加密经济学研究进展*

冯碧梅　王诗桁　张继钦

摘要:加密经济学作为一个新兴交叉研究领域,综合运用了经济学、密码学、计算机科学等多学科理论,主要研究如何在分布式系统中形成共识。本文在总结梳理加密经济学的学科属性、理论渊源的基础上,对加密经济学的研究对象、发展演进、应用场景等进行了梳理。首先,本文通过回顾"拜占庭将军问题"介绍了加密经济学的起源,并阐述了加密经济学的研究对象、理论基础和学科属性。然后,本文梳理了加密经济学在共识算法、激励机制、智能合约等方面的发展演进。最后,本文总结了加密经济学在分布式系统的去中心化特征、安全性特征、可拓展性特征等方面的应用研究,并对加密经济学的未来研究进行了展望。

关键词:加密经济学　共识机制　工作量证明　权益证明

随着数字经济的快速发展,在线支付和供应链金融等经济活动愈发活跃,并在分布式、匿名化系统中取得共识,但因缺乏可受信任第三方机构,共识的形成需依靠个体决策基础机制并充分考虑现实信息交换等问题。"加密经济学"(cryptoeconomics)概念最早由以太坊社区开发者 Vlad Zamfir 在 2015 年的一次演讲中提出,他认为加密经济学主要研究去中心化数字经济中的协议,这些协议用于生产、分配和消费的治理。2017 年以后,研究者逐渐接受了"加密经济学"这一概念,并开展了相关研究(Mclean,2017;Buterin,2019;Berg et al,2019)。与很多新兴学科一样,加密经济学的研究范畴并没有形成统一的定义,大部分的学者认为加密经济学主要研究如何在分布式系统中通过个体激励和与之相关的共识机制实现共识,并抵抗风险(Dannen,2017;Berg et al,2019;Brekke,2020)。

区块链、数字货币、智能合约作为加密经济学的典型应用,其相关主题成为学者关注的热点,但由于缺乏对加密经济学理论的研究,使得相关研究难以深入甚至存在错漏。近年来,学者开始重视加密经济学学科研究,研究成果发表于《经济研究评论》(*RES*)、《金融研究评论》(*RFS*)等权威期刊。学者结合分布式系统、共识机制等基础理论研究区块链活动对竞争过程、组织形式的影响(Chiu & Koeppl,2019;Saleh,2021;Huberman et al,2021)。这些研究不仅将区块链视作一种新的技术,分析其对经济活动的影响;还通过博弈论、公共选择理论研究如何实现共识机制的优化和分布式系统个体协调。二者对比,前者将区块链技术视作一种"外来冲击",分析其对传统经济学研究范式的影响;后者深刻融合经济学理论研究加密经济学所关注的独特问题,这些问题在传统经济学研究中很少涉及。鉴于此,有必要对加密经济学起源、理论基础、学科属性、发展脉络和应用影响等方面展开系统回顾。这有助于深化对区块链、数字货币、非同质化代币(NFT)等新经济现象的理解和研究,吸引更多国内外学者参与加密经济学的理论研究,基于"中国实践"就加密经济学领域取得成果突破,提出"中国经验"。

一、加密经济学的研究对象

加密经济学始于 Nakamoto(2008)创造性提出的工作量证明机制,其来源可追溯至 1982 年由图

* 冯碧梅、王诗桁(通讯作者)、张继钦,福州大学经济与管理学院,邮政编码:350116,电子邮箱:583393142@qq.com,wangshixun@fzu.edu.cn,zhangjiqin7840@163.com。基金项目:国家社会科学基金一般项目"'双循环'新格局下我国制造业转型升级研究"(21BJY102)。感谢匿名审稿人修改建议,文责自负。

灵奖得主莱斯利·兰波特(Leslie Lamport)和其合作者提出的“拜占庭将军问题”(The Byzantine Generals Problem)(Lamport et al,1982)。此后,以 Nakamoto(2008)、Buterin(2014)为代表的从业者与研究者对工作量证明机制进行了拓展研究,提出了权益证明、有向无环图等不同机制。以此为基础,加密经济学的理论被应用于货币结算、智能合约等领域,催生了区块链、加密货币等新的组织或模式。在工作量证明机制被提出后,研究者进一步结合博弈论、机制设计、公共选择等经济学理论,形成了相对独立的研究对象、研究方法和框架体系。

(一)拜占庭将军问题

加密经济学问题的研究起源于拜占庭问题。Lamport et al(1982)进行了正式描述:若干将军指挥一场战役,他们需要对“进攻”或“撤退”进行决策,而不同将军相互之间只能利用通信进行交流,每名将军将根据其收到的信息进行决策。将军中存在一定数量的“忠诚”将军与“叛变”将军,叛变的将军会刻意传递错误信息以干扰决策。拜占庭将军问题研究的问题是:是否存在一种机制可以确保“忠诚”将军能够实现一致行动?拜占庭将军问题概括了加密经济学核心的研究问题及其研究特征,这一问题的现实复杂性推动了加密经济学的发展。

Lamport et al(1982)在提出拜占庭将军问题的同时,提出了“口头信息”(oral message)和附加签名条件的“签名信息”(signed message)两种解决方案。后续研究者开发了实用拜占庭容错算法(practical Byzantine fault tolerance,PBFT),成为加密经济学目前广为接受的算法之一(Castro & Liskov,1999)。这些解决方案通常是一套计算机算法,或是附加数字签名等假设条件,或是对节点数量和系统规模做出限制,在开放网络下容易受到攻击(Fischer et al,1985)。随着数字经济的快速发展,这些解决方案的不足在实际应用中越发凸显,对异步网络、节点数量、系统规模的限制变得更为突出,对是否能适用于数字场景应用和在分布式系统中兼顾开放性、匿名性、安全性存在疑问。

(二)加密经济学的诞生

Nakamoto(2008)提出的工作量证明机制(proof of work, PoW)提供了创造性的解决方案,成为加密经济学诞生的标志。不同于 PBFT 算法,PoW 机制依赖算力取得共识,能够有效防范攻击。如果攻击者无法控制网络 51%以上的算力,那么网络攻击无法实现。现实情况下,控制大量算力比控制大量 IP 地址成本更高,PoW 机制实现了开放匿名分布式网络的拜占庭容错,可以证明攻击成功概率随分布式系统链条的延长呈指数级别下降。与 PBFT 遵循一套流程式算法不同,工作量证明考虑到了个体行为动机和攻击的成本收益,蕴含了经济学研究的基本特征。但同机制设计方面的经济理论相比,PoW 机制增加了通信环境、信息存储、发布方式等方面的考虑,体现了加密经济学交叉学科的特点。加密经济学的后续研究一般都在 PoW 机制研究的基础上进行拓展,并探索共识机制在不同的场景应用。

(三)加密经济学的研究对象

拜占庭将军问题最初主要针对的是“分布式”和“拜占庭容错”两个与加密经济学密切相关的研究主题。分布式表明“不存在可受信任的第三方”,系统内的参与者必须自行协调并做出决策,无法依靠第三方统一协调指挥。拜占庭容错则表明系统内可能存在恶意参与者,因为存在信息非对称性,参与人无法准确识别恶意参与者,所以相关机制必须能够抵抗恶意参与者的攻击。由忠诚将军进行的一致行动被称为“共识”,对能实现共识的系统称之为具备拜占庭容错的特征系统,相关机制称作为“共识机制”。如移动支付的拜占庭将军问题,“忠诚将军”表示线上支付用户,“叛变将军”表示线上支付欺诈者,拜占庭将军问题就是研究如何使得线上支付正常进行并防范线上结算欺诈。

二、加密经济学的理论基础与学科属性

加密经济学有三个重要理论源泉,包括计算机科学的通信理论、密码学的加密原理、经济学的机制设计。随着研究的深入,经济学的公共选择理论也越来越多地与其他理论相融合并应用于加密经

济学的研究。无论是理论研究还是应用研究,加密经济学都体现了交叉学科特征,是数字经济背景下最前沿的发展方向。加密经济学起源于通信理论,但共识机制的优化离不开经济学的机制设计理论。算法在应用中是否满足个体理性,是否受风险规避等行为影响是计算机科学难以回答的问题。

(一)理论基础

1.*计算机科学通信理论*。加密经济学涉及拜占庭容错系统中的相互通信与共识取得,这与计算机科学通信理论相关联。通信理论提炼了加密经济学的研究对象及其主要特征。同时,FLP 定理和 CAP 定理等也对加密经济学共识机制的设计与完善划定了理论边界(Gilbert & Lynch,2002)。

2.*密码学加密原理*。PoW 机制实现共识需依赖节点在一定时间间隔发送信息,是节点基于密码学中的哈希算法(secure hash algorithm, SHA)对特定问题求解,率先得出解的节点可进行信息记录发送,并获得代币奖励。两次求解的时间间隔成为信息发送的时间间隔(Nakamoto,2008)。在权益证明机制中,虽然信息发送的间隔被设置为一个固定值,但代币的持有和奖励同样需经过加密(Vasin,2014)。哈希算法是加密经济学中常用的加密算法,具有快速验证特征,即在给定明文和加密规则下可以快速验证信息真实性;在现有技术条件下不可反向破解,或破解耗费算力,这充分保证了信息的安全性;特定问题求解的算力消耗随着时间推移不断增加,解的数量收敛于一个有限值,使得代币数量存在上限。

虽然加密经济学包含"加密"二字,但主流研究对加密算法原理的关注却较少,密码学的作用也被不断弱化。主要原因是哈希算法已经成熟,能够在很大程度上保障信息的安全性,而共识机制却面临主要挑战,如分叉攻击、长程攻击等,难以仅靠加密算法得到优化解决。因此,不宜将加密经济学理解为"加密技术"与"经济学"的简单叠加。而且,与加密技术直接相关的研究文献也较少。

3.*机制设计理论*。机制设计是指委托人从期望结果出发,设计一个博弈规则激励委托人实施特定行动,并由此得到代理人想要的结果(Voshmgir & Zargham,2020)。如何在自由选择、自愿交换、信息不完全等分散化决策环境下设计出一个机制让代理人按委托人意愿行事,是机制设计研究的问题,也是加密经济学共识机制所要解决的问题。如何将各种利益相关者的价值转化为机制设计的原则,这是构建有效加密系统的关键所在(Ballandies et al,2021)。加密经济学共识机制与个体决策、成本收益分析紧密相关,机制设计在加密经济学学科体系中极为重要(Vasin,2014)。共识机制设计时,如果纳入个体行为假设与理性决策,那么可以很大程度上提升系统效率、降低系统成本。权益证明机制以经济确定性取代最终确定性或概率收敛确定性,以参与人收益最大化决策防范攻击,这已充分体现了机制设计的思想(Buterin & Griffith,2017)。近年来,研究者将共识机制模型化为随机博弈,将一致性正式地定义为马尔可夫均衡,并进一步分析马尔可夫均衡对分叉攻击的抵抗能力(Biais et al,2019;Saleh,2021)。Cong et al(2021a)进一步探索了数字平台运用共识机制的方式,认为平台中引入共识机制有助于降低交易成本,降低平台用户总量的波动性并加速平台的成长。

4.*公共选择理论*。共识形成过程包含"投票""收益分配"等环节,公共选择理论便十分自然地应用于分布式系统治理和共识形成问题研究。分布式系统节点被视作是投票者,不同共识机制的形成过程确定了投票规则(Berg et al,2018,2020)。其分析结果应用于识别与优化共识机制,提高共识形成效率并抵抗攻击(Allen et al,2023)。Yu et al(2019)发布 RepuCoin 系统,通过全区块多期算力贡献,评估节点声誉并计算了共识形成中的投票权,从而替代了 PoW 机制依靠即时算力计算的投票权。针对 PoW 的"抱团"问题,Wright(2019)提出通过二次投票机制找到一种平衡,既能考虑到多数人的意见,又能保护少数人的权利。Leonardos et al(2020)在 PoS 机制基础上加入了加权投票机制,通过计算验证者做出正确投票行为的概率,为验证者分配投票权重,提高共识形成效率。虽然验证者的选择和奖励的分配遵循 PoS 机制,但共识达成的过程却由加权投票机制决定。Dimitri(2022)通过构建博弈论模型进一步研究了区块链中使用二次投票机制时节点的最佳投票数。

(二)加密经济学的学科交叉属性

从学科属性角度来看,很难将加密经济学单独归属于计算机科学、密码学、经济学任一学科。加密经济学研究是多学科交叉。计算机科学和加密学作为加密经济学的理论来源始终发挥着基础性作用,但经济学相关理论在最新的研究中发挥了越来越重要的作用,甚至成为加密经济学共识机制未来优化的重要研究方向。

加密经济学较早的研究已关注了区块链、比特币等问题,但对于分布式系统问题关注不足,相关分析也不够深入。目前主流研究更多开始从分布式系统特征和共识机制出发,对其影响机制和影响范围等进行探讨。Cong et al(2021b)通过构建垄断竞争模型分析了加密货币何以具有去中心化特征。在基于 PoW 的区块链中,参与者将联合形成矿工组织以分散风险,加强了系统的中心化功能。Ferreira et al(2023)分析了中心化特征成立的边界条件,研究发现,倘若系统中的利益相关者和系统外的设备供应者的利益有冲突,而系统外的设备供应者拥有系统治理权时,将严重损害 PoW 系统的去中心化特性。

三、加密经济学的发展演进

随着数字货币和区块链技术的快速发展,加密经济学逐渐成为数字经济领域的重要分支。共识算法、激励机制、智能合约作为加密经济学的核心概念,在数字货币和区块链技术的应用中发挥至关重要的作用。

(一)共识算法

工作量证明的共识机制提出后(Nakamoto,2008),学者从共识形成、信息发布过程等方面进行了优化,形成了权益证明(proof of stake, PoS)、有向无环图(directed acyclic graph, DAG)等不同机制。新的共识机制并非是对旧有共识机制的全面替代,在新共识机制提出后,对原先共识机制的研究并未因此减弱,旧有共识机制反而因吸收了新的共识机制的优点而得到发展。PoW 确立了共识机制的基本框架,可以概括为四个主要要素:信息存储方式、信息发布规则、共识实现、节点激励(Nakamoto,2008)。信息存储方式指的是以何种结构存储信息,例如在大部分"链"的结构中,信息被不断添加至每一区块尾部,从而使得该区块包含了此前全部记录的信息。信息发布规则指谁有权力发布信息,以及如何发布信息,例如,PoW 通过工作量证明机制发布信息。共识实现指当系统中存在多个不同信息时,如何确定何者是正确的,例如 PoW 通过最长链原则并结合哈希算法验证进行判定。节点激励方式则指如何激励节点耗费资源进行信息发布和验证,由 PoW 形成的代币激励是最为主流的激励方式。倘若说"三元悖论"决定了分布式系统的特征与不同共识机制的实现目标,以上四个要素则是支撑安全、可拓展性、去中心化特征的具体方式。

1. 工作量证明机制(PoW)。工作量证明机制(PoW)不仅是首个共识机制,更是一个具有里程碑意义的创新。它成功地在去中心化分布系统中实现了兼顾匿名性和安全性的共识,也确立了后续共识机制的基本框架。

(1)PoW 信息存储方式。Nakamoto(2008)设计的工作量证明机制是加密经济学最早使用的共识机制。PoW 确立了后续共识机制的框架,在信息存储方式上采取了"区块"和"链"的结构。所有当前和过往的信息在经过加密压缩后被写入新的区块中,其他节点则可以对该信息的正确性进行验证。此外,"链"的结构则表明各区块前后相关,后一区块所记录信息的正确性在一定程度上可以由前一区块记录的信息进行验证。这为共识实现提供了基础:攻击者无法单独篡改某一区块的信息,要成功实现攻击必须修改该区块至今的全部信息。这种信息存储方式在安全性上的优点显而易见,但随着链条延长系统需要记录的信息越来越多,资源消耗也越来越多,这也催生了后续对存储方式优化的研究(Kondru & Saranya,2020)。

(2)PoW 信息发布规则。PoW 采取了"工作量证明"的发布规则。工作量证明实质上是以哈希

算法为基础,寻求一个数学问题特解的过程。基于哈希算法特点,该特解有难于求解、不可被反向破解但易于验证的特点。这保证了一定时间范围内只有少数节点能够发布信息,避免了多个信息同时发布给共识形成带来的障碍。其缺点也显而易见的,一定时间内全网只能由单一节点发布信息,这大大限制了信息交换的速度,在交易场景中存在交易延迟的问题(Chiu & Koeppl,2017)。以交易次数衡量,一般认为以 PoW 为基础的比特币每秒交易不超过 10 次,而 Visa 的交易网络每秒则支持超过万次的交易。此外,随着链条的延长,节点需要耗费更多的存储空间,并需要耗费更多的算力进行计算,这降低了系统的总体效率。研究者测算发现,比特币进行运算耗费的电量相当于 2000 万吨二氧化碳排放量,约为 100 万次跨大西洋飞行,20 个国家的总用电量(Hern,2018)。这种信息发布规则的低效率也成为后续研究需要改进的重点方向。

(3)PoW 共识形成。PoW 采取了"最长链原则",由区块形成的链条中,最长链条记录的信息被认为是正确的。而随着工作量证明的开展,链条不断延长,由最长链原则确定的共识也就更为安全,有效攻击的难度也更高(Maurer et al,2013)。这一原则也与信息存储方式和信息发布规则有着紧密联系:"区块"和"链"的结构意味着攻击者如果想修改系统内的信息,则需要对该信息区块开始至今记录的全部信息进行修改。"工作量证明"的信息发布规则意味着这种修改极其耗费算力,攻击者的收益很可能小于攻击成本。Nakamoto(2008)形象地称其为"一块 CPU 具有一票(验证信息正确)的投票权",并给出了共识实现的一般方法与流程,但并未在严格意义上证明该流程符合个体理性,也未充分考虑个体之间潜在的策略性行为。Biais et al(2019)建立模型分析了共识机制,证明共识机制的最长链是马尔可夫完美均衡,而分叉则可能由博弈的多重均衡形成。进一步探索了影响参与者完成工作量证明并形成共识的两个经济因素:一是参与人的行动策略性互补,随着参与人实行工作量证明,其获得的收益会随之提高;二是称之为"既得利益"(vested interest)条件,进行工作量证明的参与人不能立刻消费所获得的代币,因此参与人在某一信息分叉(fork)获得的利益会支持其在该信息分叉上的后续投入。在这一基础模型之上,后续研究进一步分析了加密货币均衡价格形成等问题(Biais et al,2023)。

(4)PoW 的风险。在通常条件下,只有掌握超过 51%算力的攻击者才能实现有效攻击,随着分布式系统中总算力的增长,攻击耗费的成本将远远大于其收益,也意味着 PoW 几乎具备最高的安全性(Buterin,2019)。但这并不意味着 PoW 面对算力攻击时无懈可击,一个潜在的威胁是量子计算。随着量子计算机的发展,如果相关量子算法能够成功运行,则能轻易破坏 PoW 所构筑的算力屏障(Vandersypen et al,2001;Rohde,2021)。

在技术层面外,共识机制面临的另一现实威胁来自个体理性与风险规避。节点成功完成工作量证明的概率与掌握的算力相关,在单一节点掌握较小算力的情况下,完成工作量证明的概率便较低。个体出于风险规避和风险分担的考量,将联合形成所谓"矿工组织"以分担风险(Cong et al,2021b)。矿工组织首先集合了节点算力从而提升了群体完成工作量证明的概率,而后根据算力贡献对个体进行收益分配。虽然 PoW 是一个分布式系统,但矿工组织却有中心化的可能。根据 Cong et al(2021b)统计,截至 2018 年 2 月,矿工组织控制了比特币中超过 99%的算力(以 Hashrate 衡量)。这种中心化组织的算力集中冲击了 PoW 的理论基础,使得大部分算力集中于若干组织(Frey & Sumner,2019)。这也意味着对于共识机制的优化需要充分考虑个体对不确定性的态度,并进一步引入不确定性下理性行为的分析框架,这也成为未来共识机制优化的发展方向。

2.权益证明机制(PoS)。权益证明机制(PoS)改进了 PoW 机制下以工作量为基础的信息发布与共识形成方式,提升了共识形成的效率并提高了分布式系统的可拓展性。但同时分布式系统的安全性与匿名性却可能受到损害。

(1)PoS 信息发布规则。PoS 采取固定时间间隔的随机选择过程进行信息发布,替代了 PoW 中耗费算力进行工作量证明的过程(Lepore et al,2020)。这种方式的耗费更少,而且具有更高的结算

效率,但由于缺乏了 PoW 中依靠算力提供的安全性保障,也可能受到 PoW 较少遇到的一些攻击。这种固定时间间隔的信息发布方式本身并不复杂,研究重点在于如何识别风险并提升系统安全性、优化信息发布过程(Alrowaily et al,2023)。

(2)PoS 共识形成。PoS 共识形成方式有两种。一种是基于拜占庭容错算法的共识形成,另一种是基于链的共识形成(Buterin & Griffith,2017)。前者完全放弃了以工作量为基础的共识形成方式,而采取了用户持有的代币数量作为判断依据(Vasin,2014)。而基于链的共识形成继承了 PoW 以工作量证明为基础的共识形成,避免了少数节点算力增加带来的冲击,一定程度上缓解了"矿工组织"兴起带来的威胁。Pass & Shi(2017)提出的 FruitChain 协议,在实现与 PoW 一致性的同时,能够使得"相同比例算力"获得"相同比例区块",也就是他们称之为"公平"的区块链(fair blockchain)。在两种共识形成方式中,基于拜占庭容错算法是主流共识形成方式,且与 PoW 在信息发布和共识形成方面有着较为明显的区别。

PoS 使用了基于"权益"的投票机制作为正确信息的判定方式。系统中的节点需事先质押一定比例的代币(权益)以获得投票权,并根据投票结果决定哪一信息可被接受记录。因此,对系统的攻击不仅要求攻击者掌握大量的代币,而且其攻击行为也会导致其已经掌握的代币遭受损失,使得攻击行为并不符合参与者的经济利益。PoS 实现的确定性也因而被称作"经济确定性"(Vasin,2014)。Buterin & Griffith(2017)从通信技术的角度展开,对 PoS 的经济确定性进行了分析。虽然 PoS 的共识形成与参与人的决策和经济理性高度相关,但与之相关的第一个正式模型由 Saleh(2021)提出,他从均衡的视角全面分析了 PoS,并发现这种均衡能够解决信息发布的"无利害关系问题"(nothing at stake problem),并分析了 PoS 共识形成的条件如何较好地抵抗分叉攻击,规避无利害关系问题。

PoS 共识形成机制带来的一个潜在问题是"马太效应",持有代币数量越多的节点越有可能获得区块奖励并主导验证过程,从而无法实现共识的概率收敛。针对这一问题,主要解决思路是,随机选择参与共识形成的节点和参与信息发布或记录的节点,以减少持有代币数量较多的节点的影响力。代表性研究包括:Kiayias et al(2017)对 PoS 进行了形式化分析,并提出了一个名为"Ouroboros"的协议,该协议使用了一种简单安全的抛硬币方法使得在节点选择中尽可能增加随机性。Daian et al(2019)提出了"Snow White"协议。"Snow White"同样采取随机选择的思路对 PoS 进行了优化。然而,与 Kiayias et al(2017)提出的抛硬币方法不同,"Snow White"采用了 Pass & Shi(2017)提出的"休眠共识",修改了确定验证节点的方式,以增加随机性。

(3)PoS 的风险。PoS 面临的风险中最具代表性的是"无利害关系问题"。与 PoW 创建新的区块需要耗费算力不同,理论上,PoS 的节点可以无风险且近乎无成本地为不同信息创建新的区块。这增加了系统中链的分叉数量,削弱了区块链解决"双重支付"的能力,同时增加了达成共识的时间,降低了系统的效率(Li et al,2017)。在这一过程中,攻击者也可通过扭曲信息发布并影响后续共识形成而获益。针对该问题有两类应对措施:一类是构建惩罚机制。如 Buterin & Griffith(2017)提出的权益质押机制,参与者事先质押一定比例代币,质押代币数量越多的参与者在共识形成中有着更大的优势。但倘若参与者违反信息发布的规则时,将被惩罚失去全部质押的代币权益。通过调整参与者的质押比例、投票权益和惩罚,可以使得参与者违背规则的成本远大于遵守规则的收益,从而减少产生无厉害关系问题的经济动机。另一类则试图在网络中揭示实施行为的节点信息。Li et al(2017)给每一节点增加了数字签名,一旦不同分支链条上的区块由同一节点创新,则系统将自动揭示节点身份与信息。这种解决措施实质上牺牲了匿名性以换取安全性,并提高了对节点身份管理的要求。因此,从目前实践来看,权益质押机制是较为普遍的解决无利害关系问题的方法。

这种信息发布方式带来的另一问题在于"长程攻击"(long range attack),也被称作"历史攻击"(history attack)。由于信息发布本身并不消耗算力资源,攻击者可以从更早的区块开始(甚至是第一个区块开始),创建一条新的分支链,并替代现有主链。对于这种攻击,"检查点"是一种有效的防

范措施,即在每次验证后判明哪一区块属于“最终确定”区块,这一区块是不可被更改的,这种解决方式还可以通过对链条长度的修改进行限制得到进一步增强(Bentov et al,2016;King & Nadal,2012)。但这种措施提高了对同步性(synchronization)的要求,新加入的节点可能无法判明哪一链条是正确链条,这削弱了系统的可拓展性。其他的解决思路还包括 Li et al(2017)提出的通过可信的代码执行环境,即通过阻止验证者在历史时刻相同的两条平行链条均做出验证,以防止在相同历史时刻重复生成区块。

3.委托权益证明机制(DPoS)。委托权益证明机制(DPoS)在 PoS 的基础上优化了共识形成的方式,进一步提升了共识达成的效率,降低了能耗。由于进行验证与记账的见证人节点受到严格限制,基于 DPoS 的系统更容易存在中心化趋势。

(1)DPoS 信息发布规则。DPoS 通过引入见证人节点角色,实现了信息发布的高效和可控(Larimer,2014)。相较于 PoS 中所有节点都可以自由发布信息,DPoS 限制了信息发布权限,只有被普通节点选举出的有限见证人节点才能发布信息。由于见证人节点数量有限,在信息验证和共识达成的过程中面临的复杂性和难度较低,因此能够更迅速顺畅地达成共识。这一特点显著缩短了 DPoS 系统中达成共识所需的时间,从而提高了整个系统的运行效率,展现出更高拓展性。

(2)DPoS 共识形成。传统的 DPoS 共识实现方式在 PoS 基础上引入了委托代理过程,要求普通持币节点通过投票选举特定数量的见证人节点参与区块验证。这种机制最早由 Larimer(2014)在 BitShares 系统中实现。在该机制下,普通节点通过投票选举见证人节点来验证交易,由见证人节点轮流发布新的区块并相互验证,由于只需要少数的见证人节点达成共识,因此具有更高的共识形成效率,但存在中心化程度高、无法剔除恶意节点、节点参与不积极等问题。改进的 DPoS 通过增加随机性和优化投票机制的方式进一步改善了共识形成过程。Fan & Chai (2018)选择获得票数最多的前 N 个见证人节点构成初始验证候选池,利用确定性随机比特生成器从中随机选择最终的见证人节点,从而增强了共识形成过程的去中心化能力。在优化投票机制方面,Li et al(2023)通过引入 PageRank 算法改进投票机制,实现“一票多投”,得到每个节点的信誉值,并基于 GN 算法度量节点投票热情,设计了一种结合节点声誉和投票热情的综合选举机制,使共识能够由安全可靠的见证人节点形成。Xu et al(2019)通过增加反对票和弃权票的票型,采用模糊集合的方式选择见证人节点,同样降低了恶意节点被选为见证人节点的概率。

4.有向无环图机制(DAG)。PoS 通过更改信息发布和共识形成的方式改进了 PoW 结算效率,而有向无环图(directed acyclic graph,DAG)通过改变信息存储和共识形成的方式实现了优化改进。

(1)DAG 信息发布规则。DAG 原为图论中的术语,倘若一个有向图从任意顶点出发无法经过若干条边回到该点,则这个图是一个有向无环图(Bondy & Murty,2008)。有向无环图作为一种便捷有效的工具,也被广泛用于因果推断分析中(Cunningham,2021)。加密经济学使用 DAG,主要利用了其无回路、节点之间具有清晰指向等特点,每一节点即为分布式系统中的参与者,每个节点的信息可以同时被多个新加入节点引用,同时,新加入节点可以同时引用多个节点的信息。“有向边”确立了信息发布、共识形成的规则(Sompolinsky et al,2016)。这极大地提升了信息存储效率并潜在地优化了信息发布与共识形成过程

(2)DAG 共识形成。DAG 主要有区块型 DAG(block DAG)和交易型 DAG(transaction DAG)两种类型。这两种类型对共识形成的优化思路不尽相同(Kondru & Saranya,2020)。区块型 DAG 是在区块设计和 PoW 基础上构建的,利用 DAG 有向性和无环性,提高网络的吞吐量和交易速度。SPECTRE 协议是最早基于 DAG 结构设计的共识机制(Sompolinsky et al,2016)。SPECTRE 使用一种被称为虚拟成对投票机制的概念来确定 DAG 中任何成对块的顺序。在该机制下,每个块不仅根据 DAG 拓扑结构对其父块的相对顺序进行投票,还根据其子代块的相对顺序进行投票。

交易型 DAG 彻底放弃了 PoW 和 PoS 中的区块结构,利用 DAG 的顶点进行信息交换,利用边

进行验证，其共识形成有三种方式：一是基于主干链的共识形成方式。在 Churyumov(2016)提出的 Bytaball 协议中，共识形成的方式是先在 DAG 中确定主链，进而确定交易全序。二是基于平行链的共识形成方式。Baird(2016)提出的 Hashgraph 共识算法使网络中各节点或节点集合分别维护一条链，链间通过相互引用构成平行链结构，各节点利用此引用关系实现共识。三是基于投票机制的共识形成方式。例如最早使用 DAG 结构之一的 Nano 协议，通过主要代表节点投票决定哪些信息可以被接受(LeMahieu，2018)。一般情况下，交易型 DAG 能够大大降低交易费用，极大地提高了交易速度，并具有一定的扩展性。与 PoS 类似，DAG 不依靠求解哈希算法生成的时间间隔进行信息发布。因此，相较于 PoW，DAG 更为节能(Kondru & Saranya，2020)。

(二)激励机制

信息存储、信息发布、共识形成都需节点持续投入算力和存储资源，需对节点进行激励以维持系统持续运行。PoW 采取的代币激励的方式，成为绝大多数共识机制激励的基础。率先完成工作量证明的节点将获得代币奖励，拥有记账权的节点在该区块进行记录也会获得手续费奖励。此时节点的激励与信息发布、共识形成之间形成了正向循环。节点耗费算力进行的信息发布能够为节点提供代币奖励，使节点有动力进行更多的工作量证明运算。

1. *代币激励*。PoW 的代币属于交换代币，可作为交换手段，实现商品和服务的交易，在受监管的支付服务中提供便利(Braddick et al，2018)。后续研究进一步拓展了代币激励方式，将其拓展为资产代币与公用事业代币(Clayton，2017；Lux & Mathys，2018)。其中，资产代币表示有形或无形资产的加密资产，可以提供如所有权、特定金额的还款或未来利润份额的权利，类似于股票、债券或衍生品(Braddick et al，2018)。公用事业代币主要用于投资其他需要资金的企业，一旦开发出特定的产品或服务，投资者可以享用该产品或服务(Clayton，2017)。激励形式的拓展也将加密经济学的应用由加密货币拓展至供应链金融、电子政务、医疗卫生等领域(Benchoufi et al，2017)。

2. *声誉激励*。Gai et al(2018)提出声誉证明机制。该机制不依赖哈希算法求解实现信息间隔发布，减少了算力消耗并提高了结算效率。Chai et al(2019)提出了应用于车联网的声誉证明机制，在声誉评级上采取历史数据滚动评级的方式，避免了高声誉评级节点对资源和记账权的垄断。Wang et al(2020)在代币激励的基础上增加了声誉激励，声誉较高的节点拥有更多生成区块的机会，诚实用户和攻击者之间的算力差距可以用声誉来弥补，增强区块链安全性。Wang et al(2020)进一步引入了声誉阻塞率和竞争周期，声誉越高的节点，其声誉的增长率越低，并且在一个竞争周期内，节点无法连续生成多个区块。

(三)智能合约

共识机制带来的安全性、不可篡改性催生了智能合约(smart contract)的应用。智能合约早就被 Szabo(1996)提出，但加密经济学使得智能合约从构想走向了现实(Wang et al，2019)。加密经济学关注分布式系统的现实应用与影响。例如，加密货币对金融增长的影响(Howell et al，2020)、中央银行是否应当发行数字货币(Keister & Sanches，2023)，以及智能合约在供应链管理、能源、电子政务等领域的应用等(Jain & Sedamkar，2020；Wang et al，2021；Andoni et al，2019；Jacobovitz，2016)。

从近期研究来看，研究者逐渐从对加密货币本身的研究转向了加密货币对真实世界影响的研究。Dell'Erba(2019)认为，随着实物资产代币化的程度越来越高，央行数字货币将有助于推动传统经济向数字经济转型。Howell et al(2020)对比了 ICO 和股权众筹、风险投资、IPO 三种传统融资方式，得出 ICO 作为一种新型融资方式具有传统融资方式所不具备的优势的结论。ICO 可以为去中心化网络的发展提供融资，有助于快速形成网络效应，降低交易和监管成本等，同时具有更高的安全性、流动性和透明度。Keister & Sanches(2023)通过构建动态一般均衡模型分析了央行数字货币对利率和福利的影响。研究结论显示，引入类似现金的数字货币对利率没有影响，只有当分散市场消

费的福利权重足够高且数字货币存款利率为正时,类似现金的数字货币才会在最优政策下提高福利。Chiu et al(2023)通过构建存款市场不完全竞争的一般均衡模型进行研究发现,当央行数字货币的利率介于0.3049%~1.28%时,央行数字货币才可以增加社会总产出水平。

四、加密经济学的应用

加密经济学存在着所谓的"三元悖论"。任何共识机制都需权衡去中心化、安全性、可拓展性,但是通常这三者难以兼顾(Abadi & Brunnemeier,2018)。加密货币、数字合约、区块链本质上是不同类型分布式系统,它们的应用范围及其影响边界和三元悖论特征有关。

(一)去中心化

去中心化自治组织(decentralized autonomous organization,DAO)是加密经济学的重要应用。去中心化自治组织允许分布式系统节点以更自主的方式进行自我组织和协调,除去了传统组织中协调者或监督者角色(Buterin,2014;Wright & Filippi,2015)。

1.去中心化的应用。DAO可以改变传统组织结构和组织管理模式,增强组织功能。传统科层制组织是一种遵循自上而下原则、权力集中的等级结构。DAO依托PoW算力投票、PoS权益投票等机制,所有参与者具有相同决策权,节点之间的关系遵循平等互惠的原则,是一种去管理中心的自治组织(Mclean,2017;Diallo et al,2018)。Kaal(2018)认为,在智能合约基础上,DAO运作规则、参与者责权以及奖惩条款透明,能够有效衡量成员贡献并相应分配报酬,促进组织整体运作。同时DAO还会对传统公司理论提出挑战,依托共识机制最小化信任成本和沟通成本,使市场交易变得更加有效。但有学者也认为,随着时间推移DAO仍然存在中心化趋势(Cong et al,2021b)。如PoW中的矿工组织,直接冲击了DAO去中心化的基础。

2.去中心化的风险。加密经济学去中心化也存在一些风险。(1)安全性问题,对PoW机制的攻击同样可适用于对DAO的攻击,DAO应用还涉及服务器、通信网络、程序编写等软硬件设施,这些都有可能成为被攻击的对象。最著名的案件就是2016年6月对以太币组织DAO的攻击,攻击者利用了智能合约中的程序漏洞,导致接近六千万美元被窃取。(2)法律问题。虽然DAO在功能上可以部分替代公司职能,但仍需通过法律形式确立有限责任等权利义务边界。分散性组织如何有效控制主体行为,也对所谓"加密法"(lex cryptographica)设计提出了新的挑战(Wright & Filippi,2015)。(3)竞争性影响问题。去中心化还可能影响市场竞争过程,对竞争绩效是否有影响仍未有定论。Ferreira et al(2023)建立产业生态模型,通过PoW实现交易验证,研究发现,由于存在同质商品和沉没成本,所以大企业仍占据了核心治理地位。Cong & He(2019)认为,去中心化共识机制能够改善信息不对称的问题,通过增强竞争性改善消费者福利,但去中心化共识形成过程容易引起合谋。Huberman et al(2021)研究发现,去中心化机制有助于解决潜在垄断定价问题。

3.去中心化的治理。Allen et al(2020)结合公共选择理论研究如何优化DAO治理,在此基础上提出了"加密民主制度"(cryptodemocracy)概念。这里的"民主制度",并不完全等同于政治学中的民主,而是公共选择理论所关注的在交易成本约束下的公共选择问题。DAO影响了信息协调,在参与者偏好影响下扩展了制度可能性边界。此时DAO中心化需要权衡"失序"和"集中"带来的社会损失,进而实现制度优化演进(Berg et al,2017;Allen et al,2023)。

(二)赋能安全性

加密经济是更加安全、高效、自由的数字经济。Hastig & Sodhi(2020)识别了重要因素,成功地进行了区块链部署。事实上,区块链的应用经历过不同发展阶段,依托于共识机制,企业资产、交易成为区块中的状态信息,链可以为所有类型的交易提供完整的、不可篡改的审计跟踪(Jain & Sedamkar,2020)。共识机制的强制自动清算降低了结算和支付中的欺诈风险,供应链上的任何一个需要融资的供应商都可以利用核心企业的优质信用提升银行对其的信任,降低整个供应链的融资成本

(Wang et al,2021)。区块链 1.0 指的是加密货币的扩大应用阶段(Choi,2021),主要是对首次代币发行(initial coin offers,简称 ICO)(Iris,2019;Lin & Nestarcova,2019)、点对点支付(Guo & Liang,2016)等问题的研究。此外,也有学者结合货币政策理论、资产定价理论等,对加密货币供应、发行、币值波动和加密金融等问题进行研究(Kaal,2018;Shorish,2019;Biais et al,2023;Fosso Wamba et al,2020)。在区块链 2.0 中,智能合约通过计算机程序自动执行许多协议条款(Saberi et al,2019)。区块链 3.0 通过区块链的去中心化特性实现了透明化功能。Chang et al(2020)通过建立与区块链 3.0 相关的"协作模式",研究区块链的全球供应链部署。区块链 4.0 主要是包含不同行业对区块链的应用和影响。如首次代币发行(Choi,2020a)、产品出处披露等。Dutta et al(2020)考察了区块链 4.0 的应用和社会影响。区块链 5.0 使用机器智能和数据分析自动化智能应用程序的流程。Choi et al(2020b)验证了区块链 5.0 在相关社交媒体中的使用。

智能合约的优势之一在于其可追踪性与可审计性。由于共识机制不可篡改,智能合约一旦发布就不能任意更改,因此,所有交易都是可追踪和可审计的,减少了金融欺诈、医疗欺诈等恶意行为(Gatteschi et al,2018;Yong et al,2019)。优势之二与去中心化特征有关,有助于降低管理成本,提升运行效率。由于共识机制可以确保对整个系统的信任,无须依赖可信任的第三方,因此,智能合约可以以去中心化的方式自动触发、执行预先设置的操作,提高流程效率(Kosba et al,2016;Hewa et al,2021)。优势之三在于其缔约时间可以更为灵活,能够潜在地解决由于缔约时序引起的不完全合约问题,这使得智能合约有望实现更为广泛的应用(Goorha,2019)。对于物联网行业,针对数据收集易侵犯隐私这一问题,智能合约可以设置访问规则、条件和时间,允许某些个人或用户组拥有、控制或访问数据(Khan & Salah,2018)。对于医疗保健行业,智能合约可增强临床试验的透明度(Nugent et al,2016;Benchoufi et al,2017);或是记录疫苗接种和流通情况,保证疫苗记录不被篡改,增强疫苗信息安全性(Yong et al,2019)。对于能源行业,发电机组通过自主交易代理直接与消费者或能源零售供应商进行交易,省去了交易所和交易机构等中介机构(Mengelkamp et al,2017;Andoni et al,2019;Al Sadawi et al,2021)。对于电子政务行业,智能合约则可作为一种新的信息存储、通信方式,保障信息安全,这在中国、美国、瑞典、英国等国家得到了初步应用(Li et al,2019;Jacobovitz,2016;Einaste,2018;Fridgen et al,2019)。对于贸易行业,应用在链上的智能合约集成到贸易流程中可以增强支付及融资的透明度和自动化(Chang et al,2019;Belu,2019),此外大量研究还讨论了链和智能合约在提升贸易物流可追溯性和降本增效中的作用(Koh et al,2020;Belu,2019;Gesmann-Nuissl,2019)。

(三)应用场景的拓展

尽管可拓展性是共识机制优化的核心内容之一,但目前关于加密经济学中可拓展性特征的应用和影响的研究较少。部分研究将共识机制的可拓展性对应于经济学中的"自由进入"(free entry),研究可拓展性对其他特征产生影响的边界条件。Prat & Walter(2021)通过建立 PoW 算力竞争模型发现,可拓展性为工作量证明的回报确定了上界,回报会随着竞争者数量的增加而迅速减少。Cong et al(2021b)研究发现,可拓展性带来的竞争增加是去中心化能带来收益的重要影响因素。

从 PoW、PoS 的发展过程来看,这种可拓展性与进入含义并不完全等同,还涉及共识形成的收敛速度、数据读取的速度和数据存储量等一系列问题。Croman et al(2016)指出,比特币的可拓展性可以用最大吞吐量、交易确认所需的时间、达成共识的成本和引导时间衡量,其中最大吞吐量和交易确认所需的时间是对用户体验感有重大影响的指标。优化共识机制的可拓展性是区块链在不同领域的广泛应用中面临的挑战之一。部分研究者根据不同行业的特性研发设计相适应的高拓展性共识机制,在保证安全性和去中心化的前提下,尽可能地提高可拓展性。Dorri et al(2019)针对物联网需求,集成了轻量级共识机制、分布式信任算法和吞吐量管理算法等多种优化方式设计用于物联网的轻量级可拓展区块链,为物联网提供安全性和隐私性的同时,减少了所需带宽数量、延迟和数据包开

销。Sarfaraz et al(2022)指出基于基础区块链的供应链系统随着节点的增加,费用可能会大幅增加,采用分片的可拓展的共识机制可以提高吞吐量和存储效率,从而减少通信、计算和数据存储的费用。

五、加密经济学研究未来展望

加密经济学作为新的交叉学科,由于研究者学术背景差异,许多问题的研究还处于起步探索阶段。计算机科学和密码学的研究者对经济学理论并不十分精通,而经济学研究者也较少接受过系统的密码学或计算机科学的研究训练。对于一门新兴学科,试图总结任何确定性的研究方向是十分困难的,甚至在一定程度上违背了学科自身发展规律。尽管如此,作为一篇加密经济学的综述性文章,本文仍希望基于现有研究归纳若干重要尚待解决的研究主题。

(一)借助更多的经济分析工具或经济学理论优化共识机制

CAP 理论提出了分布式系统的基本权衡:一致性、可用性、分区容错性不能同时成立(Gilbert & Lynch,2002),这为加密经济学中共识机制的设计目标制定了边界范围。加密经济学还面临着"安全性、可拓展性、去中心化"的三元悖论,不同机制在解决拜占庭将军问题取得共识的同时,总是进行多目标的权衡取舍。因此,如何通过技术改进尽可能优化乃至逼近理论上的边界是共识机制发展优化的方向。从 PoW 到 PoS,前文已展示了"经济意义上的最终确定性"这一共识机制的取得思路,经济学者亦建立了正式的博弈模型分析 PoW 和 PoS 机制。后续研究可进一步从这些成果出发探索更多经济理论在共识机制优化中的作用。

研究还可以将去中心化系统以外更为复杂的环境和行为因素纳入共识机制中,以评价共识机制在现实中的一致性与稳定性。将代币与外部稳定资产挂钩以保持币值稳定就是其中的尝试,但仍存在受市场情绪影响大和挤兑等问题,这表明与外部稳定资产挂钩的机制设计仍然存在很大优化空间。特别地,在缺乏可受信任的第三方进行调节缓冲的情况下,如何保持代币价值稳定也是加密经济学发展的重要方向之一。

(二)深入分析数字货币、区块链等应用的影响

尽管目前研究中并不乏以数字货币、区块链为对象的分析讨论,但大多将其视作一个新的经济现象,对根本特征的揭示不足,也忽略了这些分布式系统在不同共识机制下的异质性特征。现有的高水平研究已经开始尝试将分布式系统的特征乃至共识机制本身纳入分析框架,但对于不同共识机制的比较研究仍然较少,对于去中心化、安全性、可拓展性多目标权衡的探索仍然有限。后续研究也可借鉴这些分析框架,更为深入地探讨加密经济学具体应用的影响。具体问题包括:在不同共识机制的支撑下智能合约具有怎样的表现?在不同场景下,如何对三元悖论进行权衡,以构建更为适当的分布式系统?

(三)在主流经济学研究中吸收加密经济学的最新研究成果

加密经济学的基础理论催生了许多新的经济活动现象,其中一些经济现象已对主流经济学理论形成了一定冲击。例如,去中心化自治组织是加密经济学应用的重要形式,有些学者认为这已冲击了科斯、德姆塞茨、阿尔钦等人提出的公司与产权理论。未来需探讨如何将这一新形式引入主流经济学研究范式,如何在主流经济学框架特别是产权理论、公司理论的框架中归纳共识机制作用,从而在理论上揭示去中心化对组织和分工变革影响的一般规律,延伸对加密经济学和现代公司理论的研究。

参考文献:

Abadi, J. & M. Brunnermeier(2018), "Blockchain economics", NBER Working Paper, No. 25407.

Allen, D. W. E. et al(2020), "Cryptodemocracy and its institutional possibilities", *Review of Austrian Economics* 33(3):363－374.

Allen, D. W. E. et al(2023), "The exchange theory of web3 governance", Social Science Research Network Working Paper, No. 4209827.

Alrowaily, M. A. et al(2023), "Modeling and analysis of proof-based strategies for distributed consensus in blockchain-based peer-to-peer networks", *Sustainability* 15(2), 1478.

Al Sadawi, A. et al(2021), "A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract", *Technological Forecasting and Social Change* 173, 121124.

Andoni, M. et al(2019), "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", *Renewable and Sustainable Energy Reviews* 100(2):143-174.

Baird, L. (2016), "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance", Swirlds Tech Reports, No. TR201601.

Ballandies, M. C. et al(2021), "Finance 4.0: Design principles for a value-sensitive cryptoecnomic system to address sustainability", Twenty-Ninth European Conference on Information Systems, June 12, 2021, Marrakech, Morocco.

Belu, M. G. (2019), "Application of blockchain in international trade: An overview", *Romanian Economic Journal* (71):2-16.

Benchoufi, M. et al(2017), "Blockchain protocols in clinical trials: Transparency and traceability of consent", *F1000Research* 6, 66.

Bentov, I. et al(2016), "Cryptocurrencies without proof of work", International Workshop on Financial Cryptography and Data Security (FC).

Berg, A. et al(2018), "Crypto public choice", Social Science Research Network Working Paper, No. 3236025.

Berg, A. et al(2020), "Blockchains and constitutional catallaxy", *Constitutional Political Economy* 31(2):188-204.

Berg, C. (2017), "Populism and democracy: A transaction cost diagnosis and a cryptodemocracy treatment", Social Science Research Network Working Paper, No. 3071930.

Berg, C. et al(2019), *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*, Edward Elgar.

Biais, B. et al(2019), "The blockchain folk theorem", *Review of Financial Studies* 32(5):1662-1715.

Biais, B. et al(2023), "Equilibrium bitcoin pricing", *Journal of Finance* 78(2):967-1014.

Bondy, J. A. & U. S. R. Murty(2008), *Graph Theory*, Springer Publishing.

Braddick, K. et al(2018), "Cryptoassets taskforce: Final report", available at https://www.gov.uk/government/publications/cryptoassets-taskforce.

Brekke, J. K. (2020), "Hacker-engineers and their economies: The political economy of decentralised networks and 'cryptoeconomics'", *New Political Economy* 26(4):646-659.

Buterin, V. (2014), "DAOs, DACs, DAs and more: An incomplete terminology guide", available at https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

Buterin, V. (2019), "Introduction to cryptoeconomics", available at https://.ca/files/introcryptoeconomics.pdf.

Buterin, V. & V. Griffith(2017), "Casper the friendly finality gadget", arXiv Preprint Paper, No. 1710.09437.

Castro, M. & B. Liskov(1999), "Practical byzantine fault tolerance", OSDI '99: Proceedings of the Third Symposium on Operating Systems Design and Implementation, Feb. 22-25, New Orleans, USA.

Chaim, H. et al(2019), "Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles", *IEEE Access* 7:175744-175757.

Chang, S. E. et al(2019), "Exploring blockchain technology in international trade: Business process re-engineering for letter of credit", *Industrial Management & Data Systems* 119(8):1712-1733.

Chang, Y. et al(2020), "Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities", *International Journal of Production Research* 58(7):2082-2099.

Chiu, J. & T. V. Koeppl(2017), "The economics of cryptocurrencies-Bitcoin and beyond", Queen's Economics Department Working Paper, No. 1389.

Chiu, J. & T. V. Koeppl(2019), "Blockchain-based settlement for asset trading", *Review of Financial Studies* 32(5):1716-1753.

Chiu, J. et al(2023), "Bank market power and central bank digital currency: Theory and quantitative assessment", *Journal of Political Economy* 131(5):1213-1248.

Choi, T. M. (2020a), "Financing product development projects in the blockchain era: Initial coin offerings versus traditional bank loans", *IEEE Transactions on Engineering Management* 69(6): 3184－3196.

Choi, T. M. et al(2020b), "When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management?", *Transportation Research Part E: Logistics and Transportation Review* 135, 101860.

Choi, T. M. (2021), "Creating all-win by blockchain technology in supply chains: Impacts of agents' risk attitudes towards cryptocurrency", *Journal of the Operational Research Society* 72(11):2580－2595.

Churyumov, A. (2016), "Byteball: A decentralized system for storage and transfer of value", available at https://obyte.org/Byteball.pdf.

Clayton, J. (2017), "Statement on cryptocurrencies and initial coin offerings", available at https://www.sec.gov/news/public－statement/statement－clayton－2017－12－11.

Cong, L. W. & Z. He(2019), "Blockchain disruption and smart contracts", *Review of Financial Studies* 32(5):1754－1797.

Cong, L. W. et al(2021a), "Tokenomics: Dynamic adoption and valuation", *Review of Financial Studies* 34(3): 1105－1155.

Cong, L. W. et al(2021b), "Decentralized mining in centralized pools", *Review of Financial Studies* 34(3):1191－1235.

Croman, K. et al(2016), "On scaling decentralized blockchains", *Proceedings of the 20th International Conference on Financial Cryptography and Data Security*.

Cunningham, S. (2021), *Causal Inference: The Mixtape*, Yale University Press.

Daian, P. et al(2019),"Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake", International Conference on Financial Cryptography and Data Security, FEB 18－22, St Kitts & Nevi, pp. 23－41.

Dannen, C. (2017), *Introducing Ethereum and Solidity*, Apress.

Dell'Erba, M. (2019), "Stablecoins in cryptoeconomics from initial coin offerings to central bank digital currencies", *Journal of Legislation and Public Policy* 22(1):1－47.

Diallo, N. et al(2018), "eGov-DAO: A better government using blockchain based decentralized autonomous organization", 2018 International Conference on eDemocracy & eGovernment, April 4－6, Quito, Ecuador, pp. 166－171.

Dimitri, N. (2022), "Quadratic voting in blockchain governance", *Information* 13(6), 305.

Dorri, A. et al(2019), "LSB: A lightweight scalable blockchain for IoT security and anonymity", *Journal of Parallel and Distributed Computing* 134:180－197.

Dutta, P. et al(2020), "Blockchain technology in supply chain operations: Applications, challenges and research opportunities", *Transportation Research Part E: Logistics and Transportation Review* 142, 102067.

Einaste, T. (2018), "Blockchain and healthcare: The Estonian experience", available athttps://nortal.com/blog/blockchain－healthcare－estonia.

Fan, X. & Q. Chai (2018), "Roll-DPoS: A randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems", 15th EAI International Conference on Mobile and Ubiquitous Systems-Computing, Networking and Services, Nov. 5－7, 2018, New York City, USA, pp. 482－484.

Ferreira, D. et al(2023), "Corporate capture of blockchain governance", *Review of Financial Studies* 36(4):1364－1407.

Fischer, M. J. et al(1985), "Impossibility of distributed consensus with one faulty process", *Journal of the Association for Computing Machinery* 32(2):374－382.

Fosso Wamba, S. et al(2020), "Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain", *Production Planning & Control* 31(2－3):115－142.

Frey, S. & R. W. Sumner(2019), "Emergence of integrated institutions in a large population of self-governing communities", *PLoS One* 14(7), e0216335.

Fridgen, G. et al(2019), "Supporting communication and cooperation in the asylum procedure with blockchain technology: A proof of concept by the Federal Office for Migration and Refugees", available at https://www.researchgate.net/publication/331534023_Supporting_communication_and_cooperation_in_the_asylum_procedure_with_Blockchain_technology_－_A_proof_of_concept_by_the_Federal_Office_for_Migration_and_Refugees.

Gai, F. et al(2018), "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network", Database Systems for Advanced Applications: 23rd International Conference, May 21—24, 2018, Gold Coast, Australia, pp. 666—681.

Gatteschi, V. et al(2018), "Blockchain and smart contracts for insurance: Is the technology mature enough?", *Future Internet* 10(2), 20.

Gesmann-Nuissl, D. (2019), *In Responsible, Sustainable, and Globally Aware Management in the Fourth Industrial Revolution*, IGI Global Press.

Gilbert, S. & N. Lynch(2002), "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services", *ACM Sigact News* 33(2):51—59.

Goorha, P. (2019), "The contractual cryptoeconomy: An arrow of time for economics", *Journal of the British Blockchain Association* 2(2):1—9.

Guo, Y. & C. Liang(2016), "Blockchain application and outlook in the banking industry", *Financial Innovation* 2(1):1—12.

Hastig, G. M. & M. S. Sodhi(2020), "Blockchain for supply chain traceability: Business requirements and critical success factors", *Production and Operations Management* 29(4):935—954.

Hern, A. (2018), "Bitcoin's energy usage is huge—We can't afford to ignore it", available at https://www.theguardian.com/technology/2018/jan/17/bitcoin—electricity—usage—huge—climate—cryptocurrency.

Hewa, T. M. et al(2021), "Survey on blockchain-based smart contracts: Technical aspects and future research", *IEEE Access* 9:87643—87662.

Howell, S. T. et al(2020), "Initial coin offerings: Financing growth with cryptocurrency token sales", *Review of Financial Studies* 33(9):3925—3974.

Huberman, G. et al(2021), "Monopoly without a monopolist: An economic analysis of the bitcoin payment system", *Review of Economic Studies* 88(6):3011—3040.

Iris, H. Y. (2019), "Pathways to European policy and regulation in the crypto-economy", *European Journal of Risk Regulation* 10(4):738—765.

Jacobovitz, O. (2016), "Blockchain for identity management", Ben-Gurion University Technical Report, No. 16—02.

Jain, N. & R. R. Sedamkar(2020), "A blockchain technology approach for the security and trust in trade finance", 14th International Conference on Innovations in Information Technology (IIT).

Kaal, W. A. (2018), "Crypto economics—The top 100 token models compared", Social Science Research Network Working Paper, No. 3249860.

Keister, T. & D. Sanches(2023), "Should central banks issue digital currency?", *Review of Economic Studies* 90(1):404—431.

Khan, M. A. & K. Salah(2018), "IoT security: Review, blockchain solution, and open challenges", *Future Generation Computer Systems* 82:395—411.

Kiayias, A. et al(2017), "Ouroboros: A provably secure proof-of-stake blockchain protocol", 37th Annual International Cryptology Conference (Crypto).

King, S. & S. Nadal(2012), "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", available at http://inplus-lab.sysu.edu.cn/files/blockchain/proof_of_stake.pdf.

Koh, L. et al(2020), "Blockchain in transport and logistics-paradigms and transitions", *International Journal of Production Research* 58(7):2054—2062.

Kondru, K. K. & R. Saranya(2020), "Directed acyclic graph-based distributed ledgers—An evolutionary perspective", *International Journal of Engineering and Advanced Technology* 9(1): 6096—6103.

Kosba, A. et al(2016), "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", 2016 IEEE Symposium on Security and Privacy (SP), May 23—25, 2016, San Jose, USA, pp. 839—858.

Lamport, L. et al(1982), "The byzantine generals problem", *ACM Transactions on Programming Languages and Systems* 4(3):382—401.

LeMahieu, C. (2018), "Nano: A feeless distributed cryptocurrency network", available at https://nano.org/en/whitepaper.

Leonardos, S. et al(2020), "Weighted voting on the blockchain: Improving consensus in proof of stake protocols", *International Journal of Network Management* 30(5), e2093.

Lepore, C. et al(2020), "A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS", *Mathematics* 8(10), 1782.

Li, J. et al(2019), "Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases", *Automation in Construction* 102:288－307.

Li, W. et al(2017), "Securing proof-of-stake blockchain protocols", 12th International Workshop on Data Privacy Management (DPM), Sept. 14－15, 2017, Oslo, Norway, pp. 297－315.

Li, W. et al(2023), "Delegated proof of stake consensus mechanism based on community discovery and credit incentive", *Entropy* 25(9), 1320.

Lin, L. & D. Nestarcova(2019), "Venture capital in the rise of crypto economy: Problems and prospects", *Berkeley Business Law Journal* 16(2):533－571.

Lux, T. & V. Mathys(2018), "Guidelines for enquiries regarding the regulatory framework for initial coin offerings", Acts of Swiss Financial Market Supervisory Authority.

Maurer, B. et al(2013), "When perhaps the real problem is money itself! －The practical materiality of bitcoin", *Social Semiotics* 23(2):261－277.

Mclean, H. (2017), "A democratic social media and cryptoeconomic network", available at https://www.pdf－archive.com/2017/02/09/ezira－whitepaper－v1－0/ezira－whitepaper－v1－0.pdf.

Mengelkamp, E. et al(2017), "Designing microgrid energy markets", *Applied Energy* 210:870－880.

Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system", available at https://nakamotoinstitute.org/bitcoin/.

Nugent, T. et al(2016), "Improving data transparency in clinical trials using blockchain smart contracts", *F1000Research* 5, 2541.

Pass, R. & E. Shi(2017), "The sleepy model of consensus", International Conference on the Theory and Application of Cryptology and Information Security, Dec. 3－7, 2017, Hong Kong, China, pp. 380－409.

Prat, J. & B. Walter(2021), "An equilibrium model of the market for bitcoin mining", *Journal of Political Economy* 129(8):2415－2452.

Rohde, P. P. et al(2021), "Quantum crypto-economics: Blockchain prediction markets for the evolution of quantum technology", arXiv Preprint Paper, No. 2102.00659.

Saberi, S. et al(2019), "Blockchain technology and its relationships to sustainable supply chain management", *International Journal of Production Research* 57(7):2117－2135.

Saleh, F. (2021), "Blockchain without waste: Proof-of-stake", *Review of Financial Studies* 34(3): 1156－1190.

Sarfaraz, A. et al(2022), "Towards a scalable permissioned blockchain framework for supply chain management", 2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Dec. 7－10, 2022, Kuala Lumpur Convention Centre, Malaysia, pp. 960－964.

Shorish, J. (2019), "Hedonic pricing of cryptocurrency tokens", *Digital Finance* 1(4):163－189.

Sompolinsky, Y. et al(2016), "Spectre: A fast and scalable cryptocurrency protocol", IACR Cryptology Preprint Paper, No. 1159.

Szabo, N. (1996), "Smart contracts: Building blocks for digital markets", *EXTROPY: Journal of Transhumanist Thought* 16(2):28－40.

Vandersypen, L. M. et al(2001), "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", *Nature* 414(6866):883－887.

Vasin, P. (2014), "Blackcoin's proof-of-stake protocol v2", available at http://blackcoin.co/blackcoin－pos－protocol－v2－whitepaper.pdf.

Voshmgir, S. & M. Zargham(2020), "Foundations of cryptoeconomic systems", Vienna University of Economics and Business Working Paper Series, No. 1/2020.

Wang, E. K. et al(2020), "PoRX: A reputation incentive scheme for blockchain consensus of IIoT", *Future Generation Computer Systems* 102:140－151.

Wang, L. et al(2021), "Value creation in blockchain-driven supply chain finance", *Information & Management* 59(7), 103510.

Wang, S. et al(2019), "Blockchain-enabled smart contracts: Architecture, applications, and future trends", *IEEE Transactions on Systems Man and Cybernetics Systems* 49(11):2266－227.

Wright, A. & P. De Filippi(2015), "Decentralized blockchain technology and the rise of lex cryptographia", Social Science Research Network Working Paper, No. 2580664.

Wright, D. J. (2019), "Quadratic voting and blockchain governance symposium issue: Blockchain technology and the law", *University of Missouri-Kansas City School Law Review* 88(2):475－496.

Xu, G. et al(2019), "Improvement of the DPoS consensus mechanism in blockchain based on vague sets", *IEEE Transactions on Industrial Informatics* 16(6):4252－4259.

Yong, B. et al(2019), "An intelligent blockchain-based system for safe vaccine supply and supervision", *International Journal of Information Management* 52, 102024.

Yu, J. et al(2019), "Repucoin: Your reputation is your power", *IEEE Transactions on Computers* 68(8):1225－1237.

Research Progress on Cryptoeconomics

FENG Bimei　WANG Shixun　ZHANG Jiqin
(Fuzhou University, Fuzhou, Fujian)

Abstract: Cryptoeconomics, as an emerging interdisciplinary research field, comprehensively applying interdisciplinary theories such as economics, cryptography, and computer science, mainly studies how to form consensus in distributed systems. On the basis of summarizing and sorting out the disciplinary attributes and theoretical origins of cryptoeconomics, this article summarizes the research objects, development evolution, and application scenarios of cryptoeconomics. Firstly, this article introduces the origin of cryptoeconomics by reviewing the Byzantine Generals Problem, and elaborates on the research object, theoretical foundation, and disciplinary attributes of cryptoeconomics. Secondly, this article reviews the development and evolution of cryptoeconomics in areas such as consensus algorithms, incentive mechanisms, and smart contract. Finally, this article summarizes the applications of cryptoeconomics in the decentralization, security, and scalability characteristics of distributed systems, and provides prospects for future research in cryptoeconomics.

Keywords: Cryptoeconomics; Consensus Mechanism; Proof of Work; Proof of Stake

(责任编辑:刘洪愧)
(校对:李仁贵)