



11月6日下午，央行网站公布最近工作论文，徐忠和邹传伟在论文中表示，目前真正落地并产生社会效益的区块链项目很少，除了区块链物理性能不高以外，区块链经济功能的短板也是重要原因。

不要夸大或迷信区块链的功能，区块链应用要立足实际情况，目前区块链投融资领域泡沫明显。应在持续研究和试验的基础上，理性客观评估区块链能做什么、不能做什么。

区块链的经济功能

论文中对区块链应用场景所属行业进行分类，比如Goldman Sachs (2016)。文章根据区块链应用对Token的使用情况提出一个新的分类方法，并讨论这些应用涉及的经济学问题。

(一) 区块链的主要应用方向

表 1：区块链的主要应用方向

应用方向		代表性应用	应用逻辑
不涉及 Token (即无币区块链)		以联盟链为代表，比如区块链用于供应链管理、防伪溯源、数据共享、社会诚信、贸易管理和金融信息披露等；以及在贸易融资、应收账款等场景的应用	发挥区块链的公共共享账本功能，但区块链不直接涉及产权和风险的转移。
涉及非公开发行交易的 Token		资产上链以及区块链在供应链金融和数字票据等场景的应用。	Token 代表区块链外的资产或权利。
涉及公开发行的 Token	以 Token 作为计价单位或标的资产的经济活动	比特币期货、比特币 ETF。	依赖区块链外的法律框架。
	以 Token 作为支付工具和激励手段构建去中心化经济活动	公有链以及基于公有链的分布式应用。	用区块链重构现实经济活动，用智能合约和区块链内的去信任环境来降低或消除对受信任第三方机构的依赖，用去中心化安排和基于 Token 的机制设计替代中心化机构。

区块链应用分成了4类。

第一类应用不涉及 Token，主要将区块链作为分布式数据库或去中心化数据库来使用。代表性案例是中国人民银行数字货币研究所的湾区贸易金融区块链平台和基于区块链技术的资产证券化信息披露平台。

第二类应用以 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。代表案例是数字票据交易平台设计方案。

第三类应用以 Token 作为计价单位或标的资产，但依托区块链外的法律框架和主流经济合同。一个重要方向是所谓的稳定加密货币 (stable token 或 stable coin)。

第四类应用试图用区块链构建分布式自治组织有从业者提出分布式自治组织能替代现实中公司的功能。这方面至今没有广受认可的成功案例，主要受制于：公有链的

物理性能不高，支撑不了大规模交易；智能合约的功能短板；oken价格的高波动性限制了Token作为支付工具和激励手段的有效性；加密经济学（token economics 或 crypto economics）模型设计不合理等。

区块链的治理功能

区块链能支持一些有别于传统的治理机制。

比如，对分布式自治组织，不存在传统意义上的资产负债表，也不存在代表股东权益的股票，但可以通过智能合约赋予某些Token以收益权和治理权，其中收益权通过分红、回购等方式实现，治理权通过参与治理投票来实现。这类股权型Token还可以兼具功能属性，代表是一些加密货币交易所发行的所谓平台币。平台币持有者可以用平台币向加密货币交易所支付交易费用，有时还能享受打折的交易费用。平台币给予其持有者通过投票参与加密货币交易所治理的权利。加密货币交易所承诺定期拿出一定比例的利润，回购平台币并销毁。股权型Token与公司股票有显著差异。

但区块链存在一些不容忽视的治理短板。

第一，Token价格波动对基于Token的激励机制的影响。在公有链的共识算法（特别是POS型）、分布式自治组织以及侧链项目中，出现了很多精巧的机制设计，用Token激励区块链有关参与者的行为趋向预期目标。如果Token价格波动性很高，期权估值也会很高，意味着需要给Token持有者很高的奖励才能激励他们锁定Token。

第二，智能合约的功能短板使现实世界中一些普遍使用的治理机制很难移植到区块链场景中。

首先，在区块链内根据智能合约构造贷款、债券和衍生品等金融工具是比较困难的，而这些金融工具有重要的治理功能。因为不存在负债，分布式自治组织不存在破产问题（尽管其活跃用户数、经济活动量以及发行Token的价格可以趋零），其发起者和运行者也不会像公司所有者和管理者那样面临来自债权人的约束。对分布式自治组织，也无法引入债转股和优先清算等条款。其次，对赌条款是保护投资者权益的重要手段之一，是投融资双方针对未来不确定情况（主要体现为融资方业绩）的一种约定。但因为去中心化预言机的缺失，很难可信地将区块链外的业绩信息写入区块链，也就很难用智能合约实现对赌条款。

第三，Token的快速变现机制影响了区块链项目投融资双方的利益绑定。现实中很

多投融资条款的前提是股权不能转让，股权的非流动性将投融资双方的利益绑定在一起，激励他们共同努力，直到公司上市后他们的股权才可能变现退出。

第四，链内治理（on-chain governance）和链外治理（off-chain governance）的结合问题。链内治理的特点是地址匿名、去信任化环境以及智能合约自动执行，链外治理的特点是真实身份、诚信记录、重复博弈形成的信任和声誉、非正式的社会资本和社会惩罚以及正式的法律保障。两类治理能否有效结合，是一个复杂、有待进一步研究的问题。



图片来源：摄图网

区块链系统的性能和安全性

一些学者从经济学角度对区块链系统的性能和安全性做了有价值的研究。

第一，关于区块链的“三元悖论”，即没有一个区块链系统能同时具有准确、去中心化和成本效率这三个特征。Abadi和Brunnermeier(2018)的理论分析表明，中心化账本具有准确性和成本效率，其维护者可以获得垄断租，特许权价值激励它们准确记账。分布式账本给予记账节点奖励以激励它们准确记账，但通过POW选出记账

节点又牺牲了成本效率。信息在区块链分叉之间的可转移性以及“矿工”之间的竞争，会促成“分叉竞争”。“分叉竞争”有助于消除单个区块链系统享有的垄断租，但也可能带来不稳定性和不协调性。

第二，关于POW的利弊。以比特币为代表的POW仍是区块链中占主流地位的共识算法，POS的安全稳定性还没有像POW那样经受长时间检验。Biais et al.(2018)认为，在基于POW的公有链中，随着“挖矿”总算力上升，“挖矿”难度将往上调，单个“矿工”对算力的投资将构成对其他“矿工”的负外部性。这样就会引发“挖矿”算力的“军备竞赛”，并造成“挖矿”领域的过度投资。Ma et al.(2018)的理论分析发现，比特币“矿工”可自由进入的安排，是比特币“挖矿”消耗资源的主要决定因素，而比特币算法内嵌的“挖矿”难度调整机制对“挖矿”消耗资源影响不大。

第三，POW“挖矿”的经济学问题，特别是交易费率的影响因素。Houy(2014)从理论上研究了比特币“矿工”在打包交易时面临的经济学问题。一方面，打包的交易越多，“矿工”越有可能获得手续费。但一方面，打包的交易越多，区块越大，区块在分布式网络中传播并成为区块链共识所需的时间越长，就越有可能成为“孤块”。

第四，关于区块链的经济安全边界。Budish(2018)从经受攻击的角度，研究了以比特币为代表的基于POW的公有链的安全性，并提出了若干提高安全性的经济激励措施。作者认为，这类区块链的经济重要性越高（比如，设想比特币市值接近黄金），那么恶意攻击它们的可能性也越高，因此要对公有链的大规模应用持怀疑和审慎态度，企业和政府在数据安全方面有比公有链更便宜的技术。

真正落地并产生社会效益的区块链项目很少

总的来说，目前真正落地并产生社会效益的区块链项目很少，除了区块链物理性能不高以外，区块链经济功能的短板也是重要原因。应在持续研究和试验的基础上，理性客观评估区块链能做什么、不能做什么。

一是不要夸大或迷信区块链的功能。这些年的行业实践已经证明一些区块链应用方向是不可行的。特别是，现代金融体系在发展过程中不断吸收各种技术创新。技术创新只要有助于提高金融资源配置效率以及金融交易的安全性、便利性，就会融入金融体系。迄今为止，还没有一项技术创新对金融体系产生过颠覆性影响，区块链也不会例外。加密货币供给没有灵活性，缺乏内在价值支撑和主权信用担保，无法有效履行货币职能，不可能颠覆或取代法定货币。区块链的匿名特征反而会增加金融交易中反洗钱（AML）和“了解你的客户”（KYC）的实施难度。但也要看到，我国的一些国情提供了实践区块链的机会，比如数字票据交易平台有助于缓解我国

票据市场分散化的问题。

二是区块链应用要立足实际情况，不要拘泥于一些过于理想化的宗旨。比如，用科技来替代制度和信任是非常困难的，在很多场景甚至就是乌托邦。再比如，去中心化与中心化各有适用场景，不存在优劣之分。现实中完全的去中心化和完全的中心化场景都不多见。很多区块链项目从去中心化宗旨出发，但后期或多或少引入了中心化成分，否则就没法落地。比如，区块链外信息写入区块链内，往往需要一个可信任的中心化机构，完全的去中心化是不可能的。

三是目前区块链投融资领域泡沫明显，投机炒作、市场操纵甚至违规违法等行为普遍，特别是涉及公开发行业务的Token的项目。政府有关部门应加强监管，防范金融风险。