

# 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

# 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

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

## 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。

---

◆ 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

# 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。

# 目 录

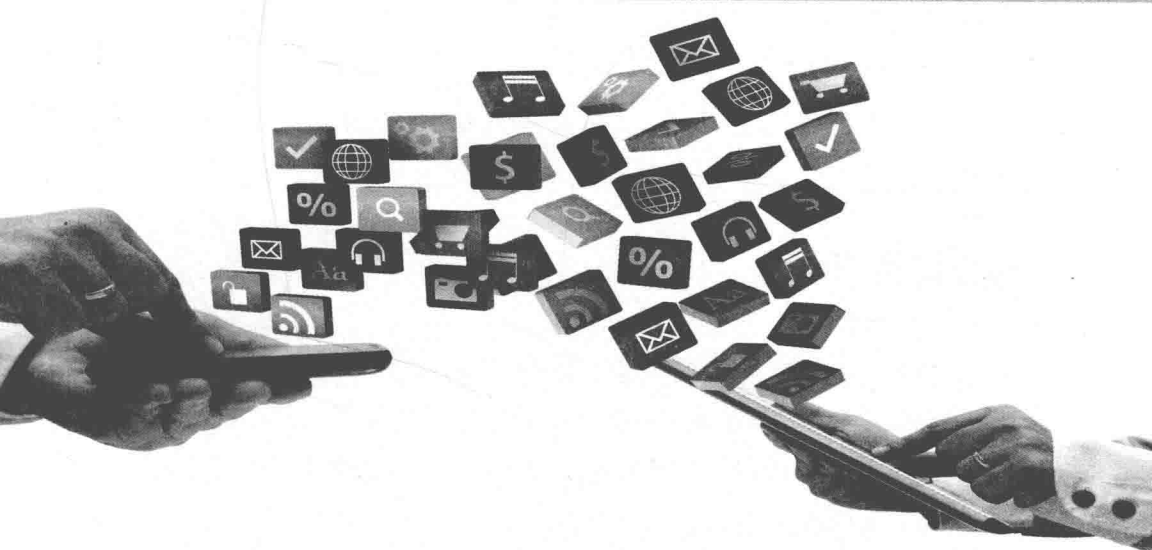
<b>第一章 解密区块链，你所不知道的神秘区块链</b>	<b>/01</b>
自带比特币基因	/02
区块链的3个进阶阶段	/10
区块链的4种技术创新	/23
区块链如何运作	/33
区块链的技术挑战	/37
区块链将颠覆我们的世界	/41
<b>第二章 人工智能时代，区块链带来金融科技的新蓝图</b>	<b>/47</b>
区块链重构金融业	/48
互联网金融 VS 区块链金融	/52
区块链助力共享金融的实现	/59
区块链变革金融服务的基础设施	/62
<b>第三章 人工智能时代，区块链与金融大数据</b>	<b>/67</b>
“区块链 + 大数据”创造数据神话	/68
大数据时代区块链再造信任体系	/72
“区块链 + 大数据”破解传统风控难题	/74
<b>第四章 人工智能时代，区块链构建金融信用长城</b>	<b>/79</b>
从数字货币到信任社会	/80
开启全新的金融信任时代	/83
区块链技术构建金融信用生态圈	/85
区块链构建银行业客户信用体系	/88

<b>第五章 人工智能时代，区块链金融的六大应用场景</b>	<b>/93</b>
数字货币	/94
跨境支付与结算	/97
数字票据	/100
银行征信	/104
有价证券交易	/107
股权众筹	/109
<b>第六章 人工智能时代，区块链在数字金融资产中的应用</b>	<b>/113</b>
区块链在银行业的应用	/114
区块链在保险业的应用	/119
区块链在资产托管中的应用	/122
区块链在信用借贷中的应用	/126
<b>第七章 人工智能时代，金融行业区块链的落地策略</b>	<b>/129</b>
各大金融机构争相逐鹿区块链	/130
IBM 与中国银联探索区块链技术落地应用	/133
商业银行对区块链技术发展的应对策略	/136
<b>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</b>	<b>/141</b>
银行系：从担忧到拥抱	/142
传统 IT 和新兴互联网企业：积极拥抱区块链	/145
专项投资机构：翘首以盼	/149
<b>第九章 人工智能时代，区块链让金融监管简单化、智能化</b>	<b>/153</b>
区块链技术对金融监管提出了新挑战	/154
区块链改写 P2P 网贷监管格局	/157
区块链让金融法制的执行走向智能化	/161
区块链有效解决金融监管排斥问题	/164
<b>第十章 区块链金融，金融创新的下一个风口</b>	<b>/167</b>
区块链成金融支付的下一个“爆破点”	/168
区块链开启人工智能金融 2.0 时代	/171
未来互联网金融环境基于区块链技术的蜕变	/174
区块链加速实现普惠金融	/177



## 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

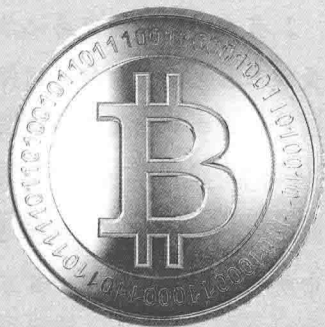
所谓比特币，就是一种 P2P 形式的数字货币。众所周知，2008 年，出现了一场非常严峻的、全球性的金融危机，以雷曼兄弟的倒闭为开端，金融危机在美国逐渐达到高潮并且向全世界蔓延。

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保障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。

## 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。在比特币发行之之前，赖特和计算机取证分析师大卫·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，赖特已经否认

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。

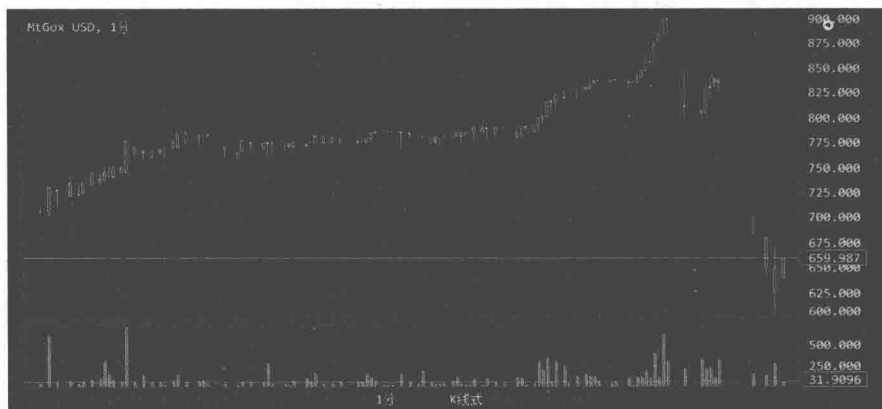
## 价格波动，时代造就

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。



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

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

## 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。

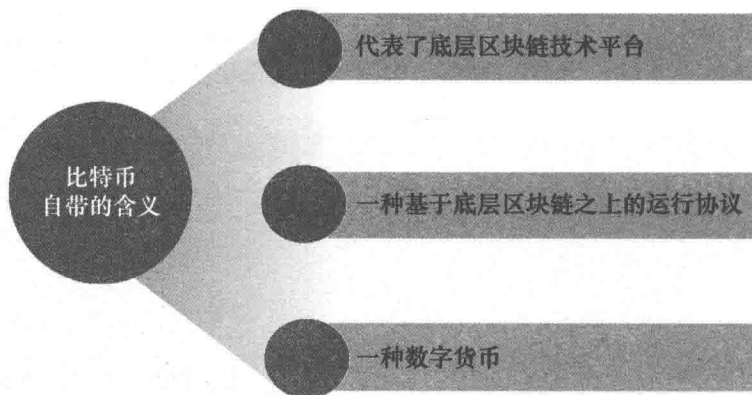


图 1-2 比特币自带的含义

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  
有密钥才能打开

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