Block Chain

西南财经大学中国区块链研究中心

区块链+时代

区块链在金融领域的应用

帅青红　段江　夏可　编著

Era

西南财经大学出版社
Southwestern University of Finance & Economics Press

西南财经大学中国区块链研究中心

Block chain + Era

the Application of Block Chain in the Financial Field

区块链+时代

区块链在金融领域的应用

帅青红 段江 夏可 ○编著

编写组组长 帅青红
编写组副组长 段 江 夏 可
编写组成员 杨 成 康 立 罗旭斌
胡宏鑫 杨 启 王维婷
肖志扬 陈 郁 熊辰辰 等

西南财经大学出版社
Southwestern University of Finance & Economics Press
中国·成都

图书在版编目(CIP)数据

区块链+时代:区块链在金融领域的应用/帅青红,段江,夏可编著.—成都:西南财经大学出版社,2018.6
ISBN 978-7-5504-3531-5

Ⅰ.①区… Ⅱ.①帅…②段…③夏… Ⅲ.①电子商务—支付方式—应用—金融—研究 Ⅳ.①F83

中国版本图书馆CIP数据核字(2018)第124170号

区块链+时代:区块链在金融领域的应用

QUKUAILIAN+SHIDAI:QUKUAILIAN ZAI JINRONG LINGYU DE YINGYONG

帅青红 段江 夏可 编著

责任编辑:汪涌波
封面设计:何东琳设计工作室
责任印制:朱曼丽

出版发行	西南财经大学出版社(四川省成都市光华村街55号)
网　　址	http://www.bookcj.com
电子邮件	bookcj@foxmail.com
邮政编码	610074
电　　话	028-87353785　87352368
照　　排	四川胜翔数码印务设计有限公司
印　　刷	成都金龙印务有限责任公司
成品尺寸	165mm×230mm
印　　张	16
字　　数	245千字
版　　次	2018年6月第1版
印　　次	2018年6月第1次印刷
书　　号	ISBN 978-7-5504-3531-5
定　　价	88.00元

前言

自2008年比特币诞生以来，区块链概念逐步受到社会各界的关注。经过近十年的发展，区块链在2018年迎来了爆发的一年，其在行业中的应用开始显现。金融业顺势而为，也大力开展区块链的应用与研究。

有人把区块链比作互联网的4.0时代，因为区块链是基于互联网的一项新技术。其实它也和互联网一样，是一项基于底层的基础技术。从长远来看，尽管区块链在概念提出之初存在资本过热、ICO虚高等问题，但它毕竟是一项基本技术，有为经济和社会系统创造新基础平台的巨大潜能。区块链是产业互联网向价值互联网转变的重要基石，是现代数字货币体系的重要技术之一。它以密码学技术为基础，通过分布式多节点“共识”机制，可以“完整、不可篡改”地记录价值转移（交易）的全过程。区块链采用的具体技术包括密码学、共识协议、博弈论、数据存储、P2P通信等，是多种已有技术的融合创新。

国内互联网巨头特别是B（百度）A（阿里巴巴）T（腾讯），纷纷开展了区块链技术与应用的研究。

腾讯从2016年起就开始自研区块链底层技术，2017年完成底层技术完整积累，目前已进入商业应用阶段，进入金融、公益、法务、物流等多个领域。早在2016年4月，腾讯推出了区块链落地“公益寻人链”，第一次实现各大公益平台的信息共享；同年5月，微众银行就在深圳参与发起了金融区块链合作联盟——金链盟，其目的是共同开发适用于金融机构的联盟区块链；在金融和公益之外，腾讯

还在2017年9月和英特尔达成合作，宣布双方将共同开发区块链技术，用来提高物联网场景中的安全防护能力。腾讯发布的《腾讯区块链方案白皮书》披露了其区块链整体架构：底层是自主研发的Trust SQI平台，中层的Trust Platform是构建区块链应用平台产品，顶层的Trust Application则是用来向最终用户提供区块链应用。

百度在2016年6月投资美国区块链技术支付公司Circle；2017年5月，百度金融与其他金融机构联合发行了区块链技术支持的ABS项目，发行规模4.24亿元；2017年9月，“百度—长安新生—天风2017年第一期资产支持专项计划”发行，是国内首单场内公募ABS；2017年10月，百度金融正式加入Linux基金会旗下超级账本；2018年1月，百度推出区块链开放平台BaaS，该平台被命名为“百度Trust”，主要用来帮助企业联盟构建属于自己的区块链网络平台，目前已经支撑了超过500亿元资产的真实性问题。

阿里巴巴已基于区块链技术去中心化、分布式存储及防篡改的特性落地了多个应用场景，包括公益、正品追溯、医疗等，且主要集中于区块链的底层技术，如“共识”机制、平台架构、隐私保护和智能合约等。2016年7月，蚂蚁金服将区块链技术应用于支付宝爱心捐赠平台；2016年10月，阿里与微软、小蚁、法大大等合作开展“法链”；2017年3月，阿里与普华永道展开合作，应用区块链技术实现食品可溯源；2017年8月，阿里健康与江苏常州合作推出“医联体+区块链”试点项目；2017年10月，蚂蚁金服技术实验室宣布开放区块链技术，支持进口食品安全溯源；2017年11月，阿里巴巴与蚂蚁金服宣布承建数字雄安区块链实施平台；同月，天猫国际宣布升级全球原产地溯源计划。从合作项目来看，目前蚂蚁金服已经成为阿里系内部对区块链应用最深的团队。

区块链技术为我们解决信任和价值传递问题提供了一个新颖而实用的方案，我们可以不用只是依靠纸质合约的所谓约定，通过区块链技术，可以将里面的条款编写成智能合约，部署在区块链系统

上，系统将会严格地按照事先的约定条件来执行，没有人能够去篡改，也没有人能够撕毁。

区块链是数字货币的技术载体，是发展数字经济的重要形态，它不仅可以重塑货币市场、支付系统、金融服务及经济形态的方方面面，而且将会改变人们生活的多个领域。金融行业由于是最数字化的行业，所以也被认为是可以最先应用区块链技术的行业。我国中央银行也正在研讨数字货币方案。而大部分区块链创业者的目标，也瞄准了各种各样的金融行业应用。目前比较成熟的有支付、跨境汇款、众筹、数字资产交易等，还有几十个金融应用场景正在各大金融机构的区块链创新实验室里进行试验和验证。因此，区块链技术将日益成为整个数字化社会运行的基础平台，将把我们带入价值高速公路时代。

随着人们对区块链技术的认识的加深，大家终将意识到，与其说这是一类技术，不如说这是一类思想，它代表了一种公正透明、信任协作的价值观。我们将沿着历史发展的路线，从最初的黄金屋（加密数字货币）走到智能合约，再走向更有前景的区块链社会。

文明的发展就像河流一样，每时每刻都静静地朝着一个方向流动着，而总会在某一刻，一颗包裹着新科技的石子落进了河流中，激起了新文明的浪花，并且产生了连续的波动，波动所到之处，皆会发生改变，我们就在这一次又一次的波动中，从遥远的蛮荒，奔向文明的未来。区块链技术就是这其中的一颗石子，就在某年某月某日，它就那么滚落了进来，在它的附近开始激起了一些涟漪，然后有人发现这种技术真是太妙了，它能创造出数字货币，能创建信任网络，能用它来解决太多的问题。于是产生了越来越多的波动，越来越多的人开始讨论这种新思想，传统的思路开始发生变革，难以解决的问题开始有了新方案，它将开始爆发。让我们做好准备，我们每个人都将会成为新技术文明中的一员，站在风口浪潮之前，迎接这已到来的文明的波动！让我们一起迎接区块链时代的来临吧！

在本书的撰写过程中，参考了许多中外有关研究者的文献和著作，在此一并致谢。本书编写时间仓促，笔者阅览、借鉴了大量国内外的出版物和网上资料，由于文中体例限制而未一一注明，或在参考文献中有个别未予列出，在此谨向诸多学者、同仁表示由衷的敬意和感谢。

笔者非常感谢所有关心、支持和帮助过笔者的朋友、同事和家人，在此一并致谢！

在本书的编写过程中，西南财经大学中国区块链研究中心、“互联网金融创新与监管协同创新中心”——2014 四川省协同创新中心、“金融智能与金融工程”——四川省重点实验室、“中国支付体系研究中心”、西南财经大学互联网金融与支付研究所给予了大力支持，在此表示衷心的感谢！特别感谢成都摩宝网络科技公司（MO宝支付）长期以来提供的大力支持与帮助！

本书可作为高等院校电子商务、金融学、信息管理与信息系统、数据科学与数据技术、互联网金融以及其他相关专业的教学和参考用书，也可作为对区块链、电子商务金融学进行研究学习的参考读物。

区块链技术及其应用，是一个新生事物，也是一个不断创新的领域，许多模式尚在发展和探讨之中，观点的不同、体系的差异在所难免。由于笔者的水平有限和这门技术的特殊性、内容新、范围广，书中难免有不尽如人意和错误的地方，真诚地希望能得到专家、同仁和读者的指正，以利于今后修改和订正，便于进一步完善。联系方式：E-mail:3035216254@qq.com.

帅青红

2018 年 5 月 17 日于光华园

目 录

1 区块链的起源

1.1 比特币的诞生

提及区块链的起源，就不得不了解比特币的诞生。作为目前世界上应用区块链技术最成功的项目，比特币自诞生之初就充满了神奇的色彩并引来颇多争议，而且伴随着其价格的大涨而越来越多地出现在公众媒体与大众的视野中。2018 年是比特币问世的第十年，也是区块链技术出现的第十年。区块链从最初的默默无闻到如今的震惊世界，并成为未来科技主流发展的方向之一，这期间比特币到底经历了什么？让我们来短暂地回顾一下。

在 2008 年 11 月，也就是全球经济危机全面爆发之际，一个网名为“中本聪”的人通过互联网发表了一篇题为《比特币：一个点对点电子现金系统》（*Bitcoin: A Peer-to-Peer Electronic Cash System*）的文章。在这篇文章里，中本聪构想了一种基于区块链（block chain）的比特币系统，没错，如今大火的区块链技术，其创造者正是中本聪。

这篇研究报告最初只是在一个隐秘的密码学讨论小组中提出的，随后他又开发出最早的比特币发行、交易和账户管理系统。在 2009 年 1 月 3 日，中本聪挖掘出了第一个区块链，最初的 50 个比特币宣告问世。至此，比特币这套系统可以算是真正诞生了。而这个最初的区块链也被称为“上帝区块”，被比特币的信仰者与追随者们视为一切的开端。

1.1.1 神秘的创始人

所有人都知道比特币的创始人化名为“中本聪”，但值得一提的是，直到现在，他的真实身份依旧扑朔迷离。相关专家从未听说过他，有关他的信息也寥寥无几。

网络上的简介显示他居住在日本，但他的电子邮箱地址来自德国的一个免费服务站点。他很少透露自己的信息，在网上谈论的话题也只限于源代码技术的讨论。2010 年 12 月 5 日，在比特币使用者开始要求维基解密接受比特币捐赠后，中本聪首次参与到了技术业务以外的话题，

并在论坛发帖表示“这个项目需要逐步成长，这样软件才能在这个过程中不断增强。我呼吁维基解密不要接受比特币，它还只是一个萌芽阶段的小型测试社区。在这个阶段，如果不能妥善处理，只会毁了比特币”。

接下来，就像他的神秘出现一样，中本聪再次消失了。格林尼治时间2010年12月12日6点2分，他在论坛发了最后一个帖子，谈到软件最新版本中几个无关紧要的细节，电邮回复也完全终止，只与少数几个核心开发者还保持间断联系。而到了2011年4月26日，他对核心开发者安德烈森的邮件也不再回复了。

安德烈森告诉编码员，中本聪希望他们在公开谈论比特币时应淡化“神秘创始人”的话题。

作为比特币的创造者，中本聪本人据说拥有约100万个比特币，按照如今的市值换算，价值至少有100亿美元，即便放在顶级的富豪圈子里也绝对是巨头级的人物。而因为区块链的不可篡改性与私钥签名，这些最初的比特币也是能够证明他身份的最有力的证据。

人们将很多在区块链上有着杰出技术的人猜测为中本聪。首个获得此殊荣的，是一个叫多利安·S. 中本聪的日裔美国人。多利安被绑上“比特币之父”的标签是在2014年。国外媒体挖出来的情报显示，此人毕业于加州州立理工大学，获得物理学学士学位，曾经供职多家公司，参与过国防保密项目，从事过很多机密工作，这些“履历”都很容易让人将其同比特币联系起来。不过，尽管媒体一度笃信多利安就是比特币的发明人，然而多利安始终不承认自己同比特币的诞生有关。实际上，媒体找到多利安时，后者正过着穷困潦倒的生活，怎么看都不像是一个坐拥近百万个比特币的“隐豪”。而决定性的转折是那个曾经消失了近5年的“中本聪”突然借互联网重现江湖，发了一则极为简短的消息：“我不是多利安。”

在多利安被排除是中本聪的可能性后，人们并未放弃寻找“比特币之父”的努力。2016年5月，第二个中本聪很快就“浮出水面”。这回被冠上“比特币之父”的，是一个名叫克雷格·赖特的澳大利亚企业家。值得一提的是，赖特是主动公开站出来宣称自己就是“中本聪”

的。现实中的赖特是一名计算机科学家兼商人，曾在澳大利亚证券交易所、会计师事务所 BDO Kendalls 及多个信息技术公司任职，其一大成就是他于 1999 年设计了世界上第一个网上赌场 Lasseter's Online。重点还在于，赖特本身就是一个比特币大玩家，而他名下还有一家从事数字加密货币的公司。那么赖特为何要公开“承认”自己就是比特币的发明者呢？对此，赖特的说法是为了结束大家多年来的猜想。当然，空口无凭，赖特也出示过所谓的证据，包括一份用“中本聪”账号的私钥所产生的签名，不过这只是比特币第一笔交易的密钥签名，发生于比特币出现后的第 9 天，并不是与最初那 50 个“上帝区块”比特币有关的密钥，不具备实际说服力。

很快，赖特的信誓旦旦就迎来了考验——澳大利亚政府长期对比特币在内的数字加密货币持近似于敌对的态度，甚至赖特过去好几次尝试在澳大利亚开设数字货币相关业务都被政府阻挠，而这回赖特的高调终于引发了政府的不爽，于是以“税务调查”的名义出动联邦警察搜查了赖特的公司和住所。就在政府的搜查行动结束后没多久，赖特以无法应对外界的质疑为由删掉了他用来证明自己是比特币发明者的证据，淡出了公众的视线。也有人认为这不过是赖特在炒作自己的骗局被戳破后为退场找的借口而已。

而目前最后一个被认为可能是中本聪本尊的人是哈尔·芬尼。哈尔·芬尼在 2014 年因为“渐冻症”去世，并且死前他选择参与名为“人体低温贮藏”的实验项目，也就是将自己的尸体用零下 195 摄氏度的超低温保存起来，以期未来人类科技进步到能够让人起死回生时再让自己复活。撇开“人体低温贮藏”先驱实验者的身份不提，之所以如今有人将芬尼同比特币的诞生联系起来，是因为有很多事实都从侧面证明了这点：芬尼生前乃是 IT 界公认的“技术大拿”，他是 PGP（开创性的加密软件）的第二个开发者，创造了匿名软件 Tor 的前身。

此外，中本聪进行第一次比特币的交易对象正是芬尼，并且芬尼当时还是除中本聪以外最早一批为比特币的开源项目提供技术支持的开拓者之一。有人认为，中本聪其实就是芬尼用来掩饰其真身所特意创造的