区块链在金融领域的应用：理论依据、现实困境与破解策略

本文作者：

吴桐：中央财经大学金融学博士，商务部 CECBC 区块链专委会副主任、数字经济商学院院长，数字资产研究院研究员，中国财富管理 50 人论坛青年研究员，香港国际新经济研究院高级研究员，区块链和数字经济领域知名学者，着有《链改：重塑社会结构与经济格局》、《链政经济：区块链和政务系统的融合》。

张礼卿：普华永道中国首席经济学家，中央财经大学金融学院教授、国际金融研究中心主任、全球金融治理协同创新中心主任，享受国务院政府特殊津贴。

原文发表于《改革》（CSSCI）2019 年第 12 期（12 月），《改革》系中国经济学品牌期刊，CSSCI 来源期刊、RCCSE 中国权威学术期刊，继 2013 年、2015 年蝉联“中国百强报刊”后，2017 年《改革》再度荣膺这一官方最高奖项。首发论文十余篇荣获中国经济学最高奖——孙冶方经济科学奖。**《改革》首倡学术期刊服务中央决策，推出系列创新性举措，产生了广泛的社会效应。**

摘要：区块链具有去中心化、无须事先信任、开放性和自治性等特征，这使得区块链和金融具有内在耦合性，金融成为区块链应用落地的重点领域。但由于区块链在技术成熟度、治理机制和基础设施等方面存在缺陷，理论上的优势并未能在金融领域完全发挥，存在一定的落地困难。推动区块链在金融领域的应用，应进一步完善区块链金融监管治理框架，逐步弥合区块链金融与现有法律政策体系的鸿沟，推出法定数字货币，在合规的基础上构建面向用户的区块链金融商用体系。

关键字：区块链；金融创新；金融基础设施；金融风险防范

2019 年 10 月 24 日中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，中共中央总书记习近平强调，要把区块链作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展。区块链的去中心化、无须事先信任、基于代码运行和自治性等特征改变了传统金融的信任模式，为金融问题的解决提供了新的方案。尽管区块链在支付、征信、保理、贸易融资、供应链金融、证券交易等金融细分领域实现了一定程度的应用，但是，由于其在技术成熟度、治理机制和基础设施等方面仍存在缺陷，使得区块链的应用价值难以完全发挥，大规模推广存在一定困难和潜在风险，如何克服这些局限是区块链进一步实现金融应用价值的关键。基于此，本文在概述区块链之技术特征及创新性的基础上，全面阐述区块链在金融领域应用的理论依据及现实困境，并有针对性地给出破解策略，以期在防控金融风险的前提下，有效推动区块链在金融领域的应用，进而使其在建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

一、区块链的内涵、外延及应用概况

自 2016 年以来，随着区块链在多个行业的落地应用，关于区块链技术及其对经济社会影响的研究也逐步增多。区块链作为一个跨学科、跨领域的复合型技术，其发展和应用与多个学科都息息相关，涉及到计算机、商业金融、数学、法律等近百个领域。当前学术研究的重点仍然集中在计算机科学和密码学上，对区块链在经济、金融、管理和商业应用等方面的研究较少，其中区块链与金融相关的研究主要集中在加密货币层面，缺乏更为一般性的研究。

区块链是将每个数据区块按照时间或者其他逻辑顺序组合成的一种链式数据结构。根据记账方式和开放程度不同，区块链可分为公有链、联盟链和私有链。在公有链中所有节点都参与记账，帐本完全通过公开和可查询，所有节点可自由加入和退出，是市场化程度最高的区块链结构。联盟链是多个机构组成联盟并共同维护管理的区块链系统，由预先选定的节点进行记账，帐本完全或部分对所有参与者公开，是宏观调控和市场化相结合的区块链结构。私有链由单一的中心化机构记账，数据读取权或对外完全开放，或不同程度地受限开放，是管控程度最高的区块链结构。

现有文献对“去中心化”、“自治性”、“无须事先信任”等区块链特征做了概念化的分析与阐述，但基本未涉及特征的具体内涵和实现条件。例如，“去中心化”这一概念仅是对部分公有链而言，联盟链、私有链和部分具有若干超级节点的公有链仍然具有中心化特征；联盟链既可部分解决信息不对称，又能在一定程度上满足隐私要求，同时便于监管、风险可控，因而成为各国政府便于接受的区块链金融落地模式。例如，2016 年 12 月中国人民银行推动的基于区块链的数字票据交易平台已测试成功，并付诸使用；截至 2019 年 10 月，2018 年 4 月

上线的中国建设银行区块链贸易金融平台交易量已超过 3600 亿元，可实现国内信用证、福费廷、国际保理、再保理等功能。二者都是基于联盟链的架构，提高了特定节点对区块链平台的管控程度。同时，Facebook 推出的数字货币 Libra 初期也是采用联盟链架构，并给出向公有链转换的路线图。但现有文献对联盟链在金融领域的应用研究较少。

二、区块链在金融领域应用的理论依据

区块链的技术特征和数据结构可以在不同程度上缓解信息不对称、降低组织和交易成本以及构建更加完善的网络体系，从而为区块链在金融领域的应用提供了坚实的理论依据。

（一）缓解信息不对称性

区块链具有分布式帐本、token 以及智能合约等构成要件。分布式帐本通过去中心 化的方式基于特定共识机制集体维护数据库。任一节点失效，其余节点仍能正常工作。运行规则公开透明，所有数据信息公开，各节点之间基于技术信任无需公开身份，不超过一半节点对数据库修改无法影响其他节点的数据。每笔交易通过密码学实现相邻两个区块串联，可追溯任何一笔交易[1]。

与银行帐本相比，公有链的不同之处主要体现在三个方面：第一，区块链账户是匿名的，帐本交易细节则全部公开，而银行账户是实名制的，帐本交易信息并不公开。匿名开户保证了比特币白皮书中阐述的电子现金的匿名性，唯一性则是通过共识机制来实现，帐本在全网达成共识的基础上，通过私钥控制账户余额。第二，二者做账方式有差异：银行记账是基于复式记账法的“1+1 借贷式”；区块链记账方式是基于共识机制（POW、POS 等）的“1+N 式记账”，表现为一方记账，多方核对帐本。第三，区块链帐本是交易型帐本，银行帐本是账户型帐本。

在传统会计核算体系中，资产负债表和现金流量表相对独立，区块链帐本则将支付、清算和结算实现并行，将记账方式从复式记账变回流水记账，弱化了资产负债表作用，增强了现金流量表作用[2]。如果这一模式在标准化下实现大规模推广，将显著提高金融交易信息披露。

联盟链则是公有链完全分布式结构和传统中心化结构的折中方案，只针对特定成员和有限第三方开放，从联盟中预先指定若干节点为记账人，区块生成由记账节点共同决定，其他节点可参与交易，但不记账，第三方可通过系统开放的应用程序编程界面（API）进行限定查询。联盟链的准入机制提高了交易性能，避免参差不齐的参与者导致的问题，也在一定程度上缓解了信息不对称[3]。2019年基于联盟链的万向区块链供应链金融服务平台在上线 4 个月内融资金额已超过 1 亿元。此外，联盟链是在全球对各种形式代币融资监管趋紧情况下，针对特定公司或组织搭建的区块链架构，不需要通过 token 进行治理，也是各国政府力推的区块链金融模式。

私有链的记账权掌握在特定的中心化组织手中，其他机构都没有记账权，数据结构和信息传递方式与传统中心化组织无本质区别，主要作用在于对企业内部的组织管理进行重构，降低企业组织与沟通成本、实现内部激励以及确保企业数据的不可篡改。

将每个区块链项目作为独立系统考察，能在一定程度上缓解信息不对称，但系统间的互通障碍限制了其应用空间，造成了大量“信息孤岛”的存在。在传统金融市场中，人力、商品以及资金的互联互通对于拓展市场边界、提高资源配置效率、增强市场有效性等都具有重要作用。为解决这一问题，力图实现价值跨链流转的跨链技术应运而生，这使得区块链有望真正成为新一代价值互联网[4]。

（二）降低金融业组织和交易成本

分布式帐本、智能合约以及 token 治理可以降低金融业的组织和交易成本。组织和交易成本曲线的移动会产生新型市场单元——分布式自治组织（DAO）。DAO 依靠一系列公开规则进行运作，可以在无人干预和管理的情况下实现自我运营，参与者可通过购买其 token 分享该组织发展的收益或者消费该组织提供的商品和服务。由于 DAO 对于增强微观主体的金融市场化程度具有重要作用，投融资等金融活动可更加无摩擦地展开，同时具有对企业制度实现迭代的可能性。

企业和市场是两种相互替代的资源配置机制，有限理性等原因使得市场交易费用高昂，企业制度成本主要表现为组织成本。市场和企业的边界存在于交易边际成本与组织边际成本相等的“临界点”[5]。具体到金融业，企业制度对应的是以银行等金融中介为代表的间接融资模式，市场制度对应的是以发行股票、债券为代表的直接融资模式。各国之所以拥有不同的金融制度边界，在于其利用金融市场和机构的“比较优势”存在差异[6]。随着信息经济学的兴起，出现了大量从微观层面上研究信息对金融交易成本和资源配置影响的文献。由于市场在信息和结构方面的不完善所导致的交易成本增加即为金融摩擦，金融摩擦的存在意味着金融市场存在缺陷，当交易中止和市场功能崩溃时，交易成本已趋于无穷。

分布式记账不仅可以在“治本”上通过削弱信息不对称降低交易成本，智能合约则可以在“治标”上降低金融市场的交易成本，并减小金融摩擦。解决由信息不对称产生的“逆向选择”和“道德风险”的一种有效途径是通过合约解决委托代理问题。由于信息不对称和有限理性等原因，所有合同和契约都有遗漏和疏忽之处，都是不完备契约[7-8]。这意味着降低交易成本的“治标之策”同样存

在问题。不完全契约由于借贷契约事后的“受限执行”也会造成金融摩擦。基于区块链的智能合约极大地提高了满足触发条件时的执行力以及对多场景下复杂条件的适应性[9-10]，进而夯实链接物理世界和数字世界的桥梁。

智能合约的概念最早由 Nick Szabo 于 1994 年提出，他认为一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在其上执行这些承诺的协议。智能合约可概括为商业合约的代码化表达，区块链的出现为智能合约的表达提供了极佳的执行环境。智能合约具有自动化和强制化的特点：自动化即智能合约通过程序就可自动执行；强制化即赋予监管部门在特定情境下的某些特定权力。现阶段智能合约已被运用于减少交易成本的金融实践中，如支付清算、供应链金融、保险、征信等。智能合约在金融领域的应用具有深刻的理论和现实意义，为适应金融场景的复杂性，智能合约在增加参数的复杂性、增加标准化代码的普及程度、使用独特语言作为支撑以及建立智能合约标准体系等方面具有较大提升空间。

此外，区块链在降低企业组织成本层面也能发挥重要作用。现代管理学有两个核心问题，一是博弈问题，二是合约问题。相比人工智能、云计算等着力于提高生产力的技术，区块链作为改变微观个体信息和价值互通方式的技术，有望重塑生产关系。区块链深刻改变了企业激励模式和治理机制，引起管理要素的重新匹配，token 治理有望沿着“博弈论—机制设计—新制度经济学—激励兼容”路径为博弈问题的解决提供方案，智能合约则有望沿着“科斯定理—合约理论—产权理论—交易成本理论”路径为合约问题的解决提供方案，见图 1。具体到金融业，近年来金融企业面临着日益增长的人员规模和内部开支，这一问题在金融利

润率下降的情况下尤为严峻。基于私有链架构的金融内控体系成为探索削减金融企业管理层级、提高目标管理的可控度以及保障金融数据隐私性的重要路径。

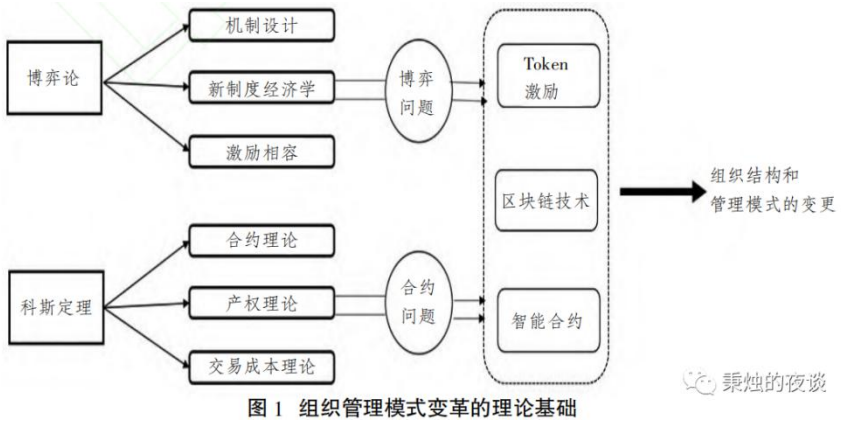

图 1 组织管理模式变革的理论基础

此外，介于市场和企业间的企业间网络也越来越多地受到学界和业界关注。企业间网络既不同于市场也不同于科层，它是一些企业通过正式契约和隐含契约所构成的互相依赖、同担风险、长期合作的组织模式[11]。在企业间网络中，参与相关活动的双方或多方也签订具有法律意义的正式契约，但由于信息不对称和契约非完备，相关方面临多次重复博弈的局面使得各方具有通过隐含契约来协商执行的动机。基于联盟链的企业间网络在减轻信息不对称的同时又通过更加完备的契约进一步完善了原有业务网络，强化了声誉机制，增强了市场和企业之外的“第三种力量”。例如，供应链金融比较契合企业间网络模型，基于区块链的供应链金融主要通过拆分流转应收账款和延伸信用链条实现盈利，易见股份等上市公司已实现基于区块链的供应链金融全产业链服务。　　综合而言，区块链对金融业交易和组织成本都具有显著的降低效应。但对组织成本而言，每个最基本业务模块成本是企业组织活动的边际成本，这一成本在可预见的未来仍旧显著大于零。而随着记账节点的增多和市场范围的扩大，区块链金融交易的边际成本会出现递减。两条成本曲线的交点则是金融企业和市场的边界，在这一交点上大量市

场组织会以 DAO 的形式存在，关于 DAO 的研究也会成为区块链经济和治理的研究热点。

（三）形成更加完善的金融网络

区块链经济模型本质上是一种网络经济，而且是更加接近理想化的网络经济。网络经济并不必然基于互联网，贸易体系和货币体系也是一种网络经济。乌家培在互联网经济发展之初总结了网络经济的七个特点，即无时限经济、全球化经济、虚拟化经济、产销直接联系经济、竞争与合作并存型经济、高效率经济以及创新型经济[12]。

互联网经济的七个特征在基于区块链的数字金融市场中得到了进一步的发展与延申：数字货币的“7×24×365”的市场交易机制真正实现了无时限经济；数字货币打破了国别之间的界限，实现了全球化定价和交易；某些数字货币仅具有支付和交易职能，项目本身不产生现金流，无法采取现金流贴现等传统方法估值，虚拟化程度大大增强；区块链为实现点对点的直接金融提供了坚实的技术条件，在业务流程上实现了去中介化；基于区块链的金融市场相对于以 SWIFT 为代表的传统转账体系更加高效和快捷，传统金融机构和组织已开始吸纳区块链技术，2018 年 9 月 SWIFT 的开发人员完成了在超级帐本 Fabric 区块链上的概念验证；区块链第一次以比特币的形式出现，初衷是以点对点的电子现金系统替代传统支付体系，比特币通过“挖矿”产生，产量每四年半衰，通过控制总量的方式防止通胀，本质上是基于科技的金融创新。

全节点记账和 token 低摩擦流通的特征使区块链系统具有完备金融网络的属性，在高效率实现价值传递和资源配置的同时，也为风险传染提供了途径。在现代金融系统中，金融网络是由银行、券商、基金等金融机构作为节点，金融机

构间的业务关系作为边相互连接所形成的价值网络，其特点在于复杂性和方向性[13]。区块链系统则是一个各节点间都可以直接进行价值交换与传递、所有节点呈现标准化状态的金融网络。利用金融网络研究风险传染路径的文献主要从微观和宏观两个层面切入。区块链作为一个标准化程度更高、摩擦更小的金融网络，其风险传染路径发生一定变化，数字金融网络与传统金融网络应既有相似又有不同。相比于传统金融网络的系统性风险，区块链的系统性风险更大程度上来自于分叉（Fork），当社群内部就如何进行版本升级发生意见分歧并难以达成一致时，就会发生分叉，分叉本质上也是治理问题。

三、现阶段区块链在金融领域应用的现实困境

尽管区块链在金融领域具有巨大应用空间，但现阶段存在治理机制尚不成熟、智能合约难以履行完全契约职能、数字资产价格波动过于剧烈以及无法支撑起安全的商业应用等三、现实困境。造成现实困境的原因不只是技术成熟度有待提高，还有治理机制和基础设施不完善、投机炒作现象严重以及社会接受度和理解力较弱等。如何克服这些局限性是进一步推进区块链金融落地的关键所在。

（一）治理机制尚不成熟

根据区块链治理和决策方式的不同，可分为链上治理和链下治理。链上治理与传统金融治理模式具有一定的相似性，比如持有公有链 token 可获得类似于股票的收益权和治理权[14]。但公有链链上治理与传统金融治理机制也有所差异，公有链的组织形式大多不是公司，而是 DAO，不存在传统意义上的资产负债表。同时 token 还具有消费功能，可在公链生态内进行消费。基于 POW 的公有链出块确认遵循“少数服从多数”原则，一旦一方掌握超过 51%的算力，便能够成功篡改和伪造链上数据。

链下治理在区块链治理中也发挥着重要作用，现阶段重要程度更甚于链上治理。比特币技术开发团队 Bitcoin Core 在版本升级前一般会开放社区辩论，讨论是否应该升级及实施机制，社群意见领袖在其中发挥重要作用，在各方意见达不成一致的情况下，区块链就可能面临分叉，每次分叉都会对公有链共识程度和 token 价格产生重大影响。2017 年 8 月由于就比特币区块大小等问题达不成一致，比特币发生硬分叉，产生比特币现金。2018 年 11 月 Bitcoin ABC 团队和以 Craig Wight 为代表的开发团队就比特币现金版本升级产生意见分歧，再次引发硬分叉。此外，政府监管政策、社会认知水平、部署区块链成本等也构成链下治理的要素。

同时区块链也存在一些不容忽视的治理短板。第一，证券法通过原始股锁定机制实现原始股东和公司的激励兼容，公有链由于缺乏监管难以实现强制锁仓制度，对 token 锁仓相当于放弃了在二级市场高价出售的权利，项目方为实现锁仓只能实行经济激励，为锁仓者支付较高利息，这增加了项目运行成本，也提高了协调项目方和 token 持有者利益的难度。同时 token 进入交易所流通的价格一般数倍于其私募价格，也增大了 token 持有者在上所后的抛售动机和锁仓难度。第二，区块链项目的运营主体往往是 DAO，DAO 不产生负债，也不像公司需要面临负债约束，通过债券及其衍生品发挥治理机制难以实现。第三，通过区块链实现价值广泛流转需要交易概念中的“货币”和“商品”同时上链，否则若商品流转发生在链下，则仅靠区块链难以完成。实现物理资产上链的一个方案是用上链的电子凭证来表征物理资产，从而做到一一对应，但这同样会面临悖论。仅靠区块链而不依赖中心化机构难以保证电子凭证与物理资产间的一一对应关系，物理资产变动与对应的电子凭证同步更新则需要依赖物联网等技术的发展。在现阶段区

块链更适合处理不需要现实物流、能实时交割的数据资产和链上资产，在技术条件、法律政策以及社会接受度等条件全面成熟后再涉及实物资产交割。

（二）智能合约在应用层面存在局限性

智能合约是部署在区块链节点中离散的计算机程序组件，其工作原理类似于计算机程序的“if-then”语句，越复杂的智能合约包含越多语句。当智能合约被部署的时候，代码的哈希值会被计算出来并打上数字签名，单向哈希值、数字签名和代码会被同时复制到由参加区块链的节点组成的网络中，并被盖上时间戳，这使得智能合约具备难以篡改和伪造的特点。

智能合约被赋予实现经济学中“完全契约”的使命，但就现实状况而言，智能合约距理想状态存在较大差距，主要体现在以下六点：第一，智能合约仍是不完全契约，复杂的现实状况可能会让基于代码的智能合约与本意背道而驰。第二，智能合约需要通过链下信息触发，现阶段去中心化预言机尚不成熟。第三，智能合约难以保证链上债务和义务的履行。第四，不依靠中心化机构难以保证链下义务的履行。第五，智能合约没有完善的修正和退出机制。第六，各国法律政策的差异限制了智能合约的适用空间。第七，智能合约质量参差不齐，在缺乏统一标准的情况下，每一次合作都需要较大成本审查代码。

经典理论假定契约是完全的，在现实并非如此。Maskin E. et al.将导致不完全契约的原因归结为三种：一是预见成本，各契约方只能做到有限理性，无法预见所有或然状态；二是缔约成本，以一种各缔约方没有争议的语言形成契约需要成本；三是证实成本，契约的重要信息对缔约方是可观察的，对于第三方证实则需要成本[15]。基于区块链的智能合约本质上是将传统合约中的商业语言转换成

代码，传统合约中的条款转换成代码中的预定义规则，智能合约框架上呈现“if-then”的语言状态，如果达到“if”语句中触发的时间或事件，则执行相应“then”语句中的行为。从导致不完全契约的三种成本看，尽管智能合约采用“if-then；else-then”的语句，仍然难以穷尽所有细分的可能结果，从而导致预见成本的产生。智能合约采用代码编写，不仅具有法律门槛，而且具有技术门槛，这反而可能会增加缔约成本。智能合约最有可能降低的是证实成本。因此智能合约同样是不完全契约，如果缔约方在协商时没有考虑到某些情景而将其归入到“else”语句中，可能会出现与本意背道而驰的结果。

当智能合约的触发条件取决于链外资讯时，需满足的前提条件是将相关信息预先写入链内，现阶段主流解决方案是预言机。预言机是一个为区块链系统提供外部信息的平台，允许区块链连接到现有 API，提供履行合约的必要条件。预言机发挥作用主要依赖两种路径：一是依赖以媒体为代表的中心化信息源，但媒体信息并不能保证完全真实，也极大提高了中心化程度；二是将链外资讯进行分布式处理后在经济激励下依靠集体决策记录到链上，根据结果对投票人按照既定原则实施奖惩，机制类似凯恩斯的“选美理论”，并不能保证大多数情况下决策的科学合理。总结而言，链上和链下仍处于相对割裂状态，弥合二者需要基础设施、治理机制及其他技术等多方面支持。

智能合约保证链上债务和义务履行的基础是交易方具有履约能力。数字货币是系统内运行智能合约的“燃料费”，当履约条件触发时，债务方履约的前提是地址内有不少于须支付数量的数字货币作为备付金。链下债务履约可基于抵押、担保和声誉机制等方式放松备付金要求，链上则缺乏这些柔性机制，其数字账户的资金占用率会比链下模式更高，数字衍生品由于可通过加杠杆进行双向投资，

其备付金数量更加难以确定。Lawrence .L 早在 21 世纪前就将代码和法律并列，主张用技术手段代替传统纸张法典，用代码代替文字，在互联网时代这一现象并未形成[16]。随着区块链的发展，“Code as Law”和“Code is Law”的阐述再次引起讨论，能否实现存在较大不确定性，链外义务履行是智能合约的薄弱之处，不依靠中心化机构难以保证。

智能合约没有完善的修正和退出机制，完全基于预设条件及触发机制自动履行，一旦启动就不可撤销，整体运行过于刚性。同时，智能合约没有价值判断功能，在对社会产生福利损害或违法违规的情况下也无法自行修正和退出，公共安全领域已开始考虑如何防止基于智能合约实现悬赏杀人等危害公共安全的事件发生。如果欲对某人实行暗杀，可以设计智能合约将暗杀行为的诸多要素（如悬赏金额、完成时间、揭榜押金）发布到链上，当有人支付数字货币作为押金揭榜，并在约定时间内完成暗杀后，悬赏金额和押金就会以数字货币的形式自动转到支付押金的账户，暗杀是否完成则需通过预言机进行验证。区块链的技术中性决定了其没有价值判断能力，而社会主体在使用区块链时则不可不进行价值判断。

各国法律政策的差异限制了智能合约的适用空间，并引发潜在冲突。智能合约链上治理的盲点决定了通过中心化机构进行链下治理的必要性。区块链的全球性特征与各国法律政策的差异导致鉴定链下治理依据何处的法律政策存在不确定性，法律适用的属人管辖和属地管辖也可能会存在冲突。智能合约对标准统一的需求客观上要求更加多维和深入的全球化，这与现阶段全球化困境具有潜在矛盾。

此外，现阶段智能合约质量参差不齐，其中可能蕴含着未知缺陷，甚至包含恶意逻辑。智能合约的编写和审查提高了合约缔结成本，在缺乏统一标准的情况下，每次合作相关方都需要耗费精力去编写和审查智能合约代码，这抑制了智能合约在实践中的运用。而智能合约缺乏修正和退出机制则提高了审查代码的必要性，这也进一步推高了成本。

（三）数字资产价格波动过于剧烈

货币的三大基本职能为价值尺度、流通手段、贮藏手段，尽管习惯上把基于区块链发行的 token 称为“加密货币”，但缺乏价值内涵、价格波动剧烈等原因导致其难以发挥货币基本职能，实质上更类似于金融资产。在基于主权信用的法币时代，贮藏手段职能已消失殆尽，价值尺度和流通手段成为货币最基本的职能。

除价格波动过大外，主流加密货币如比特币、以太币等数据吞吐量都较低，比特币 TPS（每秒处理交易笔数）约为 7，以太坊 TPS 约为 25，这难以满足流通手段职能。此外大量经济学者通过不同方式论证其作为流通手段的不足之处[17]。履行流通手段职能的另一个要素是低廉的交易费用，不同于主要依据金额大小收取交易费用的传统金融机构，比特币交易费用取决于交易数据字节在区块中所占的空间，因此比特币交易费用相对金额边际增速递减，使用比特币进行大额支付相比传统方式支付成本更加低廉，基于比特币的小额支付相对于传统支付方式成本相对高昂[18]。这一特点也被比特币的反对者抨击为“交易费不亲民”，这种交易费用特征会导致在金融网络中长尾流动性的缺失，进而不利于发挥流通手段职能[19]。

从价值尺度层面考察，当前仅存在部分主流加密货币（如比特币）为其他加密货币进行定价，绝大多数加密货币都可以用法币（如美元）进行标价。2018年5月后，加密货币进入价格下行通道，法币对加密货币的定价权增强，锚定法币的稳定币（如USDT、TUSD等）流动性比重也逐步增大。此外行使价值尺度的另一必要条件是币值保持相对稳定，为克服加密货币价格波动过大以及推进跨境支付发展，Facebook在2019年6月发布了定位于全球数字货币的Libra白皮书，意在锚定一篮子银行存款和短期国债实现价格稳定。除锚定法定货币的稳定币外，加密货币价格波动幅度都较传统金融资产更大[20]，致使无法行使价值尺度职能。

以比特币为代表的加密货币风险性近年被广泛讨论，其全天候、无涨跌停的交易机制和无统一监管的现状使其具备了良好的投机性。比特币的初始价格近乎为零，大多数比特币投资者也是认可其成长性才进行风险投资。比特币区块链不具有可拓展性，无法产生现金流，仅可作为交易媒介进行流通，不具备内在价值，因此无法利用传统模型进行估价，这也是部分学者将其认定为投机品和资产泡沫的原因[21]。

综合而言，稳定币之外的加密货币的货币属性较弱，资产属性较强。2018年11月中国人民银行发布的《中国金融稳定报告（2018）》中将以比特币、以太币为代表的加密资产单独列出。报告指出，加密资产是一种民间金融资产，其价值主要基于密码学和分布式记账技术，加密资产不由货币当局发行，不具有法偿性与强制性等货币属性，不具有与货币等同的法律地位。

（四）无法支撑起安全的商业应用

《金融市场基础设施建设原则》（PFMI）是各国金融市场基础设施建设的纲领性指导档。2008年国际金融危机爆发后，国际社会得到的一个就是要建立安

全、高效、透明、规范的金融市场基础设施。PFMI 由国际清算银行支付结算体系委员会（CPSS）和国际证监会组织（IOSCO）于 2012 年 4 月共同发布，是加强和保证金融稳定性的关键标准之一[22]。效率和安全是 PFMI 的主要目标，其中安全目标旨在控制和减少系统性风险，增强金融基础设施透明度和金融稳定性。PFMI 同样也应成为区块链金融商用的重要标准。

加拿大央行在 2017 年率先使用 PFMI 评估区块链系统，随后欧洲央行、日本央行和 SWIFT 等机构也先后在多个金融科技项目中就区块链进行评估，初期结果并不乐观，尽管后续随着区块链技术发展评估结果渐趋积极，但距符合 PFMI 支撑起大规模、安全金融商业应用的要求仍然任重道远。具体而言，当前区块链系统还达不到可监管性、可回滚性、实时交易性等 PFMI 基本要求。

金融发展遵循“创新—监管—创新”的历史轨迹，背后逻辑是效率和稳定的平衡，这种平衡的实现依托金融监管制度化。当前对区块链监管仍然秉承互联网监管的平台逻辑，监管重点对象是本辖区内的互联网服务提供商和提供互联网基础服务的大型中介机构，这些机构往往被授权维护互联网秩序。但区块链和互联网存在区别，互联网之所以能被政府有效管制，在于其不是完全分布式，而是存在中心控制点，这些中心控制点的运营商通常位于特定实体空间，在特定国家管辖范围内运作，政府可通过监管运营商来施加影响。而公有链则是完全分布式的，互联网监管的平台逻辑对监管以加密货币交易所为代表的区块链平台和联盟链效果较好，对监管分布式运作的公有链则力有不逮，整体而言可监管性并没有实现。

可回滚性是健全完善的金融市场基础设施的必要条件之一，意味着商业体系的容错机制，可有效防控操作风险和恶意交易。当用户密码丢失时，可通过手机、

身份证等信息找回，但基于区块链的数字货币私钥丢失则无法找回。可回滚性从技术上并非无法做到，基于 POW 的区块链联合 51%以上的算力就可以实现回滚，在需回滚交易之前矿工重新挖一个分叉，剔除掉那笔需要回滚的交易和后续交易，正常打包原链上的其他交易，在新分叉长度超过原来的链后就会发生区块重组。但这种模式意味着后续相关交易都必须回滚，而不只是回滚特定的单笔交易。与此同时，这种模式下的回滚需要较高的经济成本。在 2019 年 5 月加密货币交易所币安被盗 7000 余枚比特币后，比特币核心开发者 Jimmy Song 估算了通过区块重组恢复被盗比特币的经济成本，最经济的模式是 100%矿工同意重组，其成本为 725 个比特币（市值约为 4000 万人民币）。此外，交易回滚可能会对区块链共识机制造成影响，进而引发新一轮的分叉。

此外，大多数公有链系统难以满足实时交易性。“三元悖论”是指区块链技术难以同时实现去中心化、安全性、高效率三项目标。去中心化程度可用权利相同的记账节点的数量衡量，记账节点数量越多，去中心化程度越强。安全性主要基于身份验证、访问控制、加密体系和隐私、密码算法、匿名性、抗攻击能力等六个方面考察。效率主要体现在数据处理能力上，高效的区块链系统意味着高的数据处理能力和低延迟。较为经典的区块链项目如比特币、以太坊等选择了去中心化和安全性的角点解，舍弃了高效率，比特币的 TPS 约为 7，以太坊的 TPS 约为 25，这种数据处理能力难以与中心化处理器进行匹敌，微信、支付宝和 Visa 的平均 TPS 都至少在千数量级。

在区块链技术没有取得突破性进展的情况下，对区块链“三元悖论”的解决方式是将选择从角点解转向非角点解。为进一步研究“三元悖论”，

将“三元悖论”进行了空间化(见图 2)，即建立以去中心化程度 X、数据吞吐能力 Y 以及安全性程度 Z 的三维坐标系，这三个方向分别代表了区块链项目所期望的三个目标。为了简化分析，将去中心化程度、数据吞吐能力以及安全性程度三个变量都单位化。在 X 轴上去中心化程度在[0，1]之间进行选择，0 表示完全中心化的区块链项目，如私有链等；1 表示完全去中心化的区块链项目。在 Y 轴上数据吞吐能力在[0，1]之间进行选择，越接近 1 代表数据吞吐能力越强。在 Z 轴上安全性程度在[0，1]之间进行选择，越接近 1 代表安全性越强。在点 F(1，0，1)表示舍弃数据吞吐能力，保留安全性强和去中心化的区块链项目，比特币和以太坊比较接近这种组合。相应地，点 G(1，1，0)表示舍弃安全性，保留数据吞吐能力和去中心化的区块链项目，安全性对于区块链具有极其重要的作用，没有安全性区块链项目难以发展；点 D(0，1，1)表示舍弃去中心化，保留数据吞吐能力和安全性的区块链项目，比如各公司内部部署的私有链。

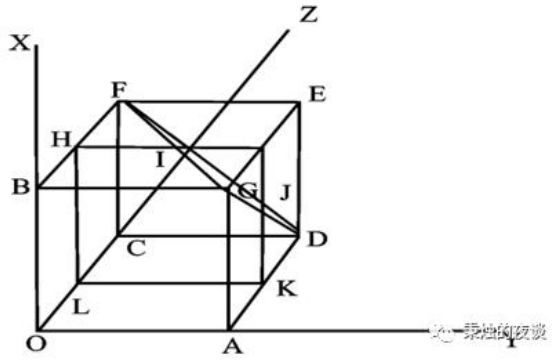

图 2 三维坐标下的区块链“三元悖论”

安全性是区块链发展的基础和前提，当前区块链项目的基本发展思路是在保障安全性的前提下寻求去中心化和高数据吞吐能力的平衡，在三维坐标下则意味着在尽可能使 z 为 1 的前提下平衡 x 和 y 的大小。比较典型的公有链如采用代理权益证明（DPOS）共识机制的 EOS，通过削减记账节点的数量（21 个超级节点）

来提高系统数据吞吐能力。联盟链同样只有若干记账节点，数据吞吐能力较强，全球头部联盟链项目的数据处理能力都非常可观，根据 2018 年的实测数据，Hyperledger Fabric 的 TPS 在 300~500 之间，FISCOBCOS 单链 TPS 可达到 1000 以上，Coco 的 TPS 约为 1600，Quorum 在 Istanbul BFT 协议下的 TPS 可达到 400~800。处于防控金融风险的考虑，各国政府在积极推广许可区块链应用的同时，对大部分非许可链项目仍采取审慎态度。尽管许可区块链具有较高的数据处理能力，但由于保留了部分的中心化色彩，也在一定程度上背离了区块链去中心化的初衷，难以形成市场化程度较高的区块链经济系统。

四、**推动区块链在金融领域应用的现实策略**

尽管区块链作为一种跨领域的复合技术还有诸多需要完善之处，但其必将成为金融参与者的重要竞争工具，并深刻地改变全球金融的业态和格局。2019 年习近平总书记在中共中央政治局第十八次集体学习时指出，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。国内外诸多大型金融机构已在快速谋篇布局和抢占赛道之中，2017 年 7 月高盛的“SETLcoin”加密货币结算系统被授予专利，2019 年 2 月摩根大通推出了基于区块链的 JPMCOIN，2019 年 6 月以瑞银集团为首的 14 家金融公司联合发行基于区块链的 USC 结算系统，2019 年 6 月 Facebook 发布了锚定一篮子银行贷款和短期国债的数字货币 Libra 的白皮书。

与此同时，各国政府和国际金融组织也在加紧对法定数字货币和区块链金融进行研究和测试：2014 年中国人民银行成立了数字货币研究团队，2017 年 1 月

由中国人民银行推动的区块链数字票据交易平台已测试成功，2018 年 9 月由中国人民银行支持推出的区块链贸易融资平台在深圳测试成功，2019 年 8 月中共中央和国务院支持在深圳开展数字货币研究与移动支付等创新应用。此外，加拿大央行的 CAD-COIN、英国央行的 RSCoin、荷兰央行的 DNB Coin、 欧洲央行和日本央行联合开展的 Stella 反映了全球主要央行对区块链在金融领域应用的重视。除主权国家外，诸如 BIS、IMF 等国际金融组织也对区块链进行研究和布局，2019 年 7 月 BIS 表示支持各国央行发行数字货币，2019 年 7 月 IMF 提供了一个新的概念框架分析数字货币，并在探索将来发行全球数字货币 IMF Coin 的可能性。

区块链金融应用赛道已呈全球竞争加剧之势，我国作为新兴金融大国，无论是政府部门还是科技企业和金融机构都应积极回应中央号召、主动拥抱变局，积极研发区块链底层技术，完善区块链金融监管与治理机制，适时推出法定数字货币，大力培养专业人才，积极参加区块链国际标准制定，争取行业话语权，通过区块链助力金融改革、促进金融创新、防范金融风险，实现金融大国向金融强国的转变。现实策略包括如下五个方面：

第一，完善区块链金融监管治理框架，务实推进区块链金融应用落地。推进区块链金融应用需要完善的监管治理框架作为支撑和约束，不仅要注重链下治理框架的构建，更应注重链上治理框架的完善。监管层应充分利用包括区块链在内的金融科技改进监管，发展监管科技，可采用沙盒监管模式，在风险可控的前提下，大力推进金融创新和实践，在试错和迭代中完善区块链治理框架，不断丰富场景应用，成熟一个就推广一个。同时应务实推进区块链金融应用落地，加大对公有链和联盟链的混合链的研究和实践，构建可监管的自金融体系，在充分利用

联盟链许可性和监管性强的基础上，将可公开的数据放到公有链上，接受公众监督，也可使公众享受到数据产生的权益。

第二，逐步弥合区块链金融与现有法律政策体系的鸿沟，提高智能合约在实践中的适用性，适时推动立法。现有法律政策体系对智能合约、DAO 等新生事物约束力下降，社会各界应在推进应用落地的实践中提高区块链要件的适用性，通过发展物联网、大数据等技术为智能合约触发提供客观真实的信息源，将链上金融行为与链下金融权利义务对应，弥合依靠代码驱动的区块链金融设施和现有法律政策体系的鸿沟。

第三，发展以价值为支撑的数字金融，货币金融当局应适时推出法定数字货币。仅靠投机炒作难以实现数字金融的可持续发展，寻找“价值锚”是实现数字金融高水平发展的必要途径，推进物理资产向数字资产迁徙是实现价值支撑的必由之路。货币金融当局应充分发挥数字金融运营成本低、触达能力强、可监管程度高的优势，大力发展数字普惠金融，把握弯道超车机遇，谋求跨越式发展，适时推出法定数字货币，在全球新一轮的数字金融竞争中取得先机。

第四，在合规的基础上构建面向十亿数量级用户的区块链金融商用体系。金融机构和科技企业等商业主体应在合规基础上积极主动推进区块链金融商用体系构建，使之愈加符合 PFMI 要求，着力实现区块链与金融的双向融合与相互促进，在防范金融风险的基础上促进金融创新，推动区块链成为金融基础设施，进而更好地服务实体经济。

参考文献

[1] NakamotoS. Bitcoin: A peer-to-peer electronic cash system. 2008
[2] 吴桐，李家骐. 区块链和金融的融合发展研究[J]. 金融监管研究，2018（12）：98-108

[3] Zheng Z,Xie S, Dai H, et al. An overview of blockchain technology: Architecture, consensus, andfuture trends[C]. *2017 IEEE International Congress on BigData(BigDataCongress) IEEE*, 2017
[4] Tasca P,Thanabalasingham T, Tessone C J. Ontology of elockchain technologies.principles of identification and classification[J]. *Social ScienceElectronic Publishing*, 2017
[5] Coase R. Theproblem of social cost[J]. *Journal of Law and Economics*, 1960, 3, 1-44
[6] Allen F,Gale D. Comparing financial systems[M]. *Cambridge*, MA: MIT Press,2001
[7] Jensen C,Meckling H. Theory of the firm: Managerial behavior, agency cost and ownershipstructure[J]. *Social Science Electronic Publishing*, 1976, 3(4)
[8] GrossmanS J, Hart O D. An analysis of principal-agent problem[J].*Econometrica*,1983, 51(1): 7-45
[9] Buterin V. Anext-generation smart contract and decentralized application platform[R].*Working Paper*, 2014
[10] Kosba A,Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preservingsmart contracts[C]. *2016 IEEE Symposium on Security and Privacy(SP)*.IEEE, 2016: 839-858
[11] 杨瑞龙，冯健．交易成本、法律传统与金融制度边界的决定[J]. 中国工业经济, 2003(11): 5-13
[12] 乌家培．关于网络经济与经济治理的若干问题[J]. 当代财经, 2003(7): 3-7
[13] 巴曙松，左伟，朱元倩．金融网络及传染对金融稳定的影响[J]. 财经问题研究, 2013(2): 3-10
[14] 徐忠，邹传伟．区块链能做什么、不能做什么？[J].金融研究，2018（11）：1-15
[15] MaskinE, Tirole J. 1999 ,“Unforeseen Contingencies and Incomplete Contracts” ,*Reviewof Economic Studies* 66 : 83 —114.
[16] LawrenceLessig. Code, and other Laws of Cyberspace:BasicBooks,1999.
[17] UrquhartA. The inefficiency of Bitcoin[J]. *Economics Letters*, 2016(148):80-82

[18] Houy N. Theeconomics of Bitcoin transaction fees[J]. *Social Science ElectronicPublishing*, 2014
[19] 童牧，何奕．复杂金融网络中的系统性风险与流动性救助--基于中国大额支付系统的研究[J]. 金融研究, 2012(9): 20-33
[20] DyhrbergA H, Foley S, Svec J. How investible is Bitcoin? Analyzing the liquidity and transactioncosts of Bitcoin markets[J]. *Applied Economics*, 2016(19): 1799-1815
[21] Bouri E,Jalkh N, Molnár, Peter, et al. Bitcoin for energy commodities before andafter the
December2013 crash: diversifier, hedge or safe haven[J]. *Applied Economics*,2017: 1-11
[22] CPSS and IOSCO,“Principlesfor Financial Market Infrastructures: Disclosure Framework and AssessmentMethodology”, 2012.

2019 年 10 月 24 日总书记发表区块链重要讲话后，许多传统行业、党政机关和央企国企的朋友都对区块链表现出极大的关注和兴趣，并有进一步学习的计划。区块链不仅是一种技术，更是一种思维理念和经济范式。我在 2018 年 11 月出版的**《链改：重塑社会结构和经济格局》**从经济、管理、金融、技术角度全面阐述区块链，非常适合非技术人员了解和学习区块链，总书记高屋建瓴地指出区块链的落地路径也是“链改”所倡导的路径，深入推进链改是贯彻落实总书记指示的必由之路。同时，我的新书**《链政经济：区块链和政务系统的融合》**也将在近期出版发行。愿我们都做当前伟大时代的参与者，不做旁观人。