吴桐 | 区块链共识机制的经济学分析

吴桐：中央财经大学金融学博士，香港国际新经济研究院高级研究员、CECBC区块链专委会副主任、数字经济商学院院长，数字资产研究院学术技术委员会委员，伏羲智库兼职研究员，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》。

原文发表于《广义虚拟经济研究》2020 年 02 期（季刊）。

《广义虚拟经济研究》杂志（季刊）由中国航空工业集团公司主管，中航出版传媒有限责任公司主办，中航出版传媒有限责任公司出版。广义虚拟经济是一个由中国航空工业集团公司原董事长，中共十八届中央委员会中央委员，中国航空学会理事长林左鸣教授提出的新的经济学理论体系。他讲广义虚拟经济定义为将同时满足人的物质需求和心理需求（并且往往是以心理需求为主导的经济），以及只满足人的心理需求的经济的总和，它是一种基于生活价值论的以人为本的经济。

摘要：

区块链作为一项蕴含经济学内核的前沿技术，理解其共识机制的经济学含义、优化共识机制的经济模型设置对推进区块链技术落地、赋能实体经济发展具有重要意义。本文分别阐述了区块链的三种共识机制——算法共识、

决策共识和市场共识的内涵、外延，分别分析了主流算法共识 POW、POS、DPOS、DAG 的经济学含义以及不同算法共识的融合发展趋势，并为如何协同区块链三种类型的共识机制给出发展建议，以期促进区块链技术创新和产业发展。

一、引言

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在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，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。区块链作为一种涵盖了 P2P 网络、加密算法、共识机制、智能合约等要件的复合型技术，经济模型、决策机制和激励模式在其中发挥着至关重要的作用。[1]区块链在全球范围内应用落地不仅与区块链本身的成熟度、区块链与其他技术（如人工智能、大数据、物联网等）的融合程度、相关基础设施建设密切相关，还离不开共识机制的设置与发展，理解区块链共识机制的经济学含义具有重要的理论和现实意义。

狭义上的区块链共识机制是指算法共识,算法共识旨在通过机器语言和机制设计解决两个核心问题 ：第一，谁有权利写入数据 ；第二，在分布式帐本中其他节点如何同步数据。较为经典的算法共识有工作量证明机制（Proof Of Work,POW)、权益证明机制（Proof Of Stake,POS)、委托权益证明机制（Delegated Proof Of Stake,DPOS）、有向无环图(Directed Acyclic Graph,DAG) 等。理解算法共识的经济学含义对于促进区块链技术

与应用场景的融合、完善区块链监管与治理机制、弥合区块链与现有法律政策体系的鸿沟均有重要意义。

事实上，算法共识仅是区块链共识机制的一部分，构成了区块链链上共识机制的主要内容。在现实中，依靠社群成员通过集体决策做出决定的决策共识和依靠各市场参与者的市场交易行为形成的市场共识同样发挥重要作用，二者构成区块链链下治理的主要内容。算法共识、决策共识、市场共识三者构成完整的区块链共识机制体系，三者互相关联而密不可分。算法共识是分布式网络中节点运行的算法规则，决策共识反映分布式节点的控制实体制定或修改算法规则的过程，市场共识是算法共识和决策共识在市场和价格层面的反映，也会对算法共识和决策共识产生重要的反作用。如何理解区块链共识机制体系的经济学含义对于推动区块链技术创新和产业发展具有重要作用。本文分别阐述了区块链的三种共识机制——算法共识、决策共识和市场共识的内涵、外延，分别分析了主流共识算法 POW、POS、DPOS 以及 DAG 的经济学含义，并为如何协同区块链三种类型的共识机制给出发展建议，以期促进区块链技术创新和产业发展。

二、区块链三种类型的共识机制

当前对区块链共识机制的讨论，一般停留在狭义层面，即指区块链的算法共识机制。这体现了机械的区块链观，只注重链上共识机制，而忽略链下共识机制。当前实物、数据、资产上链还处在早期阶段，链下共识机制的重要程度更甚于链上共识机制。链下共识包括决策共识和市场共识，又

被称为“人的共识”。[2][3] 厘清区块链三种类型的共识机制之间的内涵和联系，具有重要的理论和现实意义。

（一）区块链的算法共识机制

区块链的算法共识是通过机器语言编程的算法解决“谁有权利写入数据”和“在分布式帐本中其他节点如何同步数据”这两个核心问题。“谁有权利写入数据”决定着“在分布式帐本中其他节点如何同步数据”。根据写入数据的主体不同，区块链可分为公有链、联盟链和私有链。在公有链中，任何节点都有权利写入数据，通过“挖矿”算力竞争、持有 token 的“币龄”（Token day）进行治理，不仅需要考虑网络中存在故障节点，还需要考虑作恶节点。在公有链中常见的共识机制有 POW、POS、DPOS、DAG 等。公有链又称“非许可链”，其经济系统在规则之外再无规则，是管制最少、市场化程度最高的区块链经济系统。

与“非许可链”的概念相对应，许可链包括联盟链和私有链。在联盟链中，只有特定的节点具有写入数据的权利，任何新加入的节点都需要验证和审核，同样需要考虑故障节点和作恶节点；但相比作恶节点，故障节点已经成为重点考虑的问题。在联盟链中常见的共识机制有实用拜占庭 容错 算 法（Practical Byzantine Fault Tolerance，PBFT）等，Facebook 发布的全球稳定币项目 Libra 白皮书中，Libra 采用的即为 PBFT 共识。[4-5] 联盟链经济系统属于有管制的市场经济体系，其市场化程度与记账节点的数量成反比。联盟链在一定程度满足场景需要的同时，能够实现可监管性和风险可控性，因此成为我国政府大力倡导的落地架构。[6]

私有链本质上属于中心化的封闭系统，只有该节点具有写入数据的权利，不需要考虑新节点的加入及退出，也不存在作恶节点，当单一的记账节点出现问题时，整个经济系统就处于崩溃状态，因此私有链不需要算法共识机制。

经济社会最核心的权利是记账权，与之配套的基础设施是如何同步帐本，保证各市场主体拥有相同的公共帐本和各利益相关者拥有相同的私有帐本。当单个的交易发生时，如果这一交易不能被市场机制捕捉并作为因子纳入其中，则这一交易实质上并没有为市场价格的形成发挥作用。同样，在区块链经济系统中，整个经济行为的市场化流程如下 ：第一，从全体利益相关者组成的社群集合 {M} 中选出记账节点集合 {A}，这一过程用 f({M}）→ {A} 来表示，记账节点集合 {A}拥有该经济系统的记账权。第二，记账节点集合{A} 按照区块容量、交易等待时间、交易费用等多因素综合排序后，将当前时间段内整个经济系统中的交易打包到一个区块中，并将生成的新区块广播给全体验证节点集合 {D} 或其代理节点 D。第三，全体验证节点集合 {D} 或其代理节点 D 受到被广播的新区块后，验证其交易的正确性。若新区块中的交易被大多数验证节点认可，则被更新到区块链中。第四，记账节点集合 {A} 将新区块添加到最长的主链上，主链记录着从创世区块到最新区块的完整交易信息。如果主链发生分叉，则需根据其算法共识选择一条分支作为主链。

综合而言，算法共识机制即将集体决策的方式和集体决策的结果“广而告之”到每一个成员的方式用代码进行表达。区块链的算法共识机制相当于在经济系统中起基础性作用的资源配置机制，但具体的资源配置机制

也会随着人类的群体意识、人类掌握和运用技术的能力等因素发生变化，当前包括区块链在内的数字技术正在深刻改变传统经济制度。同时，政府的宏观经济政策也会对资源配置产生深刻影响。宏观经济政策体现了政府的经济理念以及对经济形势的判断等主观意见。类似地，算法共识机制也是可以被开发团队人为修改的，比特币技术开发团队 Bitcoin Core 多次将比特币区块链进行升级，以太坊的开发社区也做了将共识机制从 POW 转向 POS 的长期规划，并分为“前沿”（Frontier）、“家园”（Homestead）、“大都会”（Metropolis）以及“宁静”（Serenity）等四个阶段。区块链算法共识受决策共识的直接影响，但当决策共识达不成一致时，就会出现分叉，产生具有各自算法共识的区块链系统，分叉也成了现阶段区块链经济系统最大的系统性风险来源。

（二）区块链的决策共识机制

决策共识指在区块链发展过程中,社群成员做出一个各决策主体认为的对群体最有利的决策。不同于算法共识解决如何在缺乏中央控制的分布式网络中确保帐本一致性的问题，决策共识解决的是在无中心的群体中，如何就最优决策（或群体主观上认为的最优决策）达成一致的问题，本质上是相关人的共识。决策共识的形成体现了区块链经济系统的各利益相关方（矿工、token 持有人、生态消费者等）在一定的议事规则和治理结构下将不同意见收敛到单一意见的过程 ；若无法收敛意味着决策共识没有达成，则很有可能发生分叉。

相对于算法共识要求不篡改交易的正确性和分布式一致的全息性，决策共识本质上体现了在客观信息的基础上人的意识共识，不仅要求收敛性

和一致性，而且要求所有参与者相信其决策是最优的。决策共识体现了各利益相关节点对于作为该区块链经济系统内微观运作机制的算法共识修改和完善的意识一致性，新的决策共识达成将直接改变算法共识。

比特币区块链系统从 2009 年主网上线，诞生时间已超过十年，决策共识在比特币区块链的发展历程中起到了关键作用。Satoshi Nakamoto 在 2010 年 7 月将比特币区块链的最大区块容量设置为 1M，比特币区块链大约每 10 分钟出 1 个区块。这在较好地保障了中小矿工利益的同时，也限制了比特币经济系统的数据处理能力，随着链上交易的增多，交易延迟越发频繁，交易费也在增加，这使得比特币难以发挥货币的流通媒介职能，也无法成为事实意义上的货币。[7] 针对这一问题，比特币社群的各利益相关者从 2015 年 5 月开始通过公开阐述、辩论、举办会议、互相攻击、链上投票等方式提出不同的比特币扩容方案，进行了漫长而复杂的决策共识形成过程，其中包括决策共识难以收敛而导致的两次影响深远的硬分叉 ：一次是 2017 年 7 月发生的比特币硬分叉，产生了现在的比特币和比特币现金（Bitcoin Cash，BCH）；另一次在 2018 年 11 月发生的 BCH 硬分叉，产生了 Bitcoin ABC 和 Bitcoin SV。

两个主流的比特币扩容方案反映了两条对比特币区块链经济系统改革的道路 ：第一条是激进的市场规则改革方案——直接扩容，将最大区块容量提高到 2M，然后每两年翻倍。这种方式直接增加了市场容量，提高了数据处理能力，但更高带宽和存储提高了记账节点的门槛，导致节点中心化程度增强，损害了广大中小矿工的利益。另一条是温和的市场规则改革方案——“隔离见证+ 闪电网络”（SegWit+Lightning）模式，即实施隔离见

证把交易和交易签名分开，将交易签名置于区块外，通过设置多重签名钱包、构建双向支付通道并延展成为闪电网络，实现间接扩容的方式。这种方式没有直接增加市场容量，但由于将签名置于区块之外，使得 1M 大小的区块可以容纳更多市场交易数据，将区块链的清结算功能分离，将主链退化成单纯的结算网络。

截至 2019 年 7 月，比特币通过分叉累计产生了 105 个分叉币，分叉在以太坊、莱特币等区块链项目中也时有发生。以比特币区块链为代表的区块链决策共识形成的复杂曲折程度反映了人的共识形成的难度更甚于机器共识，也反映了区块链作为一项包含经济模型、治理机制和激励模式的复合型技术与传统技术的不同之处。算法共识的演进与发展动态影响着决策共识，而决策共识的达成则直接影响新的算法共识的产生。

（三）区块链的市场共识机制

公有链由于没有准入门槛，本质上需要通过 token 实现治理。区块链的市场共识指 token 参与交易时形成的市场均衡价格。区块链市场共识的形成既包含 token 与法定货币的交易（法币交易），也包含不同 token 之间的交易（币币交易）。算法共识和决策共识作为基本面、技术面和消息面影响市场共识的形成 ：当区块链算法共识的安全性难以保证时，该系统的 token 价格必然一落千丈 ；当决策共识难以收敛时，也会分散系统内的资源，动摇各节点的信心，进而对市场共识造成负面影响。反过来，市场共识对算法共识和决策共识也有重要的反作用，均衡的市场价格和良性的市场共识形成机制对于算法共识和决策共识具有正面效应。

此外，在当前以主权信用为基础的现代经济体系下，区块链市场共识形成过程中的最终流动性来源于法定货币。市场共识的形成不仅与其内因（算法共识、决策共识等）有关，还与全球宏观经济和金融环境密切相关，市场共识机制是多个因子综合作用的输出结果。

准确理解区块链三种共识机制的含义和关系对于推进区块链落地具有重要意义。从经济学角度而言，形成均衡的市场共识是任何经济系统追求的目标，因此也是区块链系统的目标因变量，算法共识和决策共识都会对市场共识起到重要作用，同时市场共识也会反作用于算法共识和决策共识。适合区块链系统发展的算法共识有利于实现和巩固决策共识，而决策共识则会对算法共识产生修正作用。

从因果关系而言，算法共识机制最先由创始人设定，随着区块链项目的发展，社群会逐步壮大，生态会逐步完善，在社群内会产生不同的利益诉求群体，需要通过决策共识机制实现项目的进一步发展 ；同时，随着区块链项目价值的增大，承载其价值的 token 定价日益市场化，需要市场共识机制发挥作用。决策共识机制和市场共识机制可统一纳入现有经济管理框架内（社会治理、激励兼容、资产定价等），而理解通过机器语言表达的算法共识的经济学含义具有深刻的现实意义。

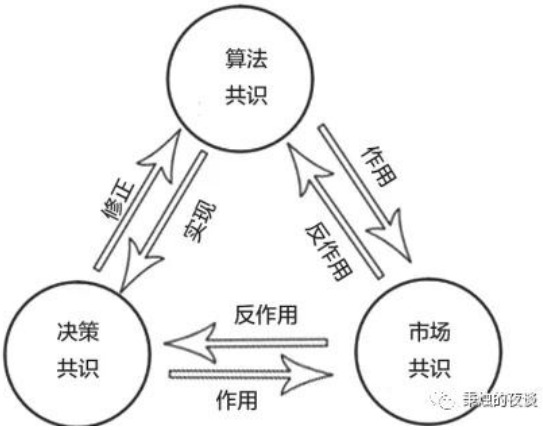

图 1　区块链三种类型共识之间的关系

三、不同算法共识的经济学含义

当前萦绕在区块链行业内的一个阻碍是机器语言和经济语言之间的鸿沟。机器语言的编程人员对经济学缺乏了解，同时经济学工作者由于看不懂代码和技术图又难以对区块链经济系统进行修正和完善，这深刻地阻碍了兼具技术属性和经济属性的区块链的发展。从经济学角度阐述区块链的算法共识具有深刻的理论和现实含义。

（一）工作量证明机制（POW）及其经济学含义

POW 在区块链系统中成熟的标志是 2009 年比特币主网的上线。作为区块链最为经典的共识机制其核心思想是通过去中心化节点的算力竞争来保证系统交易数据的一致性，驱动算力竞争的经济激励是获得下一区块的记账权和该系统自动生成的 token 奖励。就比特币区块链而言，工作是指求解复杂但是验证容易的 SHA256 数学问题，在算法上这一问题的求解被标准化。[8] 生产方式的标准化推动了分配方式的标准化。

POW 的思想由来已久，即通过增加经济成本来提高市场诚实参与者的比重，以此来筛除非诚实节点。1993 年 POW 的思想被用来解决垃圾邮件问题，要求邮件发送者必须算出某数学题答案来证明发送邮件者的诚实度，提高恶意邮件发送者成本。[9]1999 年 POW 的概念被正式提出，这为 POW 在区块链系统中的应用奠定了坚实的基础。[10]POW 的运行模式和分配制度生动地再现了数字经济范式下的马克思劳动价值论和按劳分配制度 ：商品价值由无差别的一般人类劳动凝结而成 ；在数字经济时代，无差别的一般人类劳

动很大程度上并非由人类直接劳动完成，而是基于算力实现。与生产方式相对应，分配到 token 的数量与市场参与者贡献的算力成比例。2008 年的国际金融危机是比特币和区块链产生的直接原因，而 POW 也体现了区块链经济系统对由中心化的财政政策和货币政策主导的信用经济体系的反对与抵触。此外，POW 需要部署矿机、开发芯片、建设产业园，这会带动整个产业链经济的发展，有助于区块链实现脱虚向实、赋能实体，也更容易被传统经济和金融业接受。2019 年 11 月比特币矿机生产商嘉楠科技在纳斯达克挂牌上市，成为“全球区块链第一股”。

同时，POW 也引起了广泛争议，包括强大算力造成的巨大电力消耗。根据 2018 年 5 月 Arvind Narayanan 向美国参议院能源和自然资源委员会提交的报告，当时比特币挖矿每天消耗的电力约为 5GW，已接近全球耗电量的 1%。而随着比特币下一个减半周期的临近，算力增长非常迅速，这造成了更大程度的电力消耗。另一个方面，POW 的支持者们认为，标准化后的电力是全球通用的一般性产品，算力和电力凝结了无差别的人类劳动，这是基于 POW 的区块链产生的 token 区别于“空气币”的重要原因，持续增长的算力这也反映了社会对比特币的共识程度增强。但毫无疑问的是，在人类能源问题的解决取得突破性进展之前，POW 区块链项目无法大规模采用 POW。近年来，包括以太坊在内的部分区块链项目都启动了从 POW 向其他共识机制的转换路线。

采用 POW 的另一个问题是区块链系统难以实现商业化应用。比特币的出块时间约为 10 分钟，当大量的交易发生时不能被及时确认。即使此后诞生的基于 POW 的区块链做出了一定程度的改进，如莱特币的出块时间缩短

为 2.5 分钟，但仍难以满足商用需求，这也为 POW 的推广带来了很大困难。尽管 POW 存在能耗大、出块时间长等问题，但其理念得到了一定程度的认可，不少新的区块链项目在原生 POW 的基础上进行了共识算法的改进，主要的改进方向是降低能耗和提高出块速度。实现这一改进有三条基本的经济路径 ：一是直接增大市场容量，同时等比例提高市场交易和数据处理速率。这种路径只能提高出块速度，对能耗没有直接影响。二是基于 POW 产生区块链经济系统的“关键少数”，“关键少数”在一定时期内随机更新，由“关键少数”完成剩余的记账等经济活动，这部分经济活动的数据可能不在主链上。这种经济路径既提高了出块速度，又降低了能耗。三是将区块链系统进行分片(Shard) 处理，将全部的市场经济活动分区并行处理和存储。这种经济路径既提高了出块速度，又降低了能耗，但破坏了每个区块内保存交易数据的完整性。

2016 年 3 月在 POW 基础上产生的一种新型共识算法 Bitcoin-NG 将时间切分为不同的时间段，在各时间段上由一个领导节点负责区块生成和交易打包。Bitcoin-NG 中包含了用于选举领导节点的关键区块和包含交易数据的微区块这两种不同的区块：关键区块基于 POW 生成，关键区块选举产生领导节点，领导节点被允许以小于预设阈值的速度生成微区块。[11]Bitcoin-NG 在经济层面的解决思路与“隔离见证 + 闪电网络”相似，即不改变区块的市场容量，通过选举领导节点放弃某一时间横截面上的去中心化，提高了生成区块的效率，从而间接增加了市场容量。

2016 年 10 月提出的 Elastico 作为第一个基于拜占庭容错的安全分片协议，通过将全区块网络进行分片增强系统的可扩展性，其思路是将

区块链网络隔离为多个分片，这些分片可并行处理互不重合的经济交易集合。[12] 分片改变了区块链系统的出块和存储结构，尽管提高了出块速度、降低了能源消耗，但破坏了每个区块内保存交易数据的完整性。

2017 年 在 Elastico 共 识 的 基 础 上，Omni Ledger 提出 ByzCoinX 共识，通过一种抗预测的公共随机协议选择具有统计代表性的大型分片处理经济交易，并引入跨分片提交协议进行原子级交易处理。[13]ByzCoinX 共识结合了 Elastico 共识和选举类共识的优势，通过并行跨分片数据处理优化区块链系统性能，是一种既能提供可扩展性而又不必长期去中心性的架构。沿着将选举类共识融入 POW 类共识的发展路径，消逝时间证明共识机制（Proof of Elapsed Time, POET）、运气证明共识机制（Proof of Luck,POL）、空间证明共识机制（Proof of Space,POSP）以及有益工作证明共识机制(Proof of Useful Work, POUW）等无须消耗算力进行挖矿的算法相继诞生。在现阶段去中心化、高效率、安全性三者不可兼得的情况下，基于 POW 类共识机制的区块链项目必定要有所取舍。尽管当前 POW 类共识效率低、能耗高等缺陷难以根除，但 POW 仍是历史最久、影响最大的共识机制，被广泛接受的工作量仍然为区块链项目的价值提供了坚实的支撑。

（二）权益证明机制（POS）及其经济学含义

2011 年 7 月，名叫 Quantum Mechanic 的区块链爱好者在比特币论坛中首次提出了 POS 算法共识。在 2012 年 8 月诞生的点点币是首个基于 POS 共识机制的区块链项目，由该经济系统中具有最高权益的节点获得记账权，其中的权益表现为节点对该区块链系统 token 的所有权，称为“币龄”

（Token day），类似于传统金融中的股权治理机制，只是将时间因素囊括其中。在最经典的 POS 机制中，“币龄”等于 token 的数量乘以持有时间 ：Token day=Token*Timeweight。在 POS 的改进版本中，“币龄”在其原始经济含义的基础上根据不同项目做了不同程度的修改。截至 2019 年 6 月，全球已有超过 400 个区块链项目采用 POS 共识机制，总市值超过 140 亿美元。考虑到以太坊等项目正在从 POW 向 POS 转换，而以太坊又具有最丰富的经济生态，未来 POS 类共识可能成为最主流的共识机制。

POS 共识机制诞生初衷是克服 POW 共识机制的不足,事实上也在一定程度减轻了出块速度慢和能源浪费等问题，同时进入门槛较 POW 更低，对中小节点更加友好，中小节点不需要部署矿机和厂房即可参与记账。但是也存在一定的缺陷 ：第一，初始的 token 分配方式存在问题。不同于 POW 通过算力竞争记账权，POS 的初始分配方案难以机制化。一般而言，在 POS 项目发展的初期，难以对 token 进行广泛的社会化分发，只能集中在少数的项目创始人及重要利益相关者手中。第二，不同于 POW 验证节点作恶具有成本的约束机制，POS 验证节点作恶的成本在 token 价格较低时非常低。对于作恶低成本带来的问题是作恶节点会频繁出块和签名，或者在多条链的分叉上签名，并为获得更多奖励攻击区块链系统，即所谓的“无利害攻击”（Nothing at Stake）。第三，在 POS 共识中，需要足够的节点对 token 进行 持有才能维护系统的健壮与安全，区块链经济系统才有良性发展的空间。这会导致以下两个问题 ：一是,POS 项目在早期参与者较少,如果 token 持仓的集中度非常高，则很有可能出现数量很少的记账节点垄断出块的现象，这会极大提高区块链的系统性风险。二是，即使 token 的持仓分布较

为合理，但并非所有节点都是记账节点。受限于持仓量、成本和专业度等因素，token 持有人往往会选择将 token 委托给节点运营商（包括数字货币钱包提供商、数字货币交易平台、第三方服务提供商等）管理，由节点运营商代为行使出块、投票等权利，而 token 持有人享有分红等权利，这也就是所谓的“Staking Economy”。2019 年 3 月，Coinbase Custody 对基于 POS 共识的区块链项目 Tezos 为客户提供 token 托管服务，扣除相关费用后，投资者的年收益率约为 6.6%。

对 POS 共识机制的改进主要针对其三个缺陷进行，但对三个缺陷进行改进的难度各不相同。初始的 token 分配方式问题是 POS 共识的内生性问题，解决方式一般是先采用 POW 共识机制，在生态发育良好后再向 POS 共识机制转化。对于 token 持仓量的分布性问题则需要依靠经济激励和营销管道去解决，在现实中很多非法集团采用传销去解决这一问题，这事实上给区块链行业带来了巨大的负面影响。如何从经济模型上设计一套完善的初始 token 分发机制进而形成合理的 token 持仓分布是进一步完善 POS 共识的关键。

对于“无利害攻击”则主要从算法上对 POS 进行修正解决，形成了 Tendermint、Casper、Ouroboros、Tezos 和 HoneyBadger 等新型共识算法。原始 POS 算法共识假设系统节点在长期是静态和稳定的，这在现实区块链系统中并不存在。2014 年诞生的 Tendermint 共识将动态验证器集合和循环领导节点选举纳入 POS 共识，为解决“无利害攻击”这一弊病，Tendermint 节点须缴纳保证金，若有作恶行为保证金则会被没收。同时，Tendermint 基于 PBFT 共识算法，可抵御区块链系统中三分之一的作

恶节点攻击，具有较好的鲁棒性。[14]2016 年诞生的 HoneyBadger 算法是可在无任何网络时间假设的前提下实现经济系统的活性，同时可实现渐近有效性的原子广播协议，每秒交易量（Transactions Per Second，TPS）可到达万量级。[15]2017 年 8 月诞生的 Ouroboros 提出了一种新型奖励机制驱动 POS 共识机制，使得诚实节点的行为趋近纳什均衡，可有效抵御区块截留和自私挖矿等矿工策略性行为导致的安全攻击。[16]

（三）委托权益证明机制（DPOS）及其经济学含义

DPOS 共识机制本质上属于 POS 类共识，为克服 POS 在区块容量、出块速度等方面的局限而产生，但因其在经济模式上的创新和现实中的影响一般将其视为一种新型共识机制，2013 年 8 月由去中心化的数字资产交易所 BitShares 首次提出。DPOS 共识的基本思路类似我国的人民代表大会制度，采取民主集中制的原则，区块链系统中的每个 token 持有者都有选举出块节点的权利，也有被选举成为出块节点的权利。在比特股中，出块节点的数量是 101 个，在愿意成为出块节点的所有节点中获得投票前 101 名的节点将成为出块节点，按照既定时间表轮流对交易进行打包、结算及出块。[17] 出块节点的义务包括提供带宽及算力、参与出块过程、维护系统安全等。出块节点可通过出块获得区块奖励和交易费用，但若 token 持有者认为出块节点未能履行义务，其记账权会被取消，由得票最多的候选节点递补。每个出块节点服从相同概率随机获得出块记账机会，被抽中时有 2 秒权限生成区块、完成记账。若出块节点未能按时出块，出块权限则交给下个时间区间对应的出块节点。出块节点按照最长链原则选择在高度

最高的区块后添加自己的区块。DPOS 共识机制由于减少了出块节点的数量和出块时间，可实现 VISA 和 MasterCard 级别的数据吞吐能力。

BitShares 采用的原始 DPOS 共识在每个时间区间都是由单个记账节点完成，尽管记账节点被随机抽出，但仍有作恶的可能性。2018 年 6 月主网上线的 EOS 在原始 DPOS 共识的基础上融入拜占庭容错算法，采用了 DPOS-BFT 共识，在投票选举出记账节点的基础上，使用 BFT 类算法在记账节点间形成共识。EOS 共有 21 个出块节点，BFT 类共识可对 1/3 的记账节点容错，即任一区块得到 15 个及以上的记账节点确认即可最终确认。[18]

DPOS 共识机制能解决 POW 共识的能源消耗和联合挖矿对区块链系统去中心化构成威胁的问题，也能弥补 POS 共识中部分拥有记账权益的节点只关注收益率而不希望参与记账的缺陷，对高效率、去中心化、灵活度等系统重要经济目标取了一个内部解的折中方案。但是 DPOS 共识机制由于记账节点数量有限并且公开，攻击者想要发动攻击较为容易，记账节点需要额外保护措施，增加了节点运行成本。此外，区块链原教旨主义者认为 DPOS 共识机制破坏了比特币区块链去中心化的特征，是向中心化经济系统的妥协。

（四）有向无环图（DAG）及其经济学含义

有向无环图指任意一条边有方向、不存在环路的图形结构。DAG 共识机制改变了区块链系统的市场结构，DAG 中的交易单元包含了交易、签名及父辈单元信息，交易单元间以哈希相关联，在经济系统中不存在区块概念，自然也没有出块、打包等过程，DAG 通过用户间相互确认缩短交易确认时间。在 DAG 共识机制中所有交易都并发进行，无交易吞吐量瓶颈限制，节点越

多交易确认速度越快，在链式结构无此类优点。DAG 结构和链式结构本质上都是分布式结构，其本质区别在于帐本的异步性与同步性 ：DAG 作为一种典型的谣言传播算法，通过在节点间发送帐本数据，将记账行为进行异步处理来增加数据吞吐量 ；链式结构则是实现定期同步检查点的数据库同步机制。[19]

DAG 共识机制通过以下步骤防止双重支付：第一，节点尝试使用两个相同的输出单元时，当其中一个单元包含另一个单元时、且有先后顺序时，则直接拒绝后面单元。第二，两个相同的输出单元，无先后顺序，则在整个 DAG 经济系统中，建立总顺序后，出现早的单元得以确认，出现晚的单元无效。第三，设置总顺序的定义，相同地址发布超过一个单元时，要求每个后续单元包含所有先前单元。第四，若节点恶意发布顺序相同的两个单元，无论这两个单元输出中有无相同字符按照全网总顺序处理，后续单元 无效。第五，若用户按照协议尝试同一输出两次排序后生成单元，则按照本身顺序，晚生成单元无效。

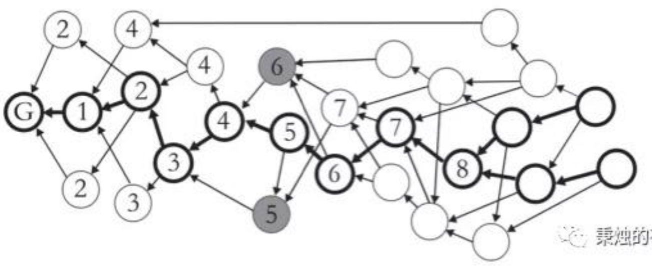

图 2 DAG 共识机制的数据结构

DAG 在革新数据结构和记账方式的同时，也存在一些问题 ：第一，无法保证交易状态的原子性和帐本的统一性。从时间维度而言，可能存在某节点在确认某笔交易时候，其交易确认时间无法估计 ；从节点维度而言，可能存在某节点没有被广播到某时间的交易信息，从而导致交易无法更新。

第二，在并行处理模式下，随着交易量增多，DAG 数据结构会日益复杂，对安全性提出的要求也会日益增加。

表 1　区块链算法共识汇总表

算法共识名称	共识形成方式	是否拜占庭容错	代表性项目
POW	通过竞争记账权形成共识	是 (<1/2)	Bitcoin、Ethereum
POS	通过竞争记账权形成共识	是 (<1/2)	Peercoin、Nxt
DPOS	通过选举间接形成共识	是 (<1/2)	EOS、BitShares
DAG	直接对交易形成共识	是	IOTA、Conflux、Qitmeer

总结而言，不同算法共识的经济学含义都是解决“谁有记账权”和“在分布式系统中如何同步帐本”这两个核心问题，在 POW 共识机制提出问题的解决方案后，POS、DPOS 以及 DAG 等新型共识机制试图对 POW 的缺陷进行改进，或对于区块链经济系统的不同政策目标进行取舍。同时，不同算法共识具有融合的趋势，尤其以 POW 与 POS 共识机制的有机结合最为突出，POW 解决了 POS 的初始 token 分配问题和作恶节点成本低问题，而 POS 在一定程度减轻了 POW 出块速度慢和能源浪费问题。此外，若在 POW 的基础上引入 POS，则将区块链系统的安全性建立在诚实节点拥有超过一半权益的基础上，即同时掌握超过 51% 的算力和权益才能发起 51% 攻击。

四、如何协同区块链三种类型的共识机制

区块链作为一项蕴含经济学内核的技术，理解其共识机制的经济学含义、优化共识机制的经济模型设置对推进区块链技术落地、赋能实体经济发展具有重要意义。狭义上的区块链共识机制指算法共识，算法共识是构成区块链的必需要件，也是区块链项目的基本面之一。但同时“人的共识”——决策共识和市场共识，也在区块链的发展中起到不可替代的作用。决

策共识起到对算法共识不断修正的作用，决策共识的收敛与否决定了算法共识的稳定性。市场共识代表了区块链系统内的利益相关者通过“用脚投票”的方式表示对该项目的认可程度。当前将区块链共识机制狭义化的现状割裂了三种不同类型的共识机制，对区块链的深化发展造成了阻碍。

区块链三种共识机制的割裂本质上体现了链上治理与链下治理的分离。任何一个区块链系统都在时刻与外界进行着信息与价值交换，即使是公有链也会受到链外中心化设施的影响，因此完全意义上的去中心化是不存在的。自 2009 年区块链正式诞生，决策共识治理机制缺失导致的各种分叉和市场共识缺失导致的 token 价格暴涨暴跌深刻地影响了区块链的演进与嬗变。此外，围绕区块链的法律、政策等链下治理设施对链上的算法共识也有重要影响。因此，推动促进区块链三种类型共识机制的协同发展对于贯彻落实习近平总书记区块链重要讲话精神具有积极意义。

第一，要把区块链作为核心技术自主创新的重要突破口，强化基础研究，着力攻克一致性、可用性和分区容错性三者难以兼容的技术瓶颈，不断完善现有算法共识，根据形势创建适合应用场景的新型算法共识机制，加大人员和资金投入力度，进一步打通创新链、应用链、价值链，加快推动区块链技术和产业创新发展，着力推进区块链同人工智能、物联网、大数据等前沿科技的深度融合。

第二，为区块链决策共识机制的建立提供完善的基础设施和健全的法律政策环境，着力提高社会对区块链的接受程度和认知水平。探索实现区块链项目利益相关者同区块链项目的激励兼容机制，提升我国在决策共识

形成过程中的国际话语权和规则制定权，对有价值、有意义的区块链分叉保持开放态度，保持和巩固中国在主流公有链挖矿产业的领导地位。

第三，尽管联盟链是我国区块链落地的主要方式，但仍应正视公有链在技术创新、微观治理等方面的重要作用，通过市场共识引导建立均衡的算法共识和决策共识机制。加大对公有链和联盟链的混合链的研究和实践，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，落实十九届四中全会将数据作为生产要素和分配要素的决定。

参考文献：

［1］张礼卿，吴桐 . 区块链在金融领域的应用 ：理论依据、现实困境与破解策略 [J]. 改革，2019（12）：65-75.

［2］袁勇，倪晓春，曾帅，王飞跃.区块链共识算法的发展现状与展望[J].自动化学报，2018（11）：1-12.

［3］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.

［4］Libra 白皮书 .https://libra.org/zh-CN/association/.

［5］吴 桐， 郭 建 鸾 .Facebook 加密货币 Libra 的经济学分析 : 背 景、 内 涵、 影响 与 挑 战 [J]. 贵州社会科学 ,2019(9):144-152.

［6］吴桐，李铭 . 区块链金融监管与治理新维度 [J]. 财经科学 ,2019(11):1-11.

［7］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.

［8］Satoshi Nakamoto.Bitcoin: A Peer-to-Peer Electronic Cash System,2008.

［9］Dwork C, Naor M. Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA: SpringerVerlag, 1992. ： 139-147.

［10］Jakobsson M, Juels A. Proofs of work and bread pudding protocols (extended abstract). Secure Information Networks. Boston, MA, Germany: Springer, 1999. 258-272.

［11］Eyal I, Gencer A E, Sirer E G, et al. Bitcoin NG: a scalable blockchain protocol. In: Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. Santa Clara, USA: USENIX Association, 2016. ： 45-59.

［12］Luu L, Narayanan V, Zheng C D,et al. A secure sharding protocol for open blockchains.In: Proceedings of the 2016 ACM SIGSAC Conference onComputer and Communications Security. Vienna, Austria:ACM, 2016 ： 17-30.

［13］Kokoris-Kogias E, Jovanovic P, Gasser L, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding [Online], available:http://eprint.iacr.org/2017/406, April 10, 2018.

［14］Kwon J. Tendermint: consensus without mining [Online], available: https://tendermint.com/static/docs/tendermint.pdf, April 10, 2018.

［15］Miller A, Xia Y, Croman K, et al. The honey badger of BFT protocols. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 31-42.

［16］David B, Gazi P, Kiayias A, et al. Ouroboros Praos: an adaptively-secure, semi-synchronous proof-of-stake protocol[Online], available: http://eprint.iacr.org/2017/573, April 10, 2018.

［17］BitShares. Delegated proof of stake [Online], available:http://docs.bitshares.org/bitshares/dpos.html, April 10,2018.

［18］https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.