对贸易金融和信用证的代理银行业务活动受到限制，同时也不便于监管工作的开展。

这3个部门之所以受到金融监管的影响，关键在于在出现非预期后果的时候缺乏一定的透明性。那么如何才能很好地解决这种金融监管的排斥问题呢？答案当然是区块链技术。

区块链作为一种分布式共享账本，显然是解决上述问题的最有效的工具。传统金融模式下，单个银行系统中的信息并不是公开透明的，即不可以实现共享，这样就很可能因为同一个客户在A银行、B银行、C银行甚至在更多家银行都有自己的个人账户，这种情况下就会造成多个监管主体和金融机构对于同一位客户信息的重复记录。

区块链本身就是一种具有开放性、透明化特点的创新技术，可以将每个银行的所有用户数据信息都归纳到区块链上，这样所有的银行都可以同时看到该用户在其他银行中存储的相关数据信息，同时也可以分享到其他银行中自己没有的客户信息，一旦信息实现了共享，那么对于金融监管机构来讲，最大程度地降低监管成本和费用，从而可以服务和监管更多的企业和个人。

总之，在一个自动共享的数据库中存储交易和记录，能够消除银行和监管者同步记录所需的复杂程序。这样就有效降低了金融风险、节省了时间和金钱成本，同时也有利于金融监管工作的顺利、快速开展，有效解决了金融监管机构的监管挑战问题。

## 第十章 区块链金融，金融创新的下一个风口



比特币交易和人工智能在国内金融业大行其道，Fintech（金融科技）已经成为最火热的名词，然而在越来越多的业界人士眼中，去中心化的区块链技术将会使金融科技落地生根。正是因为这样，比特币背后的区块链技术正逐渐得到政府以及金融机构的认可，并在全球范围掀起一场区块链金融研究浪潮。可以说，区块链金融是金融创新的下一个风口。

## 区块链成金融支付的下一个“爆破点”

曾几何时，支付已经走入了我们的生活，尤其是在电子商务崛起之后，第三方支付开始逐渐进入人们的视野，并深入渗透到我们的生活当中，网络支付成为金融支付的主要手段。然而，电子支付的PC时代在移动互联网以及移动智能设备的普及下，逐渐被移动客户端手机支付所取代，因此，诸如加密支付、支付宝、微信支付等各种金融支付创新的出现，给我们带来了一种错觉：金融支付已经发展到如此高端的阶段，已经看不出未来还会出现任何改进的可能和余地。然而，事实上真的如此吗？

区块链技术在各个领域中的应用前景成为当前的热门话题，作为一种底层技术的区块链，它因为重塑并颠覆金融以及经济社会领域的各个方面而受到产业和资本的热捧，如图10-1所示。



图10-1 区块链对各个领域的颠覆作用

### 1. 简化支付步骤

区块链技术并不是一个上层的业务模式，而是更像一个底层的协议来解决具体流程中遇到的一些痛点，例如，跨境支付领域中，应用区块链技术可以使得支付效率更高、成本更低，并且更加快捷。从跨境支付的资金流和现金流中，我们非常清晰地发现，从一个跨境消费者发出境外网站的购物并提交订单直到整个验证结束，以及这个合规体验的结束，共需要经过11个步骤，实在过于繁杂，并没有给跨境支付带来任何效率的提升，如图10-2所示。

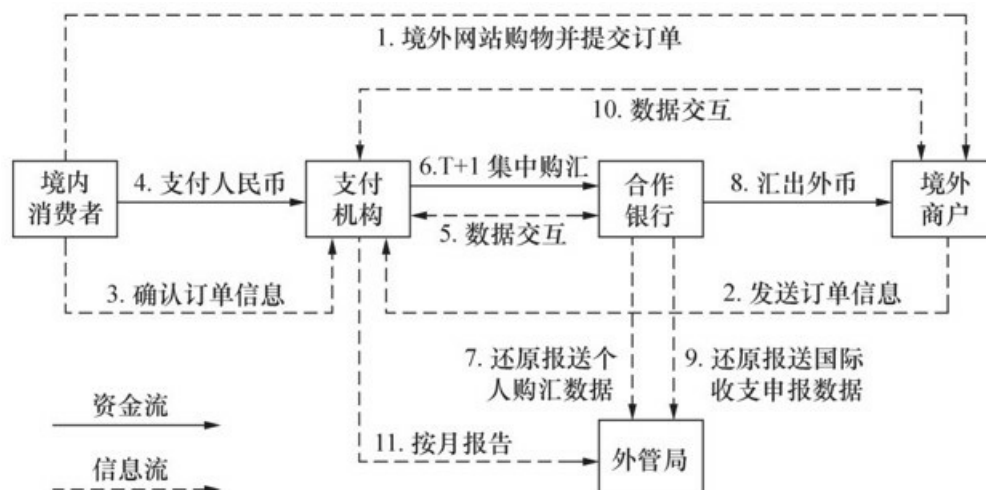


图10-2 传统跨境支付流程

试想一下，如果在跨境支付的过程中某个技术出现一个痛点，就会有相应的技术出现来提供最佳的解决方案。区块链就是基于这种特点的技术。可以说区块链技术是金融支付实现创新的一个“爆破点”。这主要是取决于区块链的4个特点：不可篡改性、分布式存储的完整数据库系统、安全性、可追溯性和可最终性，基于这些特性，相当于使得区块链这种底层协议上形成了一套共识机制——一套基于底层可以构建信任的机制。

假如没有区块链，那么每一次支付、汇兑，或者一次金融价值传输的操作，就必须先通过商业银行A，然后A到央行之后，然后再从央行到下一个程序，最后再将款项寄出。如果是线上完成这种非面对面的交易，我们就必须寻找一个恰当的、可被信任的中介来完成整个支付以及汇兑流程。区块链产生以后，就形成了一个价值传输网络，因为它把所有的账户以及交易信息基于底层，基于算法，基于协议来进行。

因此，区块链的一个有别于其他技术的优点就是在于能够摒弃中转银行在中间的参与，实现点到点的快速支付，并且将从根本上降低因中介参与其中而产生的额外中转费用，即从根本上降低支付成本。与此同时也会降低因中转而带来的金融支付风险，加快决算和清算的诉求，提升了资金的利用率。

## 2.传递信任支付协议

区块链本身具有去信任的特点，在加之其本身又是一个公开化、透明化的分布式账本，这样就能够更好地解决跨境支付方案，例如，跨账本协议能够帮助银行之间实现快速清算，通过区块链技术让所有参与协议的各方都能看到一个相同的账本，从而有效减少参与各方的不一致性。另外，区块链还可以看作是一个类似于信任传递的协议，如果客户甲要转账给丁，但是客户甲和客户丁之间原本不存在信任关系，恰好客户甲信任客户乙，客户乙信任客户丙，客户丙信任客户丁，这样就可以实现信任支付协议的传递。

## 3.实现支付的智能化

区块链不但是一种底层协议，还具有一种特殊的属性，即可编程性，也就是前文中讲的智能合约。基于这一点，我们不但可以将区块链作为一种支付系统和汇兑系统来操作，而且还可以运用代码来执行和编写可执行的条约。

2016年，迈阿密区块链技术博览会上的一家名为“哈罗森特”的企业，该企业利用区块链的可编程性，在区块链上设置一些执行操作的前置条件，这样，企业内的程序无论是收货、验货还是支付，都能够自动执行，无需人员操作。该企业制定的实施方案是将传感器安装到红酒瓶里，当传感器测定红酒的温度和湿度能够达到智能合约中设定的参数数值，整个订单就可以被完成，否则就会被取消。

这家“哈罗森特”企业能够借助区块链技术实现订单流程的智能化，甚至实现支付的智能化，因为万事万物本身就是基于网络的一种互联互通，人们可以设置参数条件以及想要达到什么样的行为结果，这样就能够实现许多智能化的操作。这也正是人工智能时代全球央行关注区块链的根本原因。

虽然当前区块链技术在各个领域中的应用还处于初级的探索和尝试阶段，但是区块链技术对金融科技的运行和发展具有很强的操控和监管能力，可以说区块链这种热门的创新技术，足以给整个金融领域带来惊人的变革。

## 区块链开启人工智能金融2.0时代

2016年8月，全球四大银行（瑞士银行、德国银行、桑坦德银行、纽约梅隆银行）已经按捺不住内心的心潮澎湃，开始对区块链做出一些令人惊讶的举措，即联手开发新的数字货币。四大银行希望通过区块链技术来清算交易，并成为全区银行业通用的标准，同时还希望在2018年以前推出一个商业及区块链系统。紧接着在2016年9月19日在上海举办了全球区块链技术峰会。

这些国内外在区块链的接连布局和会议的召开，充分说明目前区块链技术虽然在各个领域中的应用还处于初级阶段，但各领域对区块链的关注热情依旧高涨，并有逐渐升温之势。作为比特币的底层技术，区块链目前还主要应用于虚拟货币领域，但是越来越多的权威金融机构调研发现：区块链技术对传统金融机构的影响越来越不可低估，甚至可以说区块链将为传统金融开启了前往人工智能金融2.0时代的一扇大门，尤其是对银行业的再造与重构所产生的颠覆性结果已经超过互联网技术的作用，如图10-3所示。

### 1.降低金融交易成本

银行作为金融领域中的大佬级别的金融机构，需要通常投入大量的人力、物力、资金等去建立客户数据库，同时还需要耗费大量成本经常性地维护和更新数据系统，但是，随着系统规模的逐渐扩大，维护成本就日积月累，超乎想象。区块链技术的出现，可以帮助银行实现去中心化，通过分布式记账与集体性数据维护，银行业的成本将会大幅下降。西班牙最大的银行桑坦德银行的一份报告中提到：“如果2020年左右全世界的银行内部都使用区块链技术，每年大概能省下200亿美元。”足以说明区块链将给传统金融领域带来的巨大变革和突破。



图10-3 区块链开启金融2.0时代大门的原因



## 2.提升金融交易效率

在诸多金融交易中，银行可以进行电子转账、资产托管等具有第三方服务职能的交易业务，但是在区块链技术下，财富的所有者对自己的账户全权管理，往往会选择绕过银行这个中介机构直接点对点转账，这足以说明在区块链技术应用于转账等交易过程中，银行的中介价值已经不复存在。另外，现代银行还具有贷款审查等非常复杂的监管职能，并且放贷过程中需要经过的手续是非常繁杂的，交割时间也非常长，还同时涉及多个交易方。但是在区块链技术的基础上，银行不但可以更加便捷、精准地甄别借贷者的资质、信用程度以及还款能力，还可以及时获取与借贷人相关的担保者的所有信息，非常有利于银行做出放贷计划和安排，从而使得贷款业务的效率较以往传统模式有很大提升。

## 3.提升金融交易的安全性

传统模式下，银行数据管理往往是一种中心化管理方式，由本银行内部进行管理。这样往往会形成数据孤岛，使得每个银行内部的数据只能供自己享有和使用，最终无法以最快的速度扩大自有数据量。区块链技术的应用则使得银行对数据的中心化管理变为分布式管理，并且具有不可篡改的特点，使得银行的数据系统变得较以往传统模式更加安全与可靠。不但如此，在区块链技术支持下的数据可以实现分散式自动生成，既节约了银行数据采集成本，也降低或完全避免了数据采集过程中因主观因素而造成的误差和错误，进而有效降低银行的道德风险。除此以外，区块链本身是一个具有公开性、可追溯性、不可篡改的分布式总账系统，银行可以借助区块链技术对资金流动状况进行实时监控和查询，有效防止和杜绝了违规资金转移、洗钱、资金诈骗等非法行为的发生。

银行只是金融领域中区块链应用场景中的一个，除银行以外还有证券交易、P2P网贷、保险等金融交易场景。高盛集团曾做过这样一个预算：“区块链技术在美国证券交易中每年能够节省20亿美元成本，这样的话，从全球范围来看，假设成本和股市市值成比例，那么每年节省的成本可能超过60亿美元。”同样在保险行业，由于每一笔交易都可以实现追溯性，借助区块链技术可以帮助保险业有效解决保险欺诈问题，同时还可以激活互助保险等许多传统保险模式。在P2P网贷领域，区块链的应用使得交易双方不再需要经过平台的撮合，直接点对点完成资金的供需配置，这样就很好地避免了平台倒逼和跑路风险的出现。

相关数据显示：“截至2016年9月，高盛集团、摩根大通、花旗银行等全球知名银行在内的全球顶级金融机构在过去两年中投入到区块链相关科技公司的资金达到了17.9亿美元，而且仅2016年第一季度的投资就已经达到了1.6亿美元。”

正是基于区块链在金融领域的应用具有诸多优势，区块链即将开启人工智能金融2.0时代，国内外的众多金融机构纷纷将区块链作为一种市场竞争工具应用到自身发展过程中，国际巨头也争相迈开步伐，开始在区块链领域提前布局。

## 未来互联网金融环境基于区块链技术的蜕变

2015年年底，互联网金融发展的环境突然恶化，P2P企业，尤其是e租宝事件使得行业声誉严重受损，并且已经波及整个互联网金融行业。进入2016年以来，互联网金融环境逐渐开始好转，尤其是区块链技术受到金融界的热烈讨论和应用探索之后，互联网金融的发展环境日趋改善。

马云曾说过这样一句话：“大家还没搞清PC时代的时候，移动互联网来了，还没搞清移动互联网的时候，大数据时代来了。”诚然，在当大家还没有充分弄明白大数据的时候，区块链时代来临了，如图10-4所示。

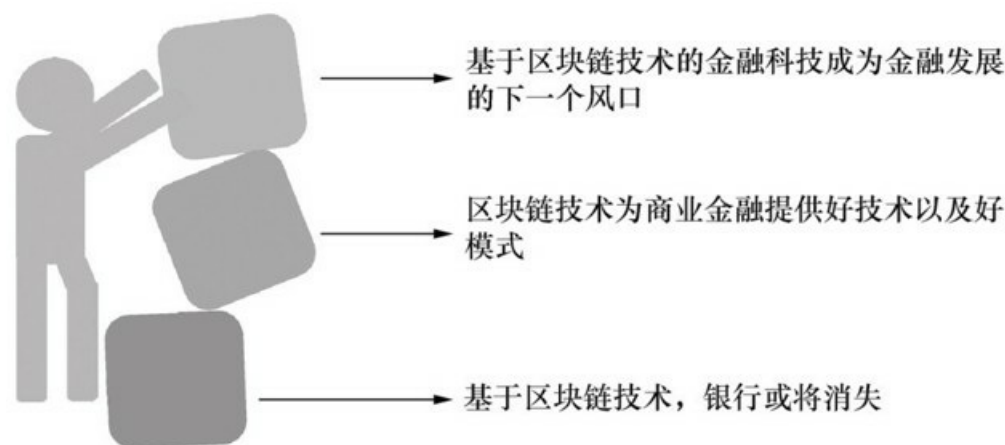


图10-4 未来互联网金融环境基于区块链技术的蜕变

### 1. 基于区块链技术的金融科技成为金融发展的下一个风口

2016年7月下旬，在北京、上海、广州连续举办了各种财经论坛，这些论坛往往是关乎当前市场发展前景的风向标。在过去两年里，“互联网金融”成为各大财经论坛中热点话题，然而，进入2016年，金融科技（Fintech）逐渐取代了“互联网金融”而一度在金融领域走俏。

金融科技从概念上讲，强调大数据、云计算、人工智能、移动互联网、区块链为代表的新一轮信息技术来提升金融效率和优化金融服务。然而，当前很多贴有“金融科技”标签的企业却是以往那些非常热衷于“互联网金融”的企业。随着蚂蚁金服、京东金融、众安保险、宜信等行业巨头开始将自己定义为“金融科技”公司，这个概念已经在国内广泛传播，并且成为业界的流行词。

目前，在我国有两大类金融科技公司：第一类是拥有BAT等老牌互联网背景的公司，第二类是从互联网公司转型而来的公司。事实上，金融科技是互联网金融发展的一种延伸，是对现有金融机构产品和发展模式的一种革新，两者之间存在的差别仅在于，互联网金融强调的是金融，而金融科技的侧重点在于技术。金融科技取代互联网金融是金融行业发展的必然趋势。

区块链作为金融科技中的技术之一，已然在互联网金融被金融科技逐渐取代的过程中起到举足轻重的作用。

（1）区块链作为一种分布式技术，也被称为“分布式账本”，即将区块链看作一个公共账本，从每笔数字货币的诞生开始，所有转账、交易都将被记录在区块上，每个区块相互连接起来形成区块链。任何人都可以在区块链上查询交易记录，但仅能在这里查询相关

记录，却不能对其中的信息进行任何更改。

(2) 去中心化、去中介化、去信任、公开透明化是区块链的显著特征，当数据被记录在一块区块链上的时候，其他区块链上同样会记录相应的数据信息。简单来讲，就是“真相只有一个，真相掌握在每个人手中”，这样所有的金融交易在区块链上的每个节点都有记录，所有的交易参与方都能够清晰地看到记录信息。

(3) 智能合约作为区块链的核心技术，推动交易各方在执行合同的时候实现智能化，即所有的合同执行都按照条约内容自动执行，这样就不会出现欺诈、跑路等情况，有效降低金融风险，推动了人工智能金融的实现。[shu籍 分 享 微 信 whair004]

两个人为一件事情打赌，约定输了的一方给赢了的一方100元，在没有约束的前提下，结果出来后，输了的一方可能会对赌约赖账。但是如果将区块链技术加入智能合约中，双方在下赌注的时候，先将各自100元冻结在智能合约中，一旦结果公布，系统就会自动核实谁是赢家，进而将100元赌资打入赢家的账户中。在整个过程中，完全无需相关的中介人员作证或者裁决，而是完全实现了去中介化、去中心化，无需信用背书。

互联网金融发展的终极目标就是实现真正的点对点、端对端、个人对个人的金融服务，去掉中介，在充分保证信任的技术基础上完成金融交易。然而，当前，互联网金融并没有通过发展真正实现金融业务的低成本运作。所有的这些愿景，都将基于区块链技术在金融领域中的应用而变为现实。

## 2. 区块链技术为商业金融提供好技术、好模式

早在2014年的时候，怀揣创业梦想的达鸿飞和几位朋友共同创造了小蚁区块链，小蚁区块链的成立其实是国内最早一批关注区块链一个的创业模式。2015年10月底，小蚁以仅接受比特币的方式在业内举办了一次产品众筹活动，筹得的资金金额折合人民币465万元。目前，小蚁是区块链领域中较为成熟的项目之一。小蚁的商业模式：基于区块链技术将实体资产、权益数字化，为登记发行、转让交易、清算交割等金融业务提供去中心化的网络协议。以普通股权转让业务为例，通常转让股权需分为四步：签订转让合同、银行转账、变更股东姓名、工商局登记。小蚁要做的事情就是将前三个步骤进行捆绑，在签订电子合同的时候，转账和更名同时进行，这样就可以很好地避免毁约以及不配合更名的风险。

当前，在我国像小蚁这样做区块链底层技术的公司不到10个。主要因为：一方面是因为国内对区块链技术的普及程度还不够；另一方面是因为当前区块链技术与商业应用之间还需要经历一定的磨合期。区块链技术会为商业金融提供良好的技术和模式，这将加快未来互联网金融蜕变速度。

## 3. 基于区块链技术，银行或将消失

当前，网络存在于生活中的各个角落，计算机设备也变得越来越精密、便捷，信息处理的速度也越来越快，传统银行的付款流程正在这个互联网时代受到了巨大的挑战，银行已经走到了底层基础架构急需改变的关键时刻。

一直以来，银行依然没有将旧的系统更换为IP系统，是因为IP网络在数据传输过程中不可避免地会发生错误或遗漏，而对于金融系统来讲安全至上。区块链正好是一个极具公开化、透明化、不可篡改的数据库，一个区块上记录相关数据，则几十万个区块同时会复制这些数据，从而保证数据的安全、准确。这样，就能够在一定程度上很好地解决信任问题，双方无需相信对方，只需要相信区块链中存储的数据的真实性即可。这样，传统银行在以往的金融交易过程中所起到的第三方中介的高大形象就逐渐淡化，其信用背书变得可有可无。

正是意识到未来生存道路上可能遇到的重重威胁，众多银行开始站在区块链的位置上另谋生路，微众银行、浙江网上银行等互联网巨头旗下的民营银行纷纷集合到区块链大树下，充分结合自身特点和优势，调整和优化业务模式，以期在金融领域的巨大竞争市场中能够站稳脚跟，进而拔得头筹。

总而言之，当前区块链技术在各个领域中的应用探索与实验必将给各领域未来的发展带来前所未有的变革。金融领域更是如此，相信未来进入人工智能时代，互联网金融环境基于区块链技术的应用必将实现惊人的蜕变。

## 区块链加速实现普惠金融

当前各个领域中热议的区块链技术就其技术构成的本质来讲，其实已经不是一项完全基于创新的、单一的技术了，而是结合现有多项技术形成的一种技术合体，它包括了加密算法、P2P（点对点）文件传输、交易确认的拓扑结构等，并且将这些技术与数据库结合在一起，形成一种看似全新的数据记录、传递、存储的呈现方式。简而言之，区块链技术的本质：一种去中心化的、寓于分布式结构的数据存储、传输和证明方法。也正是这种技术在金融和其他领域中的应用改变和创新的模式，甚至改变了人们的生活方式。

如果在全球范围内建立一个庞大的数据库，那么借助区块链技术可以解决数据库建立过程中通常存在的3个问题：第一，如何保证数据库既能存储大量信息，又能在没有中心化结构的体系下确保数据库的完整性？第二，当系统中的某一节点出现错误或者崩溃时，如何保证这个全球性数据库的正常运行和信息完备性？第三，如何能让所有人相信区块链中的信息都是真实、可靠的，保证区块链中的信息不被随意更改、伪造，防止数据库用户在互联网没有实名制的背景下出现诈骗情况？区块链解决这些问题的关键就在于前文中讲述过的区块链技术的特点，即去中心化、基于技术建立信任关系、信息的公开透明化、高容错性和高包容性、智能合约自动执行、匿名性等特征。这些也正是实现普惠金融所需要的关键点。

互联网金融发展正当其时，给民众带来了快捷的金融服务，带来了以往稀缺的金融资源，但同时也带来了扩散型金融风险，带来了“金融成长中的烦恼”，在进一步实现普惠金融上还存在一定的瓶颈。

普惠金融具有很强的社会目标，即给所有的人提供发展的机会和可能。普惠金融就是给社会各个阶层的人，尤其是贫困低收入人群提供有效与可持续的金融服务。作为当代经济发展的核心资源配置工具，应该让所有人拥有获得金融服务的最好途径。金融排斥的原因有很多，包括金融基础设施难以渗透到最后一公里以及信息的不对称等。信息技术可以帮助解决传统金融工具难以克服的障碍，通过信息技术应用的全面覆盖来增加金融服务的覆盖面。区块链就是当前能够保证数据信息全球覆盖，能够以高效率、低成本解决“金融成长中的烦恼”，进而实现普惠金融的有效技术。

区块链作为一项去中心化的技术，对于加快实现普惠金融具有颠覆性的创新，主要体现在以下几个方面，如图10-5所示。

### 1. 区块链金融的“分布式”

区块链技术是一种具有去中心化特点的技术结构。在现有信息技术系统中，所有的信息交换和数据存储都是由中心服务器来实现的。区块链则是通过构建分布式体系和参与者建立共识机制，形成不需要中心的大规模数据库系统。

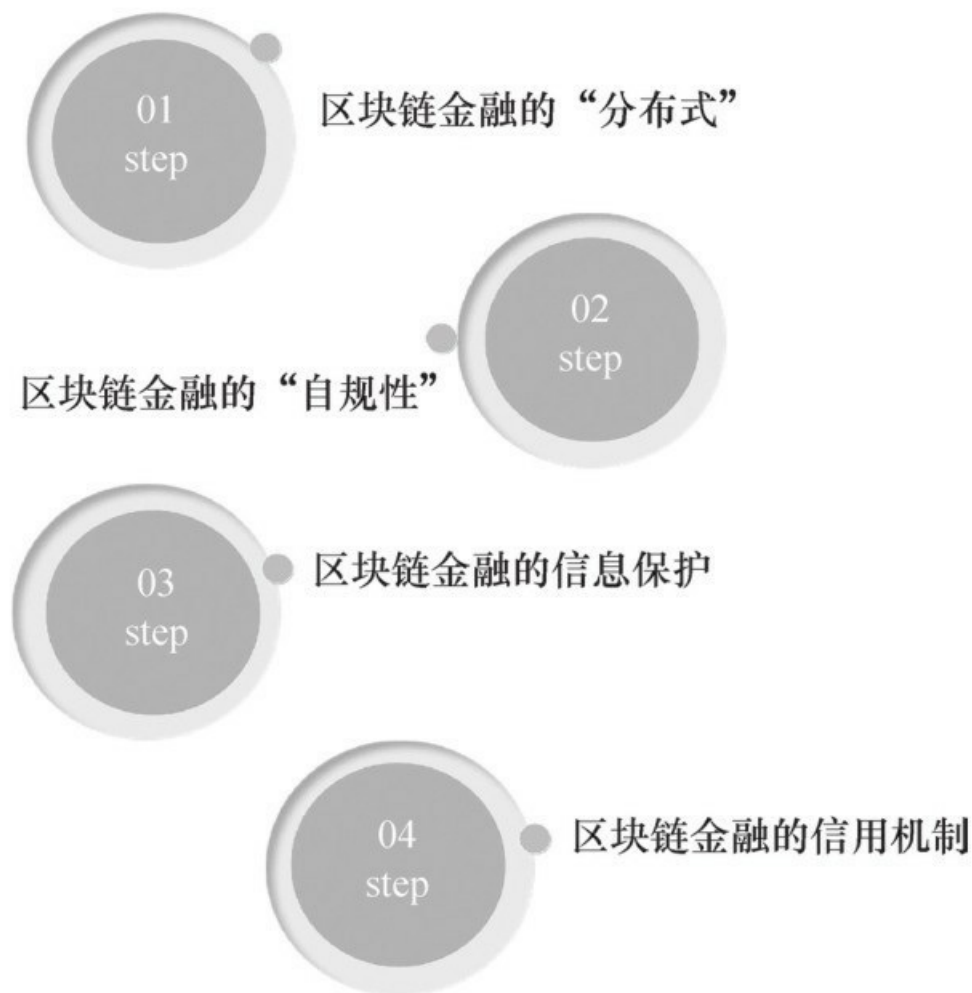


图10-5 区块链加快实现普惠金融的创新路径

事实上，区块链技术对硬件方面有很高的要求：第一，海量数据存储需要很大的空间；第二，数据实现同步需要高速的网络；第三，各个节点的容纳能力都需要达标并且需要实现均衡化。基于这三点要求，一旦每秒产生的交易量超过了系统的容纳能力，或者超过最弱节点的容纳能力，那么交易就自动进入排队状态。按照顺序排列，则越排在后边的节点耗时越长，就会给节点上的参与者带来不良的体验感受。基于这样的原因，完全的“去中心化”结构只适用于那些流量很低、每秒发生几笔交易的应用中。而在金融应用场景中，高频次交易量是常态，银行卡、股票、外汇等金融业务的峰值能够达到每秒万笔以上。同时，金融产品和金融服务通常跨平台实现。简单举个例子，如果使用区块链技术构建数字票据，就必须解决数字票据交易系统与资金清算系统的实时对接问题。传统的“中心化”结构显然无法适应那些高频次、跨平台的金融应用场景。

因此，在区块链技术规模化应用的探究和实验当中，出现了诸多的“私有链”和“联盟链”。像IBM、微软、R3金融区块链联盟在进行研发和实验的过程中都采用分布式账本技术。

以我国金融发展特点为例。我国当前的金融基础设施比较发达，大型金融机构已建成超高速、大容量、中心化的信息技术系统。区块链技术应用于金融领域，使得众多大中小型金融机构共同组建了分布式“联盟链”，从而实现了现有系统与创新系统的无缝对接，这样，所有的金融机构，不分大小，都可以通过共享互联互通的技术平台，为更多的客户提供更好的金融服务，这对于我国的普惠金融的发展是非常有利的，也有助于充分利用现有



科技资源，达到节约投资、节约交易成本，确保交易速度，实现合规控制的目的。

## 2.区块链金融的“自规性”

区块链金融与传统金融和互联网金融之间存在的一个显著特征就在于，区块链金融是自定义共识规则、自动实施规则，用自身具有的信任特点来提升商业信用能力。

市场经济大环境下，信用的建立是在契约原则的基础上形成的。在传统金融模式下，信用的形成往往是通过可信的中央节点（如将人民银行作为征信的中心）或者支付平台（如支付宝）作为共同的规则来验证信息、执行规则、积累信任。区块链金融则有所不同，是通过借助技术方法落实契约原则，解决信任问题的，即通过共识协议和可编程的智能合约两种形式来制定和执行交易各方认同的商业条款，以及引入法律法规和监管控制节点，从而确保价值交换符合契约原则和法律规范，避免无法预测的、可能出现的交易风险。

### （1）共识机制

区块链是通过数学算法来解决信任问题的，所有的规则都可以通过算法程序来表达，只要交易各方对共同的算法程序表示信任，那么就可以在金融交易中借助这个共识机制建立起人与人之间的信任关系。

### （2）智能合约

区块链可以实现点对点的价值传递，可编程性的引入使得交易双方在价值传递的过程中可以嵌入相应的编程脚本，进而形成“智能合约”，这样在处理一些特殊的交易模式的时候可以更加便于实现。

基于区块链的这种功能，可以通过共识机制建立相互信任、创造各交易方的信用关系，借助智能合约节约信用形成所需的时间和资金成本，容纳更多的金融业者，对于普惠金融的发展有极大的帮助：有利于契约关系和契约原则的维护和执行，有利于维护金融诚信，对于良好社会秩序的形成和维护、市场经济的健康运行具有重要的推动作用，对于人工智能时代的实现具有重要的促进作用。

在当前的金融票据业务中往往会存在难于监管和防范操作性风险、道德风险的缺陷，主要包括贸易背景造假、票据真实性认证失败、“一票多买多卖”、利用票据违规融资套利等风险问题。现行票据业务监管只能通过现场审核的方式对这些风险问题进行监管，这样就严重缺乏全流程快速调阅和审查的手段，严重降低了监管效率、提升了监管成本。如果在票据业务中应用区块链技术，就可以通过可编程的智能合约来实现对商业约定的具体限制，并引入监控节点，由交易各方确认交易，从而确保价值交换的唯一性。

## 3.区块链金融的信息保护

当前，随着经济的不断增长，随之产生的数据信息也呈几何级增长，形成了海量信息。通常，信息可以分为共享信息、专有信息、私密信息，如图10-6所示。共享信息要求在进行共享时保持其真实性，因此就必须维护其权威性；专有信息强调的重点在于归属性，因此必须维护其知识产权；私密信息强调的是可靠性和安全性，因此需要维护其安全。互联网的发展在一定程度上促进了信息的产生和传播，但同时也存在一些欠缺，即难以证明共享信息的真伪性、难以维护专有信息的知识产权、难以维护私密信息的安全性。也正是基于这些原因，互联网平台上诸如伪造共享信息进行诈骗、盗用私密信息进行诈骗的事情频频发生。信息得不到很好的保护，损害了大众利益的同时，也在很大程度上影响了金融服务在民众中的普及。



图10-6 信息的3种类型

区块链技术的出现和应用，将从理论上为信息保护提供新屏障。区块链的分布式功能，通过构建分布式数据库系统和参与者共识协议，保护数据的完整性。区块链的时间戳功能通过生成一定时间段的信息区块链以及区块链间首尾相连的数据链，使得形成的数据具有可追本溯源、可逐笔验证、不可随意更改、不可伪造的特点；每个参与者在生成信息区块时加盖时间戳，能够证明原创性和所有权的归属问题。区块链的非对称加密功能，对于保护信息的私密性具有重要作用。

#### 4. 区块链金融的信用机制

区块链如何与普惠金融联系到一起的呢？实际上，区块链技术在本质上是一种利用计算机实现的代表公信力的机制，区块链技术可以实现去中心化、去中介化的效果，这样就推动了整个商业流程的改变，会让整个商业服务在高效实现的同时还有效地降低了成本、重构了信用机制。另外，在区块链上登记的所有交易信息都可以实现追根溯源，区块链上的所有数据都是公开透明、不可篡改的，因此，在公益捐款等的普惠金融场景中使用区块链再合适不过了。

在金融领域，借助区块链技术更好地为普惠金融服务的典型代表就是蚂蚁金服。蚂蚁金服从支付宝开始至今，一直秉承为普惠金融用户服务的原则，为用户提供与日常生活息息相关的业务，包括缴费、出行、购物以及订餐等便民服务；通过理财业务为用户增加收入；为广大网购用户提供退货险服务；为众多小微企业提供小微贷款服务。蚂蚁金服的服务理念是“让信用等于财富”，因此，蚂蚁金服一直在解决信任问题上进行不断探索。区块链技术就是通过共识算法和安全技术来打造信任机制，用公信力代表公信力，因此就决定了区块链的应用方向，即适用于需要信任和需要公开透明的场所。蚂蚁金服注意到了区块链的这一优势，就将公益作为区块链解决信任问题的应用场景。如果有用户捐款，则捐款记录就记载到区块链上，这样，用户所捐的款项就好比打成了一个包裹，然后交给区块链平台，这就好比是去邮局邮寄资金包裹，而整个资金的运送过程中，因为中间需要经过公益机构和一些非政府组织机构最后才会到达受捐人手中，也就是要经过一个比较长的链条，在这个过程中，区块链平台上邮寄的每一笔资金每经过一个节点都会盖上戳，之后再送到受捐人手里。这样就能够确保每笔资金无论是1分钱还是100元，都会受到非常认真的对待，区块链技术会把整个流程全部记录下来，并且运送过程中所经过的每个节点都会对整个流程非常明了，整个流程都是开放、透明的，这样就不必担心资金丢失的问题。

普惠金融服务最典型的应用场景之一就是农村金融领域，让金融服务真正走到基层，走到农村。区块链技术不仅仅属于技术革命，更能够随着农村互联网技术的发展，从根本上解决金融的盲点问题，主要体现在以下两个方面。

##### （1）解决农村金融的征信问题

在过去，征信主要是通过抵押物来实现的，对于农民来讲，虽然拥有较大面积的耕种

土地，但是国家明文规定国有土地不能非法交易，这就使得农民能够作为抵押的物品少之甚少。区块链技术就能够很好地解决这一农村金融的征信问题。区块链技术改变农村征信主要采取中心记录、中心查询模式，从根本上解决了农村信息不完整和不对称、维护成本高、数据滞后等问题。借助区块链技术，可以将农村产生的海量行为信息数据记录在区块链上，并将其存储在每个节点上，实现了信息透明化，防止非法篡改并从根本上降低了维护成本。这样，农民在申请贷款的时候，只要从区块链上查询相关贷款人的信息就可以快速完成审批，从而实现了真正意义上的“闪电贷”。这样确实为广大农民解决了以往贷款难的问题，使得贷款变得更加便捷。

## （2）解决农村金融的支付问题

目前，在我国农村很少有ATM机，然而对于广大农民来讲，一方面由于互联网技术没有得到全面普及，另一方面由于自身知识量有限，这样就在操作移动支付的过程中造成了一定的困难。基于这两方面的原因，就使得现行支付模式严重影响农村金融的发展，使得当前农村的支付方式呈现出一种中心维护模式。因此，农村的交易记录、账户余额、账户安全管理等基础设施都是以中心支付系统为核心来构建的，即通过农村信用合作社来实现的。这种中心支付系统将会给农村金融带来以下几个问题。

①安全风险：一旦中心支付系统被攻破，那么后果将不可设想。

②成本过高：为了防止中心支付系统不被破坏，那么中心支付系统就不得不投入巨额资金进行风险防范，同时还得投入大量的人力去运营，这样就会造成银行结构和层级臃肿。

③中心集权：话语权完全掌握在银行机构手中。

④信用危机：传统意义上来讲，借款人申请贷款时往往依靠银行、保险、征信机构等场所来记录相应交易信息数据，但是，这种记录方式通常会存在数据不准确、信息不完整等情况，从而无法保证借款人的信用度足够高，容易产生信用危机。

区块链技术就可以有效、轻松地解决这些问题。相信用不了多久，一个基于区块链的农村会在交易多方向建立信任关系。区块链在农村金融领域中的应用，会使农村交易变得更加快捷，成本更低，并且能够真正实现与城市同步，缩短城市和农村金融之间的差距，从而使得普惠金融的主动权完全回归到了单个个体手中，使得农民获得了以往享受不到的金融产品和服务。

总之，区块链应用于不同的金融交易场景中，都需要有效保护数据信息，这是区块链在应用过程中的一条准则。这种数据信息的保护是维护金融诚信的要求，同时也是发展普惠金融的要求。

# Table of Contents

[扉页](#)

[版权信息](#)

[目录](#)

[内容简介](#)

[前言](#)

[第一章 解密区块链，你所不知道的神秘区块链](#)

[自带比特币基因](#)

[区块链的3个进阶阶段](#)

[区块链的4种技术创新](#)

[区块链如何运作](#)

[区块链的技术挑战](#)

[区块链将颠覆我们的世界](#)

[第二章 人工智能时代，区块链带来金融科技的新蓝图](#)

[区块链重构金融业](#)

[互联网金融VS区块链金融](#)

[区块链助力共享金融的实现](#)

[区块链变革金融服务的基础设施](#)

[第三章 人工智能时代，区块链与金融大数据](#)

[“区块链+大数据”创造数据神话](#)

[大数据时代区块链再造信任体系](#)

[“区块链+大数据”破解传统风控难题](#)

[第四章 人工智能时代，区块链构建金融信用长城](#)

[从数字货币到信任社会](#)

[开启全新的金融信任时代](#)

[区块链技术构建金融信用生态圈](#)

[区块链构建银行业客户信用体系](#)

[第五章 人工智能时代，区块链金融的六大应用场景](#)

[数字货币](#)

[跨境支付与结算](#)

[数字票据](#)

[银行征信](#)

[有价证券交易](#)

[股权众筹](#)

[第六章 人工智能时代，区块链在数字金融资产中的应用](#)

[区块链在银行业的应用](#)

[区块链在保险业的应用](#)

[区块链在资产托管中的应用](#)

[区块链在信用借贷中的应用](#)

[第七章 人工智能时代，金融行业区块链的落地策略](#)

[各大金融机构争相逐鹿区块链](#)

[IBM与中国银联探索区块链技术落地应用](#)

[商业银行对区块链技术发展的应对策略](#)

[第八章 人工智能时代，金融业扛旗者走在区块链金融最前端](#)

[银行系：从担忧到拥抱](#)

[传统IT和新兴互联网企业：积极拥抱区块链](#)

[专项投资机构：翘首以盼](#)

## [第九章 人工智能时代，区块链让金融监管简单化、智能化](#)

[区块链技术对金融监管提出了新挑战](#)

[区块链改写P2P网贷监管格局](#)

[区块链让金融法制的执行走向智能化](#)

[区块链有效解决金融监管排斥问题](#)

## [第十章 区块链金融，金融创新的下一个风口](#)

[区块链成金融支付的下一个“爆破点”](#)

[区块链开启人工智能金融2.0时代](#)

[未来互联网金融环境基于区块链技术的蜕变](#)

[区块链加速实现普惠金融](#)