姚前：算法经济：资源配置的新机制 | 互联网金融

原创： 姚前 清华金融评论 *2018-10-16*

文/中国人民银行数字货币研究所所长姚前

算法经济的发展颠覆了传统认知，甚至引发了争议。本文沿用科斯新制度经济学的分析框架和思路，利用契约经济学研究了从传统经济到共享经济、加密经济等算法经济的演化逻辑，剖析算法机制运行的经济机理、优点缺点及其与市场和企业的边界。研究发现，算法经济不仅不会走向计划经济，反而是一种更加接近自由市场的经济模式。

图灵奖获得者、Pascal之父Nicklaus Wirth曾提出一个著名公式：“程序=算法+数据结构”。这个公式深刻地揭示了程序的本质特征，如果将其扩展至更为广泛的业务流程，该公式完全可以修正为“智能业务=算法+数据”。常说的云计算、大数据、人工智能、分布式账本技术等，实质上均是“算法+数据”的体现，无非侧重点各有不同。因此有人对算法推崇备至，认为构建算法模仿，超越并最终取代人类，是21世纪最重要的能力，未来属于算法和其创造者。

依此，我们对算法经济进行定义。算法经济是指人们将生产经验、逻辑和规则总结提炼后“固化”在代码上，使生产经营活动无须人工干预，自动执行的经济模式。算法经济的意义在于，传统上市场供需匹配依靠市场的自发力量实现，而随着现代信息技术的发展和应用，市场供需匹配在自发力量的基础上，通过算法的应用大幅改善匹配效率和交易成本。根据算法对企业的不同替代程度，算法经济可分为共享经济和加密经济。共享经济中，供需双方通过算法直接对接交易，但共享平台的建设和运营依然依靠企业的组织、管理与协调功能，而在加密经济中，企业等经济个体通过激励相容的算法规则和相关契约安排，“无组织”地开展分布式协同生产。

资源配置的三种机制：价格、企业与算法

市场经济通过自动的价格机制实现资源的流动与配置。价格涨跌间资源的供给与需求自主调整着，反过来又推动价格变化，最终达成市场均衡。价格机制一向被经济学家们奉为圭臬。但事实上许多资源的组织协调通常是在没有价格机制参与的情况下进行的，如企业的生产活动。

D.H.罗宾逊对企业有个生动描述：“在不自觉的统筹协调的大海中的自觉力量的小岛上，它如同凝结在黄油牛奶中的一块块黄油。”对此，罗纳德·科斯（R.H.Coase）提出了经济学史上的一个“惊世”之问：“假如生产是由价格机制调节的，生产就能在根本不存在任何组织的情况下进行，面对这一事实，我们要问组织为什么存在。”1937年科斯发表著名论文《企业的本质》，开创性地利用交易费用理论分析了企业

的本质及其与市场的关系和边界所在，并因此于1991年获得诺贝尔经济学奖。他认为，企业产生的原因是企业组织劳动分工的交易费用低于市场组织劳动分工的费用。作为价格机制的替代物，企业是一种替代市场进行资源配置的组织。两种机制交易费用高低决定了两者间的边界。

科斯的交易费用理论完美阐述了企业在一个专业化的交换经济中出现的根本原因，时至今日仍闪烁着智慧的光芒。企业与价格机制成了大家广泛认同的现代市场经济的主要资源配置模式。然而，随着移动互联网和现代信息技术的快速发展和广泛应用，传统意义上的企业发生了“异化”，出现新的组织形态，比如共享经济的平台型企业，更有甚者，出现了企业的“消亡”。那就是本文所探讨的完全依靠算法而运行的“无组织形态的组织力量”——以比特币、以太坊等加密代币为代表的自治去中心化组织（Decentralized Autonomous Organization，简称DAO）。

共享平台型企业的特征是，原先企业内部的生产活动大量被外移至共享平台，打破了长期生产要素对企业的依附，直接向最终用户提供服务或产品。如共享打车，司机与共享平台之间没有固定的雇佣关系，自由地接入或退出共享平台开发运营的打车app，根据自我意愿直接向顾客提供打车服务获得收入。自治去中心化组织进一步将共享平台企业的去中介化进行到底，完全“抹除”了企业的组织形态。于是就有了类似“科斯之问”的第二个问题：传统的经济学理论告诉我们，生产要么由价格机制调节，要么由企业组织开展。面对这一结论，我们要问，DAO组织为何存在？它和企业有何区别？它与企业和市场的边界在哪？这些问题尚待研究。

回顾科斯的经典论著《企业的本质》，他的解释首先来自一个朴素的观察：“在企业之内，市场交易被取消，伴随着交易的复杂的市场结构被企业家所替代，企业家指挥生产”，因此自然而然地推导出：“企业的显著特征就是作为价格机制的替代物”，进而，科斯利用交易费用理论解释了在什么情况下资源的配置由价格机制决定，在另一种什么情况下资源的配置依赖于作为协调者的企业家，从而“在经济理论上的一个鸿沟上架起一座桥梁”。

我们若以相同的视角去审视共享平台和DAO组织的经济活动，亦可以得到一个朴素的发现：在这些组织里，由企业家指挥的生产变少了，而市场交易活动变多了，但协调、控制等组织功能依然存在，只是这些功能原先由企业家承担，现在则通过算法来实现。比如，通过算法，共享平台自动搜寻和匹配产品的供需，快速达成交易，无须需预测、计划、协调与控制等企业管理活动；比特币、以太币等DAO组织平台则以密码学技术为基础，通过分布式多节点共识机制，“完整、难以篡改”地记录价值转移（交易）的全过程，构建了去中心化、多中心化的应用或商业逻辑，并且通过运行在区块链上的代码即智能合约，保证业务逻辑的自动强制执行，整个流程无需任何管理人员的介入，自动完成了商品的生产、交易与消费。据此，我们就找到了回答DAO组织为什么存在的切入点，即在价格机制和企业机制之外出现了第三种市场资源配置机制：算法机制。

> **科斯框架：研究资源配置机制演化的一般逻辑**

（一）交易的自愿原则

自愿原则是现代经济学分析的基本假定。诚如科斯所言：“经济体制‘自行运行’，并不意味着没有私人计划。每个人都在不同方案之间进行着预测和选择。假如要使经济体制有秩序的话，这就是不可或缺的。”在市场价格的统筹协调下，众多个体的自愿交易行为“不自觉”地完成了资源的配置。究其根本，是个体的自愿交易动机，来源于交易双方对帕累托改进的“追求”。只有让任何参与个体的境况变得更好，个体才会有更大的激励去参与交易。因此，任何成功的交易必应是一个激励相容的交易。

自愿原则是任何市场化资源配置机制的基础，企业亦不例外。各类经济个体自愿加入企业，这就意味着与价格机制相比，企业必须是一个帕累托改进的安排。那么，为何由企业组织生产活动要比价格机制更能实现帕累托改进呢，科斯认为，这是因为企业的交易费用更低。

（二）契约与交易费用

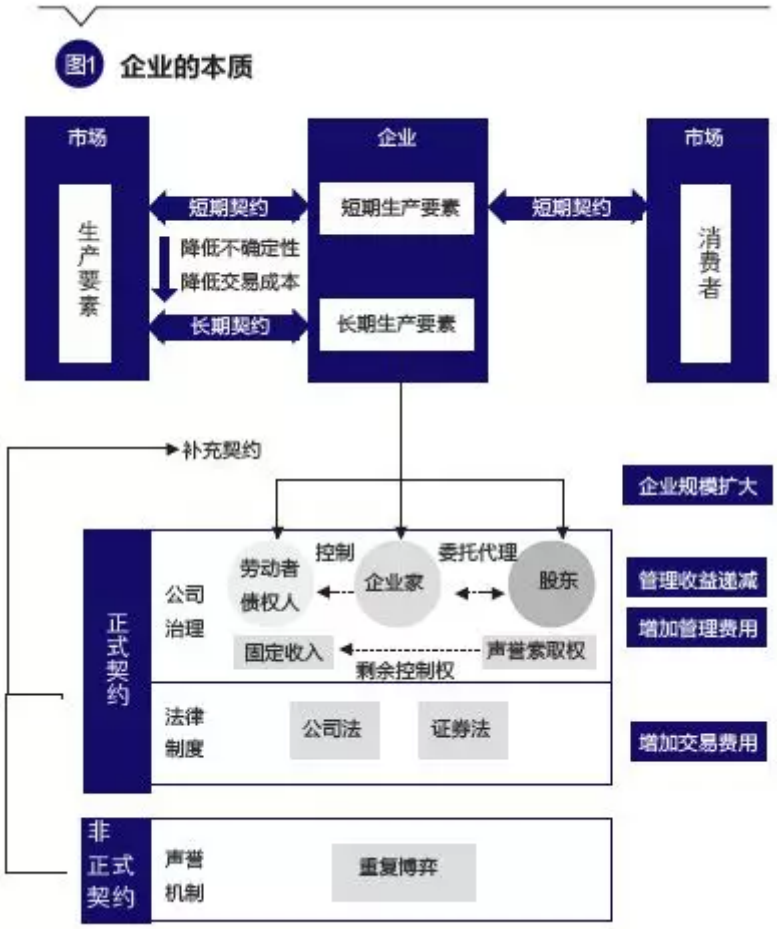
交易费用与契约有关。契约是指当事人双方关于权利和义务的安排，每一次市场交易都可以看成是买卖契约的一次订立与履行，从这个角度看，市场是由许多契约关系组成。通过市场形成的契约关系可能是正式的，如法律意义上的合同；也可能是非正式的，如口头上的允诺。而交易费用则是指当事人达成和执行契约时所需要耗费的成本，由搜寻成本、谈判成本、签约成本与监督成本等构成。

交易费用源于不确定条件下信息的不完备：未来信息的不完备以及他人信息的不完备。具体而言，在签约前，由于信息的不完备（事前隐藏信息），需要花费相应的成本搜寻合适的交易对手；在签约中，由于信息的不完备，需要在契约里事先规定交易各方的权利、责任和义务，而在明确这些权利、责任和义务的过程中需要花费成本和代价；签约后，由于信息的不完备（事后隐藏行动），执行契约亦需要费用，比如监督执行契约、更改契约以及违约后的追偿等。

（三）长期契约与短期契约：企业对价格机制的替代

契约可根据权利与义务的分隔时间长短区分为长期契约和短期契约。权利与义务的分隔时间越短，如“一手交钱一手交货”的“一锤子”买卖是短期契约，而分隔时间越长，则是长期合约。根据科斯的观点，企业是一组契约安排。他指出，“契约的本质在于它限定了企业家的权力范围。只有在限定的范围内，他才能指挥其他生产要素”。其中的契约更多意指长期契约，在企业里有一系列的长期契约，如企业与员工、经理人签订的雇佣合同、与银行签订的借贷合同、与出资人签订的出资合同等。正是这些相关个体相互讨价还价而订立了一系列的长期契约，最终集合成了企业这一组织形态。科斯认为，之所以企业在组织生产方面要比价格机制更具有优势，在于每一笔短期契约均要耗费搜寻、谈判和签约成本，而企业通过更少的长期契约替代大量的短期契约，由此大大降低了交易费用。他分析：“如果签订一个较长期的契约以替代若干个较短期的契约，那么签订每一个契约的部分费用就将被节省下来”“企业或许就是在期限很短的契约不令人满意的情形下出现的”。

显然，企业的长期契约主要针对生产要素，因此，经济学家张五常认为，企业是用要素市场代替产品市场。我们将通过长期契约提供的生产要素称为长期生产要素，包括劳动力、管理、资本等。那么，为何人们更愿意签订长期契约呢？科斯认为，这是“由于人们注重避免风险，因此宁愿签订长期契约而不是短期契约”“如果没有不确定性，企业的出现似乎是不可思议的”。因为面对风险，不同个体有着不同的风险承受能力，且不同个体有着不同的风险偏好。因此，通过签订长期契约，有些人规避了风险，获得稳定的固定收入，比如普通劳动者的工资、债权人的利息，而有些人承担了相对更高的风险，虽然仅获得剩余索取权，但不排除因此获得更高收益的可能，各方根据自己的资源禀赋和风险态度，均实现了帕累托改进。长期契约所节省下来的交易费用即为帕累托改进的总和，固定收入者（普通员工、债权人等）和剩余索取权者（股东）共同分配了企业所创造的“经济租金”。



（四）长期契约的不完备性

固然，长期契约有助于减少短期契约，节省了事前搜寻、谈判和签约的交易费用，但由于不完备性，长期契约存在着一项不可忽视的事后交易费用，那就是契约的执行成本。

契约的完备性是指如果契约能够详细说明未来可能出现的所有状态、每种状态下各方当事人的权利和义务，以及权利和义务的执行机制，那么，这样的契约是完备的，否则就是不完备的。在现实中契约常常不是完备的，这是因为很难预料到未来可能出现的所有状态，即使对未来的各种可能性都预料到了，但要把这些可能性全部描述出来也是相当困难的。进一步讲，即使事前的描述很完备，但是事后的解释也可能产生分歧，而且执行成本也可能会相当高。从交易费用角度看，虽然完备的契约能够降低事后讨价还价的可能性，使事后的交易费用得到节约，但它也使得事前的交易成本上升。因此，综合上述各种因素，权利和义务间隔的时间越长，当事人越倾向于选择“走一步看一步”的策略：长期契约往往只是以一般条款规定一下，具体细节则留待以后解决，完备性低于短期契约。那么，为了降低因长期契约的不完备性而带来的执行成本，需要补充的契约安排来“打补丁”，以控制事后交易费用的上升。

（五）长期契约的补充安排：公司治理

根据Jensen和 Meckling（1976）以及 Easterbrook和Fischel （1996）的观点，公司治理结构是一系列契约的集合，包括股东与股东之间、股东与企业之间、企业与高级管理人员之间、高级管理人员与员工等之间的合约。涉及股东的剩余控制权、股东与企业家之间的委托代理以及大股东与小股东之间的委托代理等权利和义务的安排。

这些安排有助于弥补长期契约的不完备性，以股东的剩余控制权为例，股东的剩余控制权是指合约中无法事前规定的、对企业资产和经济活动的指挥权。由于长期契约不完备，相关主体可能会隐藏行动，比如工人的努力水平，而剩余控制权规定了当发生长期契约上没有注明的情况时究竟谁有权做出企业的决定，这对长期契约进行了补充，避免了在组织内的无休止“讨价还价”，有效降低交易费用。再如，由于信息不对称，经营权与所有权的分离带来了委托代理问题，针对这些问题，一方面可通过合理的激励机制来解决，如建立与业绩挂钩的薪酬制度和晋升制度；另一方面可给予管理层股权激励，让企业家也成为股东，从而内部化企业家行为的外部性，实现企业家与股东利益的一致。

（六）长期契约的补充安排：法律制度

法律本身实际上也是一种契约，它对企业中长期契约形成了有效的补充，大大降低交易费用。一方面，法律在事前为当事人提供了通用契约，使当事人的契约谈判可以集中于相对特殊问题的解决，比如组建公司，当事人只需要做两件事：一是根据公司法选择特定的企业组织形式；二是将公司法中没有规定的条款进一步明确，指定公司章程和条例，由此省去了事前的谈判和签约成本。另一方面，法律具有强制性的权威，列出的原则性规定，所有人都必须接受，因此节约了事前的交易成本。同时，法律为契约的事后执行提供了纠纷解决机制，转移了事前约定和事中监督的压力，也降低了事后执行成本。比如，少数股东权益受到大股东或管理层侵害时可向行政机关请求救济或者向法院提起诉讼，用事后的制裁形成威慑，替代事前监管，节约监督成本，从而缓解大股东与小股东之间、股东与管理层之间的委托代理问题。

（七）企业与市场的边界

企业通过长期契约对短期契约的替代，节省了事前交易费用，但并不能完全消除交易费用，反而因长期契约的不完备性增加了事后交易费用。虽然公司治理、法律制度和声誉机制等补充契约安排有助于控制事后交易费用的上升，但这些补充的契约实质上也新增了额外交易，企业需要付出相应的代价。比如公司治理中的管理与控制增加了企业的管理费用。这些交易费用可能会随着企业规模的扩大而不断上升，并且企业规模的扩大同时还可能会让企业家不能成功地将生产要素用在它们价值最大的地方，导致资源浪费。科斯将这些因企业规模扩大而带来交易费用的上升，称为“管理收益递减”，反映了企业的机构困境（Institutional Dilemma），即企业的存在是为了利用群体的努力，但它们的某些资源又为了引导这些努力而慢慢流失。因此，企业规模不可能无限扩大的，它与市场的边界在于，“在企业内部组织交易的成本或是等于在另一个企业中的组织成本，或是等于由价格机制‘组织’这笔交易所包含的成本”。

> **共享经济：算法对企业的辅助**

（一）共享算法：短期契约对长期契约的替代

早在1937年撰写《企业的本质》时，科斯就注意到了信息技术发展对企业组织形态的影响。他指出：“倾向于降低空间组织成本的电话和电报的技术变革将导致企业规模的扩大，一切有助于提高管理技术的变革都将导致企业规模的扩大。”企业经营和管理的信息化、自动化和智能化，优化了企业的生产流程和管理结构，加快信息流速率，提高决策效率，大大降低了企业管理成本和费用。信息化和数字化，已成为现代企业经营的基本战略。从契约经济学的角度看，这其实是通过算法的应用，大幅降低了企业长期契约的交易费用，从而进一步强化了企业在资源配置上的优势，扩展了企业与市场的边界。

然而，随着互联网技术、大数据分析、云计算和人工智能的发展，越来越多的由算法控制的信息化系统融入当前企业，算法对企业的影响已不再停留在以往简单的辅助功能上，而是从根本上改变了企业的组织形态和运营模式，涌现出了一大批供需双方直接对接交易的共享平台，其中最为典型的就是Uber、滴滴为代表的网约车平台。在这些平台上，生产者与消费者直接进行动态、多变、复杂的网状连接和点对点交易，而有效支撑这些网状连接和点对点交易的则是平台企业所设计、维护和运营的强大算法。并且随着环境和市场的变化，算法不断调整和优化。不同于以往支撑企业内部信息管理的算法，这些算法的作用不在于帮助企业提高管理技术，以此降低企业执行长期契约的费用，而是“减少”了长期契约，破除长期生产要素对企业的依附，将许多经济活动移到企业外部，由供给者和消费者直接对接进行“一锤子”买卖，大幅增加了短期契约的数量。比如共享打车平台，司机与共享平台之间没有固定的长期雇佣关系，无须遵循传统的管理规则，自由地接入或退出共享平台开发运营的打车app，向顾客直接提供打车服务。这是短期契约对长期契约的替代，是算法对预测、计划、协调与控制等企业管理活动的替代。之所以能够发生替代，原因在于，大数据、云计算和人工智能等现代算法技术的应用大幅降低了海量短期契约的交易费用，包括搜寻匹配的费用、谈判签约的费用、执行监督的费用。

（二）搜寻匹配的算法机制

由于信息不对称，市场交易需要搜寻匹配，而这将耗费成本。随着群体规模的扩大，一个人同另一个人的直接互动变得越来越不可能，相互之间的交易搜寻匹配成本越来越高，因此每个个体往往是以“就近原则”在有限的范围内开展市场交易，由此许多可能的商品和服务的生产和消费没有变成现实。比如个人闲置的不具有标准化特征的个性商品，如闲置的家用汽车、闲置的电脑硬盘空间甚至是闲置的时间和精力等，难以进行有偿的共享与交易。

移动互联网的发展首次打破了人与人之间的物理隔绝，大幅扩展了人的集体行动范围。但要达成人与人之间的市场交易这还不够，更直接和广泛的信息传播只是提高了集体行动的可能性，没有在根本上彻底解决订单搜寻和匹配的信息成本问题，直到大数据、云计算和人工智能等算法技术的应用后，海量短期契约的搜寻和匹配成本才大大降低。以共享打车为例，共享平台每天需要处理的订单是海量的，一天的成交订单量有数百万，如何低成本、快速、高效地搜寻和匹配这些订单成了关键。共享打车平台首先运用云计算搭建了大规模实时分单处理平台，实现多维度最佳订单匹配。用户输入一个目的地，最佳合理调度都由云计算以毫秒级的速度来计算。其次，共享打车平台运用了大数据分析技术。以滴滴打车为例，它覆盖了交通路况、用户叫车信息、司机驾驶行为、车辆数据等多个维度的数据。基于这些大数据，可应用分类、聚类分析、关联分析、神经网络、机器学习等数据挖掘技术来进行订单的供需预测，从而帮助平台快速地达成供需匹配。最后，由于司机和用户永远在运动和变化中，共享打车平台在供需预测的基础上，运用了路径规划和预计到达时间（Estimated Time of Arrival，简称ETA）两项地图技术围绕最低的价格、最高的司机效率和最佳交通系统运行效率等指标进行最优动态规划，然后通过大规模分布式计算来实现上述的最优撮合，实现智能派单。据悉，当前共享打车平台的动态规划算法可以预测每一单出行的时长以及预估在每一个路口前的等待时长。

（三）谈判签约的算法机制

为了平衡各方利益，共享平台制定了规则，并将其转化为算法自动运行。这些以算法形式表达的规则通常都会被清晰明确地告知到所有参与主体，由各主体根据自愿原则选择是否参与，若选择参与，则须遵守相关规定。类似法律制度，算法本身就是适用于每个主体的通用契约，降低了交易双方“讨价还价”的谈判成本，同时，这些规则对各方利益进行了平衡，有利于进一步优化市场的供需平衡，降低供需失衡的可能性，提高契约的成功匹配效率。以滴滴打车为例，它设计了动态调价和“滴米”派车的算法机制调整优质稀少资源匹配的有效程度，通过价格杠杆来调节供需。区域供需失衡时，算法会基于实时交通状况，计算出一个合理的建议加价倍数。动态调价情况在叫车前就会告知乘客，如果乘客同意，才确认发出订单，否则可直接取消叫车且不会收取违约金。“滴米”派车类似积分制度，司机积累的“滴米”高了，就更好抢单，以此来平衡各种不同单子的供需。

（四）执行监督的算法机制

虽然短期契约在完备程度上高于长期契约，但由于无法“穷尽”所有信息，仍存在不完备性，因此在契约的事后执行监督上依然需要耗费成本。对此，共享平台设计了类似声誉机制的奖惩机制，将其转化为算法自动运行来约束各方的行为，并利用大数据分析和人工智能技术进行事后判责。以滴滴为例，它建立了服务信用体系，使用大数据技术分析乘客打分、乘客评价以及取消率等变量，综合计算出每个司机的服务分值，服务分越高，司机可获得的订单和收入越多。除了服务分，共享打车还通过人工智能进行智能的司乘判责。

（五）共享平台的委托代理问题

共享平台的算法机制依然没有脱离传统企业的组织形态。平台规则和算法由企业设计、维护和运营。在一定程度上，共享平台的算法机制可看作是企业所提供的SaaS服务（Software as a Service，应用即服务），即共享平台的算法是企业向平台参与者供给的一种长期产品。从契约关系上看，企业与各平台参与者之间存在着长期契约关系。

这一长期契约存在信息不对称性，表现在虽然规则上会清晰明确地告知到所有参与主体，但规则背后的算法的具体原理、参数以及每次执行的实际情况，对外部主体保密，只有共享平台的运营企业才能知道，这就可能会发生算法滥用和利益侵占的事件，从而引发参与者对算法的不信任。比如，共享打车的动态调价算法就曾被质疑过企业是否在利用算法来谋取私利。对于这种委托代理问题，业界提出了“计算机道德”和“算法伦理”的概念，督促企业自律，如谷歌曾经把“不作恶”视作公司的口号以增强顾客对平台的信任。另外，就只能通过“用脚投票”的市场机制来进行约束企业的行为。

> **加密经济：算法对企业的替代**

如果说共享平台的算法机制还“残余”着企业的影响，去中心化、去组织化的加密经济的算法机制则完全“抹除”了企业的任何“痕迹”，成为一种完全独立于企业的全新的资源配置机制。也正是因为完全“抛弃”企业的管理控制功能，加密经济的算法机制所要承担的功能和解决的问题，难度甚于共享平台。首要的问题是，没有企业的组织、管理与协调，由谁去开发算法？怎么“无组织”地组织分布式协同生产。对此，加密经济通过激励相容的算法规则和相关契约安排，明确了各方的经济利益，充分调动了各方的积极性，使有效的分布式协同生产真正成为可能。

作为加密经济的基石，区块链技术可分为数据层、网络层、共识层、激励层、合约层和应用层六个层次。其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等技术；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要包括保障节点数据一致性的各类共识算法和协议；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制，以及相对的惩罚机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。

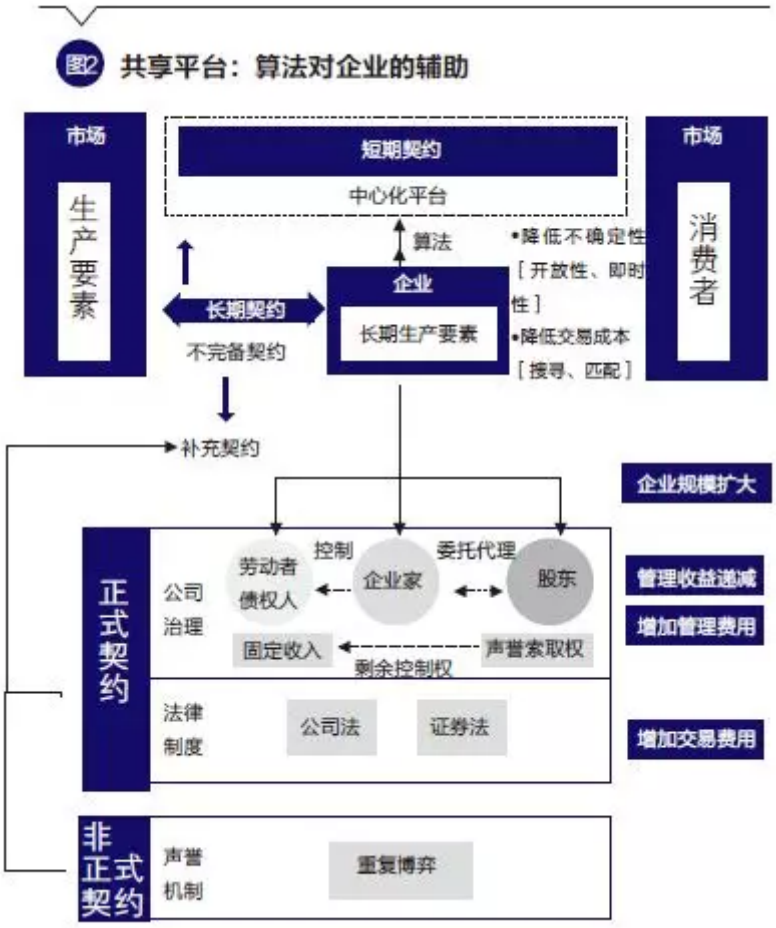
从契约经济学的角度看，数据层和网络层对应的功能是契约的搜寻匹配；共识层和激励层对应着契约的谈判签约；合约层则包含了契约的执行监督功能。加密经济不仅有技术逻辑层上的支撑，又有经济逻辑层上的保障，加密技术与经济机制设计的结合使加密经济成为具有巨大潜力的新兴经济模式。

（一）搜寻匹配：DLT的去中心化与开放性

根据统计研究，自组织存在幂律特征：个体等级越高，对组织的贡献越不均衡，或可称“二八法则”，即20%的人提供了80%的贡献，而另外80%的人贡献了20%。对于企业而言，他们通常采取的策略是，通过事前甄别和事后淘汰机制“搜寻”出前20%的贡献者，与他们签订固定的长期契约，而忽略后80%的人，使他们成为经济活动的偶然参与者，因此，企业的开放性是有限的。

但对于DAO组织而言，“无用”不代表不重要，不代表可以舍去，正是因为对参与者的无歧视对待，任其自由加入和退出，DAO组织才可最大限度地做大样本，无需“搜寻”就可获得尽可能多的贡献者。且从交易费用角度看，参与者的自由加入与退出不耗费DAO组织的任何资源，即不存在交易费用，而企业不一样，他们与参与者需要签订长期契约，每个参与者的进入和退出，都会让企业付出相应的交易费用，通俗讲，企业不养“闲人”。因此，企业对参与者选择了封闭性策略，而DAO组织采取了开放性策略。

可以说，对于任何的分布式协同生产，开放性都是关键性的。诚如Eric S. Raymond（2000）研究发现，当大量的贡献者以一种去中心化的组织结构持续不断地协同合作时，项目开发的效率最佳。而区块链技术的出现正是使得互联网变得更加开放，更加去中心化，更加安全，更加隐私，更加平等以及更加易于进入。这是因为：一是区块链系统异构多活，灵活性强。区块链技术采用P2P网络协议，基于一致的P2P协议，不同节点可由不同开发者使用不同的编程语言、基于不同的架构、实现不同版本的全节点来处理交易。二是区块链系统不依赖于个别节点，容错性强。区块链技术通过共识算法保持各节点数据的高度一致，每一个全节点都会维护一个完整的数据副本，整个系统的正常运转不依赖于个别节点，同时还能保证整个系统的7×24小时不间断工作。三是区块链系统安全可信，可靠性强。安全机制是区块链系统中最为核心与关键的组成部分，主要包括隐私保护、共识协议安全性、智能合约安全性、数字账户安全（钱包私钥保护）、离链交易安全机制、密码算法的实现安全及升级机制等。比如，区块链在身份认证、权限控制和签名验签部分，使用了非对称密码技术，保证交易的安全可靠，且通过哈希函数、时间戳、默克尔树等巧妙的数据结构设计并辅以密码学和共识算法，实现数据库历史记录的难以篡改。在隐私保护上，区块链技术吸纳了零知识证明、多方保密计算、环签名、基于格的密码体制、全同态密码学、链外信息互换通道等前沿技术，以更好地解决隐私保护问题。



（二）谈判签约：共识机制的激励相容

区块链技术通过巧妙的经济激励和技术设计，创造了一种新型自由开放系统的协作机制，能够很好地适应经济一体化深度发展下大规模多边协作的技术需求。本部分以工作量证明机制（PoW）为例阐述共识机制的激励相容设计，更详细讨论请见笔者发表于《清华金融评论》2018年9月刊的文章。

激励机制

区块链是一个公共可见的账本，用来记录交易的历史信息。当一笔新的资产交易被创建时，资产转出方需要通过签名脚本来证明自己是资产的合法使用者，并且指定输出脚本来限制未来对本交易的使用者（即资产收入方）。如果是合法创建并签名的，则该笔交易现在就是有效的，它将被广播到区块链网络并被传送，每一个收到交易的节点将会首先验证该交易，确保只有有效的交易才会在网络中传播，而无效的交易将会在第一个节点处被废弃，直至抵达挖矿节点。

挖矿节点在验证交易后会将这些交易添加到自己的内存池中构建新的区块。在PoW机制，矿工们接着通过反复尝试求解一种基于哈希算法的数学难题来竞争获得记账权，具体而言，矿工不断更换区块头的填充随机数并计算这个区块头信息的哈希值，看其是否小于当前目标值。如果小于，则成功“出块”，随后矿工将这个区块发给它的所有相邻节点。这些节点在接收后进行一系列的检查标准，去验证区块的正确性。检查的标准包括区块的数据结构和区块包含的交易合法有效；区块头的哈希值小于目标难度（确认包含足够的工作量证明）等。一旦一个节点验证了一个新的区块，它就会将新的区块连接到累计了最大工作量证明的区块链中，矿工挖矿成功。

在上述过程中，矿工获得两方面奖励：一是代币奖励。矿工构建的新区块中的第一笔交易是一笔特殊交易，称为创币交易或者Coinbase交易。矿工挖矿成功后，将获得这笔新创造的加密代币。在比特币网络，每隔10分钟将一个新的区块添加至链上，每添加一个区块可以获得50枚比特币作为奖励（每四年减半）。二是记账决策权与交易手续费。矿工拥有记账决策权，有权决定将哪些交易添加至新构建的区块，并对收录在区块内的所有交易收取手续费。

惩罚机制

通过惩罚设计，PoW设置了两道门槛：第一道门槛设在矿工竞争记账权的时候，使得矿工不能随便“发言”（新增区块）。一方面，矿工为获得记账权，须不断求解哈希难题，因此付出“不菲”的成本，这一成本是沉没成本，只要矿工想参与“发言”，那么无论他最终能否成功“发言”，他均必须付出这一笔建言成本；另一方面，由于哈希难题的验证要比求解来的简单，对新出区块的验证成本微乎其微，因此只要矿工一错误“发言”（如交易无效、格式不符等），就会很快地被其他节点检测出来废弃掉，他之前付出的建言成本相当于对他的惩罚。

第二道门槛则设在区块被成功添加区块链后的修改，使得矿工不能随意更改区块链。在比特币网络，每2016个区块(大约两周)后，所有客户端把新区块的实际数目与目标数量相比较，并且按照差异的百分比调整目标HASH值，来增加（或减少）产生区块的难度，确保每10分钟 1 块的恒定出块速度。挖矿难度值的提高，增加了攻击的成本。攻击者如果要构造出一条比真实区块链更长的秘密区块链，需要在比特币网络产出6个区块的同时秘密产出7个区块。

截至2018年2月，专业的比特币挖矿机器（以Bitmain生产的AntMiner S9为例）价格为2700美元，这台矿机以2017年2月27日为基准可挖0.0012枚比特币。一台AntMiner S9每天耗电33度，按照居民用电价格计算，大概每天电费2.6美元。假定AntMiner S9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。那么，无论攻击成功与否，攻击者都需要付出4250*7=29750美元，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，显然对算力提出了巨大的要求：只有掌握了比特币全网51%算力的攻击者，才可以用这些算力来重新计算已经确认过的区块。

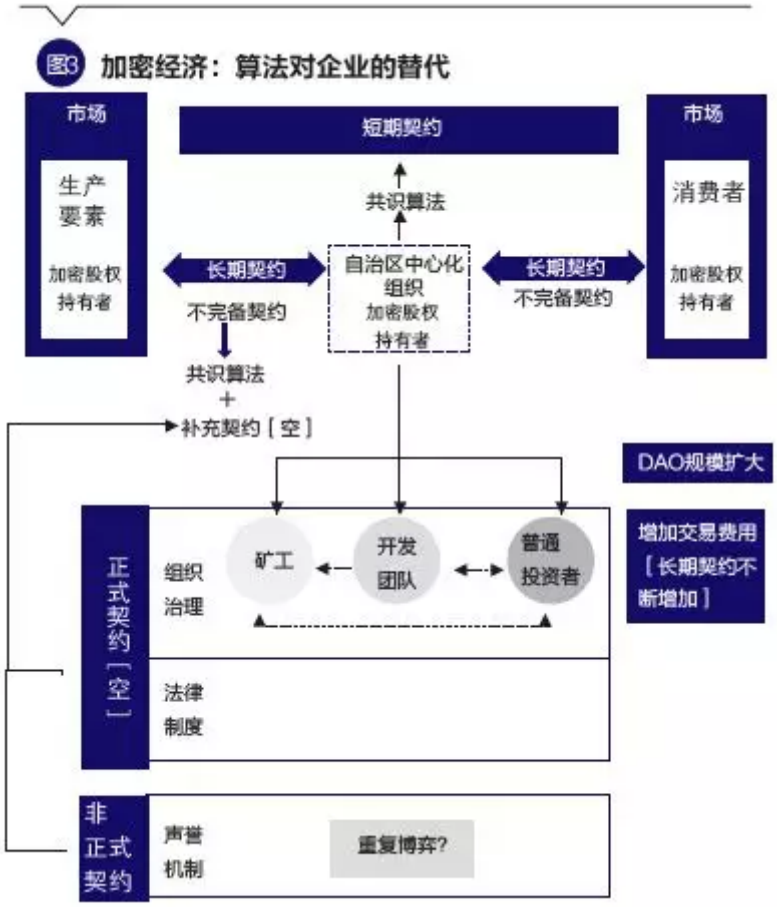
上述两道门槛使得无论是新增还是更改区块，均需要付出不菲的成本，尤其是对后者的要求更为苛刻，这就是Nakamoto面对“拜占庭将军问题”的全新思路。某种意义上来说，PoW机制的“工作量”相当于现代资产交易或拍卖的保证金制度，免除了随意报价，同时还确保了比特币各区块哈希值的唯一性及难以篡改，这正是PoW这一机制设计精巧的地方。

（三）执行监督：智能合约的强制执行

由于契约的不完备性，契约中权利与义务间隔期限越长，契约的执行成本就越高。对此，网约车等共享平台设计了类似声誉机制的奖惩机制，将其转化为算法自动运行来约束各方行为，并利用大数据分析和人工智能技术进行事后判责，从而降低了契约的执行成本。同样，加密经济也是通过具有强制执行特征的算法机制来执行契约，那就是智能合约。智能合约最早由密码学家尼克·萨博于1993年提出，它是区块链上可以被调用的、功能完善、灵活可控的程序。

一定程度上，比特币协议中的脚本已具有“智能合约”的特征。脚本是一种基本的基于栈的语言，包含检查哈希是否相等以及验证签名等操作。当一笔新的交易被创建时，转出方需要通过签名脚本来证明自己是这笔资金的合法使用者，同时创建一个锁定脚本来限制未来对该笔资金的使用，下一个使用者继续使用相应签名脚本来花费它。实质上，每笔转账交易不仅指向地址，而是指向一个简单的“智能合约”。

但比特币系统的脚本语言存在一些缺陷，比如缺少图灵完备性等。以太坊对比特币的脚本进行了扩展和提高，使得开发者能够创建任意的基于共识的、可扩展的、标准化的、图灵完备的、易于开发的和协同的应用，任何人都可在智能合约中设立他们自由定义的所有权规则和交易方式。智能合约具有透明可信、自动执行、强制履约的优点。可以说，智能合约将组织的规则进行了编码，进一步降低与契约不完备性相关的交易成本，提升了区块链技术的价值，使加密经济模式的适用范围和领域不断扩大。



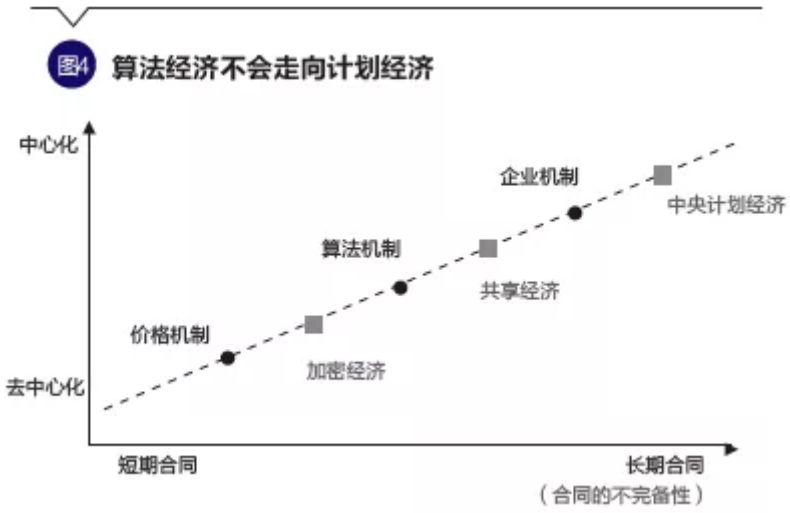
资源配置机制比较：算法经济会走向计划经济吗

随着算法经济的发展，尤其是近几年大数据技术的提高，人们开始讨论或"担忧"通过大数据、人工智能去建立计划经济的可能性。基于前述讨论，我们认为，算法经济不仅不会走向计划经济，反而是一种更加接近自由市场的经济模式。

一是从中心化的角度看，中央计划经济以高度集权为特征，否定经济个体的自由意志，经济封闭，不允许经济要素的自由移动，而算法经济则以半中心化或去中心化与开放性为特征，强调和尊重市场交易的自愿原则，发挥市场价格的统筹协调机制，推动经济要素的自由流动和资源配置，在经济自由度上，不仅高于中央计划经济，甚者还高于企业机制，比如生产要素与共享平台之间没有长期固定关系；加密经济则抹除了企业的组织形态。

二是从契约关系看，在中央计划经济中生产要素被绑定在各种组织形态中，经济的契约关系更多体现为长期契约，而相比较，算法不仅可以帮助企业提高管理技术，降低企业执行长期契约的费用，还可以"减少"长期契约，破除长期生产要素对企业的依附，将许多经济活动移到企业外部，以短期契约的形式开展。因此，算法经济与中央计划经济截然不同，不仅没有提高经济的集中度，反而提高了经济的自由度。

但算法经济也有缺点，比如一系列加密代币委托代理问题等。因此，算法经济不可能完全替代现有的经济模式，使企业和市场完全消失。正如企业与市场的边界一样，算法经济与现有经济模式的边界取决于，算法经济中组织交易的成本与现有经济模式中组织交易的成本的比较，前者成本越低，算法经济越具有优势，边界越大，反之越小。



更准确地说，算法经济是对现有经济模式的一种有效补充。比如，有观点认为，加密经济的加密股权融资方式有助于克服经济网络效应的“拔靴问题”(Bootstrapping Problem，指网络发展到一定规模时才能盈利)。