基于区块链的金融监管展望

——从数据驱动走向嵌入式监管

巴曙松 魏 巍 白海峰

摘要： 从区块链作为战略性技术写入《“十三五”国家信息化规划》以来，区块链技术发展迅速，其在金融行业的应用场景尤其突出，而区块链技术衍生而来的加密货币也备受关注。如何有效地防范加密货币底层技术的风险，约束加密货币的野蛮生长，以及构建加密货币的良性生态圈，将是未来监管机制的重要发展方向。现阶段，全球范围内的监管机构在开发、应用以及规范区块链科技的过程中也遇到了各种问题和挑战。文章关注对区块链应用带来的潜在风险，并分析如何利用区块链等新技术来强化金融监管，为完善区块链监管机制进行理论探索。

关键词： 区块链；金融监管；嵌入式监管

DOI： 10.19836/j.cnki.37-1100/c.2020.04.017

一、区块链的概念与发展现状

（一）区块链的概念

Nakamoto最早提出，区块链可作为资产货币的底层技术①。区块链的特点是在对点网络下，通过透明和可信规则构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式，其中事务处理包括但不限于可信数据的产生、存取和使用。从技术层面上来看，区块链是由不同节点共同参与的分布式数据库系统，表面形式上是一个数据库系统。

侯周国和梁欢按照区块链涵盖三个基本概念，即区块（Block）、链（Chain）和交易（Transaction）来定义区块链②。其中“区块”指在某一个时间段记忆储存期间全部的状态改变和交易的最终结果，是一次对数据账本状态的共识；“链”指存储整个数据账本从开始到结束的状态变化，是由区块遵循一定的次序排列组成；“交易”是指通过对数据账本的一次作业，打乱账本的原始情态，改变系统的状态。每一次交易就是试图改变数据账本的状态，每一个区块按照生成顺序排列联结组成链表，也就是“区块链”的由来，而要确定这个新生成的区块的资格，就必须要统一共识，这是一个只能新增、不能删除的数据账本③。

以王硕为代表的部分学者详细解释了区块链技术的原理：区块链技术主要让参与系统中的任意节点使用密码学方法产生相关联的数据块，每个数据块中包含了一定时间内的系统全部交易数据，并且生成密钥用于验证其数据的有效性和链接下一个数据块④。其中，每个节点由一系列存储全网信息

收稿日期： 2019-11-01

作者简介： 巴曙松，北京大学汇丰商学院教授（深圳 518055；bashusong@163.com）；魏巍，清华大学银色经济与健康财富研究中心研究助理（北京 100084；2116390661@qq.com）；白海峰，东北大学工商管理学院博士研究生（辽宁 110167；baihf@cmfchina.com）

① Nakamoto S.，“Bitcoin：A Peer-to-Peer Electronic Cash System”，*Manubot*，2019.

② 侯周国、梁欢：《区块链技术发展现状及特色应用研究》，《科技创新与应用》2016年第30期。

③ 徐忠、邹传伟：《区块链能做什么、不能做什么？》，《金融研究》2018年第11期。

④ 王硕：《区块链技术在金融领域的研究现状及创新趋势分析》，《上海金融》2016年第2期。

的数据区块链接而成。如比特币系统中的每个区块存储的是某一时间段的全球比特币全部交易数据,每10分钟通过算法,生成新的模块,以此类推,滚动记录交易信息。具体分析,每个数据区块由四个关键要素构成,分别是前一区块的哈希值、本区块的时间戳、一个随机数和本区块的哈希值树。其中,前一块的哈希值用于将本区块与前一区块构建对应关系,头尾对应构成一条链;时间戳用于记录存储模块的时间段;随机数可用于挖矿奖励,保证大家有动力做这个事情,同时也提供了系统需要的计算能力;而哈希值树则是该模块下各类存储信息的密钥阵列,客户需要密码才能获取数据区块下的某部分信息。总而言之,区块链技术以加密算法为基础,通过去中心化的链条相通、时间有序的方式,构建起记录和更新交易信息的全球分布式可信网络数据库。Niranjanamurthy等认为区块链技术包含密码学、数学、算法和经济模型,结合了点对点网络,使用分布式共识算法来解决传统的分布式数据库同步问题,是一个集成的多领域基础架构,并且认为区块链技术主要包括六要素:中心化、透明、开源、自治、匿名和不可修改①。

(二)区块链的发展现状

自2016年区块链首次作为战略性技术写入《"十三五"国家信息化规划》以来,推动区块链发展的各类政策层出不穷,如表1所示。从具体政策来看,工业和信息化部等部委的政策更加侧重于将区块链技术作为试点应用,并给一些城市提供相关技术开展政策支持。

表1 中央层面关于区块链方面的政策梳理

政策名称	发布时间	发布部门	相关内容
《国务院关于印发"十三五"国家信息化规划的通知》	2016年12月	国务院	区块链首次作为战略性技术写入
《软件和信息技术服务业务发展规划(2016-2020年)》	2017年1月	工信部	提出区块链等创新达到国际先进水平
《关于进一步扩大和升级信息消费持续释放内需潜力的指导意见》	2017年8月	国务院	开展基于区块链、人工智能等技术的试点应用
《关于积极推进供应链的信用评价机制》	2018年1月	国务院	建立基于供应链的信用评价机制
《2018年信息化和软件服务业标准化工作重点》	2018年3月	工信部	推动组建全国区块链和分布式记账标准化委员会
《2019年区块链信息服务管理规定》	2019年1月	网信部	推动全国区块链企业备案
《2019年食品安全重点工作安排》	2019年5月	国务院	提出推进"互联网+食品"监管,重点运用大数据、区块链技术
《关于支持深圳建设特色社会主义先行示范区的意见》	2019年8月	国务院	支持在深圳开展数字货币研究与移动支付创新应用

资料来源:作者整理。

在政策推动下,区块链产业迅速成型、快速发展。据IT桔子数据库数据显示,2014年至2019年,我国涉及区块链业务公司数量已达到1570家,产业已经初步形成规模。从新成立公司数量变化情况来看,2014年之前每年涉及区块链业务的新公司不足百家,2014年之后新增公司显著增加,2017年和2018年分别新增530家和474家,2019年有所下降。随着区块链概念快速普及以及技术逐步成熟,大量创业者涌入这一新领域。从全球专利申请量的变化趋势来看,区块链领域专利申请数量稳步上涨,中国的增长趋势和全球趋势十分接近。

① Niranjanamurthy M., Nithy B. N., Jagannatha S.,"Analysis of Blockchain Technology: Pros, Cons and SWOT", *Cluster Computing*, 2019, 22(6), pp. 14743-14757.

二、区块链在金融中的业务场景

目前，有关区块链技术的应用大都还在实验阶段，但其展现出的广阔前景吸引了越来越多的关注与思考，在金融、监管方面的应用路径已较为清晰，具体应用发展如图 1 所示。与蓬勃发展的区块链商业应用相比，区块链的基础理论和技术研究仍处于起步阶段，许多更为本质性的、对区块链产业发展至关重要的科学问题亟待研究跟进。贺海武等认为，目前智能合约技术的基础理论和技术研究尚处于起步阶段，仍缺乏对基础理论、关键技术以及对行业发展至关重要的科学问题的研究与探索，因此区块链技术的运用仍然存在极大的挑战①。张婷对我国商业银行区块链的应用给予了肯定，认为虽然区块链技术的运用存在着风险，但未来随着商业银行组成银行间区块链内外协同、多业务布局联盟的产生，会大大降低区块链技术运用的风险②。蔡丹丹认为区块链技术与实际的应用需要存在一定的分歧，在应用区块链技术的同时，要采取有针对性的控制策略，从而保障二者能够有效契合③。

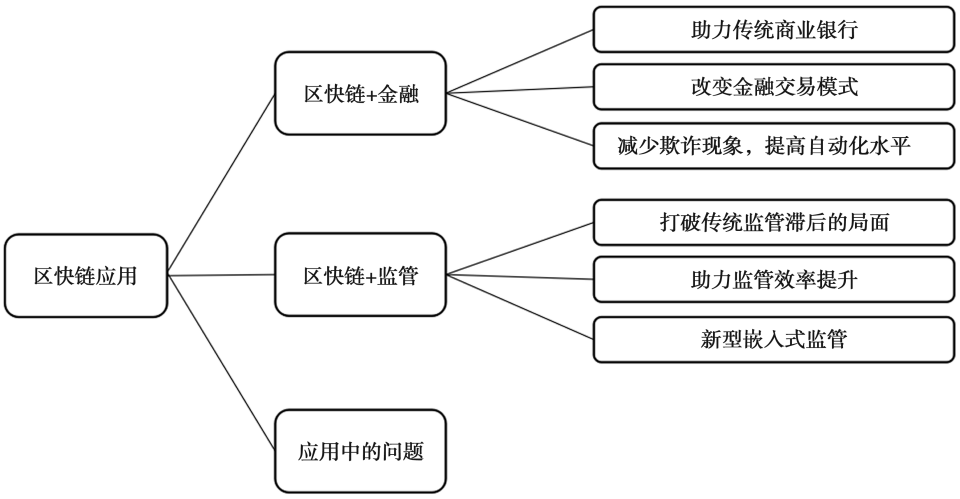

图 1　当下区块链的应用发展

资料来源：作者整理。

（一）区块链在银行系统中的应用

区块链在我国商业银行的应用主要集中在通过平台和系统的搭建来提高交易和信息处理效率等方面，由于规模、业务模块侧重点的不同，结合自身业务发展实际情况，不同商业银行间在区块链应用方面又存在一定的差别。

具体来看，招商银行凭借其传统零售银行的优势，在区块链应用方向主要体现在消费金融、资管方面。2019 年招商银行资管 ABS 区块链系统成功上线，这一系统依托了招商银行 FinTech 基金的支持开发建设。依托此平台，信托等外部平台可以将底层消费金融资产入链上传入招行银行系统，助推“小额债权”资产证券化业务的发展升级。

农业银行因其在涉农投融资方面的优势，区块链应用方向体现在农业互联网相关的电商融资系统方面。中国农业银行基于趣链科技底层区块链平台，上线了基于区块链的涉农互联网电商融资系统。平台首期推出了“E 贷链”产品，将区块链技术优势与供应链业务特点深度融合，在 2017 年 8 月 1

① 贺海武、延安、陈泽华：《基于区块链的智能合约技术与应用综述》，《计算机研究与发展》2018 第 11 期。

② 张婷：《我国商业银行区块链技术的应用与前景展望》，《新金融》2016 年第 7 期。

③ 巴曙松、白海峰：《金融科技的发展历程与核心技术应用场景探索》，《清华金融评论》2016 年第 11 期。

日完成国内银行业将区块链技术应用于电商供应链金融领域的首笔线上订单支付贷款。

建设银行凭借其在国际业务方面的优势,区块链应用方向主要与国际保理、跨境交易业务相关。2017 年 9 月,中国建设银行与 IBM 合作在香港开发和推出"区块链银行保险平台",为零售和商业银行业务提供服务。2017 年 11 月,建设银行完成首笔区块链福费廷交易。2018 年 1 月,建设银行首笔国际保理区块链交易落地,成为国内首家将区块链技术应用于国际保理业务的银行。

此外,中国工商银行将区块链技术运用在了扶贫工程中。其与贵州省贵民集团合作,依托区块链技术"交易溯源、不可篡改"的特性和优势,启动扶贫攻坚基金区块链管理平台,通过工商银行金融服务链和贵州省政府扶贫资金行政审批链的信息互认,实现跨链整合,最终达到政府扶贫资金"透明使用""精准投放"和"高效管理"的效果。

(二)区块链应用的技术优势

区块链改变支付清算系统,建立分布式清算机制。银行间的支付通常依赖于中介清算公司的处理,涉及一系列复杂的过程,包括簿记、交易对账、余额对账、付款启动等。因此,传统的支付过程是冗长且成本高昂的。以跨境支付为例,每个国家的结算程序不同,因此跨境汇款往往需要数天才能到达。在这种情况下如果使用区块链技术,借此削弱第三方金融机构中介作用,将极大地提高服务效率,降低银行交易成本,并使银行能够满足快速便捷的付款清算要求。目前,渣打银行开始使用企业级区块链平台 Ripple 来实施其跨境交易,该平台只需花 10 秒就能完成结算过程;澳大利亚国民银行(NAB)也开始使用了 Ripple 的分类账技术①。

区块链将实现安全高效的机构间数据共享。区块链技术可以使商业银行自动记录数据,而且还可以在机构内存储和共享客户信用信息的加密形式,以便于共享信用数据。在"了解客户"(KYC)的过程中,银行将客户信息存储在自己的数据库中,然后采用加密技术上传摘要,并存储在区块链中。在有查询请求时,可以运用区块链技术通知提供商并执行查询指令获得原始数据。因此,各方可以在搜索外部大数据的同时也不会泄露其核心业务数据。

(三)区块链在非银行系统中的应用

证券业务的交易模式是区块链的重要应用领域,传统的证券交易需要经过中央结算机构、银行、证券公司和交易所等机构的多重协调,而利用区块链自动化智能合约和可编程的特点,能够极大地降低成本和提高效率,避免繁琐的中心化清算交割过程,实现方便快捷的金融产品交易。同时,区块链可以实现即时到账,从而实现比银行 SWIFT 代码体系更为快捷、经济和安全的跨境转账。这也是目前各大银行、券商等金融机构相继投入区块链技术研发的重要原因。

在保险领域中,运用区块链技术,可以建立分布式保险反欺诈数据共享平台。保险机构可以在保留数据所有权和控制权的前提下,对黑名单、风险保额、身份识别等数据进行行业内共享,有效提高整个保险行业在核保阶段识别潜在欺诈对象的效率。在健康险方面,通过区块链健康险直付平台连接保险机构及医疗机构,分布式账本记录保单、医疗费用等信息,并通过智能合约实现医疗费用自动理算和赔付。非对称加密技术的使用提升了数据安全性,而理赔自动化则大幅提升了保险公司的理赔效率以及用户的体验。在再保险方面,普华永道研究结果表示,再保险业采用区块链技术可以将大部分业务流程自动化,减少人为错误,节省劳动成本,为再保险企业节省 15%至 20%营运费用。通过区块链再保险平台与保险公司系统进行对接,运用分布式账本记账避免了保险公司的重复录入、定期人工对账的繁复工作,将再保险中的对账工作自动化,能够大幅度地提升了再保险的效率②。

① Guo Y., Liang C., "Blockchain Application and Outlook in the Banking Industry", *Financial Innovation*, 2016, 2(1), pp. 1-12.

② 曾于瑾:《区块链在保险行业的应用现状与未来》,《清华金融评论》2017 第 12 期。

三、加密货币的监管方向

加密货币是利用区块链技术进行去中心化管理的数字化资产①。数字货币包括加密货币，指以数字化形式存在的货币，与实物货币不同之处在于可以实现即时交易和无边界所有权转让，可以是去中心化管理也可以是中心化管理。

虽然区块链和加密货币被广泛地混用，但实际上，区块链是加密货币的底层技术，而不能等同于加密货币。加密货币是分布式网络中用户进行资金交换的媒介，它的所有交易记录均可通过区块链进行追踪，且可在参与者双方之间直接发生而不需要任何中介。

比特币是市场上最知名的也是世界上第一个加密货币，其背后的核心思想是构建一个基于数字证明和加密学的独立且去中心化的电子支付系统。现在市场中充斥着许多类型的加密货币，且每一种加密货币都具有其独特的性能和机制，但是并不是所有的加密货币都拥有独立的区块链，加密货币开发者既可以选择创造一个新链条，也可以选择基于已存在的区块链进行开发。换言之，区块链是因，加密货币是果；加密货币是区块链的技术应用，但更广泛的数字货币不一定用到区块链技术。我们只讨论基于区块链技术的加密货币，而声称是加密货币但并未应用区块链技术的币种并不在我们的讨论范围内。

（一）加密货币底层技术的风险

加密货币与法定货币相比，具有双重风险，即底层技术本身的风险和金融应用的风险。从底层技术来看，加密货币中的区块链技术包括密码学、共识机制和激励机制，可以从两个方面来评估技术风险，一是合规监管的能力，二是防攻击和防欺诈的能力。

合规监管的能力反映进行监管控制的难易程度，指是否支持超级权限节点对全网节点、数据进行监管。不同类型区块链合规监管能力不尽相同。区块链按每个节点的集中程度从高到低可以分为私链、联盟链和公有链。私链完全抛弃了去中心化的性质，写入权限仅在一个组织中，虽然可控性强，但丧失了区块链的不同组织进行协作的独特功能。联盟链的开放程度有所限制，参与者是被提前筛选出来或者直接指定的，交易成本低只需要被几个受信任的高算力节点验证，且规则灵活，可以很容易地修改规则、还原交易，修改余额等。因此，联盟链可控性较强，适用于不断修正迭代变革的监管规定，且可以有一定的隐私性。公有链是完全去中心化，任何人都可以读取和参与共识的开源系统，主要采取工作量证明机制（PoW）、权益证明机制（PoS）、股份授权证明机制（DPoS）等共识方式。公有链的所有数据是默认公开且缺乏隐私性，所以可监管难度较大。

防攻击和防欺诈的能力反映整个系统的技术安全性。公有链面向全球用户，所有用户均可登录，不设访问权限，是黑客攻击的重点。二线加密货币如比特币，曾多次出现攻击者利用多于其他参与者的算力修改、控制交易记录的欺诈事件。联盟链和私有链上的安全事故大多发生在其算法和底层设计本身，偶有黑客出于商业目的进行攻击。

从合规监管、防攻击防欺诈两方面能力来看，联盟链和私链可监管性强，系统安全性较高。而公有链由于其开源的特征导致可监管性差，其安全性较低。在联盟链和私链中，私链的应用场景较低，基于联盟链的加密货币可能是未来融入稳定金融体系的新型货币的方向。

（二）加密货币交易所的监管手段

全球范围内至少有超过 200 家加密货币交易所。目前这些交易所没有上市任何被视为证券的数字资产，它们绝大多数都不受监管限制。随着加密货币市场规模的扩大，这些加密货币交易所的活动持续渗进市场，因此现在应该关注如何对交易所的进行监管。韩国的《特别金融交易信息法》法律修

① Lakhani K. R., Iansiti M., "The Truth about Blockchain", *Harvard Business Review*, 2017, 95, pp. 118-127.

正案规定，虚拟资产交易所必须在韩国金融服务委员会（FSC）进行注册，违者将面临最高五年监禁或者最高 5000 万韩元的罚款。所有虚拟交易所都必须设立所谓的真实姓名虚拟银行账户（即交易所主要账户的子账户），以满足 FATF 的国际反洗钱指南要求。与此同时，立法中还放宽对交易所信息安全管理认证的要求，对于首次验证失败的机构，允许其在宽限期内完成调整并再度提交申请。借鉴韩国经验，对当前设立的交易所进行整顿，让加密货币行业脱离监管灰色地带，接受有效、合理的金融监管。

（三）通过共识机制内嵌监管规则来约束加密货币

从金融应用来看，区块链的应用主要在于加密货币的发行与交易。未来监管的重点在于对发行方的约束以及对共识机制的把控。

区块链从底层技术到共识机制再到价值传递已经是相对完整的一套体系，目前监管所针对的加密货币都是从这一套体系中产生的。如今区块链技术以及传递体系都较为稳定，大多数监管问题出现在具备把控传递环节能力的货币发行方。加密货币的发行更像是证券发行，有类证券属性，需要监管部门严格定制发行规则。

区块链的基础架构有五层，包括网络层、共识层、数据层、智能合约层和应用层，如图 2 所示，每一层分别有一项核心的功能，各层之间互相配合，从而实现了去中心化的信任机制。共识层作为区块链最底层的运行基础，能够让高度分散的节点在去中心化的系统中针对区块数据的有效性达成共识。区块链中比较常用的共识机制包括工作量证明、权益证明和股份授权证明等。在共识机制中内嵌监管规则就是建立适当的惩罚机制，促使区块链参与者符合监管要求。从监管层面来看，把监管程序写进共识机制里让区块链自动运作，以及建立共识机制层面的应急方案均具备重要意义。共识行为存在于每一个生产环节，共识产生激励和惩罚机制，激励机制和惩罚机制也存在于每一个环节中。

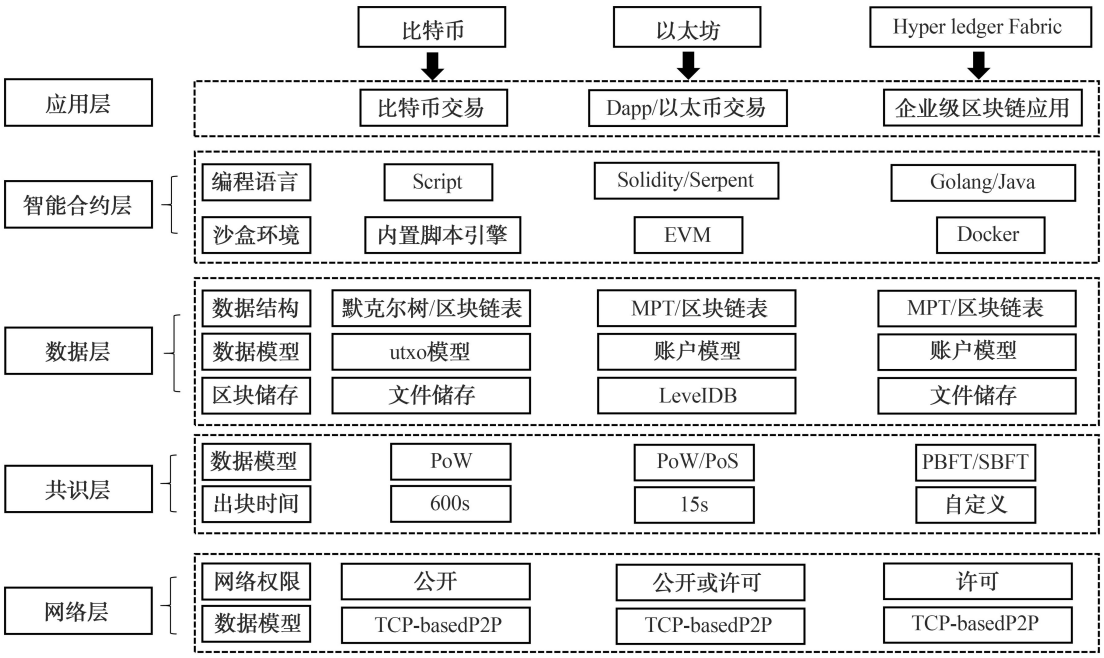

图 2　加密货币的结构

资料来源：作者整理。

工作量证明共识机制（PoW）中，惩罚机制通过损耗求解哈希难题的沉没成本，防止参与者随意违规新增区块和更改区块，达到提高区块链安全性的目的。通过惩罚设计，工作量证明共识机制设置了两个安全关卡：第一道关卡设在参与者竞争记账权的时候，使得参与者不能随便新增区块。一方面，参与者在试图获取记账权之前要耗费大量算力求解哈希难题，这一成本是沉没成本，只要参与者试

图获取记账权，那么无论他最终能否成功新增区块都要付出一定的算力成本；另一方面，由于哈希难题的验证远远比求解容易，对新出区块的验证成本非常之小，因此，只要参与者新增的区块交易无效、格式不符等，就会很快地被其他节点检测出来废弃掉，他之前白费的挖矿成本相当于对他的惩罚。

第二道关卡则设在区块被成功添加区块链后，参与者不能随意修改区块链。以比特币为例，在比特币网络上大约 2 周之后，所有客户端将根据新区块的实际数量与目标数量差异的百分点调整目标哈希值，增加或减少块创建的难度，确保每 10 分钟 1 块的恒定出块速度。随着挖矿难度提高，进攻成本也相应提高。进攻者要建立一个比真实的区块链长的秘密区块链，例如，在比特币网络中建立 6 个区块，同时在秘密的区块网络中建立 7 个区块。

可以简单计算一下攻击者的成本。假设一台比特币挖矿机器价格为 2700 美元，一天可挖 0.0012 枚比特币，每天耗电 33 度，每天的电费是 2.6 美元。假定矿机的折旧年限为 3 年，可推算每天固定资产折旧为 2700/(365×3)＝2.5 美元，加上耗电费用 2.6 美元，得到挖出一枚比特币的生产成本为 (2.5 + 2.6)/0.0012＝4250 美元。由此推算，攻击者在攻击成功前要付出约 3 万美元的成本，而且这一成本随着挖矿难度的增加不断上升，再加上与诚实者的算力竞争，显然对算力提出了很高的要求。只有拥有比特币全网 51%算力的攻击者，才可以重新计算已经确认过的区块。

上述工作量共识机制中的两道关卡使得参与者随意违规新增区块和更改区块时均要付出高昂的成本，确保了比特币各区块哈希值的唯一性及难以篡改。共识机制中的惩罚机制最大限度地激励网络中的理性行为人，使他们在最大限度满足自己的利益时也达成了整个系统的利益最大化，实现了激励相容。

权益证明(PoS)机制可以有助于防止 P + Epsilon 攻击。在该攻击中，攻击者会用可信的承诺贿赂其他参与者攻击，但事后却无须付出任何成本。假定攻击者给予参与者们一个可信的贿赂预期：当其他人选择“协作”时，如果你选择“攻击”，我将给予你比选择“协作”更高的收益，通过这样的贿赂，在假定其他人都选择协作时，理性的参与者就会选择攻击。但如果所有参与者都被贿赂成功，此时的纳什均衡解就变为(攻击，攻击)，各自的收益均为-1，攻击者无需付出成本，不用兑现贿赂承诺。也就是说，攻击者只要以可信的预算和承诺(例如将资金锁定在智能合约)，就可零成本地实现对系统的攻击。例如在表 2 的例子中，假定博弈双方都选择协作，双方的收益都是 8，如果都选择攻击，双方的收益都是-1。在攻击者给予一个可信的贿赂预期，使得一方攻击，另一方协作时攻击方得到 8 + ε 的收益(ε 可为任意大于零的值)，大于都协作得到的收益 8，而协作方获得-2 的收益，那么所有参与者就都会选择攻击。但这时所有人的收益都是-1，攻击者就无须兑现贿赂承诺。

表 2　博弈双方收益矩阵

	协作	攻击
协作	(8,8)	(−2,8+ε)
攻击	(8+ε,−2)	(−1,−1)

权益证明(PoS)机制中可以引入严厉的惩罚对上述攻击行为予以预防。如上所述，参与者需要提取一定比例的私人权益作为保证金，投注于未来的区块中，随后根据投注的情况进行处罚。比如，如果事后可以明确地证明一个特定的区块是有问题的不合规区块，那么就会对这个区块的投注者进行最大限度的惩罚，没收投注者的保证金，这就改变了 P + Epsilon 攻击时参与者的预期收益。他们选择攻击时的收益会显著减小，有更大的动力选择协作，继续在真实链上工作，而不是参与作恶，同时又大大增加了攻击者的贿赂预算。理论上，攻击者需要拥有 51%的权益，才有可能发起成功的攻击，这对权益的要求是巨大的。因此即使攻击者攻击成功，自身的权益也会受到很大的损失，这就降低了发

起 P + Epsilon 攻击的激励。

在实际监管的设计中,可以通过监管沙盒设计适当的惩罚机制、调整惩罚力度,激励参与者遵守规则,最大限度营造合规的网络体系。例如,可以让区块链自身在监管沙盒范围内试错,通过总结经验、自我学习,将一定的惩罚机制写入共识。在试错完成后,这套体系将正式运作,并最终达成通过区块链技术对现有的加密货币生成方式进行优化的目的。

在加密货币监管上,我们还需要摸索和构建区分劣币良币的标准。现阶段,从安全机制(Safety)、环境(Environment)与交易机制(Transaction)三个维度构建的"SET"指标评估体系来监管加密货币是较为理想的模式。从安全角度看,技术与机制在面对外界攻击时的稳定性、数据流量的承载力以及对监管的透明度,是衡量加密货币优劣与否的首要因素。从环保角度看,区块链应用和加密货币的生成必然会伴随着能源的消耗和散热,评判其单位能耗高低将是一个非常重要的考核维度。从交易机制看,低交易成本与高处理速度是衡量加密货币算法优秀程度的重要方面,也是构建标准的重要考量。

四、区块链对监管科技的推动与改造

(一)区块链与监管科技的结合

大量的数据是监管科技加速落地的直接推动力,在 2008 年金融危机后,全球范围内的金融监管均普遍加强①,更多更高质量的数据报告涌现,存储容量和计算能力的增长以及数据科学的进步也为监管科技的应用提供了技术条件。

与巴塞尔银行监管委员会(BSBC)2018 年定义类似,Broeders 和 Prenio 将监管科技(Suptech)定义为"监管机构使用创新技术去进行金融监管"②。不同于 Regtech 意为支持受监管金融机构遵守监管和报告要求的创新技术的应用,Suptech 特指监管机构自身使用的技术,这种技术能力的获取既可以来自于独立研发,也可以来自于合作。他们还统计了全球范围内监管机构在数据收集(如自动报告、数据管理和虚拟协助)和数据分析(如市场监管、不当行为分析、微观审慎监管和宏观审慎监管)中使用的监管科技,发现大数据、机器学习、人工智能、云计算等已经得到相对广泛的应用,但区块链在监管科技中的应用较为欠缺。由于新型科技技术在金融机构应用的出现,传统的监管技术手段无法满足现有的监管需求,因此要大力发展监管科技。

监管科技领域也经历了明显的迭代,由第一代以信息流管理为主要技术,已演化成第三代融合大数据和第四代叠加人工智能的技术。利用区块链系统内部搭建以大数据和云计算为核心的金融风险预警机制,实现金融风险的实时防范能力是近期监管科技的重要方向。

结合区块链技术的新型嵌入式监管可以缓解数据可用性与成本之间的冲突,解决数据收集、验证以及隐私等相关问题。传统的监管方式下,金融机构的合规支出投入很大,尤其对于中小机构,在获取所需数据和保持成本之间面临权衡取舍,而新型嵌入式监管则可以很好地解决这一问题。在运用新型嵌入式监管时,也有两大原则需要注意:其一,新型嵌入式监管要求适当的监管,充分了解基于分布式账本技术 DLT 的交易可以实现以及不能实现的目标;其二,在设计嵌入式监督时,监督者需要考虑自己的行为对受监管市场的影响。

(二)全球监管机构对区块链技术的态度

区块链技术具有去中心化、不可篡改、透明度高等特点,在一定程度上能够解决交易中存在的安

① Arner D. W., Barberis J., Buckley R. P, "FinTech, RegTech and the Reconceptualization of Financial Regulation", *Northwestern Journal of International Law and Business*, 2016, 37(3), pp. 371-413.

② Broeders D., Prenio J., "Innovative Technology in Financial Supervision: The Experience of Early Users", *FSI Insights on Policy Implementation*, 2018,9.

全和信任问题，但也不可避免地削弱货币政策有效性，甚至影响金融稳定。各监管机构对区块链这一新技术开展了广泛的研究。如：国际清算银行成立创新中心，促进全球央行在金融技术方面的国际合作；美国证监会在2017年成立分布式账户小组，对区块链可能带来的风险进行识别；瑞士成立了金融市场监管局、财政部等联合工作小组，加强对区块链和ICO的跟踪研究；新加坡信管局在2016年启动了分布式账户技术在跨行清算领域的试验项目，并与香港金管局签署合作备忘录，加强对分布式账户在跨境贸易融资领域的合作。

考虑到分布式账户、区块链技术可能对金融稳定产生影响，全球范围内的监管机构都在密切关注。如欧洲央行较早地关注到密码技术在数字货币、资产登记等领域的应用，认为使用区块链技术记录资产所有权信息，即使丢失或者被盗也能够找回①。欧洲央行国际金融研究所较早地关注到分布式账本技术在金融领域的应用前景，认为智能合约可以应用于贷款、债券、保险、物联网等各个领域，指出一旦智能合约被部署到分布式账本上，通过消除人工直接参与，计算机程序可以提高合约关系的效率和经济性，减少出错、误解、延迟或争议的问题。区块链技术有助于在全球范围内更好地追踪和打击非法资金流动，监管机构需要采用切实的改革措施来支持新技术打击洗钱犯罪，特别是考虑到洗钱这一非法活动已经占全球GDP的5%，但只有不超1%的洗钱被冻结或没收。

国际组织已经在密切关注区块链对传统金融体系的影响，但倾向于继续关注，而非直接进行监管干预。如2016年初，金融稳定委员会(FSB)召开专题会议，讨论区块链对金融系统的冲击，认为目前应该从技术角度、积极关注区块链发展和应用，暂无必要制定政策进行监管。2017年初，国际清算银行(BIS)认为，分布式账户可能会改造资产形态、合约履行、风险管理等领域，但还需要继续观察。欧洲证券和市场管理局(ESMA)主要关注分布式账本技术应用于证券投资带来的影响，特别是在虚拟货币领域的应用，如以虚拟货币为标的的集合投资计划或衍生品，包括使用虚拟货币分布式账本进行独家交易的股票、基金和期权等。

在对区块链技术的应用监管上，各国的意见是一致的，即区块链作为技术手段在改造金融业务的同时，也不能脱离金融监管。如美国证监会虽然没有禁止在证券业务中应用区块链，但明确指出，使用分布式账户来替代传统的中心化记账方式不会改变证券交易本质，仍需严格遵守各类监管法律法规。英国金融行为监管局表示，监管的对象是金融活动和金融机构，在技术中立原则下，不会干预分布式账户在金融中的应用②。瑞士金融市场监管局也强调了技术中立原则，违反监管规定的行为并不会因为所使用的技术而得到豁免。瑞士金融市场监督管理局③和英国金融行为管理局④讨论了基于分布式记账的融资行为，认为分布式账本技术使得资产支持代币的分散交易成为可能，也使得基于这些代币的分散金融工程通过自动执行的智能合约成为可能，但无论是首次代币发行(ICO)或传统首次公开发行(IPO)均不会改变潜在风险。

对于区块链等新技术的应用，各国的监管态度存在一定的差异，对ICO、数字货币等尚未形成全球统一的“负面清单”，存在监管套利空间，严重的话甚至会形成区块链等新技术的“法外之地”，造成风险的外溢和跨境传播。整体上来看，美国等大型经济体对区块链等新技术更为谨慎，而部分开放经济体如香港对数字资产的交易等更为积极。如2018年11月1日，香港证监会(SFC)发布《有关针对虚拟资产投资组合的管理公司、基金分销商及交易平台营运者的监管框架的声明》，表示将与有意并

① Miseviciute, J., “Blockchain and Virtual Currency Regulation in the EU”, *Journal of Investment Compliance*, 2018, 19(3), pp. 33-38.

② Financial Conduct Authority, “Discussion Paper on Distributed Ledger Technology”, http://www.fcaorg.uk/publication/discussion/olp17-03.pdf, 2017.

③ Swiss Financial Market Supervisory Authority, “FINMA Reduces Obstacles to FinTech”, 2016.

④ Financial Conduct Authority, “Distributed Ledger Technology: Feedback Statement on Discussion Paper”, http://www.fcaorg.uk/publication/feedback/fs17-04.pdf, 2017.

已达到严格标准的虚拟资产交易平台营运者合作，将其纳入证监会监管沙盒，同时考虑在适宜时机发出牌照，对虚拟资产交易平台进行密切监察。这是在全球首个虚拟资产交易平台做出明显监管指引的地区。

五、基于区块链的“嵌入式监管”设想

对区块链技术的关注存在两方面的动因，我们既关注新技术应用带来的潜在风险，更关注如何利用区块链等新技术来强化金融监管。一方面，因目前我国金融监管部门受到信息数据约束、监管成本较高以及信息不对称的影响，导致我国对金融科技的监管严重滞后，无法与各种金融科技应用场景、应用业务和服务进行匹配①。同时，大数据、区块链和人工智能等底层技术为在技术实现过程中因算法的复杂性、不透明性和人为操纵易形成“算法黑箱”，存在巨大的欺诈风险②。虽然建设我国金融科技监管体系已经成为共识，但如何落地并没有形成共识与明确的路线图。从国外启示来看，如德国在金融科技领域中应用了大量的区块链技术，包括在完成清算领域使用区块链解决方案的试验、建立加密货币交易所、推出区块链银行账户等③；英国推行监管沙盒，实现实时化、信息化及全景化的监管④。但如何对各类金融科技应用场景实现差异化监管仍然是亟待解决的难题。王海波和马金伟提出以“区块链+监管”的思想构建“法链”监管模式，但并未给出具体的落地路径⑤。

基于区块链的“嵌入式监管”设想为使用区块链技术、自动阅读市场的分布式账本的监管方式。嵌入式监管是一种监管框架，通过阅读市场分类账，可以自动监控基于数据的市场是否符合监管标准。这将减轻企业的行政负担，同时提高数据质量，嵌入式监管需要遵守内嵌性、经济性、共识性、公平性4类原则，如表3所示。

表3 嵌入式监管需要遵守的原则

序号	内涵	说明
原则1	嵌入式监管只能作为备份的整体监管框架的一部分发挥作用。	基于分布式账本的交易可以作为资产所有权转移的证明，但底层的基础资产和数字化Token的联系需要由法律体系确认。必要时还需要引入第三方机构来保证智能合约的实现。
原则2	嵌入式监管需要适用于去中心化的市场，并且能够实现经济有效性。	如果不存在中心化的中介机构来确保资金或者证券的转移是不可撤销的，则需要采用经济的方法。需要确定一个最终交易点，从这一特定时刻起，交易一旦确定，撤销将永远无利可图。
原则3	嵌入式监管需要考虑到市场反应，形成市场共识后推进。	在未形成共识的情况下推行嵌入式监管，受监管机构能通过篡改区块链中的交易信息来欺骗监管；监管者需要确保已经形成强烈的共识，同时保持威慑，即受监管机构采用欺骗监管的方式是无利可图的。
原则4	嵌入式监管应该保持较低的合规成本，并为小型和大型企业提供公平的竞争环境。	在设计嵌入式监管时，需要考虑到成本因素，即使满足合规要求的固定成本保持在较低水平。同时，嵌入式监管应该监管市场的各个方面，以确保进入者有一个公平的竞争环境。

资料来源：作者整理。

① 杜青雨：《我国金融科技监管体系构建策略研究》，《技术经济与管理研究》2020年第1期。

② 袁康：《社会监管理念下金融科技算法黑箱的制度因应》，《华中科技大学学报（社会科学版）》2020年第1期。

③ 张伟、董伟、张丰麒等：《德国区块链技术在金融科技领域中的应用、监管思路及对我国的启示》，《国际金融》2019年第9期。

④ 徐晓莉、杜青雨：《我国金融科技监管体系研究：来自国外的启示》，《新金融》2019年第6期。

⑤ 王海波、马金伟：《金融科技监管新模式：“法链”模式发展路径研究》，《金融与经济》2019年第9期。

实现嵌入式监管需要首先正确理解基于分布式账本的交易可以实现什么、不能实现什么。根据徐忠和邹传伟的分析，区块链主要应用方向包括无币区块链、以非公开发行交易的 Token 代表区块链外的资产或权利、以改进这些资产或权利的登记和交易流程、以公开发行交易的 Token 作为计价单位或标的资产、用区块链构建分布式自治组织①。Budish 同时关注到匿名的、分散的区块链实现均衡必须同时具备两个条件：一是需要保持零利润状态，否则矿工就会进行寻租竞赛，导致区块链分叉；二是满足系统脆弱性的激励相容条件，即对于“多数攻击”的计算成本必须超过好处②。显然，如果比特币在经济上变得足够重要，它将受到多数人的攻击，导致易受攻击、系统脆弱。Abadi 和 Brunnermeier 指出，区块链存在三元悖论，即没有一个分类账户能够同时满足：正确、分散和效率三个理想条件，区块链必须通过计算成本高昂的工作证明算法，为正确性提供静态激励③。

实现嵌入式监管需要在共识机制内嵌监管规则，这是一个较大的技术挑战。区块链技术需要通过共识机制、以确保消息的真实性，而共识算法是达成协议、将验证信息添加到分类账簿、记录在区块链的算法基础。合适的共识算法满足三个条件，首先需要有自我调节的激励机制，以调动网络参与者的积极性，通过激励好的行为、惩罚坏的行为来实现。其次，需要能够防止双花攻击，以确保只有有效和真实的交易才记在公共透明的账簿中。再次，确保区块链不存在区别对待，任何人都能在同一个基础上参与进来。

可以探索的一个路径是鼓励具有公信力的第三方参与者来验证写入到区块链中的合约，实现嵌入式监管。理论上，基于分布式账本的分散数据结构能够保证数据的可信度，通过依赖分散市场的建立信任机制，不需要基于中间商的数据验证，但为制约金融机构篡改数据的冲动、强化共识机制，有必要引入具有公信力的第三方参与者来验证写入到区块链中的合约，防止金融机构撤销区块链及相关合约。这些第三方验证者还可以执行其他操作，例如 KYC/AML（反洗钱）或其他法律背景检查。

在实践中，需要注意的原则如表 3 所示，另外包括：

首先，确保区块链嵌入式监管的不可更改性。在区块链设置中，需要保证所有有效区块一旦被提交到区块链上就不会被撤销。当用户进行交易时，通常也希望在转账完成后能够保证转账操作不能随意更改或撤销。因此，在设计区块链共识协议时，确定性至关重要。

其次，作为一种新型的监管模式，在沙盒实验中进行演化和观察是必要的。在建立监管体系时，建议让区块链自身在监管沙盒范围内试错，通过总结经验、自我学习，将一定的惩罚机制写入技术中，最终达成对金融场景进行全环节、嵌入式监管的目的。

最后，要在监管和隐私保护中取得平衡。区块链技术能够形成大量的智能合约，为嵌入式监管提供了丰富的场景，但考虑到智能合约中涉及大量的客户信息，如何在保护客户信息、保持机构商业秘密和保障监管落地中需求平衡将是一个挑战。

六、对中国发展区块链金融监管的具体建议

在信息不对称条件下出现的多层激励冲突是造成监管失灵的主要原因④，嵌入式监管显然可以缓解信息不对称，提高监管效率，而且可以实现前置监管。传统的金融监管模式下，金融监管只能在金融风险发生之后，针对其订立新的规则和制度来约束其中的风险，这就使得在金融创新方面监管多

① 徐忠、邹传伟：《区块链能做什么、不能做什么？》，《金融研究》2018 年第 11 期。

② Budish E.，“The Economic Limits of Bitcoin and the Blockchain”，*National Bureau of Economic Research*，2018，No. w24717.

③ Abadi J.，Brunnermeier M.，“Blockchain Economics”，*National Bureau of Economic Research*，2018，No. w25407.

④ 蒋海：《金融监管中的激励冲突与调整》，《财经研究》2004 年第 1 期。

属于“事后监管”,由此会导致金融创新在发展前期会经历一段时间的“野蛮生长”,由此产生的后果只能事后去弥补,导致这种现象主要原因还是缺乏有效的监管工具。如果将“区块链”和“监管”相融合,可以丰富金融监管手段,打破金融监管方式总是滞后于金融创新的不利局面。其中的技术基础是,只要金融机构或者金融监管部门使用大数据技术搜集到金融数据,通过云计算技术分析符合事先设定的金融风险标准,则区块链系统将自动执行报警系统。此时,无论是外界条件发生改变,还是人为控制,都无法阻止系统对金融风险的预警,无疑会增强对金融风险的防范能力①。

2017 年 6 月,中国人民银行印发《中国金融业信息技术“十三五”发展规划》,提出要加强金融科技和监管科技研究与应用,但并未提出具体落地的步骤。从全球范围上来看,我国央行的监管科技仍然处于起步阶段,监管机构在开发和使用监管科技的过程中也遇到了各种问题和挑战。因此,对推进区块链技术的监管科技应用,提出如下建议:

一是加强全球范围内的监管科技合作。全球范围内各个监管机构虽然表示都将坚持技术中立原则,倾向于继续维持现有的监管架构,但尚未制定一个全球共识性的区块链监管战略。与各国监管机构合作构建区块链监管战略,该战略至少应包括以下三个关键要素:第一,远大但可实现的目标(例如,在未来三到五年内,哪些技术将用于监管领域,该技术将如何嵌入组织以及如何获得资金);第二,对目前数据可用性、数据质量和分析资源的评估;第三,监督机构将战略分解到落地的行动计划。

二是根据业务场景制定一个更为详细的路线图。可根据监管难度,从跨境结算—智能合约—证券投资的步骤分阶段制定技术标准和监管流程。从目前的应用场景来看,区块链在银行系统的应用相对可控,虽然没有制定统一的规范,但区块链在跨境结算等领域已经展示出明显的优势。在智能合约的应用需要一个具备公信力的平台,监管可以参与平台的搭建和维护。类似地,继续保持对 ICO、数字货币交易的高压监管态势,以防止对传统金融体系的冲击。

三是由央行牵头成立专门的机构进行区块链监管研究。IMF 最新的报告显示,全球范围内的监管机构都在积极成立监管科技部门,如新加坡金融管理局(MAS)成立监管科技办公室,作为 2017 年成立的数据分析集团(Data Analytics Group)的下设机构;荷兰银行(DNB)成立数据科学中心从事创新技术的试验性应用;澳大利亚证券投资委员会(ASIC)成立了负责数据战略的首席数据办公室和一个数据管理委员会,强化数据的适当性管理;英国金融行为管理局(FCA)也组建监管科技和高级分析团队,探索使用监管科技。而为推进区块链监管技术组建合适的、多学科背景的人才团队将是巨大的挑战。

四是与外部区块链技术供应商进行紧密合作。从过往经验来看,用于数据收集的 Suptech 应用程序往往由外部服务提供商开发。如卢旺达国家银行(BNR)将数据仓库的开发工作发包给了商业智能和分析公司 Sunoida Solutions,合作开发了一个电子数据仓库(EDW)系统,实现自动化和简化报告流程,以促进监督。EDW 系统目前覆盖了 8 家银行、3 家小额信贷机构、2 家汇款运营商和 1 家跨国公司,提高了 BNR 的运营效率,并改善了报告数据的质量、频率和范围。对于拥有复杂信息系统的银行和其他金融服务提供商,EDW 允许 BNR 自动从其系统中“提取”数据。BNR 每天都会提取与交易相关的数据,大大提高了 BNR 实时监控市场的程度。

五是探索通过第三方认证的方式,由具有公信力的第三方来验证写入到区块链中的合约,实现嵌入式监管。考虑到在共识机制内嵌监管规则面临较大的挑战,金融机构往往缺少动力进行自我验证,借鉴京东金融作为第三方推出基于区块链技术的资产云工厂底层资产管理系统,帮助消费金融服务公司实现交易数据的生成和完成结构化融资的交易案例,由第三方验证者执行 KYC/AML(反洗钱)或其他法律背景检查,可以通过密钥作为交易的唯一凭证,写入区块链,建立共识机制。

六是启动内嵌式监管的沙盒试验。监管沙盒是政府给予某些金融创新机构以特许权,使其在监

① 王海波、马金伟:《金融科技监管新模式:“法链”模式发展路径研究》,《金融与经济》2019 年第 9 期。

管机构可以控制的小范围内测试其新产品、新服务的一种机制。2018 年 10 月，央行决定在北京市、上海市等 10 个省市开展金融科技应用试点，随后北京市率先启动金融科技创新监管试点，探索构建包容审慎的中国版“监管沙盒”。因内嵌式监管是一种新型的监管方式，技术难度大、落地难度高，建议在中国版的监管沙盒环境中进行全面测试，特别是对如何内嵌监管要求、确保共识机制、选择合适的应用场景、减少监管成本等进行重点测试，为后续进行全面应用做准备。

From Data Driven to Embedded Supervision: Prospects of Financial Supervision Based on Blockchain

Ba Shusong　Wei Wei　Bai Haifeng

(HSBC Business School, Peking University, Shenzhen 518055, P. R. China;
Silver Economy and Health Wealth Research Center, Tsinghua University, Beijing 100084, P. R. China;
School of Business Administration, Northeastern University, Liaoning 110167, P. R. China)

Abstract: Since the blockchain has been established as a strategic technology in the Outline of the 13th Five-Year Plan for the National Informatization, blockchain technology has developed dramatically, especially in the financial industry. Meanwhile, the cryptocurrencies derived from blockchain technology has also attracted much attention. How to effectively prevent the risk of the underlying technology of cryptocurrencies, constrain the barbaric growth of cryptocurrencies, and construct a benign ecosystem of cryptocurrencies will be important development directions of the future regulatory mechanism. At this stage, supervisors around the world have encountered various problems and challenges in the development, application and regulation of blockchain technology. This paper will focus on the potential risks caused by the application of blockchain, and analyze how to use the new technologies such as blockchain to strengthen financial supervision, and to explore the theoretical exploration of blockchain embedded supervision mechanism.

Keywords: Blockchain; Financial supervision; Embedded supervision

[责任编辑:纪小乐]