区块链新时代：赋能金融场景

THE NEW ERA OF BLOCKCHAIN:
EMPOWERING FINANCIAL SCENES

巴曙松　朱元倩　乔若羽　王　珂／著

科学出版社

区块链新时代：赋能金融场景

The New Era of Blockchain: Empowering Financial Scenes

巴曙松　朱元倩　乔若羽　王　珂　著

科学出版社

北　京

内 容 简 介

本书从区块链技术的相关概念和基础知识入手，分别探讨了区块链技术在贷款技术、证券交易、资产管理、供应链金融、票据业务、财产权登记、大宗商品交易、保险领域、跨境支付、征信行业和数字货币这11个金融场景中的应用，在分析各金融场景目前面临的困境和难点的基础上，从理论分析的角度论证了区块链技术对其带来的优势和改进，以案例的形式展现了区块链技术在该金融场景中的应用，并对未来区块链在该领域的应用进行展望和评述。

本书是面向大众介绍区块链技术在金融领域的应用的通俗读本，可供有兴趣了解区块链技术、未来金融、未来财富的人阅读参考。

图书在版编目(CIP)数据

区块链新时代：赋能金融场景 / 巴曙松等著. — 北京：科学出版社，2019.8

ISBN 978-7-03-061068-3

Ⅰ.①区… Ⅱ.①巴… 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（2019）第 074375 号

责任编辑：张 展 叶苏苏 / 责任校对：彭 映

责任印制：罗 科 / 封面设计：墨创文化

科学出版社出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

四川煤田地质制图印刷厂印刷

科学出版社发行 各地新华书店经销

*

2019 年 8 月第 一 版 开本：B5（720×1000）

2019 年 8 月第一次印刷 印张：19 3/4

字数：330 000

定价：78.00 元

（如有印装质量问题，我社负责调换）

序 言

拥抱智能时代，在未知中寻找确定

2016 年的初秋，我邀请巴曙松教授参加了创新工场的年度峰会，与郭台铭先生等一起，共同讨论中国创投的新方向。我们均认同人工智能正步入黄金时代，这一浪潮有机会重新定义未来人类工作的意义以及财富的创造方式，带来前所未有的经济重塑。彼时，我们和众多的与会人员，甚至当时的开发者和研究者，都难以确切地料到，在此后一年多的时间里，随着数字货币的风起云涌，特别是比特币价格过山车式的大幅涨跌，区块链技术以如此广受关注的姿态闯进公众的视野。时至今日，尽管比特币的狂欢逐渐落幕，其背后的底层技术——区块链已成为信息化领域的前沿技术。在巴曙松教授组织的许多专题电话会议和网上讨论中，有不少就是以区块链和人工智能为主题的。

从技术本质去理解价值，推演未来可能的业务和应用，是另一种视角。所以当新技术出现的时候，我会用较宽容的态度打量这门技术是否拥有此前技术无法达成的能力。我相信区块链技术带来了一些特别的东西，一些前所未有的东西，但区块链技术目前也有明显的局限和不确定性。

区块链技术可以使业务“自证清白”

区块链科技是计算机科学领域中更为底层、更为硬核的部分，是分布式网络系

统，是密码学，也是安全算法和协议。它要打造一套全新的计算架构，基于对等(peer-to-peer，P2P)网络通信架构，用共识算法，实现在线业务计算逻辑的去中心运作和执行。区块链技术最早以加密数字货币的形态被大家认知，试图用货币发行原则，打造一个全球货币系统。这个项目最早从密码朋克圈子开始，逐渐拓展影响到极客社区、计算机工程师、风险投资家，一直到现在更大范围的互联网业务经营者，到传统金融机构乃至世界上一部分国家和地区，只用了 10 年时间。

2018 年夏天有个叫做 Fomo3D 的区块链游戏。游戏规则非常简单：玩家以递增的价格买钥匙，如果一段时间内无人买钥匙则游戏停止。最后一个钥匙买家赢得沉淀资金的一半，另一半资金均价回购所有的钥匙。没错，这就是一个典型的庞氏游戏，游戏说明也没有任何包装遮掩，而是直白的规则描述，项目方完全匿名，没有任何背景可查，分分钟准备“跑路”的样子。在互联网世界里，没有人会相信这样的游戏模式是成立的，因为没有人会相信你宣称的规则会被严格执行。但在区块链的世界里，游戏就在这样一个完全没有信任背书的情况下开始了。无数的玩家参与，非常火爆，甚至严重阻塞了区块链网络的正常吞吐，首轮结束时瓜分了价值 298 万美元等值的以太币。整个游戏过程中，之前约定的所有规则都被严格执行了，没有任何意外。

这就是区块链技术的核心价值之一：区块链系统是一个规则透明、规则不可篡改并保证严格执行的系统，在全部业务信息可形式化的范畴内，让这个信息服务系统可以“自证清白”。这是此前其他技术都不曾具备的“信任共识”特质。“信任”是有价值的。

区块链技术能搭建信任共识，得益于其在计算架构上的本质突破。目前通用的计算模型是 1945 年冯·诺伊曼提出的，假设计算过程始终在一个固定的计算设备上完成，计算系统有统一控制者。这个系统的控制者只要预防好黑客，控制者本人就可以完全信赖系统了。而其他人对这个系统则没有信任的依据，系统控制者也无法向第三方证明系统是可信的，即使开源了也不行，即使用上了可信计算环境技术也没什么本质帮助。区块链技术将这个计算架构进一步拓展，将计算过程同特定的物理计算设备分离。计算过程的实际步骤在全球不同的不可预知的计算设备(节点)上完成，同时通信没有一个固定接入点不依赖于特定 IP 地址。这从根本上避免计算

过程被单一控制方掌控的可能，并且计算过程无法被篡改，也很难被阻止，从而让所有人都可以信赖这个计算系统及其产生的结果。

仍有数个核心问题需要解决

但区块链技术不是万能的，能够“自证清白”地运行是有前提的。它依赖于相关业务的信息必须能够被形式化并体现在系统内部，其涉及的规则和业务状态能够被完整地形式化，否则就是“忽悠”了。而且目前的区块链技术并非完美。为脱离对特定的计算设备的绑定，区块链技术在性能上付出了很大的代价。在不同的节点上间歇完成计算步骤，需要每个节点都准备好计算所需要的上下文和输入数据。在一个计算步骤完成之后，需要每一个节点都同步，并更新上下文。期间涉及大量的冗余信息传递、存储和相应的计算。

区块链技术创造了一个可被任一第三方信赖的计算范式，我相信未来一定还会有更多优秀团队改进这一设计，提升其性能和容量。创新工场的团队 2019 年也刚刚在国际网络系统顶级会议 NSDI[①]2019 上发表了一篇关于区块链全分片架构的论文，给出了可伸缩高性能区块链的优化方案。

所以我们在拥抱区块链之前，需要解决几个核心的问题。这些问题正如巴曙松教授在该书开篇中所提出的：PoW（proof of work，工作量证明）带来的算力消耗问题尚无完美的解决方案；币链的捆绑仍然过紧，与加密货币完全脱钩的区块链应用尚未出现；统一而灵活的监管尚未明确，统一的行业标准有待制定，等等。正是由于这些不确定性，区块链还在被证明的路上，需要理论创新和产业应用的进一步突破，这需要在加强应用的不断试错中，找到更优的发展路径。根据麦特卡尔夫定律，对于区块链这样一种共享性、协议式、需要大规模社会协作参与的颠覆性技术，只有加快应用落地，吸引更多的客户、获取更大范围的认可和使用，才能形成“收益

① USENIX Symposium on Networked Systems Design and Implementation（高等计算机系统协会网络系统设计与实现研讨会），是国际计算机网络顶级学术会议之一，专注于网络和分布式系统的设计原则、实现和实际评估，2019 年的第 16 届会议在美国马萨诸塞州波士顿举办。

递增”的良性循环，真正体现出各自的价值。

信任机制是金融活动的基石

在数据为王的时代，金融领域正在成为创新技术尝试和运用的沃土。从数据量来看，金融作为数字化程度极高的行业，无论是贷款、保险还是投资，都具有高质量的大数据及客观正确的标注成果，各细分市场清晰且不跨界。从技术转化来看，金融行业距离资本较近，容易产生商业价值，利于技术的经济转化和价值提升。具体到区块链技术而言，区块链与金融具有天然的耦合性，从该书的梳理中清晰可见，诞生于金融危机的背景、首个成熟的应用就是比特币这类数字加密货币。以价值传递重构信用机制这一金融活动的基石，区块链在创造价值阶段最有希望首先敲开的是金融的大门。因此，面对复杂多样的金融产品、规模巨大的金融市场，区块链必然会在该领域不断尝试并衍生出大量的投资机会。我相信这也是巴曙松教授选择区块链的金融场景作为该书研究主题的重要原因。

就像巴曙松教授在该书回溯2000年互联网泡沫历史时总结的，泡沫的破灭让人们开始真正反思互联网的应用价值，促使其发展回归到自身的商业化上来，而与此同时，一批真正伟大的互联网公司的种子，也就在那个时候种下了。讨论区块链，我们可能也同样需要抛开比特币的短期大幅涨跌，从不确定性中找出确定性的趋势，在未知中寻找已知。从技术的本质来看，区块链实现了信息的可信传递，这种不可篡改的安全性有望在未来发挥重要作用。

目前，区块链领域正处于从“概念阶段”到“开始应用”的技术拐点，距离“规模化普及”和“很好用”还有诸多瓶颈，这无疑可能引发巨大的争议。布道者对其推崇备至、批评者驳斥其一无是处，鱼龙混杂的市场信息令大众莫衷一是，也可能会阻碍大量投资者和创业者的步伐。在这样一个充满各种分歧与争议的时代，该书从应用场景的现状和趋势出发，从金融传统业务的痛点切入，落脚在一个个具有生命力的项目案例上，以期探索技术可行性约束下区块链技术的赋能空间，无疑具有积极意义。

与其犹豫不前，不如积极拥抱，迎接智能时代的冲击；

与其舔舐恐惧，不如踏出脚步，驾驭智能时代的巨变。

对于未来的世界，最大的不变就是变化本身。智能时代已经来临，未来会有更多美妙的技术纷至沓来。或许多年后我们回望这个时代，会发现巴曙松教授这本新书介绍的区块链技术和金融应用场景，也是通往智能时代的基石。

李开复

创新工场董事长兼 CEO

2019 年 5 月 8 日

目　录

区块链在金融领域的发展简述

近年来，金融科技的发展非常迅速，成为广大学者关注与热议的话题。金融科技以技术为驱动，以数据为依托，通过将金融与科技深度融合，有望创新和颠覆传统金融模式和业务，为企业和个人提供一系列全新的服务。而区块链(blockchain)作为全球金融科技领域备受关注的核心技术之一，亦成为全球各大监管机构、金融机构及商业机构等争相讨论的对象。自2015年以来，全球主流金融机构纷纷开始布局区块链，如高盛(Goldman Sachs)、摩根大通(JPMorgan Chase & Co.)、瑞银集团(Union Bank of Switzerland)等银行业巨头分别成立各自的区块链实验室，发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司[1]。在国内，以京东、腾讯为代表的互联网企业以及各个金融机构也积极投入区块链技术研发和应用推广，区块链在金融领域的发展势头迅猛。“区块链+金融”的研究和应用正在世界范围内如火如荼地展开[2]。

一、区块链的基本技术

区块链的概念和理念由比特币的创始人中本聪(Satoshi Nakamoto)首次提出，作

为比特币等多种数字货币的底层技术，区块链依靠分布式数据存储、去中心化数据传输、加密算法等技术创造了独特的新模式，将一个个区块以链式结构连接，构成一个分布式的共享账本。在这个账本中，由共识算法来决定记账者，由密码学签名和哈希算法保证账本中的交易不可篡改，由时间戳和哈希函数保证区块间的链接不可篡改。可见区块链技术并不是一种新的技术，而是 P2P 网络、共识算法、非对称加密等技术的新型组合。自 2009 年问世以来受到了广泛关注，区块链技术革命性地解决了“拜占庭将军问题”，具有不可篡改、可追溯等安全特性，为我们提供了一种不同于以往的信用创造机制。

区块链有多种分类方式，根据开放程度划分，可分为公有链、联盟链和私有链[3]。如表 1.1 所示，公有链没有准入要求，是一种完全去中心化的、不受任何机构控制的区块链。在公有链中，网络节点可以自由加入、退出、保存和参与更新公共账簿，并就公共账簿更新达成一致。联盟链是多中心结构，只对联盟成员开放，参与用户需要事先经过审查和授权，联盟成员共同保存、更新和维护公共账簿。私有链更像是一种中心化系统，一般由一家机构负责管理整个区块链，在用户准入、共识规则和更新账簿等问题上享有控制权，该机构与各节点之间是隶属或者合作关系，因此一般不需要激励机制。

表 1.1　公有链、联盟链、私有链的比较

	公有链	联盟链	私有链
参与者	所有人	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS①	改进后的分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商	自定义
激励机制	需要	可选	不需要
中心化程度	去中心化	多中心化	中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	3～20 笔/秒	1000～10000 笔/秒	1000～100000 笔/秒
典型场景	数字货币	支付结算	发行、审计

资料来源：作者整理

① PoS: proof of stake，权益证明。DPoS: delegated proof of stake，委托授权证明。具体解释见本章第三部分。

根据独立程度划分，区块链还可以分为主链和侧链。主链是指正式上线的、独立的区块链网络。侧链并不特指某个区块链，而是遵守侧链协议的所有区块链的统称。侧链的技术基础是双向锚定技术，双向锚定技术可以暂时将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放；同样，当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放，从而实现数字货币在主链和侧链之间价值“转移”。侧链的概念是相对主链而言的，所有符合侧链协议的区块链，如比特币区块链、以太坊区块链等都可以成为侧链。需要注意的是，侧链本身也可以理解为一条主链。而如果一条主链符合侧链协议，它也可以被称为侧链。如图 1.1 所示，主链和侧链彼此之间都是独立运转的系统，但彼此又互通有无。

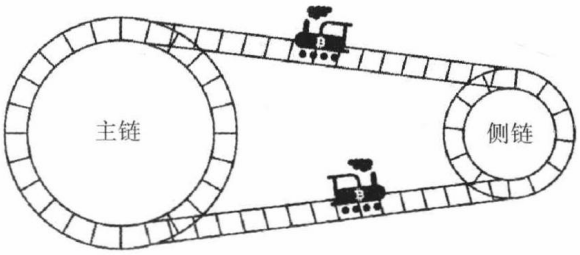

图 1.1　主链和侧链的联系

资料来源：https://www.jianshu.com/p/422741d61181[2019-02-12]

如图 1.2 所示，区块链系统自下而上可分为数据层、网络层、共识层、激励层、合约层及应用层[4]。数据层封装了数据区块、非对称加密、Merkle 树和时间戳等技术；网络层包括了 P2P 网络、传播机制和验证机制；共识层包含各种共识算法，如 PoW、PoS 等；激励层包括数字货币的发行机制和分配机制；合约层主要有脚本代码、算法机制和智能合约；应用层则是区块链的各种应用场景。

图 1.2　区块链技术的架构层

PBFT：practical Byzantine fault tolerance，实用拜占庭容错

(一)数据层——保证数据不可篡改

数据层包含哈希函数、Merkle 树、非对称加密等众多底层技术，实现了数据存储和交易安全两个功能。数据的连续分布式存储主要依靠 Merkle 树和时间戳技术来实现，交易安全则由数字签名、哈希函数和非对称加密等多种密码学算法和技术来确保，保证了交易在没有中心信任节点的情况下可以安全地进行[5]。

1. 时间戳

时间戳是一种能够表示一份数据在一个特定时间点已经存在的技术。它为用户提供一份电子证据，以证明用户的特定数据产生的准确时间。通过时间戳可以确保数据存储时的连续性、完整性和不可修改。每一笔数据登记后形成一个数据块，每一块数据在存储时都会引用上一块数据的哈希值，并盖上当前存储的时间戳，这三种数据信息一并储存，按时间串成链，就构成了不可逆向修改的“数据链”。

2. 哈希函数

哈希算法(图 1.3)是信息技术领域的核心技术，它实际是一种压缩映射，可以把任意长度的数据转化成固定长度为 128 位的二进制值，即哈希值，其优点如下。

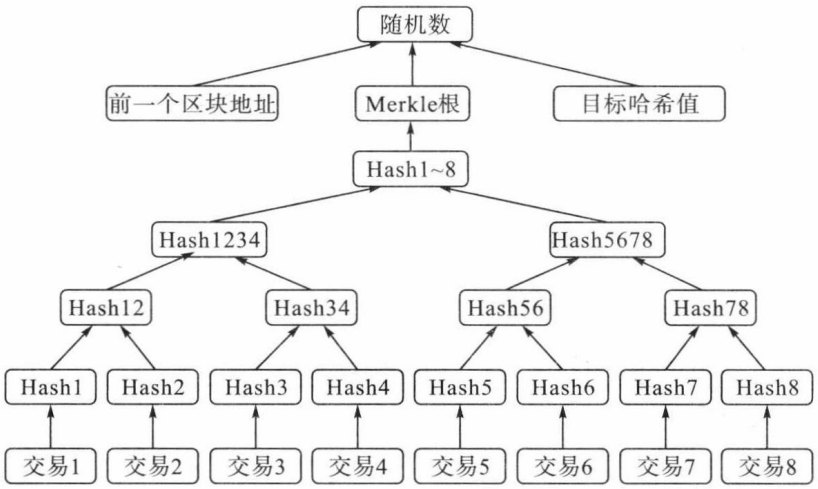

图 1.3　哈希算法结构图

1)哈希函数运算是不可逆的，即 A 经由哈希运算生成 B，而由 B 无法推出 A，即保证了数据的隐秘性。

2)输入值即使只相差一个字符，输出值也会千差万别，即保证了数据的不可预测性。

3)哈希函数会将任意大小的字符串在一个固定长度的时间内生成一个固定长度的输出值，即哈希值，比如“hello world”和“how are you”虽然哈希值不一样，但是它们的哈希值长度是一样的，而且其哈希运算的时间是一样的，即保证了数据的可控性。

3. Merkle 树

Merkle 树是一种二叉树，由 Merkle 根节点、一组中间节点和一组叶节点组成。最下面的叶节点包含存储数据或其哈希值，每个中间节点是它的两个子节点内容的哈希值，根节点也是由它的两个子节点内容的哈希值组成。Merkle 树的特点是，底层数据的任何变动都会传递到其父节点，一直到树根。

假设 A 收到 B 传过来的文件，A 需要确认文件是否正确或者文件是否损坏。A 可以对文件进行一次哈希运算，然后和 B 给的哈希值相比较，从而就可以知道文件有无损坏。但是如果文件达到几个 GB，为了保证文件传输的效率和稳定性需要把这个文件分成很多小的数据块进行传输，如果一一对照每个数据块的哈希值将是一个很大的工作量，这时 Merkle 树的作用就体现出来了。如图 1.4 所示，交易经过两两哈希运算，可以得到 Merkle 根，在实际应用中，我们只要确保获取一个正确的 Merkle 根，再计算比较文件的 Merkle 根，就可以清楚是否接收了正确的文件。

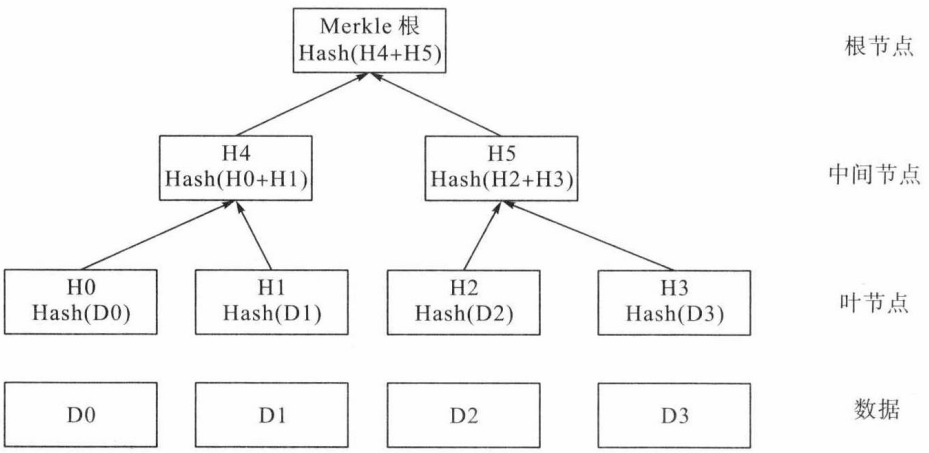

图 1.4　Merkle 树的机制

资料来源：邹均，张海宁，唐屹，等. 区块链技术指南[M]. 北京：机械工业出版社, 2016

4. 非对称加密

非对称加密算法是为确保交易安全的进一步加密机制[6]。如图 1.5 所示，非对称加密过程会使用公钥和私钥两个非对称的密码。非对称密钥对具有两个特点：一是公钥和私钥是一一对应的关系；二是私钥是必须保密的，无法通过公钥推算出相应的私钥。非对称加密技术主要应用在以下场景。

1) 信息加密场景：假设 A 给 B 发送一个信息，A 可以使用 B 的公钥对信息加密后再发送给 B，B 利用自己的私钥可以破解这个信息。

2) 数字签名场景：A 也可以使用自己的私钥对信息加密后再发送给 B，B 使用 A 的公钥可以破解这个信息。