区块链金融

未来金融的核心竞争力

刘振友◎著

BLOCKCHAIN FINANCE

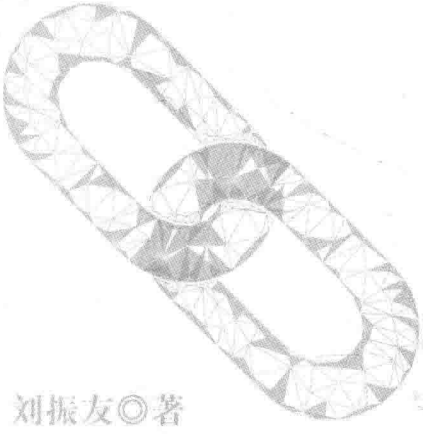
以最简单的方式
让你轻松读懂区块链金融

互联网飞速发展，掀起了“区块链”风暴
很多人都从“游戏圈”转战到“金融圈”“币圈”

文化发展出版社
Cultural Development Press

区块链金融

未来金融的核心竞争力



刘振友◎著

BLOCKCHAIN FINANCE

文化发展出版社
Cultural Development Press

图书在版编目（CIP）数据

区块链金融 / 刘振友著. — 北京 : 文化发展出版社, 2018.8

ISBN 978-7-5142-2315-6

Ⅰ. ①区… Ⅱ. ①刘… 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（2018）第 143337 号

区块链金融

刘振友 著

出 版 人：武 赫

责任编辑：孙 烨　　责任校对：岳智勇

责任印制：杨 骏　　排版设计：韩庆熙

出版发行：文化发展出版社（北京市翠微路 2 号　邮编：100036）

网　　址：www.wenhuafazhan.com

经　　销：各地新华书店

印　　刷：北京市兆成印刷有限责任公司

开　　本：710mm×1000mm　1/16

字　　数：225 千字

印　　张：16.5

印　　次：2018 年 8 月第 1 版　2018 年 8 月第 1 次印刷

定　　价：58.00 元

I S B N ：978-7-5142-2315-6

前　言

“区块链”（Blockchain）这个词刚产生的时候，对很多人来说仍是一个比较新鲜的名词，但在2015年下半年，“区块链”开始成为社会热点词汇，也因此引起了社会各界的广泛关注。那么“区块链”究竟是什么呢？简单来说，“区块链”就是比特币的底层技术，像一个分布式数据账本一样记载着所有的交易记录。

“区块链”一词最早的提出还要追溯到2008年。它首次出现是在中本聪发表的《比特币：一种点对点的电子现金系统》一文中。文中提到了区块链技术可以应用到金融服务、社会生活等众多领域中，比特币是区块链技术首次大规模应用到全球网络中的一个典型案例。随着互联网的迅速发展，区块链技术在各个领域的应用也给一些传统的模式带来了颠覆性的改变。目前，区块链技术研究领域正在迈入新的阶段。许多国家、政府以及企业已经开始关注区块链这一底层技术，并且已经开始对这一技术进行了积极的探索。首先，从政府和监管层面来看，包括联合国社会发展部、中

国人民银行、英国政府、美国证券交易所在内的组织和机构纷纷开始对区块链发声；其次，从企业层面来看，许多跨国行业巨头与创业公司正在争先恐后地进军区块链领域，并且带动了新一轮创业和创新的浪潮。

根据安永会计师事务所的统计资料显示，截至2016年年初，全球已经诞生了917家区块链领域的创业公司，全球在区块链领域的投资累计已经超过了15亿美元。以花旗银行、纳斯达克为代表的各行业的巨头且已经开始踏入了区块链技术的实验室阶段，进行了区块链在多个场景中的探索式的应用实践研究。除此之外，一些学术研究机构和转移咨询服务机构等其他研究力量也开始对区块链技术以及未来的发展趋势进行研究，区块链技术从一个陌生的词汇加速走进了大众的视野之中。

本书立足于区块链技术的起源和发展，详细分析了区块链技术在金融业、社会生活等领域的巨大作用和影响，具体阐述了区块链技术在各行各业的应用场景和应用案例，能让读者更直观地感受到区块链这一颠覆性技术所带来的改变，最后展望区块链技术的未来和发展趋势。

全书共分为三个部分。第一部分以“拜占庭将军问题”为导入，讲述了区块链技术的源头、概念、发展态势、内在特性、技术原理等基础性内容；第二部分以“区块链+”为导入，讲述“区块链+金融服务”“区块链+数字货币”“区块链+共享金融”“区块链+加密数字资产”“区块链+供应链”等方面给区块链带来的影响以及具体的应用案例，详细分析了区块链技术在这些领域的具体作用和实质性的改变；第三部分是以区块链技术的发展和其在各个领域的广发应用为导入，对区块链技术的一个展望，讲述了区块链技术给未来商业带来的影响，并且具体阐述了区块链技术将会如何重构未来的商业模式。

本书面向所有对区块链技术感兴趣、希望了解区块链技术的读者。无论你是对区块链这一技术完全陌生的读者，还是对区块链技术有浅显认识的读

者，本书都会给你提供一个全新的机会认识区块链这一颠覆性的技术。本书从最基本的概念讲述，并且结合实际运用让你更深刻体会到：区块链技术到底是什么？它的原理是什么？它有着怎样颠覆性的特性？它是如何运用到实际生活中的？它会给我们的生活带来怎样的改变？在本书中，这些问题都会被进行详细的阐述。

区块链技术是科技时代发展的趋势，因此该技术有着广阔的应用前景，但是区块链技术也存在着自身的局限性。所以，我们应该科学理性地看待区块链技术，必须准确、深入地把握区块链技术的方方面面。希望广大读者可以通过阅读本书，更深入地了解区块链技术，并能够准确理解和把握区块链技术的发展趋势，从而紧随潮流，走在时代的最前列。

目　录

第一章　弯道超车，区块链金融时代已来

第一次工业革命带来了蒸汽机，第二次工业革命产生了电力，第三次工业革命的主题是互联网，那么区块链则是拥有带来第四次工业革命可能性的新型技术，并且这场工业革命的第一战场必定会是金融领域，它将为世界带来一个全新的金融时代。

区块链的源头——“拜占庭将军问题”

区块链作为新型数字货币“比特币”的核心，在全球互联网发展中起到了巨大的作用。由于它的高容错性以及去中心的结构，世界的互联网金融贸易都为此而发生了转变，促使“互联网+金融”跨入一个新时代。

区块链模型技术的应用，让互联网金融可以跨越第三方信任机构，在节点与节点之间建立直接的信任关系，因此达到节点与节点之间能够直接进行交易的目的。这种模型彻底规避了互联网金融交易之间，依赖第三方信任机制而造成的中间浪费。因此，区块链逐渐被许多人认识到其可能产生的巨大

影响力。然而，区块链作为计算机技术的新型模型，却起源于一个看似简单的“拜占庭将军问题”。

拜占庭是东罗马帝国的首都，因此东罗马帝国又称为拜占庭帝国。在战争时期，拜占庭帝国想要攻打一个强大的敌国，一支军队在战争中往往毫无胜算，必须要让其他各个地方的军队同时攻打才能胜利。因此，拜占庭帝国就发送信息让分散在广阔国土上的各支军队能步调一致，一起攻打。但是，要想在各个军队的将军之间传送信息，只能依靠信使。军队中出现叛徒总是不可避免，而叛徒的“虚假信息”往往会让将军的决策产生混乱，进而造成军队的行动很难达成一致。因此，拜占庭帝国的将军们必须找到一个算法，让他们在交换信息的过程中能够选择正确的信息，进而能够让他们的步调一致。而这个算法的实现必须建立在以下几点的基础之上。

首先，要保证信道不能被破坏，也就是说，不能出现“拜占庭失效”的状况。“拜占庭失效”指的就是在消息传递的过程中，某位将军向另一位将军发送信息，而由于信道被破坏等原因致使另一位将军没有收到信息，而派出信使送出信息的将军也不知道另一位将军没有收到信息的事情。因此，只有确保信道不被破坏，每个信使都能将信息送到将军的手中，各个将军才能收到信息。无论信息真实虚假，他们都要进行审核对比，最终判定出正确的信息并执行。

其次，所有将军都必须在实现同一目标的基础上进行判定——一起进攻某一目标或者一起撤退。假设有五支军队，那么必须确保这五支军队的将军都是在“攻打A国”的基础上传递信息，而不是在有的军队要去攻打A国，有的军队要去攻打B国……这种无统一目标的基础上判定。因为目标不统一，信息传递最终做出的判断也毫无意义，甚至会造成更加混乱的局面。

最后，要满足“叛徒”的总数不能超过1/3。假设有三位将军准备一起进攻同一敌人，其中有一位将军是叛徒，那么总有一个将军会收到一个进攻命

令和一个撤退命令，导致收到两个不同命令的将军无法判定消息的准确性。因此，如果叛徒的总数大于等于1/3，那么“拜占庭将军问题”就是一个无解的问题。

“拜占庭将军问题”在满足了这三点要求的基础之上，就可以分别从“口头”和“书面”来解决了。

在口头传递上，信息要满足能够准确送达、知道由谁传送以及所有的将军、每个将军的信使都在传送信息这三点要求。而后，只要叛徒数量少于1/3，每个将军在收到信息后便派出许多信使给其他将军传送消息，传送的对象不包含派信使给自己传递该信息的将军。因此，用这个办法，口头传递就可以解决拜占庭问题。

在书面传递上，在口头信息传递的要求上增加两点。要保证每个将军都有个人“签名”，而且签名不可以被模仿以及所有人都能识别各个将军的签名，也就是说，所有人都能根据签名来识别信息是由哪位将军传送的。在此基础上，保证在至少有2/3将军是忠诚的情况下，收到信息的将军将派许多信使给其他将军传送信息，传送信息的对象同样也要除去派信使给自己传递该消息的将军，进而“拜占庭将军问题”依靠书面传送就可以解决。

事实上，“拜占庭将军问题”是由图灵奖得主莱斯利·兰伯特（Leslie Lamport）提出的关于计算机通信中点与点之间信息传输的问题。也就是说，在分布式的计算机网络中存在着大量的故障节点，而且这些节点在不停地向其他节点散布错误信息，但是其他节点要在这些错误节点的误导之下达到正确一致的目标。也就是说，“拜占庭将军问题”就是在“无核心”的基础之上，提出的一个错误节点可以不受限制地做任何事情的模型。因此，“拜占庭将军问题”中所设想的分布式结构里，在没有第三方信任机构的情况下，能达到彼此信息正确、值得信任的结局非常重要。

“拜占庭将军问题”可以进一步延伸到各个领域。人们在互联网上进行数

据交易的时候，总会习惯性依赖强大的第三方平台来进行信任担保。然而，这些解决人们信任问题的第三方正在逐渐失效，因为总有黑客能够抓住第三方平台的漏洞进行金融诈骗。“拜占庭将军问题”中的“叛徒”就是互联网金融交易中的“骗子”，如果第三方平台出现了大漏洞或者为了规避过多的步骤将第三方信任机构撤走，“叛徒”就会利用信息在没有第三方信任机构的担保之下进行“行骗”。在不去花费大量时间、资源揪出这个“叛徒”的情况下，能够让交易者双方都彼此信任、进行正常交易的方式就是区块链。

区块链之父——中本聪

一名代号“中本聪”的黑客，利用自创的模型完美地解决了复杂的“拜占庭将军问题”，而他解决“拜占庭将军问题”的自创模型就是区块链。

2008年，中本聪（Satoshi Nakamoto）发表了一篇神秘论文——《比特币：一种点对点的电子信息系统》。这篇论文让基于区块链技术的虚拟货币在国际上掀起了疯狂的浪潮，进而让更多的人开始关注“中本聪”。这篇没有在任何权威学术刊物上发表过的论文摘要如下：

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（Digitalsignatures）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的产生。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，而且被看作是来自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）可以随时离开或重新加入网络，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。

由此可以看出，比特币在中本聪的第一篇论文里就有了初步的概念，让基于区块链技术的特殊数字货币“比特币”在今后的发展中能够逐步稳固。在2009年，初始比特币算法软件在全球推出，并且这款软件是开放的，任何软件工程师都可以下载应用并进行修改。开源式的比特币算法软件，让更多人疯狂地参与到比特币的“挖掘”工作中，并且让比特币的价格出现了剧烈的波动。

全球最大的战略咨询管理公司麦肯锡（McKinsey & Company）在提交给美国联邦保险咨询委员会的报告中明确指出区块链很可能会颠覆广泛行业。而且，报告也表明“该行业的大部分人都认为区块链技术将会在3～5年产生‘实质性影响’”，因此也肯定了中本聪作为“区块链之父”，为社会各个行业都可能带来一场不可小觑的革命。

然而，这名创造了巨大虚拟货币财富的人却至今都不肯暴露他的真实身份。

2014年3月6日晚间消息，美国一名自由撰稿人称她已经找到了中本聪——一名隐居在洛杉矶圣贝纳迪诺的日裔美国人，而他的真实姓名就是“中本聪”，并且他曾为美国军方执行过保密工作。当记者找到他的时候，中本聪已经穷困潦倒，看上去完全不像手握100万个比特币的人，这些比特币最少价值4亿美元。这名记者与中本聪聊过许多话题，然而在记者提到比特币之后，中本聪就再也没给过任何回复。

2014年9月，由于中本聪的电子邮箱长期未使用，一名黑客入侵了中本聪的电子邮箱盗取了“中本聪的秘密”，并在网络上进行贩卖。自此之后，总有许多自称“中本聪”或者被媒体、圈内相关人员判定为“中本聪”的人出现，然而这些人最终往往被揭露他们并不是“中本聪”。

2015年12月8日，澳大利亚信息安全专家克雷格·史蒂夫·莱特被指认为是“中本聪”。9日下午，澳洲警方就搜查了他的家和办公室。澳洲警方宣称，这次搜查与比特币无关，而是为了调查莱特的税务问题。而后，多年未露面的中本聪在Linux基金会的比特币开发者群组中发出了一封名为“这次你们依旧没有猜对”（Notthisagain）的邮件。

也就是说，虽然中本聪是比特币的创始者，并且他还持有大量的比特币。然而，在大多与区块链相关的人群之中，中本聪本人就如同是一个由“密码”与“金钱”组成的精密“系统”。没有人能破解出这个系统的密码，获知他的真实身份，甚至“中本聪”到底是一个人还是一群人，或者他连“人”都不是，只是一部拥有复杂计算功能的终端，都没有人能够确定。而他又“凭空”创造了巨大的数字财富，并让这“凭空”创造的财富能够在社会上流行起来，由一开始每比特币近乎“0”的价格，涨到了每比特币上千美元的价格。而比特币从被第一次“挖掘”开始，仅仅用了5年左右的时间就