央行万字论文：区块链能做什么、不能做什么？

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。

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。

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。

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交易的 Token 的项目。

在 10 月 24 日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后，区块链再次成为市场热点，讨论热烈，亦不乏争议。

实际上，央行在 2018 年 11 月发布过一篇 1.5 万字的区块链主题论文，作者为徐忠和邹传伟，从经济学角度分析了区块链的功能，从 Token、智能合约和共识算法三个角度归纳出目前主流区块链系统采取的“Token 范式”，并给予经济学解释。

论文认为，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。**

论文还提了三点建议。

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交易的 Token 的项目。政府有关部门应加强监管，防范金融风险。

需要说明的是，央行工作论文仅为学术研讨，并不代表监管态度。

以下为论文全文：

区块链能做什么、不能做什么?

徐忠 邹传伟

摘要：本文从经济学角度研究了区块链的功能。首先，在给出区块链技术的经济学解释的基础上，归纳出目前主流区块链系统采取的“Token 范式”，厘清与区块链有关的共识和信任这两个基础概念，并梳理智能合约的功能。其次，根据对区块链内 Token 的使用情况，梳理了目前区块链的主要应用方向，再讨论 Token 的特征、Token 对区块链平台型项目的影响、区块链的治理功能以及区块链系统的性能和安全性等问题，最后总结并讨论区块链能做什么、不能做什么。

一、引言

区块链最早作为比特币的底层技术由 Nakamoto（2008）提出。但比特币的脚本语言缺乏图灵完备性 2(Turing completeness),使用的 UTXO(unspent transaction output，未使用交易输出）模型难以支持复杂的状态操作。为此，Buterin（2013）提出了以太坊（Ethereum）。以太坊是一个基于账户模型的区块链系统，脚本语言具有图灵完备性，目标是实现 Szabo（1994）提出的智能合约（smart contract）并支持分布式应用（decentralized application，简称是 DApp）。随着 2014 年美国 R3 公司创立和 2015 年 Linux 基金会发起 Hyperledger 项目，区块链受到了越来越多主流机构的重视。比如，Goldman

Sachs（2016）讨论了区块链在共享经济、智能电网、房地产保险、股票市场、回购市场、杠杆贷款交易以及反洗钱（anti-money laundering，简称是 AML）和“了解你的客户”（know your customer，简称是 KYC）中的应用。中国区块链技术和产业发展论坛 2016 年 10 月发布的《中国区块链技术和应用发展白皮书（2016）》讨论了区块链在金融服务、供应链管理、文化娱乐、智能制造、社会公益和教育就业等领域的应用场景。

2009 年 1 月，比特币网络上线标志着区块链应用落地。但从那时至今近 10 年时间里，除了加密货币（cryptocurrency）发行和交易之外，区块链没有得到大规模应用。截至 2018 年 10 月 31 日，CoinMarketCap 网站统计了全球范围内的 2086 个加密货币和 15545 个加密货币交易所，全体加密货币的市值约 2035 亿美元 (其中比特币市值占比为 54%)，过去 24 小时交易量约 106 亿美元；但 DappRadar 网站统计了以太坊及其上 1137 个分布式应用，发现过去 24 小时活跃用户数只有 12521 人，其中只有 2 个分布式应用的 24 小时活跃用户数超过或接近 1000 人，而且比较活跃的分布式应用集中在游戏、博彩和加密资产交易等与实体经济关系不大的领域。普华永道会计师事务所 2018 年 8 月对 15 个国家的 600 名公司高管的调查发现，有 84%的公司对区块链感兴趣，但 52%的公司的区块链项目处于研发状态，10%的公司有区块链试点项目，只有 15%的公司有正在运行的区块链项目 3。

区块链没能大规模应用的一个重要原因是物理性能不高（特别对公有链）。比如，比特币每秒钟最多支持 6 笔交易，而 Paypal 平均每秒钟能支持 193 笔交易，Visa 平均每秒钟能支持 1667 笔交易 4。很多从业者和研究者讨论如何

提高区块链物理性能，包括中继网络（relay network）、分片（sharding）、增加区块大小、隔离见证（SegWit）、有向无环图结构（DAG）、跨链、侧链、状态通道（以比特币闪电网络为代表）以及压缩交易信息的技术（比如Mimblewimble）等。袁煜明和刘洋（2018）对这些方向做了全面介绍。提高区块链物理性能的另一个重要方向是改进共识算法（consensus algorithm），特别是从工作量证明（proof of work，简称是 POW）转向权益证明（proof of stake，简称是 POS）。袁勇等（2018）综述了常见的区块链共识算法。在一些应用场景中使用联盟链或私有链而非公有链，也是绕开区块链物理性能瓶颈的重要方面。

本文从经济学角度研究了区块链能做什么、不能做什么。即使将来区块链物理性能瓶颈得以缓解，本文研究一些经济学问题仍将存在。本文共分四部分。第一部分是引言。第二部分是对区块链技术的经济学解释，相当于用经济学语言“翻译”区块链技术。这一部分归纳出目前主流区块链系统采取的“Token 范式”（Token 在不同语境下有多种中文翻译，比如加密货币、加密资产、代币和通证等，为避免混淆或歧义，本文主要用 Token 而非其中文翻译），厘清与区块链有关的共识和信任这两个基础概念，并梳理智能合约的功能。第三部分研究区块链的经济功能。这一部分先梳理区块链的主要应用方向，再讨论 Token 类似货币的特征、Token 对区块链平台型项目的影响、区块链的治理功能以及区块链系统的性能和安全性等问题。第四部分总结全文并讨论区块链能做什么、不能做什么。

二、对区块链技术的经济学解释

区块链涉及计算机技术和经济学。本部分对区块链技术给出经济学解释，辨析在与区块链有关的共识、信任和智能合约等方面的常见误解，为第三部分研究区块链的经济功能打下基础。

（一）区块链的 Token 范式

目前主流区块链系统，不管采取以比特币为代表的 UTXO 模型，还是以以太坊为代表的账户模型，也不管脚本语言是否具有图灵完备性或是否支持智能合约，都具有 3 个关键特征，可以归纳为“Token 范式”：

第一，共识算法针对区块链内的 Token。Token 本质上是区块链内定义的状态变量，Token 可以在区块链内不同地址之间转让，转让过程中 Token 总量不变（也就是在转出地址减少 1 个 Token 的同时，转入地址增加 1 个 Token）。有些区块链系统限定了 Token 的总量上限，比特币就属于这种情况。

Token 在区块链内不同地址之间转让时，Token 的状态（指区块链内各地址内有多少 Token）更新和交易确认同步发生。比如，Alice 向 Bob 转了一笔比特币，这笔比特币交易被记入区块链的同时（也就是交易被打包进某一区块并接入区块链），Alice 和 Bob 对应公钥的 UTXO（可以理解为比特币区块链内的账户余额）同时更新。因此，Token 被交易时，不会形成传统意义上的结算在途资金或

结算风险 5。

第二，Token 与智能合约之间有密不可分的联系。Token 本身是智能合约的体现。比如，以以太坊 ERC20 为代表的 Token 合约规定 Token 的总量、

发行规则、转让规则和销毁规则等一系列逻辑。Token 合约管理着一系列状态，记录哪些地址有多少 Token 等账本信息。在 Token 合约的基础上，可以构建对 Token 执行复杂操作的智能合约。这些智能合约执行的结果主要是，Token 的状态发生变更。

本部分第三小节将分析智能合约的功能。

第三，按照是否与 Token 的状态和交易有关，区块链内的信息分成两类——有关系的和没有关系的，这两类信息在共识算法下有完全不一样的地位。节点在运行共识算法时，重点检验第一类信息是否符合预先定义的算法规则，第二类信息作为 Token 交易的附加信息写入区块链，节点不会检验这类信息的真实准确性。比如，比特币节点会检验随机数（nonce）是“挖矿”问题的解，以及区块中的交易在数据结构、语法规范性、输入输出和数字签名等方面符合预先定义的标准。但对比特币创世区块中的“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”，节点不会也没有能力验证这句话的真实准确性。

区分这两类信息是理解区块链共识范围的关键。区块链共识针对与 Token 的状态和交易等有关的信息。比如，比特币共识决定了截至某一区块，各地址对应的 UTXO 数量以及地址之间转让比特币的记录。而区块链内与 Token 的状态或交易等无关的信息基本不属于共识的范围。特别是，区块链外信息写入区块链内的机制，一般被称为预言机（oracle mechanism）。如果区块链外信息在源头和写入环节不能保证真实准确，写入区块链内只意味着信息不可篡改，没有提升信息的真实准确性。但区块链有助于解决数据登记追溯问题，登记在区块链

内的数据有可追溯的主体身份签名并可用于事后审计，而且上链数据的不可篡改性也有助于控制操作风险。

（二）区块链内的共识和信任

共识（consensus）和去信任（trustless）是区块链两个非常重要的基础概念。这两个概念脱胎于计算机领域，很难在经济学上予以严格定义，却很容易被误解。比如，将共识等同于消除了信息不对称或实现了共同信念，将去信任等同于没有信用风险。

1。共识的界定

目前对区块链共识的讨论，涉及三种不同语境下的共识概念——机器共识、治理共识和市场共识，其中治理共识和市场共识可以称为“人的共识”。很多误解就源于混淆了这三类共识，或者泛化了共识的范围和性质。

第一，机器共识。机器共识属于分布式计算领域的问题，目标是在存在各种差错、恶意攻击以及可能不同步的对等式网络中（peer-to-peer network），并且在没有中央协调的情况下，确保分布式账本在不同网络节点上的备份文本是一致的（不是语义一致）。

对等式网络的节点（特别是负责生成和验证区块的节点）有诚实节点和恶意节点之分。诚实节点遵守预先定义的算法规则（主要是共识算法），能完美地发送和接收消息，但其行为完全是机械性的。恶意用户可以任意偏离算法规则。在一定限制条件下（比如比特币要求 50%以上算力由诚实节点掌握），算法规则

保证了机器共识的可行性、稳定性和安全性。机器共识的范围限于区块链内与 Token 的状态和交易等有关的信息。

第二，治理共识，指在群体治理中，群体成员发展并同意某一个对群体最有利的决策。比如，比特币社区关于“扩容”和分叉的讨论可以在治理共识框架下理解。治理共识的要素包括：1。不同的利益群体；2。一定治理结构和议事规则；3。相互冲突的利益或意见之间的调和折衷；4。对成员有普遍约束的群体决策。袁勇等（2018）指出，治理共识涉及人的主观价值判断，处理的是主观的多值共识，治理共识的参与者通过群体间协调和协作过程收敛到唯一意见，而此过程如果不收敛，就意味着治理共识的失败。

第三，市场共识。Token 参与交易时（不管是不同 Token 之间交易，还是 Token 与区块链外资产或权利交易），就涉及市场共识。市场共识体现在市场交易形成的均衡价格中。

三类共识之间存在紧密而复杂的关系。机器共识是对等式网络的节点运行算法规则的产物，治理共识反映由人（包括网络节点的拥有者或控制着）来制定或修改算法规则的过程。市场共识受机器共识和治理共识的影响。比如，如果分布式账本的安全性没有保障（即机器共识失效），比特币的市场价格将受到毁灭性冲击。再比如，2017 年比特币社区对“SegWit2x”的讨论（即引入隔离见证并将单个区块的大小从 1M 提升到 2M），对当时比特币价格走势有明显的影响，就体现了治理共识对算法共识的影响。下文如无特别说明，讨论的均是机器共识。

2。去信任含义的辨析

去信任源于 Token 被交易时，Token 的状态变更和交易确认同步发生这一安排。设想 Alice 以比特币向 Bob 买入某一货物。Alice 向 Bob 支付比特币这一过程无需两人之间有任何了解，也无需受信任的第三方机构，就可以在区块链内有保障地进行。这是去信任的真正含义。但在交易的另一端，Alice 如何确保 Bob 会按时向她交付合格的货物？只要做不到一手交比特币、一手交货，就存在不容忽视的交易对手信用风险。只有准确识别、评估信用风险并引入风险防范措施，很多交易才能进行。比如，在暗网交易中，交易平台通常设立第三方托管账户（escrow account）。买方先将比特币打入第三方托管账户，等收到商品并确认后，才通知交易平台将比特币转给卖方。如果没有第三方托管账目这个增信手段，比特币忠实拥趸之间的交易也会大幅减少。

因此，区块链内的去信任环境，不能简单外推到区块链外。一旦脱离 Token 交易等原生场景，区块链要解决现实中的信任问题，往往需要引入区块链外的可信中心机制予以辅助。

（三）智能合约的功能

智能合约是运行在区块链内、主要对 Token 进行复杂操作的计算机代码。目前区块链内有限的运行环境，使得这类代码远没达到智能阶段。甚至可以说，目前的智能合约，既不智能，也不是合约。这一小节针对“在一定触发条件下从 A 地址往 B 地址转 X 数量的 Token”这一基本操作总结智能合约的功能。

第一，产权层面的功能。A 地址和 B 地址可以属于账户或智能合约。地址中的 Token 具有产权含义。比如，如果 A 地址属于发行地址，那就对应着 Token 的产生（一级市场）；如果 B 地址属于销毁地址（即类似 0x0000。。0000 的

不对应着私钥的特殊地址），那就对应着 Token 的销毁；两个地址之间的 Token 转移，就对应着产权变更。

第二，流程层面的功能。一笔 Token 转让要有效，转让发起者必须拥有对 A 地址中 X 数量的 Token 的操作权限，并且智能合约的触发条件被满足。发起者将转让信息传播到分布式网络后，其他节点验证发起者是否拥有 A 地址的操作权限、触发条件是否被满足以及 A 地址中的 Token 数量是否超过 X。其中，对 A 地址的操作权限体现为相关签名操作（往往涉及多重签名），触发条件取决于区块链内外信息（其中区块链外信息需先写入区块链内），转让数量 X 既可以由人工来决定，也可以由公式来决定，从而实现或有支付（contingent payment）或比较复杂的偿付结构（payoff structure）。智能合约的执行只有“成功”、“失败”两种情形，不存在中间情形。特别是，如果转让发起者不能确保 A 地址中的 Token 数量超过 X，智能合约的执行就会失败。

第三，经济社会层面的功能：1。投票，往某一地址转 Token 可以理解为投票；2。抵押，先将一定数量的 Token 转给某一智能合约，约定在未来时点并满足一定条件时，Token 可被返还；3。冻结和解冻，冻结是将一定数量的 Token 用时间锁（time lock）锁定，从而暂时放弃 Token 的流动性，到期才解冻。基于投票、抵押以及冻结和解冻等基础功能，智能合约可以支持比较复杂的治理功能（见第三部分第二和第三小节）。

然而，智能合约的功能短板不容忽视。第一，在智能合约的触发条件取决于区块链外信息时，这些信息需先写入区块链内，但至今没有普遍适用的去中心化预言机方案。目前讨论得比较多的预言机有两类。一是依赖某一中心化信息源（比

如彭博、路透），但这与区块链的去中心化宗旨背道而驰。二是将区块链外信息离散化后用经济激励和投票写入区块链。这类机制依靠群体智慧，根据投票结果对奖惩投票人，投票越接近全体投票的平均值、中位数或其他样本统计量的投票人越有可能得到奖励，反之就越有可能被惩罚，以此来激励投票人认真投票。隐含假设是，参与投票的群体在投票时不存在系统性偏差。但这一假设在现实中不一定成立，因此至今没有普遍适用的去中心化预言机方案。

第二，智能合约难以保证区块链内债务履约。考虑某一债务合约：某一时点从 A 地址往 B 地址转 X 数量的 Token，一段时间后从 B 地址往 A 地址转 Y 数量的 Token（一般 Y>X）。在后一时点，智能合约没法保障 B 地址的 Token 数量超过 Y，这样债务就无法履约。因此，只靠智能合约没法消除信用风险。这是根据智能合约构建区块链内贷款、债券和衍生品等面临的共同问题。一个解决方法是对还款地址设置超额抵押（over-collateralization），但超额抵押会造成 Token 资源的闲置和浪费。对衍生品，因为其风险敞口可能大幅变动，更难事先确定超额抵押的规模。

第三，智能合约难以处理不完全契约（incomplete contract）。人是有限理性的，不可能预见到未来所有可能的情况，即便预见到也没法写进契约里，因此契约注定是不完全的。这就是现实中法律合同存在例外情形，以及发生争端时需要司法仲裁的原因。智能合约作为计算机协议，很难处理不完全契约。

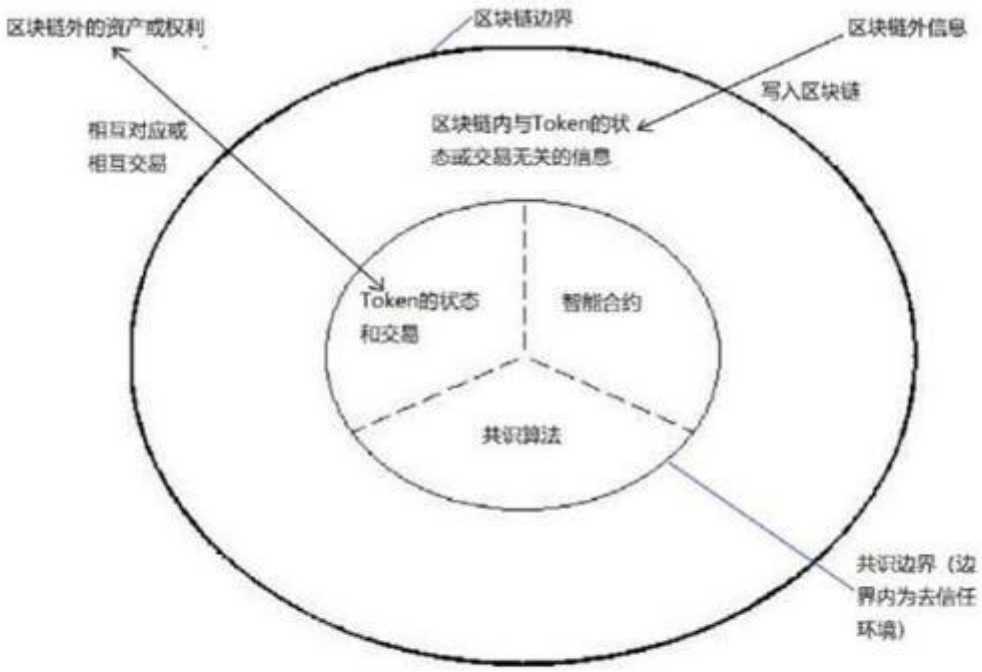

图 1：Token 范式概括

图 1 概括了以上对 Token 范式的讨论。其中，Token、智能合约和共识算法都处于共识边界内，Token 与智能合约之间有密不可分的联系，共识算法确保了共识边界内的去信任环境。区块链内与 Token 的状态或交易等无关的信息处于共识边界以外、区块链边界以内。区块链内外存在两类交互：一是区块链外信息写入区块链内；二是 Token 与区块链外的资产或权利之间的相互交易（即市场共识，见第三部分第二小节对 Token 的价格特征的讨论）或相互对应（见第三部分第一小节对区块链第二类应用的讨论）。

三、区块链的经济功能

区块链应用一般按照应用场景所属行业进行分类，比如 Goldman Sachs（2016）。本文根据区块链应用对 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。
涉及公开发行交易的 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。

表 1 将区块链应用分成了 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。区块链的公共共享账本功能有助于缓解经济活动参与者之间的信息不对称，提高他们分工协作的效率。这类应用面临的主要问题是如何保证区块链外信息在源头和写入区块链环节的真实准确。相对公有链，联盟链更适合这类应用。联盟链仅对授权节点开放，由授权节点共同维护以实现组织间共识。而授权节点清楚彼此身份，作恶会对声誉产生影响，将

虚假信息写入区块链的成本比较高。信息写入区块链的环节也可以引入第三方鉴定机构来验证信息的真实准确。但这些保障机制主要基于现实世界约束，而非区块链本身特性。第一类应用的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。但 Token 是否对应着区块链外的资产或权利，以及 Token 的状态和交易是否对区块链外的现实世界有约束力或影响力，取决于区块链外的法律和制度是否赋予 Token 以超越区块链的内涵。在这类应用中，区块链在供应链金融和数字票据等场景的应用值得关注。此时，Token 代表了某一核心机构的债权并在供应链中充当内部结算工具。Token 将供应链上下游企业之间的“三角债”轧差后替换成核心机构对这些企业的负债，能降低资金占用、提高资金周转效率。而核心机构发挥类似中央交易对手的功能，负责 Token 与法定货币之间的兑换。这些场景中的 Token 相当于王永利（2018）提出的网络社区代币或商圈币概念，Token 的应用价值则取决于场景的广度和深度。

第二类应用的代表案例是数字票据交易平台设计方案。该平台按是否引入数字货币在链上进行直接清算，设计了链外清算和链上直接清算两种方案（徐忠、姚前，2016）。其中，链上直接清算方案能实现基于区块链技术的数字票据全生命周期的登记流转交易和票款对付（DVP，Delivery Versus Payment）结算功能。

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。但 Token 价格的高波动性限制了这类应用，一个重要方向

是所谓的稳定加密货币（stable token 或 stable coin）。因此，这类应用的核心问题是如何理解 Token 类似货币的特征。

第四类应用试图用区块链构建分布式自治组织（distributed autonomous organization，简称是 DAO，见邹传伟（2018）），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，主要受制于以下障碍：1。公有链的物理性能不高，支撑不了大规模交易；2。智能合约的功能短板；3.Token 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；4。加密经济学（token economics 或 crypto economics）模型设计不合理。对前两点障碍，第一部分和第二部分第三小节分别已有讨论。后两点障碍则涉及 Token 类似货币的特征和区块链的治理功能。

（二）Token 类似货币的特征

Token 具有若干类似货币的特征：1.Token 没有负债属性；2。按同一规则定义的 Token 是同质的，并可拆分成较小单位；3.Token 在不同地址之间的转让无需受信任的第三方机构；4。非对称加密可以保证 Token 持有者的匿名性；5。区块链共识算法和不可篡改的特点可以保证 Token 不会被“双花”（double spending）；6。可以由规则定义 Token 的总量上限和发行速度。Token 的这些类似货币的特征由 Nakamoto(2008)引入,并被其他满足 Token 范式的区块链系统所遵循。

Token 的直接用途就是作为支付工具来换取区块链内外的商品或服务，此时 Token 一般被称为加密货币。在区块链内，可以由规则定义加密货币的用途。比如，在比特币系统内，比特币被用于向“矿工”支付交易手续费；在以太坊中，

以太币是运行智能合约的“燃料费”（gas）。区块链内的支付场景也涉及市场活动（见本部分第五小节对比特币手续费率的讨论），但因为区块链内的商品或服务不能用法定货币来购买，加密货币价格对这个场景一般没有明显影响。而用加密货币购买区块链外的商品或服务时，加密货币价格是一个重要影响因素。一般来说，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，价格波动高，无法有效履行货币职能。这一点有很多文献支持。

首先，关于加密货币作为支付工具的表现。Athey et al。（2016）发现，截至 2015 年中，大部分比特币由投资者和非频繁使用者持有，比特币作为支付工具的使用不频繁，而且将比特币用于非法活动的用户更倾向于保护他们的财务隐私。Foley et al。（2018）研究了比特币在非法经济活动中的应用，发现 25%的比特币用户和 44%的比特币交易与非法经济活动有关。截至 2017 年 4 月，有 2.4 千万的比特币市场参与者主要将比特币用于非法目的，他们合计持有 80 亿美元的比特币，年度交易笔数约 3.6 千万笔，年度交易金额约 720 亿美元（接近欧美非法药物的市场规模）。随着主流社会对比特币兴趣的增加以及 ZCash、Dash 和 Monero 等匿名特征更好的加密货币出现，比特币交易中与非法经济活动的比例下降了。

其次，关于加密货币的价格特征以及可能存在的价格操纵。Gandal et al。（2017）发现，Mt。Gox 交易所（当时最大的比特币交易所）在 2013 年 2 月-11 月中的两个时间段存在可疑交易活动，涉及 60 万个比特币。这些可疑交易对当时比特币价格在两个月内从 150 美元上涨到 1000 美元起到了重要推动作用。Griffin 和 Shams （2018）研究了 USDT（由 Tether 公司发行的一种

声称基于 100%美元储备金的稳定加密货币）对比特币和其他加密货币的影响，发现 USDT 被用来操纵加密货币的价格。在 2017 年 3 月-2018 年 3 月这段时间里，作者识别出 87 个小时。这 87 个小时均有大量 USDT 发行并被用来购买加密货币，而且这些大额交易均发生在加密货币市场大跌之后，在这些大额交易后加密货币市场均大幅反转。作者发现，这 87 个小时对应着比特币在研究区间（即 2017 年 3 月-2018 年 3 月）50%的涨幅，以及另外 6 种大的加密货币在研究区间 64%的涨幅。Bianchi（2018）分析了 14 种主要加密货币在 2016 年 4 月和 2017 年 9 月之间的交易数据，发现加密货币的收益率与股票、债券等传统金融资产的收益率之间不存在显著关系，加密货币与传统金融资产之间不存在波动性溢出效应，并且加密货币的交易量主要由历史收益率和市场不确定性（用芝加哥期权交易所市场波动率指数 VIX 衡量）驱动。

加密货币价格波动性太高，引入加密货币期货也难以平抑价格波动，很多从业者试验稳定加密货币。目前，由 Tether、Gemini 和 Circle 等公司推出的稳定加密货币方案都采取了以法定货币为准备金 1：1 发行稳定加密货币的方式，相当于货币局（currency board）制度。另一些稳定加密货币方案采取所谓的“算法中央银行”模式（algorithmic central bank），模仿中央银行公开市场操作，通过发行和回收以加密货币计价的债券来调控加密货币供给量，以实现加密货币价格的稳定。Eichengreen（2018）指出，“算法中央银行”难以抵御投机性攻击。因为攻击发生时以加密货币计价的债券会有显著折价，通过发行该类债券回收加密货币以支撑加密货币价格的效果会显著下降，所以“算法中央银行”有内在的不稳定性。需要指出的是，中央银行数字货币（central bank digital currency，简称是 CBDC）与稳定加密货币有本质不同。中央银行数字货币有负

债属性，是中央银行直接对金融机构和社会公众发行的电子货币，属于法定货币的一种形态，而且不一定采用区块链内 Token 的形式。本文不深入介绍中央银行数字货币，感兴趣的读者可以参考 CPMI（2018）。

加密货币监管的重点在加密货币与法定货币的兑换环节，其中一个重要问题是反洗钱。加密货币洗钱是指应用加密货币的匿名性和全球性，使得违法所得的来源和性质难以追溯。加密货币洗钱分为三个环节：1。置入（placement），将不法获取的法定货币转换成加密货币。一些加密货币交易所没有采取实名制，会给置入环节带来很大便利。2。分流（layering），使用混币（mixers）、合币（coinjoin）和翻洗（tumblers）等技术以及区块链内地址的匿名性，将加密货币在多个地址之间转移，使其来源难以追溯。3。整合（integration），将“洗干净”的加密货币整合并转到“干净”地址上，再转换成法定货币或商品。以 ZCash、Dash 和 Monero 为代表的加密货币使用了零知识证明、环签名等匿名技术，会增加反洗钱难度。此外，加密货币在全球范围内流通，不同国家或地区的对加密货币的监管标准不一、信息难共享，也会增加反洗钱的难度。

（三）Token 对区块链平台型项目的影响

一些区块链项目具有平台经济特征。Token 在这类平台型项目中可以兼具两种角色：首先是项目启动时的融资工具，体现为初始代币发行（initial coin offering，简称是 ICO）；其次是平台内经济活动的支付工具。Token 为持有者带来双重好处：一是用 Token 购买平台内的商品或服务，二是 Token 价格的上涨，并且 Token 价格受平台型项目活跃用户数和经济活动量等基本面因素

驱动。另外，一些区块链平台型项目的 Token 具有股权属性（见本部分第四小节）。

Token 的双重角色对区块链平台型项目启动和发展有重要影响。Catalini 和 Gans （2016）分析了区块链、Token 对市场形成中的两个重要因素——验证成本和网络成本的影响。他们认为，区块链允许市场参与者以较低成本验证与交易有关信息，会促进新的市场形态出现；Token 可以在无需传统受信任中介的情况下降低网络成本并启动市场。Cong et al。 （2018）用动态资产定价模型分析了 Token 价格及其对用户采用（user adoption）的影响。Token 交易为平台用户提供了跨期互补性（intertemporal complementarity），从而在 Token 价格和用户采用之间形成了一个反馈环。Token 价格反映了平台未来增长。均衡时 Token 价格将随平台生产力、用户异质性和网络规模而呈现非线性增长。

Token 的双重角色为 Token 价格带来了内在不稳定性。Sockin 和 Xiong （2018）在平台经济框架下研究了 Token 定价。用户通过参与平台内交易来提高自己的福利，“矿工”提供交易记账服务。平台内的 Token 有双重属性：一是相当于“会员资格”，用户需要先购买 Token 才能参与平台内交易；二是为平台建设发展融资，包括前期开发费用（体现为 ICO）和给“矿工”的奖励。作者考虑了平台基本面（主要体现为用户禀赋和“挖矿”成本）可公开观察以及不可公开观察两种情形。在两种情形中，要么不存在均衡，要么都存在两个均衡，其中一个均衡对应着 Token 价格高和用户参与积极性高的情景，另一个均衡对应着 Token 价格低和用户参与积极性低的情景。在平台基本面不可观察时，

Token 价格除了汇聚平台基本面有关信息以外，还起到了在不同均衡路径之间的协调作用。但总的来说，因为多个均衡的存在，Token 的价格有内在不稳定性。

ICO 是区块链平台型项目启动的一个常用策略。Li 和 Mann（2018）认为 ICO 解决了很多有网络效应的平台内在的协调失败问题，并通过汇集关于平台质量的分散信息，能发挥了群体智慧作用。Chod 和 Lyandres （2018）从理论上研究了创业者在 ICO 和 VC 两种融资方式之间的选择。他们认为，创业者通过 ICO 出售自己项目的未来产出，可以在不稀释自己控制权的情况下将部分创业风险转移给投资者，但由此产生的代理问题使得创业者可能在融资后对项目投入不足。

一些学者对 ICO 进行了实证分析。Benedetti 和 Kostovetsky（2018）分析了 2017 年以来 4003 家已执行或已计划的 ICO 项目(共融资 120 亿美元)，发现了显著的 ICO 折价现象，从 ICO 到相关 Token 开始交易（平均间隔 16 天），投资者的平均回报是 179%。在 Token 开始交易的头 30 天，买入并持有策略平均能产生 48%的超额回报率。Momtaz （2018) 分析了 2015 年 8 月-2018 年 4 月的 2131 个 ICO 项目，发现在加密货币交易所挂牌首日，Token 的收益率平均为 8.2%，相对加密货币市场整体的超额收益率为 6.8%。用挂牌首日收益率和 ICO 融资规模等作为 ICO 成功程度的指标发现，ICO 项目团队的质量越高，ICO 越容易成功；ICO 的目标越远大，ICO 越容易失败；行业负面事件（比如黑客攻击和监管行动）对 ICO 市场影响很大。

（四）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 有二级市场交易并且价格波动性较高，即使这些机制设计在区块链内能做到激励相容，区块链有关参与者的行为也可能偏离预期目标。比如，很多机制设计需要 Token 持有者将自己的 Token 锁定一段时间，并给予 Token 持有者一定数量的 Token 奖励。锁定 Token 相当于放弃了在二级市场逢高出售 Token 的权利（本质上是一个有浮动行权价的回望看跌期权，lookback option with floating strike）。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。

相比之下，区块链项目的 Token 在加密货币交易所挂牌的标准要低得多。很多区块链项目在还处于白皮书阶段时，早期投资者和项目团队持有的 Token 就可以通过加密货币交易所变现，而他们在 Token 变现后认真做项目的动力就可能显著减弱。在很多区块链项目中，因为 Token 持有者在项目治理中的地位比较模糊，Token 的快速变现机制更不利于投融资双方的利益绑定。Benedetti 和 Dostoevsky （2018）用 ICO 项目推特账户的活跃度来衡量，到 ICO 后 120 天，只有 44.2%的 ICO 项目处于活跃状态。Token 的快速变现机制也是与 ICO 有关的各种投机、炒作甚至欺诈活动的重要根源之一。

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。

（五）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”。对两个“矿工”的博弈分析发现，在一定参数假设下，两个矿工都挖“空块”（也就是不打包任何交易）可以成为博弈均衡，应对方法是提高手续费率。Huberman et al。 （2017）研究了比特币系统的物理性能对用户和“矿工”的影响。用户希望自己的交易能尽快被处理，在系统物理性能有限的情况下，会提高交易费率，以吸引“矿工”优先处理自己的交易。而“矿工”在经济激励下，也有动力维持比特币系统的基础设施。因此，物理性能有限是比特币系统在去中心化环境下维持运行的一个重要保障措施。Easley et al。（2018）对 2011 年-2016 年比特币系统的实证分析发现，比特币系统越拥堵（用比特币内存池大小和交易写入区块链前的平均等待时间来衡量），交易费率为 0 的交易写入区块链的可能性越小，写入区块链的交易的平均费率越高。

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。

四、总结

本文从经济学角度分析了区块链的功能，从 Token、智能合约和共识算法三个角度归纳出目前主流区块链系统采取的“Token 范式”，并给予经济学解释。

1.Token 是区块链内定义的状态变量，具有若干类似货币的特征。区块链内 Token 交易无需依靠受信任的第三方机构，但区块链内这种去信任环境不能延伸到区块链外。一旦脱离 Token 交易等原生场景，区块链要解决现实中的信任问题，往往需要引入区块链外的可信中心机制予以辅助。

2。智能合约是运行在区块链内、主要对 Token 进行复杂操作的计算机代码，可以实现 Token 的定义、发行、销毁、转让、抵押、冻结和解冻等功能，但无法确保区块链内债务的履约，也很难处理不完全契约。目前区块链内有限的运行环境，使得这类代码远没达到智能阶段。

3。共识算法针对与 Token 的状态和交易等有关的信息，并保证了这类信息的真实准确。但区块链内与 Token 的状态或交易等无关的信息基本不属于共识的范围。特别是，区块链外信息写入区块链内，只意味着这些信息全网公开且不可篡改，不能提升这些信息在源头的真实准确性。目前也没有去中心化预言机能真实准确地将区块链外信息写入区块链内。

基于“Token”范式，本文分析了区块链的 4 类主要应用方向：**1。无币区块链。**这类应用发挥区块链的公共共享账本功能以提高劳动分工协作效率，不直接涉及产权和风险的转移，面临的主要问题是如何保证区块链外信息在源头和写入区块链环节的真实准确性。联盟链因为仅对授权节点开放并依靠现实世界的约束，比公有链更适合这类应用。

2。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。但 Token 在物理上只是一段代码，Token 是否对应着区块链外的资产或权利，以及 Token 的状态和交易是否对区块链外的现实世界有约束力或影响力，取决于区块链外的的法律和制度是否赋予 Token 以超越区块链的内涵。

3。以公开发行交易的 Token 作为计价单位或标的资产，但依托区块链外的法律框架的经济活动。因为很难根据基本面准确评估 Token 的内在价值，这类应用只能参考 Token 在二级市场上的价格，但 Token 价格往往表现出高波动性，限制了这类应用的开展。

4。用区块链构建分布式自治组织。这方面至今没有广受认可的成功案例，主要受制于以下障碍：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；Token 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；加密经济学模型设计不合理。

本文在分析区块链的这些主要应用方向时，还讨论了其中涉及的经济学问题并综述了相关研究：1.Token 类似货币的特征，包括加密货币作为支付工具的表现、二级市场价格特征、稳定加密货币试验以及与加密货币有关的反洗钱问题；

2.Token 对区块链平台型项目融资和发展的影响，以及 Token 的双重角色造成 Token 价格的内在不稳定性；3。区块链的治理功能，包括股权型 Token 设计，Token 价格波动对基于 Token 的激励机制的影响，智能合约的功能短板对现实世界治理机制移植到区块链场景的影响，以及 Token 的快速变现机制对区块链项目投融资双方利益绑定的影响；4。区块链系统的性能和安全，包括区块链的“三元悖论”、POW 的利弊、POW“挖矿”的经济学问题以及区块链的经济安全边界。

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交易的 Token 的项目。政府有关部门应加强监管，防范金融风险。