万向区块链实验室丛书

监管区块链

BLOCKCHAIN AND THE LAW

the Rule of Code

代码之治

[法]普里马韦拉·德·菲利皮（Primavera De Filippi）
[美]亚伦·赖特（Aaron Wright） 著
卫东亮 译

深入阐述区块链技术的运作原理与应用前景
全面总结密码法的鲜明特征及其对传统法律行业的影响
具体探讨区块链技术的双重属性
系统提出政府监管区块链的可行路径

中信出版集团

监管区块链

代码之治

BLOCKCHAIN AND THE LAW

the Rule of Code

[法]普里马韦拉·德·菲利皮（Primavera De Filippi）
[美]亚伦·赖特（Aaron Wright） 著
卫东亮 译

中信出版集团 · 北京

图书在版编目（CIP）数据

监管区块链：代码之治 /（法）普里马韦拉·德·菲利皮，（美）亚伦·赖特著；卫东亮译. -- 北京：中信出版社，2019.1

书名原文：Blockchain and the Law: the Rule of Code

ISBN 978-7-5086-9617-1

Ⅰ. ①监… Ⅱ. ①普… ②亚… ③卫… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ① F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 231098 号

监管区块链：代码之治

著　　者：［法］普里马韦拉·德·菲利皮　［美］亚伦·赖特
译　　者：卫东亮
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）
承 印 者：北京盛通印刷股份有限公司

开　　本：787mm × 1092mm　1/16　　印　　张：25.25　　字　　数：360 千字
版　　次：2019 年 1 月第 1 版　　印　　次：2019 年 1 月第 1 次印刷
京权图字：01-2018-6801　　广告经营许可证：京朝工商广字第 8087 号
书　　号：ISBN 978-7-5086-9617-1
定　　价：68.00 元

致中本聪

推荐序

区块链自出现以来，就以其去中心化的特征为世人所知。中本聪在比特币白皮书中，提出要打造一个不依赖任何中介机构的点对点支付系统，这一思路也为日后的区块链创业者所延续。通过区块链，陌生主体之间分布式的协同记账得以成为现实，互联网也因为区块链而拥有了传递信任的能力，实现了价值互联网。

在此基础之上，区块链在以金融为代表的一系列领域中具有广泛的应用前景。已经有许多人在尝试将区块链应用于各类金融交易场景，代替各种需要信任的第三方机构，在交易双方之间建立起点对点的信任。由于区块链的信任传递能力，区块链能够应用于支付清算、数字票据、资产数字化、证券登记与交易、保险、供应链金融、网络借贷、征信、电子存证、身份认证、隐私保护、物联网、数字版权管理等丰富多样的领域，发挥基于技术的信用创造功能。这些场景都有许多先

行者和创业公司已经开始探索推进，尽管规模和进展不一，但都展现出区块链深远的潜力。

尤其是Token的出现，推动了区块链在融资领域的应用。Token作为共享权益凭证，在参与各方之间能够起到利益分配的砝码的作用，它同时具备股票的融资属性、钞票的流通属性、粮票的兑换凭证属性，是三票属性的共同延伸，因而笔者在刚刚出版的新著《区块链＋监管＝法链（RegChain）》中，将Token翻译为“共票”。我认为，“通证”的译法有一定的谐音要素，但是没有准确表达目前区块链上的Token所具备的属性与内涵，从翻译学的角度而言仍然欠佳。而“共票”更为准确地界定了其共享利益的属性，更能实现权益的大众化、普及化、民主化。早在2014年，笔者就提出了众筹金融的理论，即用新的无组织的社区形态取代公司制，借助新兴技术工具打破信息不对称，打破传统中心化的PE、VC等垄断的资本格局，实现金融的去中介化、去机构化，将其转变为点对点的融资方式，最终实现信息的对称，彻底颠覆旧有的生产关系。区块链的出现，用共票取代股份制，让这一理论构想成为了现实。可以说，区块链让众筹成为与股份制一样伟大的制度发明。

区块链对生产关系的变革不仅触及经济制度，更能深入到法律等社会规范的层面。在区块链发展的过程中，对区块链和法律的关系，公众的观点并不统一。去中心化的支持者认为，区块链不依赖任何中间机构，因而无法被监管，成为一片自由的“乐土”，法律似乎更是与区块链无缘。

但是从现实角度而言，区块链需要被监管。目前区块链的实践中，存在着一些不理性的市场现象，过度强调发行Token和炒币。一些投机分子技术能力不足或者根本没有技术，而假借区块链名义，声称使

用区块链技术但实际上没有使用区块链，搞“伪区块链”创新，这些情况明显不利于行业的长远发展，成为孕育“割韭菜”等恶劣行径的源头，甚至可能涉嫌诈骗等犯罪行为。这些不规范的发币行为在被国内有关监管部门禁止之后，纷纷出走境外，继续开展发币和炒币的行为；一些开设在境外的交易平台还存在内幕交易、操纵市场等恶劣行径，继续损害境内民众的合法权益。这些问题的解决之道，仍然有赖于对区块链与法律的关系进行深入细致的研究。

《监管区块链：代码之治》是这方面的一个非常有价值的尝试。该书指出，区块链需要被监管，也可以被监管，这也与我一直主张的观点相吻合。更为重要的是，区块链本身就可以用于监管和法律领域。区块链之所以能够创造伟大的价值，原因在于区块链不仅仅是一种提升生产力的技术，而是深入到了规则即生产关系的层面，给利益的分配机制带来了变化，从而对生产关系产生巨大的颠覆，给监管和法律系统带来重构。所以，区块链最大的应用场景实际上是在政府的监管领域，区块链能够化身为法律，带来法律执行效果和效率的革命性提升。

2018 年 6 月 28 日，杭州互联网法院对一起侵害作品信息网络传播权纠纷案进行了公开宣判，首次对采用区块链技术存证的电子数据的法律效力予以确认。本案的案情并不复杂，原告发现被告未经授权在网站上转载其作品，侵害其信息网络传播权，遂起诉到法院。值得关注的是，原告在向法院举证存在侵权行为时，没有采用传统的公证处公证，而是使用了基于区块链的电子存证技术。杭州互联网法院在一审判决中，认可了这种存证方式，甚至更进一步在判决中较为全面地阐述了区块链电子存证的技术细节，提出了司法上判断是否应当予以采纳的初步标准。这一判决表明了司法界在面对新技术时包容开放但又不失慎重的态度，在全国尚属首例，在世界范围内也是较为领先

的。未来，预计基于区块链的电子存证将会在司法领域得到越来越多的认可，区块链将更为深入地应用到司法领域，成为代码改变法律的先驱。

我认为，代码和法律的关系存在着两个递进的层面。第一个层面是用代码表达既有的国家法，也就是 code as law。在这一层面上，代码是一种工具，用于表达、转化现有的国家法、成文法、制定法。代码可以界定、解释和执行现有的法律，从而提高法律执行的效率。目前的监管科技也刚发展到这个阶段，运用各种技术工具，收集并分析数据、自动执行监管措施，提高监管的效果和效率。在此过程中，区块链以其独特的技术特征，扮演着极为重要的角色。《监管区块链：代码之治》对此的论述有着很高的参考价值。

第二个层面是更为深刻的层面，是指代码本身就成为法律，即真正意义上的 code is law。网络空间的高速发展，伴生了许多没有法律规制、法律无法强制或者来不及强制的场景，在这些情形下，代码直接成为最高的权威，代替法律成为网络空间中的最高社会规范。这个层面与区块链更加密不可分，因为区块链去中心化的特征，通过区块链可能实现不经政府直接在各主体之间达成共识，并得到强制执行。尽管这一前景还没有成为现实，但《监管区块链：代码之治》对此的思考值得我们每一个人阅读。

卫东亮法官在广州市中级人民法院民二庭任职多年，对商事案件的审判工作非常熟悉，又被选调进入广东省高级人民法院执行局，拥有丰富的一线司法工作经验，对公司、证券、合同、物权等商事法律有着独到的深刻见解。卫法官在繁忙的实务工作中，仍然对互联网、区块链等先进技术的发展保持着高度关注，结合自身的工作经验，抽出时间翻译完成《监管区块链：代码之治》，对区块链与法律之间关系

的研究做出了富有成效的贡献。我想，卫法官可以称得上中国第一个真正研究和传播区块链的人民好法官。卫法官在工作之余仍然潜心进行学术研究，这种钻研探索的学习精神也让我非常敬佩。期待本书能加深国内公众对区块链的理解，促进区块链应用尤其是在司法领域应用的发展，使区块链与法律、监管更好地结合在一起。

中国人民大学大数据区块链与监管科技实验室主任

杨　东

导论

蒂莫西·梅（Timothy May）是密码朋克（cypherpunk）运动[①]的创始人之一，他在1988年曾提出警告："幽灵正萦绕着现代世界。"[1]这个"幽灵"不是停滞不前的政治格局，也不是恐怖主义、种族冲突或者环境危机，而是日益增长和扩散的新型无政府主义，梅称之为"密码学无政府主义"（crypto anarchy）。[2]梅在其著作《密码学无政府主义宣言》（*Crypto Anarchist Manifesto*）中描述了未来的场景：随着互联网以及公私钥密码学（public-private key cryptography）的发展，人们将以更加匿名（anonymous）的方式交流和合作。借助不可追踪网络以及"执行加密协议的防篡改（tamper-proof）盒子"，人们可以"自

① 密码朋克运动，是1993年埃里克·休斯（Eric Hughes）在其所著《密码朋克宣言》（*A Cypherpunk's Manifesto*）中提出的一个概念。它结合了电脑朋克的思想，认为使用强加密算法能保护个体隐私的安全，反对任何政府主导的密码系统。——译者注

由交易，根本无须知道对方的真名实姓与合法身份”。[3]

最后，梅预测，个人将从国家中解放出来，完全改变“立法的性质，政府征税、控制经济交往以及保有机密信息的能力”，也会改变我们有关信任和声誉的观念。[4]加密安全协议将拆除知识产权设置的藩篱，促进信息自由流动，赋予个人新的自我组织的能力，彻底改变公司和政府的本质。[5]在梅看来，这一转变是不可避免的。“妖怪已经从瓶子里跑出来了”，梅在之后的文章中解释道，没有任何力量可以阻止因加密技术发展导致的无政府主义的蔓延。[6]

区块链在很多方面就是梅在30年前所设想的“防篡改盒子”，它借助现有的点对点（peer-to-peer）网络、公私钥密码学及共识机制（consensus mechanisms），来创建高度弹性（resilient）和防篡改的数据库，人们可以以透明和不可否认（nonrepudiable）的方式存储数据，并以假名（pseudonymously）从事各种经济交易。区块链可以转移数字货币或其他有价资产，管理产权和敏感档案。不过，它最为重要的应用是可以创建自治（autonomously）执行的被称为智能合约（smart contracts）的计算机程序。[7]

区块链与传统的数据库不同，它不需要集中维护，而是由一个遍布全球的点对点网络来共同管理。组成这一网络的数以万计的计算机，被称为“点”（peer）或“节点”（node）。[8]这些节点上存储着相同或基本相同的区块链副本，并借助软件协议来精确地控制各个节点如何储存数据，如何参与交易，以及如何执行软件代码。

由于区块链在网络中被广泛复制，所以所有存储在区块链上的数据都具有高度弹性，即使某个区块链副本被破坏，或某个节点失效，其他节点上的数据也仍然有效。并且，只要世界上还有一个有效的区块链副本，其他节点就可以修复和重构区块链，恢复之前的全部交易

记录，并进行新的交易。

为了提高区块链的安全性，确保信息的有序记录，每个区块链项目均执行特定的共识机制。共识机制是一系列预先严格界定的激励和成本结构规则，基于这一规则，任何人试图单方移除或修改区块链上的数据都非常困难，且代价昂贵。有了共识机制，即使区块链网络成员之间互不认识或互不信任，也仍能定期就共享数据库的当前状态达成一致。

借助公私钥密码学，每个区块链均可以验证所记录数据的完整性，人们可以用假名进行交易，而无须披露交易双方的真实身份。[9] 区块链无须集中维护，所以任何一方都不必控制对它们的访问权限。这意味着，在可公开访问的区块链上，任何人均可以创建由公钥、密钥和密码组成的区块链账户并进行交易，且几乎不受任何第三方的干涉。[10]

更先进的区块链，集成了被称为分布式虚拟机的去中心化计算系统，以及图灵完备（Turing complete）的编程语言，参与各方可以借此编写和部署智能合约程序。[11] 这些智能合约程序存储在区块链上，并由区块链底层点对点网络的多个成员共同负责执行，而它所创建的计算机进程一经部署就会自动运行，并且难以关闭。

自 2009 年比特币诞生以来，区块链技术已被大量应用于在线服务，用来存储信息及运行计算机程序。其中一些应用致力于实现梅 30 年前的愿景，有的应用则增进了现有的合法服务。

正如比特币所展示的，区块链技术支持基于假名的、去中心化的跨国价值转移系统。借助区块链，任何人均可以交易包括比特币在内的数字货币以及其他有价值的资产，而无须通过中心化的清算所，也无须披露交易双方的真实身份。区块链所构建的新型点对点汇款系统，降低了跨国资金转移的成本。同样，区块链技术也在金融服务领域发

现了新的机遇，它所构建的去中心化的证券和衍生品交易系统，则直击全球金融市场的要害。

短短几年，区块链就迅速扩展到支付和金融产品之外，它所支持的新型自治系统，有助于形成无须中介机构的社会经济交易结构。人们可以借助智能合约记录法律协议的部分或全部内容，从而创建出动态的、难以终止的商业交易。

各国政府开始尝试使用区块链来保护和管理关键公共档案，如至关重要的信息以及财产权属与证书。同时，政府也希望借助区块链防篡改、弹性和不可否认的特性，最大限度地保证这些关键信息的完整性和真实性。假以时日，区块链将成为新的公共基础设施，充当全球跨国系统的支柱，任何人均可联网使用。

人们开始尝试用区块链创建各种集合体，如至少其中的部分功能需要由代码来执行的新型数字化组织。由于区块链广泛可及，有助于促进经济交易，人们开始探索将其作为协调中心点，来管理现有的法律实体；通过智能合约执行基于代码的规则，来降低团队管理的成本和难度。区块链也可以用来驱动更透明、更少层级的新型组织，便于互不了解的人达成协议。将来，人们可以将区块链作为基础设施，创建完全依赖算法和人工智能的自治组织。这些组织不再由人类管理，而是借助代码规则以及其他算法治理手段来运营。

除了协调人类活动，区块链被越来越多地用于控制机器设备，并借助智能合约来界定这些连接到互联网的设备如何运行。最终，区块链将发展成熟，足以充当协调机器—人、机器—机器之间经济交往的基础层。如果这些尝试取得成功，区块链就会深入渗透到人类活动的方方面面，构建全新的机器—机器、机器—人的交互方式，并有可能改变我们与实体商品之间关系的本质。

然而，并非所有基于区块链的应用和服务都严格遵守现有的法律和规则。区块链驱动的数字货币一般跨国境交易，经常忽略现有的有关货币转移和洗钱的法规，有意规避旨在帮助政府、银行及私营部门追踪货币跨境流动的有关规则。这一新兴技术如果不加以合理的监管，就可能被用于欺诈、洗钱、恐怖融资及其他非法活动。[12]

区块链也在抢占公开交易市场。通过自治运行且不受监管的区块链数字货币交易所，人们可以交易各种基于密码保护的代币（token，也被译为令牌、通证，其中有些类似于证券）、衍生品和其他金融产品，交易额高达数十亿美元。这些区块链系统往往无视现有金融市场的法律界限，削弱了那些精心制定的、旨在限制欺诈和保护投资者的法律法规的效力。

在金融领域之外，区块链也被应用于游走在法律边缘的在线赌博和电子商务市场。这些在线赌场高度自动化运营，不受中央机构的控制。去中心化的电子商务市场方便人们自由交易，无须再依靠易贝（eBay）、克雷格列表（Craigslist）[①]等在线市场，甚至是“丝绸之路”（Silk Road）这样的地下网络。这些应用助长了毒品交易，它们的广泛应用导致政府更加难以限制由此衍生的犯罪以及其他有悖公序良俗的社会活动。

区块链进一步推动了信息流通，用于构建新型点对点文件共享应用、去中心化通信平台和社交网络。借助区块链及其他点对点网络防篡改、弹性的特征，这些应用和平台可以散播受版权保护的作品、煽动性言论和其他不雅内容。如果这些服务得到广泛应用，它们将限制

① 克雷格列表（Craigslist）是克雷格·纽马克（Craig Newmark）于1995年在美国创立的大型免费分类广告网站，是目前美国用户量最大的网站之一，建有包括中文在内的18种语言版本。——译者注

政府和企业控制、过滤以及审查网络信息的能力，也不会考虑可能产生的社会成本和政治成本。

长远来看，如果区块链技术在速度、性能、功能及可访问性方面有所改进，就可能创建出与传统公司及其他法律实体相竞争的组织，甚至可能创建出自治设备和机器人，它们独立自主运行，不受政府、中间运营商以及任何第三方的控制。

正如本书所讨论的，区块链对自治系统的推动和支持，将持续挑战政府与立法者控制、塑造或影响区块链技术发展的能力。与许多技术一样，区块链技术既可以支持现有的法律和规章，也可以削弱其效力。但是，它的特别之处在于，其所创建的弹性、防篡改及自治的全球代码系统，为人们提供了新的金融和契约工具，可以取代当前的关键社会功能。

通过区块链，人们可以构建自己的规则体系，创建由区块链网络底层协议执行的智能合约。这些系统所建立的无须法律的秩序，通过所谓的私人监管框架执行，本书称之为密码法（lex cryptographica）。[13] 软件开发者据此创建的工具和服务，可以协调各种跨越国境的经济活动和社会活动，当然，也可以规避特定国家的法律。

密码法的代码规则体系，与当前中心化在线应用采用的、基于代码的规则体系并不相同。[14] 多数在线服务要么本身即中介机构，要么借助其他中介机构，如大型云计算服务商、搜索引擎、支付服务提供商、域名注册服务商和社交网络等，来支持它们所提供的服务。这些中介机构不仅执行法律，还执行它们自己制定的规则，它们的身份易于识别，位于特定国家，因此是政府当局管控网络的中心节点。[15]

现有法律体制的监管重点，是负责控制和协调在线活动的各种中心化中介机构，而部署在区块链上的系统，如果主要或完全借助密码法运作，就难以受到现有法律体制的控制和监管。这些区块链系统由软件协议和基于代码的规则管理，由底层区块链网络自动执行，借助配套的智能合约，可以实现高度自治，必然越来越独立于中心化的中介机构。这些应用程序仅由代码组成，由区块链协议以分布式方式运行，通常也不会考虑是否遵守现有法律，这必然与现有法律体制产生冲突。

尽管区块链网络有明确的应用前景，但当前仍面临一些不确定性风险，它可能会动摇中央银行、金融市场和商业协议管理的根基，也可能会支持新形式的非法活动。这些风险之所以显得如此严重，是因为区块链技术已经开始用于重构当前社会的基础体系，重建包括支付系统、金融市场、商业协议在内的各种常见的组织机构。

今天，社会治理的重点很大程度上是由各种机构和官僚体系所决定的，它们主要通过法律和等级制度来规范社会。[16] 区块链应用不再需要依赖这一体系和规则，而是依靠密码法来组织经济与社会活动，实现其功能。[17]

随着区块链技术的进一步成熟，权力将从政府制定的法律和规则加速转移至由去中心化区块链网络支配的代码规则与软件协议。基于代码的协议，以及与其发展相关的决策，将最终控制这些系统如何工作，塑造人们交往的方式。我们或将不再遵从法治（rule of law），而是越来越服从于不受任何第三方控制的代码之治（rule of code）。[18]

本书探讨了区块链技术的新应用，分析了其优势及面临的挑战，框定了密码法的范畴。我们驳斥了区块链将导致密码学无政府主义状态这一观点，概述了监管区块链技术的策略。

互联网甫一出现，即引致无政府主义和脱法（lawlessness）概念

的滥觞。1996 年，约翰·佩里·巴洛（John Perry Barlow）在其《网络空间独立宣言》（*A Declaration of the Independence of Cyberspace*）中的描述最具代表性。他认为，互联网将形成一个新的世界，在这里，传统的“财产（property）、表达（expression）、身份（identity）、行为（movement）”，以及相关的法律概念均（将）不再适用。[19]“网络公民”（Netizens）将摆脱中心化政府当局的控制，主宰这个世界，并借助去中心化网络实现自治。[20]

然而，互联网的逐渐成熟，证明了巴洛的愿景不过是一个乌托邦式的幻想。过去的十年，互联网为了实现分散权力和鼓励自由交流的初衷，甚至放任垃圾邮件、欺诈和犯罪泛滥，但它反而变得越来越集中，越来越受到监管。手机、应用商店和云计算平台的出现，推动形成了一个更加中心化的网络，少数几家公司便垄断了大部分信息分发和网络交易。[21]

今天，互联网的无政府主义趋势已经得到很大程度的控制。政府监管的重点是本地互联网服务提供商（Internet Service Provider，ISP）和提供互联网基础服务的大型中介机构，并逐步授权由这些机构来维护互联网秩序。[22] 一些国家和地区，特别是在欧洲，甚至开始割据互联网，要求互联网数据必须本地化，以防止外国公司收集和存储与该国公民相关的信息。[23] 一些国家则更甚，以技术机制屏蔽信息的流动。[24]

我们认为，区块链技术的成熟和发展，也会遵循类似的路径。尽管区块链创建了越来越多的自治和潜在的法外系统，但政府仍有管制的办法。区块链只是减少而不是消灭了对中介机构的需求。即便“区块链真的会导致广泛的去中介化”，法律、市场力量、社会规范以及区块链代码本身，也仍然可以用来维护法治。