BLOCKCHAIN: RESHAPE THE ECONOMY AND THE WORLD

区块链

重塑经济与世界

徐明星 刘勇 段新星 郭大治 – 著

中信出版集团 · CHINACITICPRESS

BLOCKCHAIN

RESHAPE THE ECONOMY AND THE WORLD

区块链

重塑经济与世界

徐明星 刘勇 段新星 郭大治 – 著

中信出版集团 · CHINACITICPRESS · 北京

图书在版编目（CIP）数据

区块链：重塑经济与世界／徐明星等著．—北京：
中信出版社，2016.6
ISBN 978-7-5086-6211-4

Ⅰ.①区… Ⅱ.①徐… Ⅲ.①电子商务—支付方式—
研究 Ⅳ.①F713.36

中国版本图书馆 CIP 数据核字（2016）第 102180 号

区块链：重塑经济与世界

著　　者：徐明星　刘勇　段新星　郭大治
策划推广：中信出版社（China CITIC Press）
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲 4 号富盛大厦 2 座　邮编　100029）
（CITIC Publishing Group）
承 印 者：北京诚信伟业印刷有限公司

开　　本：787mm ×1092mm　1/16　　印　　张：14.5　　字　　数：240 千字
版　　次：2016 年 6 月第 1 版　　印　　次：2016 年 6 月第 1 次印刷
广告经营许可证：京朝工商广字第 8087 号
书　　号：ISBN 978-7-5086-6211-4
定　　价：58.00 元

前　言

2008 年，一个神秘的人物，直至今日只闻其名未见其人的“中本聪”通过一篇未在任何学术期刊上公开发表的神秘论文，把比特币带到这个世界。诞生于虚拟世界的比特币代表了人类对于数学算法的一种共识，基于这种共识机制，即使没有任何政府信用背书，比特币仍然获得了世人的认可，不论是从最初几十个比特币换取一份比萨，还是 2013 年 12 月 1 日，比特币的单价超越一盎司黄金的价格，比特币都在向世人展示其作为价值尺度的一面。尽管比特币价格的暴涨暴跌使其减弱了在更大范围内作为货币应用的可能，但比特币向世人展示了一种不需要中介却可以实现价值传递的可能性。这种可能性就是区块链。

正如梅兰妮·斯万（Melanie Swan）指出的那样，比特币和区块链包括三个层次的内容：区块链底层技术、协议和加密数字货币。区块链技术是点对点通信技术和加密技术的结合，基于区块链技术生成的区块链本质上是一个去中心化的分布式账本数据库；在这个数据库的基础上可以开发出数目繁多的应用，这些应用通过协议层面建立共识机制实现各种功能；最后在应用层面，客户可以实现无需中间权威仲裁的点对点的交互，当然包括比特币。有人用“组织形式上的去中心化和逻辑上实现完美一致性的技术”来形容区块链技术，也有人用“下一代全球信用认证和价值互联网的基础协议之一”来阐述区块链的特点，总体而言区块链技术的应用主要包括如下内容。

一是金融产品创新。由于金融产品基础结构的主要内容就是关于参与

各方权利义务的约定，货币、债券、股权等各类金融产品都可以通过协议层建立共识机制形成与传统金融产品类别相对应的创新金融产品。由于区块链形成了可以独立存在的共识机制，因此区块链技术具有自动执行协议的功能，人们将此类协议归类为智能合约。智能合约实施的基础是共识机制而非中心化的验证，使得智能合约的执行成本降到最低、执行效率大大提升。基于智能合约运行的创新金融产品具有高透明度、高安全性、高效率的显著特征。基于上述优势，区块链技术对金融行业的改变将是颠覆性的，现有金融体系中的一些角色将不再需要，金融中介的职能也将发生深刻变化。

二是金融基础设施的变革。区块链本身就是一个数据库，基于点对点的通信技术和加密技术使数据库的组织形式更具开放性和可追溯性。在区块链技术的基础上，每个数据节点都可以参与验证账本内容的真实性和完整性，相当于通过提高系统的可追责性降低系统的信任风险。这一特性使得区块链在征信、审计、资产确权等方面具有显著的优势，从而间接提高金融体系的运行效率。

三是智能物联网。由于区块链形成了独立运行的共识机制，区块链技术可以应用于物联网的数据处理和系统维护领域。比如已经有机构提出要使用区块链技术管理上百亿个物联网设备的身份、支付和维护任务。利用区块链技术，物联网设备生产商能够极大地延长产品的生命周期和降低物联网维护的成本。

四是共享经济的技术基础。区块链去中心化的共识机制使得计算服务的应用范围大大延伸。尽管电子支付技术的发展大大降低了支付的成本，但现有支付业务模式下极小金额的支付比如低于0.01元的支付成本仍然非常高。有公司正在开发一种基于区块链的微支付技术，为每个人的电脑利用闲置计算能力从事挖矿、存储等工作提供计量工具。这种计量服务正是多种共享经济的前提，将大大拓宽共享经济的深度和广度。

综上所述，区块链技术的主要优势在于基于分布式网络形成的共识机

制，分布式网络使得基于区块链的应用具有明显的开放性和可拓展性，这样会使一些商业模式的门槛可以降得很低，甚至产生全新的商业模式；共识机制的独立存在使合约的执行成本降到最低，执行效率大大提升，计算服务的范围也大大提升。

全球正在掀起一股区块链的热潮。来自学术界和科技界的各种力量投身区块链的开发和创业大潮之中，也诞生了一批非常有创新意识的创业公司，成为 Fintech（金融科技）中的一股重要力量；到 2015 年底，已经有超过 20 家全球顶级的金融机构、风险基金高调宣布参与各种区块链应用开发项目。当然，我们也必须要清醒地看到，区块链技术的发展不论在国际还是在国内都尚处在早期阶段，各种技术方案和商业模式等都需要进一步地探索和实践。特别是在我国，区块链作为一个全新的概念和理论，人们的认知、研究和实践刚刚起步，要想在这一领域积累优势，引领世界，还需要足够的重视，更多的投入，需要理论研究者、网络技术者、金融从业者，以及政府监管部门的积极投入和良性互动。正是在这样的大背景下，《区块链：重构经济与世界》的出版正好填补了国内关于区块链技术特点和应用分析的空白，希望此书的出版为我国区块链技术的开发应用提供一定的参考和借鉴。

目 录

第一章

探寻区块链的源头

——“重回拜占庭”

每一个时代都有自己值得骄傲的技术，无论是晶体管、激光、互联网，还是载人航天飞机。近10年中，金融网络领域最具颠覆性、最闪耀的技术发明莫过于区块链。无论是与数字货币一道横空出世，继续发力衍生出智能合约，还是可预见的未来，不断重塑整个金融世界，都使它的夺目光芒无法掩盖。然而究其源头，我们不得不追溯到“拜占庭将军问题”和“双花问题”。后者比较简单，即如何杜绝非实体货币的再次被使用，或者是双重支付（只要引入盖时间戳的电子签名就能解决）。而前者，“拜占庭将军问题”则看起来费解且扑朔迷离，但我们又不能回避，因为它是整个区块链技术核心思想的真正根源，也直接决定了区块链技术的种种与众不同的颠覆性特质。

在某种程度上，问题比答案更重要。很难想象：如果没有“拜占庭将军问题”，没有它揭示出在人类散兵游勇的状态下，永恒的“共识”困境，那么对于这种困境的反思和探索便无法成为可能，逃离困境到达光明之地也无法成为可能。所以在我们向伟大的“答案”——区块链致以敬意之时，请不要忘记它的源头，不要忘记拜占庭。

拜占庭将军的难题

古老的“拜占庭将军问题”

让人生，让人死，让人痴迷，让人疯狂。

这就是传说中繁华与没落，绝望与救赎并存的东罗马帝国首都，拜占庭。

在2013年获得计算机科学领域最高奖项图灵奖的31年前，1972年，莱斯利·兰伯特（Leslie Lamport）搬到湾区。此时，他仍然是一个寂寂无闻的美国小伙。他充当Compass（马萨诸塞州计算机合伙人公司）西海岸计划前哨基地的先锋，不幸的是，这个分支机构最终未能落实。在长达5年的时间里，他曾是Compass总部派驻加州的唯一员工。最后，他却收到撤回东海岸的指令。于是，他决定加入斯坦福国际研究院（SRI）。在那段岁月里，SRI有一个项目，要在美国航空航天局建立容错型航电计算机系统。考虑到系统的工作性质，故障是不允许发生的。这段经历孕育了两篇旨在解决一种特殊故障的论文，由兰伯特和SRI同事马歇尔·皮斯（Marshall Pies）及罗伯特·肖斯塔克（Robert Shostak）合作完成。用计算学术语说，普通故障可能会导致信息丢失或进程停止，但系统不会遭到破坏，因为这种普通故障属于一出错就会停下来的故障类型，剩下的备份的、正常的部分照样可以运转，发挥作用。就像战场上的士兵，他们一旦受伤或阵亡就停止战斗，但并不妨碍他人继续作战。

然而一旦发生“拜占庭故障”，就会非常麻烦，因为它们不会停下来，还会继续运转，并且给出错误讯息。就像战争中有人成了叛徒，会继续假

传军情，惑乱人心。当时为了解决这个问题，常常使用的技术被称为“三重模块冗余”：也就是说使用三台计算机进行万一出错的备份工作，三台独立的计算机按照少数服从多数的原则“投票”。这样，即使其中一台机器提供了错误结果，其他两台仍然会提供正确答案。但是为了证明这种方法的有效性，必须拿出证据。而在编写证据的过程中，研究人员遇到了一个问题：“错误”计算机可能给其他两台计算机发送互不相同的错误值，而后者却不会知道。这就需要使用第四台计算机来应对这个故障。

兰伯特说：“如果你使用数字签名，就可以用三台机器达成目的，因为如果‘坏了’的计算机向一台计算机发送了带签名的错误值，并向另一台发送了不同的带签名错误值，另外两台计算机就能够交换消息，以检查究竟发生了什么情况，因为两个不同的值都是签名发送的。”兰伯特还听吉姆·格雷谈论过另一个性质大体相同的问题，人们称之为“中国将军问题”。这引起了兰伯特有关司令将军和叛徒将军的联想，于是他将这个问题及其解决方案命名为“拜占庭将军问题”。

“我记得，与我的朋友怀特·迪菲（White Duffy）坐在伯克利的一间咖啡馆里，当时他描述了一个构建数字签名的问题。”兰伯特回忆说，“他说：‘如果能办到的话，会非常有用。’我说：‘这听起来并不很困难。’于是在一张餐巾纸上，我为他勾画出了第一种数字签名算法。虽然当时并不很实用，但目前已经变得切实可行。”只可惜那张餐巾纸已经消逝在时间的流沙中。在后来 1982 年正式出版的拜占庭将军论文的序言中，他这样写道：

> “我一直觉得正是因为通过用一组围坐在圆桌旁的哲学家来表述，Dijkstra（迪克斯塔）的‘哲学家就餐问题’才变得如此让人关注（比如在理论界，它可能比‘读者/作者’问题都引人注目，尽管读者/作者问题可能更具实际意义）。我认为 Reaching Agreement in the Presence of Faults（达成共识的缺陷）中所描述的问题十分重要，值得计算机科学家们去关注。‘哲学家就餐问题’使我认识到，把问题以

讲故事的形式表达出来更能引起人们的关注。在分布式计算领域有一个被称作‘中国将军问题’的问题。在这个问题中，两个将军必须在进攻还是撤退上达成一致，但是相互只能通过信使传送消息，而且这个信使可能永远都无法到达。我借用了这里的将军的叫法，并把它扩展成一组将军，同时这些将军中有些是叛徒，他们需要达成一致的决定。同时我想给这些将军赋予一个国家，同时不能得罪任何读者。那时候，阿尔巴尼亚还是一个完全封闭的国家，我觉得应该不会有阿尔巴尼亚人看到这篇文章，所以最初的时候这篇论文题目实际是 The Albanian Generals Problem（阿尔巴尼亚将军问题）。但是 Jack Goldberg（杰克·古登博格）后来提醒我，在这个世界上除了阿尔巴尼亚之外还有很多阿尔巴尼亚移民，所以建议我换个名字。于是就想到了这一更合适的叫法——Byzantine generals（拜占庭将军）。”

写这篇论文的最主要目的是将拜占庭将军这个叫法用在这个问题上。基本的算法文章在 1980 年的论文中就已经出现了。

起源：拜占庭位于现在土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了防御敌人每个军队都分隔很远，将军与将军之间只能靠信差传消息。在战争时期，拜占庭军队内所有将军和副官必须达成一致共识，决定是否有赢的机会才去攻打敌人的阵营。但是，军队可能有叛徒和敌军间谍，左右将军们的决定，扰乱军队整体的秩序。在达成共识的过程中，有些信息，往往并不代表大多数人的意见。这时候，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，就是“拜占庭将军问题”。

两军问题：军队与军队之间分隔很远，传递信息的信差可能在途中阵亡，或因军队距离不能在得到消息后即时回复，发送方也无法确认消息确实丢失的情形，导致不可能达到一致性。在分布式计算上，试图在异步系统和不可靠的通道上达到一致性是不可能的。因此对一

致性的研究一般假设信道是可靠的，或非异步系统上运行。①

“拜占庭将军问题”在通信领域的意义

“拜占庭将军问题”并非如传说中那样，源于公元 5 世纪的东罗马战场，而是产生于 1982 年一位美国计算机科学家的头脑当中。因此，我们不会使用任何 1982 年之前的案例来描述这个问题在古老年代的意义，因为再往前追溯，它并未真正、严肃地被提出并加以审视。

在原始的战争年代，将军与将军、将军与下属间只能采用原始的方式——“出行靠走，通讯靠吼”的口头传输。这对应兰伯特论文提出算法中的第一部分的口头消息算法，简称 OM（m）算法。这种情形，真伪很难辨别，只有当叛徒的总数不超过将军总数的 1/3，成为一个特殊的“拜占庭容错系统”时，才能在很大的消息验证代价后，实现最终的一致行动。这个结果非常令人惊讶，如果将军们只能发送口头消息，除非超过 2/3 的将军是忠诚的，否则该问题无解。尤其是，如果只有三个将军，其中一个是叛变者，那么此时无解。但这样的错误，这样的有意、无意的“叛徒”却可能经常出现。无论是我们把“叛变的将军”替换成以下哪种，该问题都成立。

- 一个出故障的，向其他计算机不停发出不同错误信息的服务器；
- 一份为获取暴利而做出来的金融票据；
- 一份失效的医疗纠纷合同；
- 一份含混不清的保单；
- 一个可以发出消息，做出行动的错误信息节点。

而这里，每一个错误节点可以做任意事情：不响应；发送错误信息；对不同节点发送不同决定；不同错误节点联合起来攻击其他节点等。没准会出现比这更严重、更荒谬的错误。

---

① 来自维基百科。