激励机制和区块链如何互利互惠?一项调查

韓容,西安电子科技大学网络空间安全工程学院ISN国家重点实验室,中国郑艳,中国西安电子科技大学网络空间安全工程学院ISN国家重点实验室和芬兰阿尔托大学通信与网络系梁雪琴,中国西安电子科技大学网络空间安全工程学院ISN国家重点实验室LAURENCE T. YANG,海南大学计算机科学与技术学院

基于区块链的系统缺乏中心化控制,需要系统实体的积极参与和合作行为来确保系统的安全性和可持续性。然而,动态环境和不可预测的实体行为在实践中对此类系统的性能提出了挑战。因此,设计一个可行的激励机制来规范实体行为对于提高区块链系统的性能至关重要。区块链的繁荣特性也可以促进有效的激励机制。不幸的是,目前的文献仍然缺乏对区块链相关激励机制的深入调查,以了解激励机制和区块链如何相互促进。为此,我们从激励机制的性质和成本方面提出了评估要求。一方面,我们根据区块链版本、激励形式和激励目标对区块链系统的激励机制进行了分类。另一方面,我们根据应用场景和激励目标对基于区块链的激励机制进行了分类。在回顾过程中,我们根据提出的评估要求讨论了最先进的激励机制的优缺点。通过仔细的审查,我们展示了激励机制和区块链如何互相受益,发现了许多尚未解决的问题,并指出了未来研究的相应潜在方向。

CCS 概念:·一般和参考→调查和概述; ·计算理论→算法博弈论和机制设计; ·安全和隐私→分布式系统安全;

其他关键词和短语:区块链、激励机制、货币激励、非货币激励

ACM 参考格式:

Rong Han、Zheng Yan、Xueqin Liang 和 Laurence T. Yang。2022 年。激励机制和区块链如何互利?一项调查。ACM Comput. Surv. 55,7,文章 136(2022 年 12 月),38 页。https: //doi.org/10.1145/3539604

本工作部分由国家自然科学基金(资助编号 62072351)资助;部分由芬兰科学院(资助编号 308087、资助编号 335262、资助编号 345072 和资助编号 350464)资助;部分由浙江省实验室开放项目(资助编号 2021PD0AB01)资助;部分由 111 项目(资助编号 B16037)资助。

作者地址:R. Han 和 X. Liang(通讯作者),西安电子科技大学网络空间安全工程学院 ISN 国家重点实验室,中国西安;电子邮件:ronghan@stu.xidian.edu.cn,dearliangxq@126.com;Z. Yan,西安电子科技大学网络空间安全工程学院 ISN 国家重点实验室,中国西安及芬兰阿尔托大学通信与网络系,电子邮件:zyan@xidian.edu.cn;LT Yang,海南大学计算机科学与技术学院,中国海口;电子邮件:ltyang@hainanu.edu.cn。

0360-0300/2022/12-ART136 15.00 美元
https://doi.org/10.1145/3539604

1 引言

区块链是比特币的核心技术[65],本质上是一个按时间顺序以区块形式记录数据的去中心化数据库。先进的密码技术使区块链具有去中心化、不可篡改、可追溯、透明、匿名等特点,无需依赖可信第三方。这些特性使得区块链技术在克服中心化系统存在的单点故障问题方面具有优势。区块链的发展经历了三个阶段:区块链 1.0、2.0 和 3.0 版本。近年来,区块链技术在加密货币以外的更广泛场景中蓬勃发展,包括云计算、物联网 (IoT)、车联网 (IoV)、医疗保健等。

一方面,区块链的安全性高度依赖于大量系统实体的参与[77],这增加了单个实体主宰系统并执行恶意行为(例如篡改区块)的难度。不幸的是,系统实体在实践中是理性的,它们会根据哪些行为可以为自己带来利润来制定策略。比特币系统在 2008 年设计时就已经嵌入了激励机制[65]。共识节点(称为矿工)通过工作量证明(PoW)共识成功挖掘出一个区块时,将获得由固定的 Coinbase 奖励(或挖矿奖励)和交易费组成的财务奖励[65]。同样,在以太坊中,生成已确认区块的矿工的奖励包括固定的 Coinbase 奖励、已确认区块中所有程序消耗的总执行费以及涉及叔块(即从最长/主链中排除的孤立块)的奖励[10]。尽管区块链技术中的底层激励机制为矿工提供了必要的激励,但它们忽略了其他类型系统节点的动机。例如,保存并维护区块链完整、最新副本的完整节点应该有动力将历史区块数据发送给新加入的节点,以防止攻击者篡改历史数据和控制系统。

传播节点在广播交易记录和区块中起着至关重要的作用。激励他们积极合作至关重要。一些研究人员已经认识到了这个问题,并提出了许多激励机制来激励所有利益相关者参与和合作区块链系统。

另一方面,激励系统实体参与并合作行为是一种经济有效的抑制自私行为影响的方法。这种经济方法已经被研究作为一种激励机制,它应用各种内部或外部激励来规范和相对固定系统实体的预期行为[20]。如何应用激励机制来激励系统实体积极参与已经在参考文献[68, 85, 100, 102]中得到充分研究。研究人员还在参考文献[86, 91, 92]中研究了如何设计鼓励合作行为的激励机制。

许多论文研究了移动群智感知[43, 75, 98]、异构网络[37]和延迟容忍网络[45]领域的激励机制应用技术。

这些激励机制一般由中心化的第三方执行,而中心化第三方在实践中并不完全可靠,而且大部分中心化的激励机制都是人工执行,耗时耗力,不可避免地使激励分配过程复杂化。将区块链引入激励机制,支持去中心化的激励执行,消除了中心化第三方带来的安全和隐私风险。同时,智能合约技术可以自动发放激励,防止激励分配过程中出现纠纷。我们关注到这方面的研究,发现将区块链技术引入激励机制设计的有效性和可行性。

现有关于区块链的研究主要集中在共识机制[71,84,90]、安全和隐私问题的解决方案[5,42,60,69]和应用[19,31,67]。

此外,与激励机制相关的调查大多调查以中心化方式应用的技术[43,48]。只有少数调查回顾了激励机制

近年来,区块链技术的发展也取得了显著进展。黄等人[41]讨论了区块链通证在数字经济中的发行机制和分配机制。通证是一种数字权益凭证
在区块链中流通的货币,例如比特币和以太币等加密货币。Yu 等人[97]
重点研究了区块链网络中的激励层和代币模型。王等人[84]回顾了比特币 PoW 共识协议的激励兼容性研究。刘等人[85]

[60]回顾了基于博弈论的激励机制,以防止矿工发起攻击
区块链系统上的激励机制研究尚缺乏对区块链系统中激励机制和基于区块链的激励机制的全面研究。随着区块链的普及,回顾与区块链相关的激励机制变得至关重要。

了解激励机制和区块链如何互利互惠。

在本文中,我们回顾了2010年至今不同版本的区块链技术的激励机制以及基于区块链的激励机制,

尤其是自 2010 年代中期以来。我们从五个主流数据库中收集了以下关键词的论文:区块链、激励机制和智能合约:IEEE Explorer、ACM Digital
Library、Elsevier、ScienceDirect 和 Springer。为了准确评估这些激励机制的有效性,我们提出了一套关于激励属性的评估要求
(即个体理性、激励相容性、激励真实性、激励公平性、社会福利最大化、激励自动化、激励隐私性和激励可持续性)

和成本(即计算复杂性和向后兼容性)。我们彻底审查了
根据激励形式对区块链 1.0、2.0 和 3.0 中的激励机制进行分类
和目标,以及基于区块链的激励机制,根据激励场景和目标对其进行分类。我们的审查是通过评估每篇论文提出的要求来进行的。
最后,我们详细说明了从调查中发现的一些未解决的问题,并相应地

指出了未来的几个研究方向。表1明显地比较了我们的文章与现有的
具体来说,我们文章的主要贡献可以概括如下:

- 我们率先提出了一系列关于激励属性和成本的要求
  用于评估现有区块链相关激励机制的有效性,
  包含一些可以用于评估所有激励机制的通用要求和一些针对不同场景个性化的特定要求。这些

  要求为制定切实有效的激励措施提供了指导方针
  机制。
- 我们彻底审查了有关区块链激励机制的当前文献
  1.0、2.0、3.0 以及基于区块链的激励机制,并讨论其优势
  并结合所提出的要求详细说明了其优缺点。此外,我们总结了区块链系统中哪种激励形式适合哪种激励目标,以及

  不同应用场景下的激励表现以及应用和
  不同形式的基于区块链的激励机制的局限性。具体来说,我们
  发现(1)货币激励适合鼓励节点参与意愿,(2)基于声誉的激励适合节点需要

  (3)游戏化激励机制可以用于简单的游戏场景,或作为
  (4)混合激励以高昂的成本提供理想的绩效。
- 我们找出了一些未解决的问题,并提出了研究方向,以推动对区块链相关激励机制的进一步研究。具体来说,(1)我们确定

  交易费和矿池的设计,以及广播激励措施
  节点和全节点的激励机制尚待进一步研究;(2)现有的激励机制很少

表 1. 我们的调查与其他现有调查的比较

涵盖主题	[41] [97] [84] [60]	我们的调查
提出激励机制要求 NNNN		和
回顾区块链中的激励机制	伊恩尼	和
回顾基于区块链的激励机制 NNNN		和
提出激励机制的分类	NNNN	和

Y:满意;N:不满意。

抑制各种攻击；(3)公平性和自动化是重要的激励属性
设计区块链系统激励机制时应满足的；
(4)隐私和向后兼容性是应该满足的两个重要属性
基于区块链的激励机制；(5)基于区块链的激励机制
还应该认真考虑对矿工的激励。

本文的其余部分组织如下。第2部分提供了介绍性概述
区块链。第3节给出了激励机制的分类，并提出了一套评估激励机制绩效的要求。因此，第4节和第 5节

回顾区块链 1.0、2.0、3.0 中的激励机制，以及基于区块链的激励
机制，并讨论每种激励机制的有效性
提议的要求。第6节讨论了激励机制和区块链如何相互受益。此外，我们发现了未解决的问题并提出了未来的研究方向

在第 7 节中。最后，我们在最后一节中总结本文。

2 背景

本节简单介绍区块链相关基本概念、主流共识
机制以及区块链的类型。我们还介绍了一些臭名昭著的攻击
本节末尾将介绍区块链网络。

2.1 区块链

区块链是一种分布式基础设施，采用块链数据结构来验证和
维护以区块形式记录的信息，采用共识机制进行信息的生成和更新，并使用密码技术保障数据和信息的安全。

以比特币区块链为例，它由按时间顺序链接的区块组成。图1(a) 说明了每个区块的结构和组件，每个区块由一个区块组成

区块头和区块主体。区块头存储了控制信息，包括本区块的版本号、前一个区块的哈希值、时间戳、nonce、Merkle哈希值

根节点和难度目标。区块主体存储经过验证的交易记录。
新币也被视为一笔交易，称为 Coinbase 交易。所有比特币
比特币系统内流通的货币，来源于系统发行。

区块链网络中的节点是运行区块链系统并参与对等网络的计算机。这些节点可以根据其

系统中的功能。

- 广播节点。它们执行区块链操作协议并参与
  交易记录和区块信息的验证与传播。
- 挖矿节点。他们参与共识机制并创建新区块。他们
  也被称为矿工。

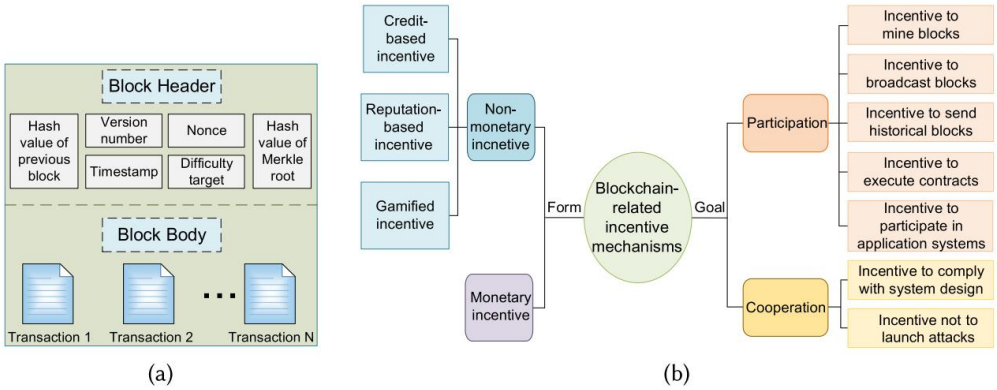

图 1. (a) 比特币的区块结构和组成部分;(b) 区块链相关激励机制的分类。

·完整节点（比特币核心）。这些节点保存并维护区块链的完整和最新副本,并具有广播节点和挖掘节点的所有功能。

下文中,我们根据表达上下文交替使用“系统节点”和“系统实体”。一般来说,它们代表的含义是相同的,即系统中具有某些功能的对象。“系统节点”通常用于表示区块链网络系统,而“系统实体”则经常用于说明激励机制。

区块链的一般工作流程如下:首先,双方发生一笔新的交易,并将该交易广播到区块链网络。收到此交易的节点验证其是否合法。验证通过后,该交易将被矿工纳入区块。全网所有矿工执行相同的共识机制,以创建有效的区块。最后,将区块广播给其他节点以验证其合法性。成功通过验证后,此区块将被追加到区块链中。

可能同时有数名矿工成功挖出区块,导致同一区块高度出现多个有效区块,这种情况称为分叉。不同的区块链系统对分叉的处理方式不同,例如,为了保证比特币区块链系统中只保留一条唯一的主链,会根据最长链规则选择一条唯一的主链。

在比特币区块链中,由于比特币挖矿竞争异常激烈,随着越来越多的矿工涌入网络,单个矿工挖出一个区块变得越来越困难。矿池将单个矿工的算力聚集起来共同挖出一个区块,并根据预定义的策略将奖励分配给矿池成员（即矿工） [70],这成功地降低了矿工收入的差异。然而,算力的集中化违背了区块链设计的去中心化目标,这可能导致中心化问题。此外,矿池之间的竞争会引发新的攻击,例如区块扣留攻击、一次又一次的分叉扣留攻击。

2.2 共识机制

在分布式系统中,节点通过共识机制达成信任关系,以保证系统的一致性和连续性。这里我们简单介绍几种流行的共识机制。

2.2.1 工作量证明。PoW 证明做了多少工作,通常需要证明者进行耗时的计算,但其计算结果很容易验证[33]。在比特币中,矿工依靠机器计算能力进行数学运算

通过获取下一个满足难度要求（即具有预期的零个数)的区块的哈希码,最先解决 PoW 难题的矿工获得记账权。

PoW具有安全、公平、容易验证的特点,但同时也浪费了算力,而且由于算力的中心化,独立矿工越来越难以完成挖矿任务。

2.2.2 权益证明。与 PoW 相比,权益证明（PoS)不需要矿工不断挖矿来生成新区块,而是通过随机选择、财富或年龄（即所谓的权益)的各种组合来确认区块,因此 PoS 比 PoW 更节能。PoS 定义了一个币值的概念,币值是代币数量乘以代币持有天数得出的数字。系统根据代币持有者的币值分配相应的权益[57]。代币持有者的权益越多,其挖矿难度就越小。一旦权益持有者成功挖出一个区块并获得挖矿奖励,其持有的代币数量将被重置为零,并重新开始计算其币值。节点获取新权益的能力取决于其已经持有的权益,因此存在不公平性。PoS 能耗低,共识时间短,但容易导致中心化。

2.2.3 委托权益证明。委托权益证明（DPoS)的出现,解决了 PoS 中少数拥有大量货币的账户可以控制区块生成的问题。DPoS 将共识机制分为两个阶段,首先由所有节点投票决定哪些节点可以信任,然后由这些被投票的节点进行交易验证和记账[57]。DPoS减少了验证节点的数量,降低了能耗,实现了较高的效率。但是,固定数量的验证节点可能会影响去中心化。

2.2.4 实用拜占庭容错。实用拜占庭容错（PBFT)解决了原有拜占庭容错算法效率低下的问题。PBFT 是一种状态机复制算法。PBFT 中存在两种节点,即主节点和备份节点。主节点一旦收到客户端的请求,就会执行三阶段程序:预准备、准备和提交,之后将回复发送回客户端[62]。PBFT的效率取决于参与节点的数量。当网络中节点较少且分叉概率较低时,PBFT 表现良好。基于 PBFT 的区块链系统的可扩展性较差。

2.3 区块链的分类

根据区块链对公众开放的范围,现有的区块链可以分为三类:公有链,即任何人都可以自由加入或离开的区块链,不需要特定的授权,任何人都可以读取和发送公有链上的交易。

私有区块链仅限于机构内部使用,联盟区块链则仅对内部成员或外部机构授权成员开放。

许可型区块链需要系统节点获得批准后才能参与,因此私有链和联盟链都属于许可型区块链。以上三种区块链,无论是公链、私有链还是联盟链,都有各自的优缺点,选择哪种区块链取决于应用场景和应用需求。

2.4 区块链中的攻击

攻击者利用区块链网络的漏洞发起攻击,以获取不正当收益。下面我们列举一些针对区块链算法和协议的攻击。

2.4.1 51%攻击。持有至少 51% 的总网络计算能力的攻击者可以
发起此攻击以任意修改区块[73]。这种攻击也称为多数攻击。通过
控制 51% 的网络计算能力,矿工可以将目标区块变成孤块
通过禁用该区块中的交易。51% 攻击是一种提高双重支付的方法,它
指在两笔交易中花费相同的未花费交易输出。双重支付通常
利用区块共识导致的交易确认的时间延迟。

2.4.2 自私挖矿攻击。自私挖矿是指矿工或矿池不发布和分发自己新挖出的区块,而继续挖下一个区块,并维持

它在挖矿领域的领先地位[27]。自私挖矿押注的是挖矿成功的概率
哈希算力,损害区块链网络的公平性。

2.4.3 区块扣留攻击 区块扣留攻击是针对挖矿
矿池[72]。矿工成功挖出一个区块后,会保留该区块而不进行广播,因此矿池无法获得该区块的奖励。但是,发起该区块的矿工
区块扣留攻击 (BWA)可以按照矿池的分配规则,分享他人挖出的区块所获得的奖励,因此BWA造成的财务损失较小。
矿工的损失和矿工的攻击成本非常低。BWA 也发生在挖矿之间
[25]。

2.4.4 Sybil 攻击 Sybil 攻击是指恶意节点非法冒充多个身份
对外界来说。这些节点的身份通常被称为 Sybil 节点。在区块链中
网络中,节点创建新身份无需任何成本。攻击者可以利用此漏洞
通过伪造身份加入网络来发起 Sybil 攻击。在掌握了大量
身份后,攻击者可以自由地进行恶意活动[78]。

2.4.5 拒绝服务攻击拒绝服务攻击 (DoS)是指故意攻击系统协议的缺陷或直接耗尽被攻击对象的资源

通过残酷的手段[11]。在区块链相关系统中,生成一个区块时消耗很少
资源,恶意矿工可以不断生成无效区块,对
系统。攻击者还可以采用恶意行为,使诚实的矿工无法
通过挖矿获利,从而阻止矿工挖矿,使区块链停止运行。

3 激励机制的分类及评价要求

本节首先介绍激励机制的分类,如图1(b) 所示,并
然后提出了一套评估现有激励机制有效性的要求。

3.1 激励机制的分类

3.1.1 激励形式。区块链中现有的激励机制可以分为两种
按激励形式分类:金钱激励和非金钱激励。
货币激励是从经济角度规范系统实体行为的,通过对实体进行金钱奖励,提高实体参与系统的效用,从而激励实体加入系统。

激励机制采用经济平衡来增加攻击或自私行为的成本,以防止攻击并鼓励实体合作。

现有的非货币激励机制又可以分为信用激励、声誉激励和游戏化激励。信用激励和声誉激励都属于非货币激励。

激励管理系统实体之间的关系,并建立信任。然而,声誉
信任是群体对个体的综合信任,而信用则强调信任者对受托人的主观依赖。大量研究将这两种激励机制运用于

防止不信任个体之间勾结的机制。游戏化激励利用实体玩游戏的心理倾向,为实体提供愉快的

完成系统任务过程中的情感体验,积极引导实体行为
作为系统设计。常见的游戏化激励机制使用积分和徽章作为激励。

3.1.2 激励目标。激励机制可根据激励目标进行分类。
激励机制可以鼓励节点参与维护区块链系统的安全性和可持续性。它们还可以防止各种攻击并缓解区块链的弱点,使系统以正常和预期的方式运行。因此,激励机制

在区块链系统中发挥着至关重要的作用[8]。一般来说,激励机制主要有两种类型
目标:激励系统参与和激励与其他节点的合作。

参与。区块链需要大量节点的参与,以确保安全性和
去中心化。现有的系统设计天真地假设节点将主动
参与度符合预期,但节点在实践中是理性的、利益驱动的,因此,
他们需要激励才能参与。我们进一步将区块链中的参与激励分为
根据系统节点的功能,我们分为 1.0 和 2.0。具体来说,我们考虑
挖矿、广播区块、发送历史区块、执行合约。在讨论区块链3.0中的激励机制以及基于区块链的激励机制时,

我们将参与激励具体到具体应用场景的参与。

合作。现有区块链系统的另一个不成熟的假设是,所有系统
节点将严格按照系统设计执行。在实践中,利润驱动的节点将最大化
通过各种自私或恶意的行为来获取利润,比如违反系统设计
以及利用漏洞攻击系统。这些行为可能会导致短期
或对系统造成长期威胁,并损害其他系统节点的利润。为了克服这一
问题,我们可以在系统中引入激励机制来鼓励节点合作。具体来说,本文讨论的合作包括两种类型的行为:严格

执行系统协议并阻止发起攻击。

3.2 要求

为了判断激励机制的有效性和实用性,我们对激励机制的性质和成本提出了如下要求。我们对现有激励机制的评估
第 4节和第 5节中的作品即基于这些要求。

3.2.1 属性。

个体理性(IR)。制度主体在实践中是理性的利益相关者,受个体利润或利益驱动。具有个体理性的激励机制可以保证制度主体获得非负收益,从而激发参与意愿。货币政策的激励机制可以提高制度主体的参与意愿,提高制度主体的参与积极性。
激励机制可以通过手动调整效用来轻松满足个人理性
参数。

激励相容性(IC)。当所有系统主体都采取自私行为以最大化其个体利益时,它们很少关心其自私行为对系统绩效的影响。关于这种情况的悲剧例子有很多,例如

公共资源[35]。系统实体都采取自私行为,试图最大化自己的
利益,而不对系统做出贡献。这将导致系统性能受损甚至崩溃,各个实体不再能从系统中获利,悲剧发生。如果

能够保证系统各主体个体利益相兼容的激励机制
群体利益[74],那么系统就能实现可持续健康发展。我们

将这样的属性称为激励兼容性,这是需要考虑的一个基本属性
在设计激励机制时。

激励诚实（IT）。自私可能导致系统实体的不诚实行为,如果
不诚实可以带来好处。一个有效的激励机制应该能够鼓励系统主体诚实行事、说真话。这种诚实的激励机制

使系统能够长期运行。当 IC 的自私行为是不诚实的行为时,
激励相容性和真实性没有区分。

激励公平（IF）。公平涉及两个含义。首先,
系统实体获得的奖励与其贡献成正比。其次,系统实体必须按预期成功向有贡献的实体支付所需的奖励金额。公平性
另外支持系统实体的诚实行为,并鼓励这些系统实体
做出尽可能多的贡献。

社会福利最大化（SW）。社会福利代表净收益的总和
所有系统实体。激励机制的设计者在决定
系统参数。设计者合理地决定参数以最大化其自身
福利。然而,社会福利更高的系统可能对大规模系统更有吸引力
实体。增加社会福利的潜在成本将在以后得到回报,因为更多的系统
涉及实体。因此,采用具有社会福利的激励机制的系统
与其他没有这种要求的系统相比,最大化更容易被接受。

激励自动化 (IA)。区块链是一个分布式系统,没有一个中心化的节点来管理整个系统。因此,激励机制应该尽量减少中心化管理,以兼容区块链的去中心化。激励触发、任务分配和奖励分配应该自动进行。此外,自动激励机制应该能够自动执行,以保证区块链系统能够自动执行任务。

消除了中心化激励管理的弱点,例如拒绝支付和修改
支付信息。实现自动化的一种广泛应用的方法是编制激励
机制融入智能合约。因此,自动化的实现在
区块链2.0和3.0中的激励机制以及基于区块链的激励机制。

激励隐私（IP）。在基于区块链的实际应用系统中,大部分隐私
威胁是交易信息和链下信息（如用户身份)的泄露。因此,我们考虑交易信息和用户信息的隐私保护。通常,区块链 1.0 中的激励机制是
针对区块链工作节点的

2.0 中,激励信息需要公开,以达到激励的目的。因此,
在讨论
区块链 1.0 和 2.0 中的激励机制。然而,在设计区块链 3.0 和基于区块链的激励机制时,不可避免地要考虑特定的隐私要求。
激励机制与具体的应用场景相关。当这些应用程序的用户向开放区块链提交或上传信息时,好奇的人可以很容易地获得
隐私信息。隐私泄露的风险降低了区块链的积极性。
用户参与这些应用,因此保护用户隐私可以使区块链3.0中的激励机制和基于区块链的激励机制更加可行。

激励可持续性（IS）。可行的激励机制需要刺激长期
各类节点的参与。可持续性可以避免系统参与者的流失和失衡,从而对系统造成资源垄断等负面影响,从而确保

长期系统运行。

激励可扩展性（SC）。可扩展性是指激励机制在参与实体数量增加的情况下仍能保持高效和有效的能力。区块链系统通常需要大量参与节点来确保系统的安全性和可靠性。因此，激励机制应具有可扩展性以确保其适用性。具体而言，区块链系统激励机制的可扩展性通常取决于系统的可扩展性，而系统的可扩展性受系统架构或吞吐量的限制。考虑到本文的重点是激励机制，我们仅在第5 节中评估了对这一要求的满足情况，其中对基于区块链的激励机制进行了概述。

3.2.2 成本。

时间成本：计算复杂度（CC）。可行的激励机制应该具有可接受的计算复杂度，尤其是在没有强大的中心化实体来维持执行的情况下。具体来说，公共区块链网络由于其开放性而具有动态性，所有系统实体都可以随时进入和离开。因此，其计算开销相当大，因此非常需要轻量级的激励机制。值得注意的是，在将算法引入激励机制时通常会考虑 CC。

实施成本：向后兼容性 (BC)。向后兼容性意味着激励机制可以与区块链的先前版本很好地配合使用。这一要求相当必要，因为并非所有区块链实体都是最新的，而所有实体都有资格获得激励。由于基于区块链的激励机制需要取代其原有机制，因此我们在第5 节的审查中忽略了这一要求。

4 区块链中的激励机制

本节回顾了区块链 1.0、2.0 和 3.0 中现有的激励机制。我们根据激励形式和激励目标对文献进行分类。对于每一项工作，我们首先指定激励机制设计，然后根据第3 节中提出的要求评论其优缺点。表2总结了我们所有的发现。

4.1 货币激励货币激励是一种以有形的

回报对系统主体进行直接激励的常用方式，用于鼓励挖矿、广播区块、发送历史区块、执行智能合约、参与应用系统、配合遵守系统设计、防止攻击等。

4.1.1 参与激励。区块链系统需要多个节点的参与才能保证其安全性和去中心化。具体来说，在区块链 1.0 和 2.0 中，需要矿工进行挖矿，广播节点应主动广播区块和交易，全节点则需要将历史区块记录发送给新节点。此外，区块链 2.0 中还需要节点执行智能合约。在区块链 3.0 中，节点的参与对于维持系统运行也是必要的。然而，考虑到资源消耗成本和隐私泄露风险，理性且利益驱动的节点可能会犹豫是否加入。

挖矿激励。比特币区块链采用的共识机制基于 PoW，这消耗了矿工大量的计算资源。因此，需要激励矿工挖矿。比特币区块链系统中矿工的货币激励是区块奖励，包括交易费和 Coinbase 奖励。

然而，比特币的发行总量是有限的，Coinbase 每四年对每个区块的奖励就会减少。因此，交易费在比特币市场中扮演着越来越重要的角色。

手续费在激励矿工参与方面发挥着重要作用。研究人员发现,如果没有 Coinbase 的挖矿奖励,比特币系统将不稳定[12,49,64]。Tsabary 和 Eyal [80]发现仅发放交易费不足以激励矿工,从而形成挖矿缺口。蒋和吴[44]认为,当交易费变得相当可观时,理性的矿工会倾向于将交易费高的交易纳入自己的区块,并生成包含尽可能多交易的大区块。然而,大区块需要很长时间才能被验证并达成共识。此外,交易费低的交易可能会被忽略。因此,单纯采用基于交易费的激励机制将对比特币区块链系统的效率和公平性产生不利影响。

Lewenberg 等人[54]提出了一种激励机制,以激励计算能力低、连接性差的矿工积极参与挖矿。该论文采用了有向无环图结构和包容性协议,其中不在主链上的区块中包含的交易费用也会奖励给该区块的矿工。但是,如果交易已经出现在主链上的区块中,那么链下区块矿工就无法获得该费用。

当出块速度过慢时,交易费奖励会降低。该协议适用于区块大小较大或出块间隔较短的情况,通过激励节点收录不同的交易,而不是只选择费用高的交易,提高系统吞吐量。网络连接较差的矿工有较高的概率生成链下区块,包容性协议用交易费来补偿生成链下区块的矿工,使得弱势矿工损失较小,因此边缘化矿工愿意持续参与挖矿,避免算力强、网络连接速度快的矿工垄断挖矿,所以该机制满足IS。虽然弱势矿工生成的区块不在主链上,但这些矿工仍然可以获得相应的奖励,因此该机制满足IF和IR。包容性协议用链下区块来奖励矿工,降低了自私挖矿攻击的成本,因此激励机制无法满足IC和IT,矿工仍然有动机发起自私挖矿攻击。本文没有讨论SW和BC,由于没有采用智能合约,没有涉及具体算法,所以该机制不支持IA和CC。

广播区块的激励。区块链网络需要广播节点自发地将收到的交易和区块信息转发给其邻居节点,以提高网络的性能和安全性。然而,在传统的区块链设计中,没有交易传播的激励。此外,接收最新区块的广播节点可以私下挖掘下一个区块,而无需广播该区块,以提高其竞争力。

研究人员研究了如何实施激励机制,以鼓励广播节点在区块链网络中传播交易和区块。

Babaioff 等人[6]将区块链网络定义为一个高度为 H 的 d 元有向树的森林,并提出了一种混合奖励方案来激励节点广播交易。当广播节点在有向树中的高度小于预定阈值时,交易传播路径上的每个中间节点与根节点共享相同的奖励 β。授权交易的矿工(位于传播路径上的第 l 个节点)获得 1 + (H − l + 1) × β 奖励。当广播节点没有将交易广播给邻近节点时,它将失去作为中间节点的奖励,这是无利可图的。

因此,该激励机制满足IT和IC,但是没有考虑网络的其他结构和不同节点的不同处理能力,因此激励机制中的IF、SW、BC、IS成为未知数,IA和CC没有被触及。

Abraham 等人[1]提出了一种激励机制,鼓励广播节点在对等网络中传播交易和区块。在这种激励机制中,当矿工

成功挖出一个区块后,交易传播路径上的每个广播节点都会获得一笔交易传播费,作为矿工设定的奖励。该机制可以防止女巫攻击,缓解自私挖矿,鼓励节点传播交易,诚实行事。

因此,该激励机制满足IC和IT的要求。但本文仅提供理论分析,并未评估其计算复杂度,也没有考虑隐私和自动化。

本文没有提及 IF、SW、BC 和 IS,也没有触及 IA 和 CC。

Ersoy 等人[24]提出了一种激励公有区块链网络节点传播交易的机制,将交易费用按照不同的份额分配给传播路径上的广播节点,该路径是从交易发起者到区块生成者的交易传播路径之一。作者规定,广播节点距离区块生成者越近,贡献越大,获得的奖励也越多,因此该机制满足 IF。根据数学分析,当一个广播节点将交易传播给所有邻居节点时,它会最大化自己的收益;对于一个以盈利为目的的广播节点来说,它会尽最大努力广播交易,因此该机制满足 IC 和 IT。这里没有提到 SW、BC 和 IS,该机制不涉及 IA 和 CC。

发送历史区块的激励。当新节点加入区块链网络时,需要向全节点发起请求以获取历史区块记录。然而,自私的全节点可能会因为带宽消耗等自私原因而拒绝向该节点发送记录。

因此研究人员提出了一些基于奖励的激励机制,以激励全节点积极性发送历史区块数据。

王和吴[88]提出新节点应该奖励传递历史区块记录的全节点。在该机制中,双方需要锁定一些币,若新节点同意支付p个币给全节点,则需要锁定2p个币,全节点锁定p个币,只有双方签名才能取回锁定的币。将新节点和全节点的互动建模为双方都想最大化自身利益的非合作博弈后,根据均衡分析,全节点的最佳策略是发送完整真实的历史区块记录,新节点的最佳策略是索取历史区块记录并支付相应奖励,因此该机制满足IT和IC,锁币策略满足IF。但是,激励机制中加入了小额支付通道,使得该机制不满足BC,没有证据评价激励机制是否满足SW和IS,不需要考虑IA和CC。

合约执行激励。以太坊区块链作为区块链2.0的发起者,由于智能合约的支持,目前非常盛行。然而,Aldweesh等人[2]发现,在以太坊区块链中,矿工执行合约的激励与矿工的成本不成比例,这可能导致激励不平衡,并对以太坊区块链的可靠运行产生不利影响。

PoW 和 PoS 都奖励拥有大部分资源(如计算能力和权益)的矿工。戴等人[22]提出了一种新的共识机制,称为价值证明(PoV)。PoV奖励产生价值的智能合约。PoV 将智能合约中的代币交易量视为该智能合约的价值。一旦智能合约被成功调用,系统将向其所有者发放奖励。智能合约的交易量越高,其所有者获得的代币奖励就越多。此外,PoV 还引入了激励参数来调整代币的生产速度。由于没有关于代币奖励分配的具体描述,因此无法评论该激励机制的效率。

激励参与应用系统。区块链技术已应用于交通运输、电网、数据传输[28]和收集[58]、信任评估[59, 93]和可信认证[30]等各种场景,开启了区块链 3.0 时代。

这些基于区块链的体系的主体都是利益驱动、理性的,因此激励机制对于激发他们的参与意愿至关重要。

胡等[39]设计了一种激励机制,以鼓励多微电网系统中的参与意愿。他们提出了一种基于区块链的协作入侵检测方法,以提高检测结果的准确性。每个微电网节点通过周期性触发模式生成检测目标。所有节点通过DPoS共识机制就检测结果达成共识。检测结果存储在区块中。在该机制中,节点的检测系数被视为权益。当一个节点生成一个区块时,它不仅会获得经济激励,而且其检测系数也会增加,从而提高其挖掘下一个区块的概率。但如果节点行为不诚实,则其检测系数会降低。激励机制鼓励单个微电网参与共识,并提高该系统的检测精度。该机制满足IR、IT和IC。作者没有考虑IP。该机制不是自动的,也不满足IA。本文未提及IF、SW、BC和IS。我们不需要考虑

抄送。

Lei 等人[53]提出了一种双链结构的可扩展公共区块链,称为 Groupchain,用于物联网中的雾计算。Groupchain 包含两种类型的区块:组区块和副区块。
矿工通过 PoW 生成群块,成为群主群的成员。群主群成员可以提交包含交易的副块,其中成员提交的副块需要得到群主群其他成员的集体签名,才被视为有效区块并被链上区块链。为了鼓励更多矿工加入 Groupchain 网络,作者提出了基于 Coinbase 奖励和交易费的奖励机制,此外,在竞争成为群主群成员中失败的矿工还会得到额外补偿,因此该机制满足 IF。论文中没有对奖励机制做详细介绍,但它保证了矿工的收益为非负数,从而让理性的矿工加入 Groupchain 网络。遗憾的是,作者没有考虑 IA 和 IP,这种激励机制是否满足其他要求很难判断。

4.1.2 合作激励。

激励机制促使用户遵守系统设计。随着区块链技术的广泛应用和激励机制的实施,越来越多的用户愿意加入区块链网络。然而,由于缺乏对用户行为的中心化监管,以及海量用户的自私和逐利特性,给区块链系统带来了非合作问题。研究人员提出了一些有效的激励机制来激励自私节点遵守系统设计。

比特币协议规定矿工应根据主链上最新的已知区块进行挖矿(也称边界策略)。然而,自私的矿工可能会偏离这一规则,故意产生分叉并获得比正常行为更多的区块奖励。Kout-soupias 等人[50]提出了一种激励机制来鼓励矿工遵循边界策略。具体来说,发现区块的矿工应该向第一个根据其区块成功挖矿的矿工支付一定的奖励。这种新机制激励其他矿工继续在特定的分支上挖矿。这种支付方式增加了不诚实挖矿的成本,并激励矿工遵循边界策略,从而提高了系统稳定性。

同时,激励机制鼓励矿工根据最新收到的区块进行挖矿,从而增加主链延伸的概率,因此该机制满足 IC 和

IT。但是,矿工获得的收益与支付并不成正比,预付激励机制针对的是计算能力强的矿工,因此该机制不满足 IF。

由于修改了区块链原有的协议,所以不支持BC,SW和IS也没有提及,IA和CC也没有考虑。

Szalachowski 等人[79]修改了比特币的共识机制,并提出了 Strongchain,使挖矿过程透明化。Strongchain 采用弱解,找到该解的难度低于挖出一个区块所需的难度。当一个矿工找到并发布一个弱解时,其余矿工会继续在该弱解的基础上解决 PoW 难题。

这种方式利用了所有资源联合出块,避免了比特币系统带来的计算资源浪费。Strongchain不仅奖励出块的矿工,也奖励找到弱解的矿工。这种基于奖励的激励机制,激励出弱解的矿工广播自己的解,其他矿工会主动将这些弱解附加到自己的解中。矿工无法通过违反共识协议而获益,因此该奖励机制满足IC和IT。出弱解的矿工的奖励和贡献相关,保证了奖励机制满足IF。奖励机制没有引入明显的开销和计算,满足BC。根据实验,不同算力的矿工的奖励差距并不大,避免了小矿工的损失和大矿工的垄断,因此该机制满足IS。

本文没有提及 SW,也没有考虑 IA 和 CC。

不发起攻击的激励。如前所述,自私矿工可能会拒绝向网络的其余部分发布和分发有效区块,然后继续挖掘下一个区块并保持其领先地位。当网络的其余部分即将赶上自私矿工时,矿工就会将一部分发现的区块释放到网络中。这种自私攻击损害了区块链网络的公平性。一些研究专注于防止矿工的自私攻击,如下所示。

Eyal 等人[26]提出了一种新的协议 Bitcoin-NG,在一定程度上改善了比特币协议的吞吐量和延迟。在 Bitcoin-NG 中,时间被划分为 epoch,区块被划分为微块和关键块,交易都放在微块中。Bitcoin-NG 的共识过程分为两个部分,首先通过 PoW 选举出领导者,然后领导者产生微块。Bitcoin-NG 中修改共识机制的目的是扩展与链长和权重区分开来的最长最重的链,链的权重是指链上关键区块的数量。在 Bitcoin-NG 中,对矿工的激励仍然来源于 Coinbase 奖励和交易费,为了获得微块的所有交易费,领导者矿工会扣留微块并在微块上挖矿,成为下一个 epoch 的领导者。因此,为了激励矿工遵循扩展的最长最重链协议,避免自私挖矿攻击,作者通过数学计算得出,当前纪元矿工通过打包交易获得的交易费的60%应该分配给下一个纪元的领导者,剩下的40%可以作为其最终奖励。这种分配机制使得矿工对区块链系统发起自私挖矿攻击所获得的收益小于遵循协议所获得的收益,使激励机制满足IC和IT。与当前纪元的领导者矿工相比,遵循协议的下一个纪元的领导者矿工对系统的稳定性做出了更多的贡献,从而获得更多的交易费奖励,因此该机制满足IF。本文未提及SW、BC和IS,也未考虑IA和CC。

然而,Yin 等人[96]发现了 Bitcoin-NG 激励机制分析中的一些缺陷。在分析数学不等式以避免自私挖矿攻击时,Eyal 等人[26]

没有考虑当前诚实挖矿的领导者成为下一个 epoch 的领导者的情况。即,在参考文献[26] 中,最长链扩展过于简单。尹等人对激励机制进行了彻底的重新分析,并提出了交易费分配的最优比例。最终的结果是,交易费分配的最优比例为

$\frac{}{3\,11}$ 和 $\frac{}{8\,11}$。

当一个矿工掌握了51%的算力,就可以发起双花攻击,获取额外收益。这个矿工可以任意更改主链上的信息,这极大地破坏了区块链网络的安全性、公平性和去中心化性。因此,非常需要能够抵御双花攻击的激励机制。

Chen 和 Wang [16]提出了一种采用两层架构的无数据开销的分片协议。一层是根链,通过占用整个系统的大部分计算能力来确保系统安全;另一层基于分片来提高系统吞吐量。为了抵御矿工发起的双花攻击,必须确保整个系统的大部分计算能力都贡献给根链。此外,分片的计算能力均匀分布在每个分片中,以保证其能够正常工作。分片和根链对矿工的奖励满足以下公式:

$$\frac{\text{区块奖励(root)}}{\text{区块奖励(区块)}} = \frac{\text{HashPower(根)} \times \text{BlockIntervalBlockInterval(根)}}{\text{HashPower(分片)} \times \text{BlockIntervalBlockInterval(分片)}}。 \quad (1)$$

这种奖励分配机制满足IR和IT,可以激励矿工合理分配自己的哈希算力,满足IC。但是激励机制中没有考虑IF、SW、BC、IS,也没有考虑IA和CC。

矿工除了对区块链网络进行攻击外,还可以对矿池进行BWA。
矿工成功挖出一个区块后,会将该区块保留不广播,这样矿池就无法获得该区块的奖励。这种攻击给矿池造成了很大的损失。以下工作旨在抵抗BWA。

Bag 和 Sakurai [7]分析了 BWA 攻击者的效用函数,并提出了一种特殊的基于奖励的激励机制来降低攻击者的激励。解决 PoW 难题并将完整 PoW 解决方案提交给其矿池的矿工将获得特殊奖励。

寻找新区块的剩余收益将按照矿工提交的份额分配给所有矿工。向矿池发起BWA的矿工无法获得特殊奖励。奖励分配方案使激励机制满足IF。激励机制阻止攻击者发起BWA,因此该机制满足IC和IT。

从理论分析来看,该机制长期来看不会减少诚实矿工的收益,反而会减少攻击者的收益,因此该激励机制满足IS。

激励机制中SW和BC没有讨论,IA和CC没有考虑。

Alzahrani 和 Bulusu [4]提出了一种基于 Tendermint [9] 的新共识机制。每个创建新区块的提议者都会随机映射到领导者,然后领导者会随机选择一些节点(称为验证者)来验证新提出的区块。该机制通过在挖掘新区块时随机选择一组验证者来提高安全性。该协议涉及基于奖励和惩罚的激励机制来规范验证者的行为。这种基于贝叶斯博弈的机制通过奖励诚实行为和惩罚不诚实行为来调整不同行为的效用。因此,该协议满足 IC 和 IT。作者还断言了所提出的机制在捍卫 BWA 方面的有效性。但是,激励机制需要更新原始协议并且不符合 BC。没有讨论激励机制的 IF、SW 和 IS。没有考虑 IA 和 CC。

DoS 攻击破坏目标系统的可用性,利用目标系统的缺陷攻击其网络服务功能或直接消耗系统资源,使目标系统无法提供正常服务。对于区块链相关系统,攻击者利用 DoS 攻击来拖慢系统速度或迫使系统停止运行。

Lei 等人[53]提出的 Groupchain 网络由于领导小组规模较小,容易受到恶意矿工的攻击。例如,恶意矿工可以通过不断生成不消耗资源的无效副块,轻松通过 DoS 攻击攻击区块链系统。因此,作者提出了一种基于押金的激励机制来防止 DoS 攻击。加入领导小组的新成员需要向历史成员支付押金。如果成员在特定时间内表现诚实,则押金将被退还。

否则,押金将分配给历史成员。综上所述,押金机制可以防止新加入的领导小组成员(矿工)发起DoS攻击。新成员的收益为非负,因此该机制满足IR。作者没有考虑IA和IP。论文中没有对押金机制做详细介绍,因此我们无法判断该机制是否能满足其他要求。

4.2 基于声誉的激励与金钱激励相比,基于声誉

的激励更注重鼓励节点进行协作。基于声誉的激励通常使用声誉值来规范节点行为。例如,设置声誉阈值可以激励节点采取合作行为以保持其声誉值处于较高水平。

为了规范矿池挖矿流程,Nojoumian 等人[66]提出了一种基于信誉的挖矿机制,激励矿工遵守矿池规定的挖矿协议,诚实挖矿。矿池由多个联盟组成,联盟由多个相互信任的矿工组成,每个联盟成员共享相同的信誉值。信誉值反映了矿工在系统中的表现,根据矿工的挖矿表现、诚实和不诚实行为计算得出。矿池管理者根据矿工的信誉值向矿工发出邀请,以组成新的联盟,增加矿池挖矿成功的机会。信誉值高的矿工被邀请加入矿池以获得更多收益的概率大。因此,这种信誉机制可以激励矿工诚实挖矿。该机制满足IR、IC 和 IT。矿工的收益与其信誉值成正比,因此该机制满足 IF。没有讨论 SW、BC 和 IS。没有考虑 IA 和 CC。

4.3 游戏化激励

不同于金钱激励、声誉激励,游戏化激励利用节点的心理因素来引导节点行为,游戏化激励给予节点成就感,而非金钱、声誉等现实利益。

Kano 和 Nakajima [47]为矿工提供基于心理因素的游戏化激励,以运营服务并参与挖矿工作,以解决挖矿的中心化问题。

游戏元素是与 5×5 棋盘上的谜题形状相对应的区块中的随机数值。挖矿工作由矿工通过可视化的随机数值操作进行,这使得挖矿工作变得有趣。本文没有提供激励方法的技术细节,因此我们无法评估它是否能满足我们提出的要求。

4.4 混合激励货币激励从经济角

度激励系统实体参与协作,但无法避免偶然的不诚实行为。

非货币激励通常给予企业无形的回报和精神上的满足,无法满足企业的经济需求,因此有学者提出混合激励来弥补货币激励和非货币激励的不足。

4.4.1 合作激励。为了激励矿工遵守协议设计并诚实行事,Han 等人[34]提出了一种新的共识机制,称为信用证明（PoC）,这是一种将信用视为权益的特殊 PoS 机制。共识过程分为两个阶段:候选人选举和领导者选举。第一步是验证节点是否有资格成为候选人。节点成为候选人后,需要一定数量的押金。当候选人背离这样的协议时,押金将被没收。

第二步是从候选者中选举出领导者,生成区块。作者提出了一种混合激励机制,由交易费激励和信用激励组成。信用高意味着成为领导者并获得收益的概率大。所有诚实执行协议并广播有效候选区块的候选人将平等分享交易费,因此该机制满足IF。该机制可以抵御自私挖矿攻击和双花攻击。如果攻击者想要进行自私挖矿攻击,那么就会冒着失去承诺的押金和信用的风险。而信用差的攻击者不会被选为候选人,从而无法提前为分叉做准备并进行双花攻击。因此,该机制满足IC和IT。激励机制需要更新原始协议,因此不满足BC。本文未提及SW和IS,未考虑IA和CC

纸。

将区块链应用到工业物联网中,共识的安全性和效率成为主要关注点。王等[81]提出了一种基于声誉的激励机制,以鼓励矿工诚实行事。每个矿工都被赋予一个声誉值。根据该机制,具有高声誉值的矿工可以以较低的难度生成新块。当矿工成功挖出一个区块并最终确认时,矿工可以获得声誉奖励和代币奖励。当矿工长期不生成区块或未生成预期数量的区块时,将受到惩罚。该声誉机制要求用户使用真实身份进行注册,因此除非攻击者可以使用他人的信息进行注册,否则该机制可以抵御 Sybil 攻击。从长远来看,如果矿工的行为对区块链系统不利,则其声誉值会下降,其挖矿难度会增加,从而损害其收益。因此,该机制满足 IC、IT 和 IS。其 IF 和 SW 无法判断。该机制不考虑 IP。作者没有在智能合约上部署激励机制,因此该机制不满足IA,其CC为o(1)。

激励机制可以建立在任何Proof-of-X（X代表任意内容,例如工作和权益)协议上,满足BC。王等[82]在文献[81]的基础上,考虑了区块链应用于物联网的情况,提出了一个分布式声誉层,应用了与文献[81]相同的激励机制。

在车载能源网络中,可再生能源可以通过电动汽车和能源节点（无线充电/放电设施)进行传输。当电动汽车充当能源卖家时,能源节点充当能源买家,反之亦然。能源节点是自私的,它们可能会采取不诚实的行为来最大化自己的利益。王等人[87]提出了一种基于联盟区块链的安全能源交付框架来防止能源节点的恶意行为,该框架采用声誉共识协议。能源节点的声誉越高,成功挖矿并获得奖励的概率就越大。货币激励来自于能源交易中收取的交易费。同时,成功挖矿的能源节点也会获得声誉的提升。当能源节点做出拒绝支付、交易伪造等恶意行为时,其声誉值会降低。当

节点的信誉值低于阈值,将被放入黑名单。因此,每个
鼓励网络中的能源节点改进电动汽车的充电/放电服务
并阻止恶意行为以提高其声誉值。激励机制
满足 IR、IC、IT 和 IF。该机制不是自动的,并且不符合 IA。该机制
不考虑IP。没有讨论SW、BC、IS,也不需要考虑CC。

4.4.2 参与和合作的激励机制。可靠、有效的车辆公告
车联网需要网络。Li 等人[55]提出了一种基于区块链的新型
隐私保护激励公告网络 CreditCoin 鼓励用户参与并诚实转发信息。在 CreditCoin 中,流量任务由云端管理

应用服务器与用户之间的交易通过区块链网络进行转发,用户构建交易后,将交易转发给附近的路边单元

(RSU),然后 RSU 对交易的有效性进行投票。随后,共识服务器确认有效交易并将其添加到链上的区块中。为了鼓励用户诚实可靠地参与网络并转发流量信息,基于声誉的

提出了激励机制。声誉点数称为硬币。用户通过以下方式获得硬币
转发或接收数据包,鼓励他们保持在线并保持网络
活跃。在一定时期内,未使用的硬币将减半,以防止硬币的积累
可用于攻击。该机制满足IR,IC和IT。这种激励机制实现了
当意外事件发生时,通过追踪恶意节点来实现有条件的隐私,因此
满足IP。此激励机制需要更新系统,因此不能满足BC。
机制不是自动的,因此无法支持 IA。IF、SW 和 IS 不在讨论范围内
并且不需要考虑CC。

5 基于区块链的激励机制

到目前为止,我们已经审查了采用激励机制来激励
第四部分,我们探讨了区块链中参与意愿和抑制不合作行为的方法。
将进一步探讨区块链技术如何促进激励机制设计
本节将介绍基于区块链的激励机制。具体来说,我们通过分层的方式回顾基于区块链的激励机制
按照激励形式、应用场景对现有作品进行分类,然后激励
目标。我们总结了每一项工作的主要贡献,并评论了它们的优点和缺点
表3根据提出的要求。我们研究区块链如何通过消除集中式参与方来使激励机制受益。由于以前的集中式激励机制的结构

机制转变为分布式机制后,BC 无法在所有激励机制中实现
在本节中介绍。

5.1 金钱激励

5.1.1 众包感知。众包感知系统采用终端设备(或移动用户)作为
传感器收集和处理数据。众包感知系统需要收集大规模的传感数据,因此需要大量设备的参与。然而,设备参与后会面临一些问题。收集的数据可能包含设备的隐私信息(如位置)。此外,感知任务会消耗电池等资源。

因此,如果没有足够的激励,理性的用户会拒绝参与众包感知。需要一种激励机制来激励各种设备参与。不幸的是,现有的

中心化激励机制依赖中心化平台来执行,不切实际
假设信任。此外,中心化激励机制也存在单点故障问题
机制。区块链可以采用适当的共识机制,摆脱对可信中心化平台的依赖,消除单点故障问题[29]。如何

[illegible]

参	[illegible]版	[illegible]型	共[illegible]机制	激[illegible]	激[illegible]标	激[illegible]	激[illegible]	[illegible]										
[54]	1.0	–	[illegible]	矿工	参与	货币激励	[illegible]	[illegible]					•	•	和	•	•	–
[6]	1.0	[illegible]	▪	播	参与	货币激励	[illegible]	是					•	•	–	•	•	–
[1]	1.0	[illegible]	PBFT	播	参与	货币	[illegible],	是					•	•	–	•	•	–
[24]	1.0	[illegible]	[illegible]	播	参与	货币	[illegible]YY						•	•	–	•	•	–
[88]	1.0	[illegible]	–	[illegible]	参与	货币激励	[illegible]	[illegible]					•	•	–	•	•	否
[22]	2.0	[illegible]	[illegible]	[illegible]	参与	货币激励	[illegible]								–	•	•	–
[39]	3.0	–	▪	[illegible]	参与	货币激励	[illegible]	是								•	•	–
[53]	3.0	[illegible]	▪	矿工	参与	货币激励	[illegible]	[illegible]N								•	•	–
[50]	1.0	[illegible]	▪	矿工	合作	货币激励	[illegible]	YYYY					•	•	–	•	•	否
[79]	1.0	[illegible]	[illegible]W	矿工	合作	货币激励	[illegible]YY						•	•	和	•	•	和
[26]	1.0	[illegible]	[illegible]	矿工	合作	货币激励	[illegible] 60%–	[illegible]					•	•	–	•	•	–
[16]	1.0	[illegible]	▪	矿工	合作	货币激励	[illegible]Y						•	•	–	•	•	–
[7]	1.0	[illegible]	▪	[illegible]	合作	货币激励	[illegible]	[illegible]					•	•	和	•	•	–
[4]	1.0	[illegible]	[illegible]	[illegible]	合作	货币激励	[illegible]	是					•	•	–	•	•	否
[53]	3.0	[illegible]	▪	矿工	合作	货币激励	[illegible]	[illegible]N								•	•	–
[66]	1.0	[illegible]	▪	[illegible]	合作	[illegible] 激励	[illegible]	[illegible]					•	•	–	•	•	–
[47]	1.0	–	▪	矿工	参与	[illegible]	[illegible]	.					•	•	–	•	•	–
[34]	1.0	[illegible]	POC	矿工	合作	[illegible]	[illegible]	[illegible]					•	•	–	•	•	否
[81]	3.0	–	–	矿工	合作	[illegible]	[illegible]YY									*		
[87]	3.0	[illegible]	[illegible]	[illegible]	合作	[illegible]	[illegible]YY									•	•	–
[55]	3.0	[illegible]	▪ [illegible]	[illegible]	[illegible]	[illegible]	[illegible]Y									•	•	否

[illegible]; -:

[illegible]:

参考	应用程序	区块链类型	共识机制	激励机制	激励措施	区块链类型	激励措施	激励机制	时间/年	其他
[83]	物联网	公共	-	无	无	无	无	无	2020	无
[95]	物联网	公共	-	无	无	无	无	无	2021	无
[95]	物联网	公共	-	无	无	无	无	无	2021	无
[40]	物联网	联盟	PoW	无	无	无	无	无	2020	无
[76]	云计算	联盟	-	无	无	无	无	无	2020	无
[23]	雾计算	联盟	-	无	无	无	无	无	2020	无
[17]	雾计算	联盟	-	无	无	无	无	无	2020	O(n)N
[18]	物联网	联盟	PBFT	无	无	无	无	无	2020	无
[21]	智慧城市	公共	PoW	无	无	无	无	无	2020	无
[103]	智慧城市	联盟	-	无	无	无	无	无	2020	无
[32]	智慧医疗	联盟	-	无	无	无	无	无	2020	无
[13]	医疗保健	公共	-	无	无	无	无	无	2020	无
[89]	内容分发	公共	-	无	无	无	无	无	2020	无
[3]	智慧医疗	联盟	拜占庭容错	无	无	无	无	无	2020	无
[36]	物联网安全	联盟	委托	无	无	无	无	无	2020	无
[46]	物联网	联盟	工作量证明	无	无	无	无	无	2020	无
[101]	云计算	联盟	派克	无	无	无	无	无	2020	无
[15]	智慧医疗	公共	无	无	无	无	无	无	2020	无
[52]	物联网	公共	无	无	无	无	无	无	2020	无
[99]	物联网安全	公共	雾计算	无	无	无	无	无	2020	无

设计基于区块链的去中心化激励机制已被许多人研究
研究人员。

为了激励移动用户参与众包感知,Wang 等人[83]提出了一种基于区块链的激励机制来实现隐私保护,并向理性的移动用户提供基于加密货币的激励。服务器发布任务后,每个用户决定是否

根据个性化任务成本以及服务器公布的奖励接受任务。
用户接受任务后,需要将相应的感知数据上传到区块链
网络。矿工根据期望最大化(EM)算法评估数据质量,并应用互信息量来量化用户的贡献。

服务器根据矿工的评估结果向用户支付费用。一种签密方法和
采用K匿名方法,防止矿工在验证数据、识别消息时获取用户的隐私信息,激励机制满足IP。

数据质量评估使得服务器能够向用户奖励大量奖励
数据质量高。此外,服务器需要提前存入一些加密货币
以防止其拒绝支付。因此,该机制满足IF。该机制可以激励用户提供真实的数据,它满足IT和IC。然而,该机制不是自动的

不符合 IA。本文考虑最大化
服务器和用户,而不考虑矿工的社会福利。因此,我们无法判断
机制满足SW,没有讨论IS、SC、CC。

Yin 等[95]提出了一种具有时间约束和质量要求的竞标机制
对于需要不切实际地收集数据的一般任务,任务的发布、投标信息的提交、奖励的分配都是通过智能合约进行的。用户提交投标价格、数据
中心根据自身预算和数据质量要求,在最大化自身利益的前提下,选择部分获胜用户。

由于大量用户提交相关数据,中心负担过重,因此该机制不
满足 SC。完成任务的用户将获得代币作为金钱奖励。该机制忽略过高竞价请求,从而避免恶意竞价。此外,

无法提供承诺质量数据的用户将不会获得奖励,并且不能再
参与任何众包感知任务。因此,竞标机制符合 IT。然而,
投标信息由中心审核,以便中心能够观察到投标的具体信息
竞价和猜测用户的偏好,这违反了隐私保护要求;因此,
机制不满足IP。每个理性用户都会以高于其资源消耗成本的价格进行竞价,因此其收益为非负,竞价机制满足IR。该机制
通过智能合约执行,并符合IA。不幸的是,本文没有具体说明
奖励分配的细节,因此无法判断竞标机制是否令人满意
IC和IF。车辆的出价是否是车辆利益最大化的最优出价是未知的,因此不能确定竞价机制是否满足SW。CC和IS无法判断,
任何一个。

单用户资源可能不足以完成对延迟敏感的紧急任务;因此,应激励多个用户完成相同的任务。

[95]提出了一种基于时间窗的多用户协作机制,
利用分配任务之间的空闲时间和多个用户的空闲资源来处理紧急
任务。任务的分配是通过拍卖来完成的。拍卖进程在智能
合约,因此该机制满足 IA。完成紧急任务的用户的利润
任务的收益按照其对该任务完成的贡献大小进行计算。仿真结果表明,随着合作用户数量的增加,每个用户的收益增加,
这意味着越来越多的用户愿意加入协作,以完成紧急
任务。时间窗口提高了用户的资源利用率,缩短了用户的任务

完成时间。与一般任务的拍卖机制类似,该机制不注重保护用户的隐私信息,因此激励模型不满足IP。而且还有一个中心来选择用户,所以该模型不满足SC。但是该方法仍然可以防止用户虚假投标和提交虚假数据,满足IT。用户的收益是非负的,所以该方法满足IR。该激励机制的CC为O(n)。同样,很难判断该机制是否满足IC、IF、SW和IS的要求。

胡等人[40]考虑在预算约束下长期收集高质量的传感数据,提出了一种基于博弈论的激励机制。将用户分为两种类型,一种是月薪用户,另一种是兼职用户。提出了一个三阶段的 Stackelberg 博弈来建模任务发起者和月薪用户之间的相互作用。他们使用区块链来匿名化用户身份;因此,激励机制满足 IP。

Stackelberg均衡有利于任务和奖励的公平分配,满足IF。激励机制利用了智能合约,满足IA。该机制最大化任务发起者和参与者的效用,激励月薪参与者持续提供数据,满足IS。IC、IT、SW、SC本文未提及,无需考虑CC。

5.1.2 云计算。

激励机制遵守制度设计。为实现多云环境下数据的安全协同共享,Shen 等[76]提出了一种基于 Shapley 值的收益分配激励机制,并使用智能合约来管理支付流,避免了合约方的否认。实验结果表明,该激励机制能够成功激励数据拥有者提供真实数据,其收益分配基于各方的贡献,因此该机制满足 IF 和 IA。数据拥有者若想提高收益,就必须诚实地提供高质量数据,因此该机制满足 IC 和 IT。然而,该激励机制并未考虑 IP,我们无法判断该激励机制是否满足 SW、IS 和 SC。CC 与该激励机制的评价无关。

不发起攻击的激励。随着云计算的发展,可验证性成为确保云中执行程序正确性的关键问题,进一步加速了云计算的应用。迫切需要一种成本合理的方法来实现云计算的可验证性。Dong 等[23]提出了一种方法,其中客户端让两个云对同一任务进行计算并交叉验证其结果。

作者提出了一种基于合约的激励机制,利用博弈论和智能合约来防止两朵云合谋,该机制支持IA。两朵云需要支付一定数额的押金,押金将返还给诚实的云,不诚实的云的押金将被没收,并视为对诚实云的奖励。为了消除云之间的合谋,设计了一个囚徒合约,具体来说,该合约奖励举报合谋的云,惩罚不诚实的云。该机制允许不受信任的云参与,并鼓励它们诚实行事。它确保云如果诚实行事,可以提高自己的利益;否则,它将受到更大的惩罚,因此它满足IC和IT。当两朵云的计算结果之间存在争议时,第三方会出现来解决争议。由于第三方并不完全可信,可能会泄露客户数据,因此激励机制不符合IP。同时,第三方的存在会限制激励机制的可扩展性,因此该机制不满足SC。我们无法判断该机制是否满足IF、SW和IS。本文未讨论CC。一般来说,CC是重复的,因为它采用双云服务器。

5.1.3 车联网。为鼓励用户参与数据收集和共享,解决车联网应用中的数据共享问题,陈等[17]提出了一种基于联盟区块链的拍卖激励机制。其拍卖流程如下。数据请求者将其数据请求发送到拍卖平台,一些数据卖家收集请求的数据。然后,数据卖家将其部分数据发送到拍卖平台。平台采用两种算法分别基于 EM 算法确定中标数据卖家和支付价格。最后,中标数据卖家将完整的数据发送到平台。RSU 作为矿工,将交易打包成区块,并将区块链接到区块链。

用户(数据卖方与数据请求者)信息与账户名的映射关系存储在可信机构的数据库中,但该第三方并非完全可信,仍存在隐私泄露风险,因此激励机制不满足IP。数据卖方的效用为非负,因此该机制满足IR。由于采用了智能合约,数据卖方可以获得预期的回报,避免了拒绝支付,因此该机制满足IF和IA。数据卖方无法通过提交低质量的数据获得高收益,因此激励机制满足IC。数据卖方在投标时通常会提交真实的成本估算,因此激励机制满足IT。平台视角的社会福利可以看作是系统的社会福利,该激励机制的目标是使平台视角的社会福利最大化。

所以满足 SW。该机制的 CC 为 O(n),并且随着数据卖家数量的增加保持线性,因此该机制满足 SC。不幸的是,IS 的实现是未知的。

电动汽车可以通过充电放电解决区域性能源短缺问题,但电动汽车车主缺乏电力交易的激励机制。陈等[18]提出了一种基于博弈论的激励性智能合约,以平衡和优化电动汽车在电力交易中的利益。当智能合约被触发时,系统会自动根据博弈中两辆车所有可能的决策计算收益,并找到对两辆车都最优的策略。然后两辆车完成电力交易并结算,交易完成后,两辆车将根据各自的贡献获得能源币。因此,激励性智能合约满足IA和IR。当电动汽车发起合谋攻击时,它们获得的能源币奖励会减少。因此,激励性智能合约迫使电动汽车合作,并满足IC和IT。作者没有考虑IP。我们无法知道激励是否满足其他要求。CC未被考虑。

5.1.4 其他。这部分主要回顾了除众包感知、云计算、车联网之外的其他应用场景的激励机制。我们根据激励目标将这些激励机制分为参与和合作两类。

激励参与应用系统。部分论文的研究重点不针对具体场景,但随着大数据、人工智能技术的发展,需要收集大量数据,因此很多研究关注数据共享。

崔等[21]提出了一种激励机制来鼓励移动设备共享数据,将挖矿奖励作为激励的手段。如果移动设备愿意与其他设备共享数据,则基站将根据共享数据的大小为移动设备分配相应的算力。移动设备应用分配的算力进行挖矿并获得相应的挖矿奖励。分配的算力与共享数据的大小之间的关系可以是线性的,也可以是非线性的。

如果是线性关系,那么移动设备会为流行度高的数据分配更多的缓存,而当是非线性关系时,最优策略是均匀缓存。当移动设备数量增加时,基站的工作负载

增大,限制了机制的可扩展性。该机制不满足SC的要求。该机制没有提到挖矿奖励如何分配给移动设备。移动设备可能得不到应有的奖励,也有可能部分分享小数据的移动设备获得的奖励不足以抵消其成本。因此,我们无法判断这种激励机制的性质。该机制不满足IA,也没有考虑IP。

人工智能公司利用大量医疗数据建立和训练模型,并与医疗机构合作为患者提供诊断服务。精准的诊断服务需要大量真实的医疗数据进行训练。朱等[103]提出了一种基于区块链的医疗数据共享模型,该模型基于各方合作为患者诊断。参与方包括构建训练模型的第三方、维护区块链的矿工、提供训练数据的数据所有者。模型的收益由需要诊断的患者提供。该模型采用Shapley值进行收益分配,并应用智能合约自动控制收益分配。数据所有者的收益是根据其数据质量对训练模型的贡献来分配的,因此其必须提供真实的数据才能获得高额收益。因此,该激励模型满足了IT和IC的要求。采用Shapley值实现了公平的收入分配。而使用智能合约分配收入可以防止拒付,实现便捷有效的支付。因此,该激励模型满足IF和IA。但是,第三方拥有医疗数据的访问权,因此该模型不满足IP。激励模型没有考虑SW,IS和SC。CC不适合用来评估该激励模型。

基于位置的服务请求者需要向服务提供者提供其位置信息,因此请求者的隐私可能受到侵犯。K匿名是一种常用的保护位置隐私的方法。需要与其他不太关注位置隐私的移动用户合作组成K匿名组。但其他移动用户没有动力参与匿名组。因此,有必要研究一种激励机制来激励移动用户加入K匿名组。

Yang 等[94]设计了一种单轮密封投标双向拍卖作为激励机制,以激励移动用户加入 K 个匿名群组。然而,拍卖是基于可信中介机构建立的。为了消除这种不切实际的假设,耿等[32]将参考文献[94]中提出的激励机制与智能合约相结合,实现了去中心化的激励机制。智能合约的应用确保激励机制满足 IA。为了防止攻击者通过交易记录识别服务请求者,作者构建了一个公共合约和一个私有合约来满足 IP 的要求。公共合约通过群签名加密并通过盲签名进行验证。私有合约仅对 K 个匿名群组成员可见,以保护隐私。激励机制将服务请求者视为投标的买家,将其他移动用户视为定价的卖家。激励机制鼓励买家提供现实的估价,并激励卖家披露其真实成本,既满足 IT 又满足 IC。

并且保证买卖双方的效用为非负数,满足IR。激励机制的CC是多项式时间的,SW、IF、IS、SC未知。

合作激励:符合制度设计。为了提高内容分发效率,在分发过程中保持内容提供者(CP)的控制权,并防止协调的内容帮助者(CH)占据过多的市场份额,吴等人[89]提出了一种新颖的内容分发框架,并构建了智能合约激励机制。CP向CH支付内容分发费用。CH需要存入

在内容分发前向CP支付预付款和押金均由智能合约管理。当内容分发成功,且CH获得了经过验证的分发证书后,即可成功收到CP的付款,押金也会被退还。但如果检测到CH分发过多或分发证书验证失败,则押金会被没收。该机制可以在一定程度上抑制CH合谋获取虚假分发证书。但本文并未给出该机制的具体设计,因此无法比较CH不诚实时的惩罚和收益。因此,我们无法判断IC、IT、IF、SW和IS。作者没有考虑IP。使用智能合约实现透明性和自动化,因此该机制满足IA。未考虑SC和CC。

合作激励:不发起攻击。延迟容忍网络的性能会受到不参与消息转发的自私节点的影响。而且,自私行为会导致较低的投递率和较长的传输延迟。Chakrabarti 和 Basu [13]提出了一种基于区块链的激励机制来消除延迟容忍网络中的自私行为。在该机制中,成功投递消息的转发节点将根据奖励分配方法获得比特币作为奖励。每个中间转发节点将向下一跳转发者支付一定数量的奖励以收集数字签名的确认(作为合作的标志)。转发节点的收益为非负数,该模型满足 IR。当转发节点想要最大化收益时,它会减少传播跳数,同时降低消息投递延迟,因此激励机制满足 IC。为了防止转发节点不诚实,当消息成功投递后,需要后续转发节点的数字签名确认后才能获得奖励,因此模型满足IT。但是激励机制的实现不是自动的,所以模型不满足IA。作者没有考虑IP。IF、SW、IS未知。SC和CC本文没有讨论。

5.2 基于声誉的激励Alghamdi 等人[3]提出了一

种针对区块链轻量级客户(LC)的具有公平支付系统的安全服务供给方案和基于声誉的激励机制。

服务提供商(SP)的信誉是有效交易的数量。SP 向 LC 发送服务代码以确认其正确性,如果代码正确,它将从 LC 获得奖励。

作者采用智能合约来验证服务。因此,激励机制符合IA。
声誉机制可以激励 SP 提供正确的服务,因此满足 IC 和 IT。应用智能合约可确保公平有效地分配奖励,因此该机制满足 IF。作者没有考虑 IP。SW、IS 和 SC 未知。CC 未受影响。

5.3 游戏化激励

机器学习需要大量的大型数据集进行训练,而这种数据集很难获得。为了鼓励参与者协作构建数据集并提高训练模型的可用性,Harris 和 Waggoner [36]提出了一个智能合约来托管持续更新的模型。数据集和训练好的模型在区块链上公开共享。

作者提出了一个游戏化的激励框架,以鼓励参与者贡献数据来提高模型的准确性。激励框架将参与者的意愿作为共同利益,鼓励参与者免费合作。此外,它还奖励参与者一些积分和徽章。该激励框架引入了智能合约,以实现激励的透明度和自动化,因此它符合IA。该机制框架

要求参与者上传数据到公链,存在隐私泄露风险,因此该机制不满足IP,SC和CC不予考虑,其他要求是否满足尚不确定,判断难度较大或未讨论。

5.4 混合激励混合激励不仅可以激

励用户参与,还可以鼓励他们诚实或合作地行事。接下来,我们将根据应用场景回顾这部分现有工作。

5.4.1 众包。Kadadha 等[46]采用智能合约提出了一种公平透明的激励机制,以提高众包中的工人参与度。在诚实工人提交相似解决方案的前提下,可以采用相似度评估方法来评估解决方案的质量。工人的收入包括基本收入和质量佣金。质量佣金与解决方案的质量成正比,可以防止工人提交错误或低质量的解决方案。工人和任务请求者的声誉值在付款完成后更新。请求者的声誉与取消的任务数量相关,工人的声誉与其解决方案的质量相关。为了获得高声誉,工人和请求者都会避免不诚实行为。因此,该机制满足 IT 和 IC。激励机制部署在智能合约中,满足 IA。同时,请求者不能拒绝付款,工人提交的解决方案的质量与其收入成正比;因此,混合激励机制满足 IF。本文中,用户(工作者或请求者)的地址是假名公钥,因此不会暴露用户身份,而任务解决方案的质量评估由智能合约完成,不会泄露工作者的隐私信息,因此激励机制满足IP。本文没有提到机制的SW和IS,也没有考虑SC和CC。

5.4.2 云计算。传统的云服务水平协议缺乏可靠的自动执行平台。周等人[101]提出了一种利用智能合约和博弈论的见证人模型,并引入了一个新的角色“见证人”,可以发现和报告服务提供商的违规行为。该模型包括审计机制和经济激励机制。

审计机制是根据见证人的行为来评估其声誉。当其声誉低于预定义的阈值时,见证人将不再参与检测违规行为,这可以激励见证人诚实行事。见证人举报违规行为,然后获得合理的收益,这是根据博弈论设计的。如前所述,激励机制满足 IC、IT 和 IF。根据实验,见证人的 gas 消耗较少,因此见证人有动力参与检测。但作者没有考虑 IP。

激励机制利用了智能合约,满足IA,SW、IS未知,不考虑SC、CC。

5.4.3 车联网。随着自动驾驶技术的发展,未来智能交通将取代传统的驾驶方式。智能交通成功应用后,自动驾驶车辆会以车队形式行驶,车队最前面的一辆车充当领头车,即车队头(PH),带领其他车辆,即车队成员(PM)。PH需要不时观察路况,调整行驶方向。因此,当 PH 比当 PM 更耗能,没有理性的驾驶员会选择当 PH。

陈等人[15]提出了一种基于声誉值和金钱奖励的混合激励机制,以激励司机担任 PH。PH 的服务显示方式如下:

其信誉值。PH的信誉值会根据其行为不断更新。
信誉值越高,车辆被选为 PH 的可能性就越大。PM 通过智能合约支付 PH 车队币（即车队区块链中的加密货币)作为服务费。服务费根据其与 PH 领导的车队的距离收取。

此机制减少油耗,也减少PM的脑力消耗,虽然PH的油耗较高,但每位PM所交的服务费可以抵消。

该机制可以保证PM和PH的收益为非负数,从而满足IR。同时PH的服务费通过智能合约支付,不会出现多付、少付、拒付的情况,满足IF和IA。但是该机制假设排数和成员数都是有限的,因此其可扩展性受到限制,不满足SC。论文中没有提到激励机制中的IC、IT、SW、IS,论文中没有考虑IP,CC的评估要求不适用于该机制。

Ledbetter 等[52]研究了如何激励驾驶员加入车队并成为自动驾驶中的 PH。作者提出了一种基于金钱和声誉的混合激励机制。想加入车队的驾驶员必须满足声誉阈值。服务费的计算与参考文献[15] 不同,后者考虑驾驶员不成为 PH 可以节省多少钱来计算 PM 应该支付给 PH 的金额。为了增加激励机制的有效性,将向 PH 支付额外奖励。激励机制可以确保 PH 获得令人满意的效用,因此该机制满足 IR。如果 PM 通过随意加入车队获得更多效用,则需要向 PH 支付一定比例的金钱,其声誉值会降低,从而大大防止了恶意行为。因此该协议满足 IC 和 IT。协议的所有支付和计算都嵌入在智能合约中,可以审计计算并确保 IF,因此该机制满足 IA。与参考文献[15]类似,该机制也假设了队列和成员的数量是有限的,因此其SC不满足。本文不考虑SW和IS,也不考虑IP。CC的评估要求不适用于该协议。

5.4.4 其他。数据交换需要安全、公平的机制,保障数据提供者的利益和数据安全,否则数据提供者缺乏共享数据的动力。郑某等[99]提出了一种基于智能合约的数据资产交换机制,保证数据交换的可靠性和透明性,并引入了基于服务质量的激励机制,鼓励数据提供者共享数据,并提出了声誉机制,鼓励数据提供者提交高质量的数据。因此,激励机制满足了 IC 和 IT。智能合约保证了奖励的公平性和有效分配,因此该机制满足 IF 和 IA。未提及 SW 和 IS。该机制不考虑 IP 和 SC。CC 不适用于评估该机制。

6 讨论

为了激发区块链系统节点的参与意愿和合作行为,人们提出了各种激励机制。研究人员利用区块链技术改进不同场景的激励机制设计。具体来说,区块链技术已被应用于众包感知场景的激励机制,以取代众包感知平台,从而解决由不可信的众包感知平台引起的隐私和安全问题。智能合约帮助云计算和车联网中的激励机制实现激励的自动分配,并消除拒绝支付问题。我们在第4节和第 5 节分别回顾了为区块链系统设计的激励机制和基于区块链技术构建的激励机制。

表4 不同激励机制形式在不同绩效水平下的绩效比较
区块链系统的目标

目标 / 形式	参与	合作
金钱激励	有效激励	节点不受信任的行为不能有效避免
基于声誉的激励	不适用	有效激励
游戏化激励	不适用	不适用
混合激励	有效激励	有效激励

表5.基于区块链的不同形式激励机制绩效比较
不同应用场景下

设想 / 形式	群体感知	云计算	车联网	其他场景
金钱激励	适用于激励参与	适用于激励参与	适用于激励参与	适用于激励参与
以信誉为本激励	适用但几乎没有使用过	适用于选择和过滤节点	适用于选择和过滤节点	适用于选择和过滤节点
游戏化激励	不适用	不适用	不适用	适用于简单游戏场景
混合激励	适用但几乎没有使用过	适用的	适用的	适用的

在研究区块链系统中不同形式激励在不同目标下的表现时,我们从第4节得出以下发现,如表4 所示。

- 所有货币激励机制通常都满足IR,这是实际操作中的先决条件节点参与和合作的应用程序。然而,很少有激励机制考虑 IR、IC、IT 和 IF 以外的属性。尽管一些货币激励在将参与作为激励目标时,没有考虑 IC 和 IT,他们关注其他属性,如 IC。他们假设只要节点能够受益于系统,节点就有参与的动机。不幸的是,这只能提供临时激励,但不保证合作和诚实的行为这些节点参与系统后。大多数审查过的货币激励措施考虑在将合作作为激励目标时,IC、IT 和 IF 是重要的,因为这些属性对于节点合作至关重要。
- 基于声誉的激励和游戏化激励很少单独用于区块链系统。根据我们的审查,基于声誉的激励机制可以激励节点通过调整声誉值来进行合作,这不适用于参与动机。尽管游戏化的激励措施已被用于激励参与和合作,但效果不太好。
- 混合激励结合了多种激励形式,弥补了激励方式单一的短板。单一激励因素的出现并提供额外的有利特性。
- 综上所述,货币激励和混合激励可以有效激励节点参与区块链系统,而基于声誉的机制和混合激励机制能有效激发节点合作。

我们通过比较不同类型的
基于区块链的激励机制在不同应用场景中的应用,如表5所示。

· 群智感知中的货币激励机制通常用于激励节点参与并提供真实数据,因此满足IR和IT。其中一些通过使用智能合约自动向系统节点分发奖励来实现IA。然而,它们中的大多数都没有考虑其他属性。云计算中的大多数货币激励机制激励节点合作并满足IC和IT的要求。在车联网中提出的货币激励机制实现了许多理想的属性并有效地激发了节点的参与意愿。在其他需要节点参与和合作的场景中,只有一些货币激励满足IC和IT,而大多数货币激励都没有考虑IF。

· 基于声誉的激励机制很少用于众包感知和一些车联网场景,因为文献通常采用拍卖等方法来激励节点提供真实数据。在其他场景中,单一的基于声誉的激励机制只有在需要监控系统节点时才具有良好的性能。游戏化激励在几乎所有场景中都很少使用,它实际上无法实现良好的性能。· 混合激励通常用于众包感知场景以外的场景,其中它将货币激励和基于声誉的激励相结合以获得良好的性能。

结合以上发现,我们总结了不同形式激励措施的应用机制如下。

(1)货币激励适合于提高节点参与意愿,根据节点行为给予直接奖励。与不参与系统时一无所获相比,节点参与系统可以获得物质奖励,因此货币激励可以有效激励参与。货币激励在激励合作时,必须更多地奖励守信行为而非失信行为,难以保证完全公平。此外,大规模系统中的系统节点并非完全理性,无法目睹整个系统的状态,难以激励其守信行为。

(2)基于信誉的激励适用于需要对节点进行监控的场景。它通常设置一个信誉阈值作为确定节点权限的基准,信誉值是根据节点行为按照预先定义的算法计算出来的。一旦节点出现不诚信行为,信誉值低于阈值,则可能被剥夺参与权或增加获利难度。因此,基于信誉的激励可以有效激励合作。遗憾的是,单纯使用信誉激励对激励参与效果甚微。

(3)游戏化激励可以运用在简单的游戏场景中,或者作为一种辅助手段。
它为系统节点提供心理上的满足,在区块链系统等场景中应用较少,因此在参与的激励目标上面临与声誉激励类似的困境,无法直接为参与者提供任何物质奖励;游戏化激励适合作为点缀,单纯地激励节点的参与积极性和合作度并不能起到很好的作用。

(4)混合激励兼具各类激励机制的优点,弥补了各自的不足,在各类应用场景中都能有效激励参与者的参与与合作。然而,良好的表现是有代价的,混合激励通常会引入额外的系统节点,或要求现有系统节点承担额外的工作量,因此其执行开销或经济成本通常高于单一激励。

(5)综上所述,当应用场景复杂、节点负担较重或已有其他方法约束节点行为时,可以分别采用金钱激励和声誉激励,以激励节点参与和合作,满足整体激励绩效;在节点较轻的应用场景中,可以采用混合激励,以期望绩效同时激励节点参与和合作。

概括而言,区块链与激励机制互利互惠,采用设计良好的激励机制可确保区块链系统持续良性发展,而区块链的引入则可提高激励机制的绩效。然而,通过广泛的回顾,我们也发现当前研究存在一系列问题,将在下一节中介绍。

7 尚待解决的问题和未来方向

7.1 未解决的问题根据以

上文献综述,我们发现了一些有关区块链中的激励机制和基于区块链的激励机制的未解决的问题。

7.1.1 区块链激励机制尚待解决的问题。首先,许多学者研究了交易费如何影响矿工的行为。然而,他们在设计激励机制时只是假设交易费包含在激励中,并没有具体的机制来指定交易费。大多数关于交易费的规则只考虑引导矿工的良性行为,而忽略了支付交易费的区块链用户的用户体验,这将进一步间接影响这些用户的效用。

其次,现有关于广播节点激励的研究大多基于简化的区块链网络,例如参考文献[6]将区块链网络简化为高度为的d元有向树森林,H. Ersoy等[24]在设计广播节点激励机制时,简单考虑了k连通的区块链网络。

区块链网络结构在激励机制设计中起着至关重要的作用,激励机制通过影响广播节点的行为来影响区块链网络结构。为了准确捕捉广播节点的实际行为并设计有效的激励机制,需要研究反映现实世界情况的区块链网络模型。

第三,目前对全节点激励机制的研究较少。大多数人认为全节点的激励微不足道,因此研究该主题的文献很少。但全节点共享历史区块记录对于统一区块链账本是必要的。王等人[88]提出,应该对传递历史区块数据的全节点进行奖励。但没有提供具体的奖励分配方案。

第四,并非所有现有的攻击都能被激励机制抑制,现有的激励机制主要是为了解决一种类型的攻击而提出的。我们的调查显示,已经提出了一些激励机制来消除自私挖矿攻击、51%攻击、BWA和DoS攻击。然而,没有考虑防御其他新兴攻击,如鲸鱼攻击[56]、叔块攻击[14]、扣留后分叉(FAW)攻击[51]等。通过发动鲸鱼攻击,攻击者通过收取高额费用的交易贿赂他人,增加了双花的机会。叔块攻击利用叔块进行区块扣留。FAW攻击将BWA与故意分叉相结合。Kwon等人[51]只提出了一种针对FAW攻击的简单对策。实际上,一个区块链系统中存在各种攻击。如何以综合的方式有效地抑制这些攻击仍然需要

进一步研究。Mirkin 等人[63]建议设置叔块奖励,以激励
减轻区块链拒绝服务攻击;然而,这种激励令人失望地增加了
自私挖矿攻击的风险。

第五,目前针对矿池提出的激励机制比较简单。虽然参考文献 [7] 已经研究了两个矿池之间的竞争,但一个场景是
多个矿池的探索尚未展开。Eyal 等人[25]假设矿池持有相同的
计算能力和应用博弈论来分析多个挖矿之间的攻击
矿池。此外,由于矿工在挖出一个区块后不会立即得到矿池的奖励
成功的激励机制应该进一步考虑时间对节点的影响
公用事业。

第六,目前的文献很少研究区块链 2.0 中矿工激励的公平性。Aldweesh 等人[2]发现以太坊中矿工的执行动机

区块链与其运营成本不成比例,这可能导致激励不平衡。
不幸的是,他们没有提出如何解决这个问题。

第七,区块链3.0中现有的激励机制很少能满足IA的要求。
具体来说,区块链 3.0 中的大多数货币激励机制都是手动分配奖励
对系统实体,从而面临在复杂流程中被欺骗的风险。

7.1.2 基于区块链的激励机制尚待解决的问题。首先,根据第5 节,我们
发现基于区块链的激励机制主要侧重于防止不诚实
行为并激励节点参与。然而,这项研究仍处于早期阶段,
现有文献中很少考虑IP和BC等一些要求。

第二,缺乏对新参与系统主体(如矿工)的激励研究。这些机制引入区块链来实现去中心化,以消除对可信平台的需求。

中心化激励机制。现有文献表明这种方法是有效的。然而,区块链的引入也带来了中心化激励机制中不存在的额外问题
机制,比如对矿工的激励。现有的文献只关注如何取代
区块链的激励机制可以激励原始
系统实体,而不考虑矿工。尽管参考文献[83]中的作者指出
矿工的贡献会得到支付,他们没有对
支付。

7.1.3 两种情况下的未决问题。首先,现有的激励机制很少同时应用所有
激励形式。从表2和表3可以看出,大多数激励机制都是基于单一激励形式提出的,其中应用最广泛的是金钱激励。

然而,货币激励机制并不像非货币激励机制那样可持续,例如
基于声誉的激励机制[61]。此外,如果仅采用非货币激励机制,则在没有详细支付机制的情况下激励是间接的,目光短浅的系统实体可能无法感知到激励。

第二,所审查的激励机制没有一个能够满足所有要求。表2和表3
说明现有的区块链激励机制和基于区块链的激励机制只能满足一些基本要求。具体来说,它们大多考虑了IR、IT和

IC。然而,他们很少考虑SW和IS。激励机制的时间成本(CC)
区块链 3.0 和基于区块链的激励机制被忽略。实施
区块链1.0、2.0、3.0中激励机制的成本(BC)研究也较少,这意味着区块链相关的激励机制还有很大的改进空间

或优化。因此,设计良好的激励机制,满足更多
实现高有效性和稳健性的需求非常高。

7.2 未来研究方向

受上述未解决问题的启发,我们得出了未来研究的以下方向。

首先,在设计交易手续费规则时,应综合考虑各参与主体的效用,不仅要从矿工的角度考虑,保证矿工收支平衡,激励矿工积极参与系统,还要从支付交易手续费的用户的角度考虑,在设计激励机制时,还要考虑用户等待的时间成本、交易处理速度等因素。用户与矿工之间的长期互动值得研究,例如可以借鉴进化博弈论,考虑区块链市场发展,结合实际成本,设计出切实有效的手续费规则。

其次,贴近实践的网络模型应建立在提出有效的激励机制的基础之上。例如,应研究如何为广播节点提供激励,使激励机制与实际的区块链网络兼容。可以采用复杂网络理论来研究区块链网络,考虑网络的演化,考察网络拓扑结构的变化。此外,可以设计与广播节点贡献成比例的激励分配,以公平地激励广播节点的参与和合作,从而形成公平、可持续的有效激励机制。

第三,应认真研究全节点的激励机制。可以参考文献[88] 提出的锁币策略,设计更详细的激励机制。例如,可以研究一种精细的支付机制,让新加入的节点为全节点的合作付费。如何利用全节点内部的竞争来减轻新加入节点的激励成本,也是今后研究的重点。

第四,还应进一步研究防止每种未经调查的攻击和组合攻击的激励机制。由于不同攻击中的攻击者类型和攻击目标各不相同,不同攻击的激励措施也不同。此外,在考虑防止不同攻击组合的激励措施时,应注意如何对不同攻击之间的权衡进行建模。一个可能的进一步方向是提出一种可调的激励机制,该机制可以根据系统设计者的期望比其他攻击更有效地抑制某些攻击。侯等人[38]应用深度强化学习对区块链中的激励机制进行自动攻击分析,这可以极大地帮助调整激励机制以积极的方式防止各种攻击。

第五,应提出严格的激励机制,以促进矿池合作。矿池中矿工的最优决策和行为会随着时间的推移而动态变化。因此,在未来的研究中应考虑时间因素,以便对矿池进行准确的调查。Zolotavkin 等人[104]提到,在考虑矿池中矿工的奖励或激励时,应采用跨时间效用模型。此外,研究较少的多个矿池之间的竞争可以建模为博弈模型。通过为具有不同策略的矿池设计合适的效用函数,我们可以将该博弈的纳什均衡调节到所有矿池都诚实行事而不会相互攻击的预期状态。为了推广激励机制,应该假设矿池的计算能力是多样化的。

第六,应提出对以太坊区块链矿工的进一步有效激励机制。现有的激励通常来自于生成区块所获得的以太币奖励。受参考文献[22]的启发,应研究通过考虑智能合约的价值来进一步改善基于区块奖励的激励。具体来说,我们可以考虑将智能合约的代币交易量作为其价值,并进一步将其设计为与区块奖励正相关。

第七,区块链3.0的激励机制可以引入智能合约
以实现IA的要求。激励机制可以整合智能合约来
实施竞标或博弈程序。这样的结合不仅可以避免不诚信行为
或人为干预引起的意外故障,同时也简化了
激励机制,包括激励设计和分配。最后,一个设计良好的智能
契约可以帮助激励机制轻松实现公平。

第八,货币激励和非货币激励相结合的激励机制将成为未来的研究热点。原因是这种混合激励机制

可以通过直接奖励激励系统实体,提高系统可持续性。现有文献已经尝试将基于信用的激励纳入货币激励,并

取得了理想的性能和令人满意的特性。我们可以进一步研究如何结合货币激励、游戏化激励、基于彩票的激励、基于合同理论的
激励等。是否涉及多种非货币激励可能更
有效性以及如何分配不同形式激励的权重也是值得关注的
进行調查。

第九,应认真研究区块链激励机制中隐私保护和矿工激励问题。隐私保护可以通过引入

将复杂的加密算法纳入激励机制或增加违反的成本
通过激励设计实现隐私。矿工的出现使系统模型、系统实体之间的相互作用以及系统实体之间的利益关系变得复杂。借贷
区块链 1.0、2.0 和 3.0 中激励矿工的想法可能会有所帮助;然而,有效性
仍需认真探索。

最后,在设计区块链中的激励机制和基于区块链的激励机制时,应该综合考虑更多的要求。我们应注意

可持续发展,同时注重社会福利最大化,以提高系统各节点的贡献积极性,维持系统长期运行。相关要求

激励成本也应考虑,这在成本敏感的应用场景中是非常需要的。具体来说,可以通过考虑有效的非货币措施来实现可持续性
激励机制和设计重复博弈。通过以社会福利最大化作为激励设计的总体目标,而不是最大化激励设计者的效用,我们可以将
最大化问题作为优化问题,并采用一些有效的算法来输出
解决方案。基于梯度的算法通常用于在以下情况下产生接近最优的解决方案:
优化问题是 NP-hard 的。值得研究的是,是否存在其他有效的
未来计算复杂度较低的算法。

8 结论

激励机制作为维持系统长期运转的动力,是
区块链系统不可或缺的元素。此外,区块链的先进特性
也可以有助于设计有效且高效的激励机制。然而,仍然存在
缺乏对激励机制和区块链技术如何使
在本文中,我们广泛回顾了与激励机制相关的学术论文
区块链中的机制和基于区块链的激励机制。为了系统地评估这些论文,我们提出了一套基于激励属性和成本的要求。
在区块链中的激励机制和基于区块链的激励机制中,我们根据激励形式、激励目标和应用场景对现有文献进行了重新审视,通过对它们优缺点的评估,讨论了激励机制如何

和区块链互相受益,并进一步总结了一些尚未解决的问题,并提出了
未来的研究方向以指导该领域的进一步研究。

参考

[1] Ittai Abraham、Dahlia Malkhi、Kartik Nayak、Ling Ren 和 Alexander Spiegelman。2016 年。Solidus：一种基于无需许可的拜占庭共识的激励兼容加密货币。CoRR abs/1612.02916。

[2] Amjad Aldweesh、Maher Alharby、Ellis Solaiman 和 Aad van Moorsel。2018 年。通过智能合约性能基准测试来评估以太坊中的矿工激励措施。第 14 届欧洲可靠计算会议 (EDCC 18) 论文集。IEEE，144–149。

[3] Turki Ali Alghamdi、Ishtiaq Ali、Nadeem Javaid 和 Muhammad Shafiq。2019 年。基于区块链的公平支付系统和激励机制的轻量级物联网设备安全服务配置方案。IEEE Access 8（2019 年），1048–1061。

[4] Naif Alzahrani 和 Nirupama Bulusu。2018 年。《迈向真正的去中心化：基于博弈论和随机性的区块链共识协议》。《国际安全决策与博弈论会议论文集》，第 11199 卷。Springer，465–485。

[5] N. Anita 和 M. Vijayalakshmi。2019 年。区块链安全攻击：简要调查。第 10 届计算、通信和网络技术国际会议 (ICCCNT 19) 论文集。IEEE，1-6。

[6] Moshe Babaioff、Shahar Dobzinski、Sigal Oren 和 Aviv Zohar。2012 年。《论比特币和红气球》。《第 13 届 ACM 电子商务会议论文集》。56–73。

[7] Samiran Bag 和 Kouichi Sakurai。2016 年。关于比特币矿池区块扣留攻击的另一篇注释。在国际信息安全会议。Springer，167-180。

[8] Roman Beck、Christoph Müller-Bloch 和 John Leslie King。2018 年。区块链经济中的治理：框架工作和研究议程。J. Assoc. Inf. Syst. 19, 10 (2018), 1。

[9] Ethan Buchman。2016 年。Tendermint：区块链时代的拜占庭容错。博士论文。

[10] Vitalik Buterin 等人，2014 年。以太坊：下一代智能合约和去中心化应用平台。白皮书 3，37 (2014)，1-36。摘自https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper 7.

[11] Glenn Carl、George Kesidis、Richard R. Brooks 和 Suresh Rai。2006 年。拒绝服务攻击检测技术。IEEE 互联网计算。10, 1 (2006)，82-89。

[12] Miles Carlsten、Harry Kalodner、S. Matthew Weinberg 和 Arvind Narayanan。2016 年。《论没有区块奖励的比特币的不稳定性》。《ACM SIGSAC 计算机和通信安全会议论文集》。154–167。

[13] Chandrima Chakrabarti 和 Souvik Basu。2019 年。基于区块链的 DTN 灾后机会性通信激励方案。第 20 届分布式计算和网络国际会议论文集。385–388。

[14] Sang-Yoon Chang、Younghee Park、Simeon Wuthier 和 Chang-Wu Chen。2019 年。叔块攻击：对于理性和不合作的矿工来说，区块链挖矿威胁超出了区块扣留的范围。国际应用密码学和网络安全会议，第 11464 卷。Springer，241–258。

[15] Chen Chen, Tingting Xiao, Tie Qiu, Ning Lv, and Qingqi Pei. 2019. Smart-contract-based economical platooning in 支持区块链的城市车联网。IEEE 工业信息学报 16, 6 (2019), 4122–4133。

[16] 陈欢和王逸杰。2019 年。SSChain：一种无数据迁移开销的公有区块链全分片协议。Perv. Mobile Comput. 59 (2019)，101055。

[17] 陈武辉、陈宇飞、陈旭、郑子斌。2019 年。面向车联网的安全数据共享：具有链上和链下保证的质量驱动激励机制。IEEE IoT J. 7, 3 (2019)，1625–1640。

[18] 陈晓峰，张晓红. 2019. 电动汽车安全电力交易与激励合同模型基于能源区块链的分布式能源系统集成。IEEE Access 7 (2019), 178763–178778。

[19] Sunghyun Cho 和 Sejong Lee。2019 年。《区块链在物联网中的应用调查》。《国际区块链会议论文集》，国际电子、信息和通信会议（ICEIC 19）。IEEE，1-2。

[20] Peter B. Clark 和 James Q. Wilson。1961 年。《激励系统：一种组织理论》。《Admin. Sci. Quart.》（1961 年），129–166。

[21] 崔欢、陈志勇、刘宁、夏斌。2019 年。区块链驱动的无线缓存 D2D 网络内容共享策略。IEEE 国际通信研讨会 (ICC Workshops 19) 论文集。IEEE，1-5。

[22] Weiqi Dai, Deshan Xiao, Hai Jin, and Xia Xie. 2019. A concurrent optimization consensus system based on blockchain. 在第 26 届国际电信会议 (ICT 19) 论文集上。IEEE，244–248。

[23] Changyu Dong、Yilei Wang、Amjad Aldweesh、Patrick McCorry 和 Aad van Moorsel。2017 年。背叛、不信任和理性：可验证云计算的智能反合谋合约。ACM SIGSAC 计算机和通信安全会议论文集。211–227。

[24] O uzhan Ersoy、Zhijie Ren、Zekeriya Erkin 和 Reginald L. Lagendijk。2018 年。无需许可的区块链上的交易传播：激励和路由机制。《Crypto Valley 区块链技术会议论文集》（CVCBT 18）。IEEE，20-30。

[25] Ittay Eyal。2015 年。《矿工困境》。《IEEE 安全与隐私研讨会论文集》。IEEE,89-103。
[26] Ittay Eyal、Adem Efe Gencer、Emin Gün Sirer 和 Robbert Van Renesse。2016 年。Bitcoin-ng:可扩展的区块链协议。第 13 届 USENIX 网络系统设计和实施研讨会 (NSDI 16) 论文集。
45–59。
[27] Ittay Eyal 和 Emin Gün Sirer。2014 年。“多数还不够:比特币挖矿很脆弱”。国际金融密码学和数据安全会议第 8437 卷。Springer,第 436-454 页。
[28] Wei Feng, Yafeng Li, Xuetao Yang, Zheng Yan, and Liang Chen. 2021. Blockchain-based data transmission control 用于战术数据链。数字通信网络。3 (2021),285–294。
[29] 魏峰, 郑艳. 2019. MCS-Chain: 基于区块链的去中心化可信移动众包. Fut. Gener. Comput. Syst. 95 (2019), 649–666.

[30] Wei Feng, Zheng Yan, Laurence T. Yang, and Qinghua Zheng. 2020. Anonymous authentication on trust in blockchain-基于移动众包的物联网解决方案。IEEE IoT J.(2020 年)。
[31] Keke Gai, Jinnan Guo, Liehuang Zhu, and Shui Yu. 2020. Blockchain meets cloud computing: A survey. IEEE Commun. Surv. Tutor. 22, 3 (2020), 2009–2030。
[32] 耿子野、何云华、牛彤、李红、孙利民、程伟、李旭。2017 年。海报:基于智能合约的 LBS 中 K 匿名隐私保护激励机制。IEEE 隐私感知计算研讨会论文集(PAC 17)。IEEE,200–201。

[33] Arthur Gervais、Ghassan O. Karame、Karl Wüst、Vasileios Glykantzis、Hubert Ritzdorf 和 Srdjan Capkun。 2016年。关于工作量证明区块链的安全性和性能。在 ACM SIGSAC 计算机和通信安全会议论文集上。3-16。

[34] 韩轩、袁勇、王飞跃。2019 年。基于信用证明的公平区块链。IEEE 计算机学会会刊。系统 6, 5 (2019), 922–931。
[35] 加勒特·哈丁。2009 年。《公地悲剧》。《自然资源政策研究杂志》1,3(2009 年),243-253。
[36] Justin D. Harris 和 Bo Waggoner。2019 年。区块链上的去中心化和协作式人工智能。IEEE 会议纪要国际区块链会议(Blockchain 19)。IEEE,368–375。
[37] 何业军、陈曼、葛宝红和 Mohsen Guizani。2016 年。论异构网络中的 WiFi 卸载:Various 激励和权衡策略。IEEE 通信调查导师。18,4 (2016),2345–2385。
[38] Charlie Hou、Mingxun Zhou、Yan Ji、Phil Daian、Florian Tramer、Giulia Fanti 和 Ari Juels。2019 年。SquirRL:使用深度强化学习自动分析区块链激励机制的攻击。网络和分布式系统安全研讨会论文集。ISOC,1-18。

[39] Bowen Hu, Chunjie Zhou, Yu-Chu Tian, Yuanqing Qin, and Xinjue Junping. 2019. A collaborative intrusion detection approach using blockchain for multimicrogrid systems. IEEE Trans. Syst. Man Cybernet.: Syst. 49, 8 (2019), 1720–1730.
[40] Jiejun Hu, Kun Yang, Kezhi Wang, and Kai Zhang. 2020. A blockchain-based reward mechanism for mobile crowd-传感。 IEEE 计算机社会系统汇刊 7, 1 (2020), 178–191。
[41] Jiyue Huang, Kai Lei, Maoyu Du, Hongting Zhao, Huafang Liu, Jin Liu, and Zhuyun Qi. 2019. Survey on blockchain incentive mechanism. In International Conference of Pioneering Computer Scientists, Engineers and Educators, Vol. 1058. Springer,386–395。
[42] Tam T. Huynh、Thuc D. Nguyen 和 Hanh Tan。2019 年。区块链技术安全和隐私问题调查。国际系统科学与工程会议论文集(ICSSE 19)。IEEE,362–367。
[43] Luis G. Jaimes、Idalides J. Vergara-Laurens 和 Andrew Raij。2015 年。移动激励技术调查人群感知。IEEE IoT J. 2, 5 (2015), 370–380。
[44] 蒋苏涵和吴杰。2019 年。带有交易费的比特币挖矿:区块大小博弈。IEEE 区块链国际会议论文集(Blockchain 19)。IEEE,107–115。

[45] 蒋鑫、白翔宇,2013 年,延迟容忍网络激励机制研究,第 10 届小波主动媒体技术与信息处理国际计算机会议(ICCWAMTIP 13)论文集,IEEE,191-197 页。

[46] Maha Kadadha、Hadi Otrok、Rabeb Mizouni、Shakti Singh 和 Anis Ouali。2020 年。Sensechain:一种基于区块链的众包感知框架,适用于多个请求者和多个工作者。Fut. Gener. Comput. Syst. 105(2020 年),
650–664。
[47] Yuki Kano 和 Tatsuo Nakajima。2017 年。区块链技术中挖矿工作的新方法。第 15 届移动计算与多媒体发展国际会议论文集。107–114。

[48] Fazlullah Khan、Ateeq Ur Rehman、Jiangbin Zheng、Mian Ahmad Jan 和 Muhammad Alam。2019 年。移动群智感知:关于隐私保护、任务管理、分配模型和激励机制的调查。Fut.
Gener. Comput. Syst. 100 (2019), 456–472。
[49] Moon Soo Kim 和 Jee Yong Chung。2019 年。可持续增长与代币经济设计:以 Steemit 为例。可持续性 11, 1 (2019), 167。

[50] Elias Koutsoupias、Philip Lazos、Foluso Ogunlana 和 Paolo Serafino。 2019.付费区块链挖矿游戏
向前。在《万维网会议论文集》。917–927。
[51] Yujin Kwon、Dohyun Kim、Yunmok Son、Eugene Vasserman 和 Yongdae Kim。2017 年。《自私自利，避免困境：对比特币的扣留后分叉
(faw) 攻击》。《ACM SIGSAC 计算机和通信安全会议论文集》。195–209。

[52] Brian Ledbetter、Samuel Wehunt、Mohammad Ashiqur Rahman 和 Mohammad Hossein Manshaei。2019 年。LIPs：针对异构动态队列
的领导激励协议。IEEE 第 43 届计算机软件和应用程序年度会议 (COMPSAC 19) 论文集第 1 卷。IEEE，535–544。

[53] Kai Lei, Maoyu Du, Jiyue Huang, and Tong Jin. 2020. Groupchain: Towards a scalable public blockchain in fog com-
物联网服务计算的发展。IEEE 服务计算汇刊 13, 2 (2020), 252–262。
[54] Yoad Lewenberg、Yonatan Sompolinsky 和 Aviv Zohar。2015 年。包容性区块链协议。国际公约
金融密码学和数据安全参考文献，第 8975 卷。Springer，528–547。
[55] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. 2018. Creditcoin: A
privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE
Trans. Intell. Transport. Syst. 19, 7 (2018), 2204–2220.
[56] Kevin Liao 和 Jonathan Katz。2017 年。通过鲸鱼交易激励区块链分叉。国际金融密码学和数据安全会议，第 10323 卷。Springer，264–279。

[57] 李林. 2019. 解构区块链（第1版）. 北京: 清华大学出版社, 清华大学，中国。
[58] Gao Liu, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. 2020. B4SDC: A blockchain system for
MANET 中的安全数据收集。IEEE 大数据汇刊 (2020)。
[59] 刘高、闫征、冯伟、荆旭阳、陈亚星和 Mohammed Atiquzzaman。2021 年。SeDID：一种支持 SGX 的用于网络信任评估的去中心化入侵检测框架
信息融合 70 (2021)，100–
114.
[60] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019.
区块链调查：博弈论视角。IEEE Access 7 (2019)，47615–47643。
[61] Tie Luo、Salil S. Kanhere、Jianwei Huang、Sajal K. Das 和 Fan Wu。2017 年。移动群体感知的可持续激励：拍卖、彩票以及信任和声誉系统。
IEEE Commun. Mag。55，3（2017 年），68–74。
[62] 杜明晓, 马晓峰, 张哲, 王祥伟, 陈启军. 2017. 区块链共识算法综述. In Proceedings of the IEEE International Conference on Systems,
Man, and Cybernetics (SMC 17). IEEE,
2567–2572。
[63] Michael Mirkin、Yan Ji、Jonathan Pang、Ariah Klages-Mundt、Ittay Eyal 和 Ari Juels。2020 年。BDoS：区块链拒绝服务。ACM SIGSAC 计算
机和通信安全会议论文集。601–619。
[64] Malte Möser 和 Rainer Böhme。2015 年。《趋势、技巧、收费：比特币交易费的纵向研究》。在《国际
国际金融密码学和数据安全会议，第 89-76 卷。Springer，19-33。
[65] 中本聪。2008 年。比特币：一种点对点的电子现金系统。《去中心化商业评论》（2008 年），第 21260 页。
[66] Mehrdad Nojoumian、Arash Golchubian、Laurent Njilla、Kevin Kwiat 和 Charles Kamhoua。2018 年。通过基于声誉的范式激励区块链矿
工避免不诚实的挖矿策略。《科学与信息会议》第 857 卷。Springer，1118–1134。

[67] S. Pavithra、S. Ramya 和 Soma Prathibha。2019 年。《云安全问题和区块链调查》。《第三届国际计算和通信技术会议论文集》（ICCCT 19）。
IEEE，136-140。
[68] 彭丹、吴帆、陈桂海。2015 年。按工作量付费：基于质量的众包感知激励机制。第 16 届 ACM 国际移动自组织网络与计算研讨会论文集。177–186 页。

[69] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu. 2021. Privacy preservation in permis-
sionless blockchain: A survey. Digit. Commun. Netw. 7, 3 (2021), 295–307.
[70] 秦睿, 袁勇, 王飞跃. 2018. 区块链矿池选择策略研究. IEEE
Trans. Comput. Soc. Syst. 5, 3 (2018), 748–757。
[71] N. Ramkumar、G. Sudhasadasivam 和 KG Saranya。2020 年。区块链技术不同共识机制调查。国际通信与信号处理会议论文集（ICCSP 20）。
IEEE，0458–0464。

[72]梅尼·罗森菲尔德。2011 年。比特币矿池挖矿奖励系统分析。arXiv:1112.4980。取自https://arxiv.org/abs/1112.4980 。

[73] Sarwar Sayeed 和 Hector Marco-Gisbert。2019 年。评估区块链共识和安全机制
51%攻击。 Appl. Sci. 9, 9 (2019), 1788。
[74] Okke Schrijvers、Joseph Bonneau、Dan Boneh 和 Tim Roughgarden。2016 年。比特币矿池奖励函数的激励兼容性。国际金融密码学和数据
安全会议第 9603 卷。Springer，
477–498。

[75] 余如意。2020. 移动众包感知系统激励策略研究。IEEE 第 11 届软件工程与服务科学国际会议论文集（ICSESS 20）。IEEE, 511–514。

[76] Meng Shen, Junxian Duan, Liehuang Zhu, Jie Zhang, Xiaojiang Du, and Mohsen Guizani. 2020. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE J. Select. Areas Commun. 38, 6 (2020), 1229–1241 年。

[77] Yonatan Sompolinsky 和 Aviv Zohar。2018 年。比特币的潜在激励机制。Commun. ACM 61, 3 (2018),46–53。

[78] P. Swathi、Chirag Modi 和 Dhiren Patel。2019 年。使用分布式矿工行为监控防止区块链中的 sybil 攻击。第 10 届国际计算、通信和网络技术会议 (ICCCNT 19) 论文集。IEEE,1-6。

[79] Pawel Szalachowski、Daniël Reijsbergen、Ivan Homoliak 和 Siwei Sun。2019 年。Strongchain：透明且协作的工作量证明共识。第 28 届 USENIX 安全研讨会论文集（USENIX Security 19）。819–836。

[80] Itay Tsabary 和 Ittay Eyal。2018 年。差距游戏。ACM SIGSAC 计算机和通信安全会议论文集。713–728。

[81] Eric Ke Wang, Zuodong Liang, Chien-Ming Chen, Saru Kumari, and Muhammad Khurram Khan. 2020. PoRX: A IIoT区块链共识的声誉激励方案。Fut. Gener. Comput. Syst. 102 (2020),140–151。

[82] Eric Ke Wang, RuiPei Sun, Chien-Ming Chen, Zuodong Liang, Saru Kumari, and Muhammad Khurram Khan. 2020. 物联网系统的 X-repute 区块链共识协议证明。Comput. Secur. 95 (2020),101871。

[83] Jingzhong Wang, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang. 2018. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access 6 (2018), 17545–17556.

[84] Wenbo Wang、Dinh Thai Hoang、Peizhao Hu、Zehui Xiong、Dusit Niyato、Ping Wang、Yonggang Wen 和 Dong In Kim。2019 年。区块链网络中共识机制和挖矿策略管理调查。IEEE Access 7（2019 年），22328–22370。

[85] Yingjie Wang, Yang Gao, Yingshu Li, and Xiangrong Tong. 2020. A worker-selection incentive mechanism for opti- 以平台为中心的移动众包系统。Comput. Netw. 171 (2020),107144。

[86] 王玉峰, 黄洁, 金群, 马建华. 2017. ABT: 众包系统中一种有效的基于能力平衡团队的激励机制. 第五届先进云计算与大数据国际会议论文集 (CBD 17). IEEE, 220–225.

[87] 王云涛, 苏舟, 张宁. 2019. BSIS: 基于区块链的能源交付安全激励方案 车辆能源网络中。 IEEE Trans. Industr. Inf. 15, 6 (2019), 3620–3631。

[88] 王志鹏和吴倩红。2019 年。区块链中历史区块数据共享的激励机制。IEEE 第十届信息技术、电子和移动通信会议（IEMCON 19)论文集。IEEE，0913–0919。

[89] 吴阳欣,郑培佳,郭建婷,张伟,黄继武。2018 年。基于区块链和 ISODATA 的可控高效内容分发框架。第 17 届 IEEE 计算和通信信任、安全与隐私国际会议/第 12 届 IEEE 大数据科学与工程国际会议（TrustCom/BigDataSE 18)论文集。IEEE,1698–1701。

[90] 肖阳、张宁、楼文静、侯 Y. Thomas。2020 年。区块链网络分布式共识协议调查。IEEE 通信调查导师。22,2 (2020),1432–1465。

[91] Hong Xie、John CS Lui 和 Don Towsley。2016 年。区块链的激励与声誉机制设计与分析 在线众包系统。ACM Trans. Model. Perf. Eval. Comput. Syst. 1, 3 (2016), 1–27。

[92] Chang Xu, Yayun Si, Liehuang Zhu, Chuan Zhang, Kashif Sharif, and Can Zhang. 2019. Pay as how you behave: A 移动众包感知的真实激励机制。IEEE IoT J. 6, 6 (2019), 10053–10063。

[93] 郑岩, 李鹏, 魏峰, Laurence T. Yang. 2021. Social-chain: 基于信任模型的去中心化信任评估 普适社交网络中的区块链。ACM 互联网技术汇刊 21, 1 (2021),1–28。

[94] 杨德军,方曦,薛国良。2013 年。k 匿名位置隐私的真实激励机制。IEEE 国际计算机通信会议论文集（INFOCOM 13）。IEEE,2994–3002。

[95] 尹波、吴玉蕾、胡天石、董嘉庆和蒋泽勋。2019 年。基于区块链的安全信息交换的车联网高效协作和激励机制。IEEE IoT J. 7, 3 (2019)，1582–1593 年。

[96] Jiayuan Yin, Changren Wang, Zongyang Zhang, and Jianwei Liu. 2018. Revisiting the incentive mechanism of bitcoin-NG. In Australasian Conference on Information Security and Privacy, Vol. 10946. Springer, 706–719.

[97] 余兆阳,刘晓光,王刚。2018 年。基于 P2P 的区块链共识与激励机制研究。IEEE 第 24 届并行与分布式系统国际会议论文集（ICPADS 18）。IEEE,1010–1015。

[98] Xinglin Zhang, Zheng Yang, Wei Sun, Yunhao Liu, Shaohua Tang, Kai Xing, and Xufei Mao. 2015. Incentives for 移动人群感知：一项调查。IEEE 通信调查导师。18,1（2015），54-67。

[99] 郑家伟,董学文,刘启航,朱星辉,童伟。2019 年。基于区块链的安全数字资产交换方案,具有 QoS 感知激励机制。IEEE 第 20 届高性能交换和路由国际会议（HPSR 19)论文集。IEEE,1-6。

[100] Bowen Zhou、Satish Narayana Srirama 和 Rajkumar Buyya。2019 年。基于拍卖的激励机制,用于混合云的开发。气溶胶移动云。 J. Syst. Softw. 152 (2019), 151–164。

[101] 周欢、欧阳雪、任志杰、苏金姝、Cees de Laat 和赵志明。2019 年。基于区块链的可信云服务级别协议执行见证模型。IEEE 国际计算机通信会议论文集（INFOCOM 19）。IEEE,1567–1575。

[102] Zhi Zhou, Fangming Liu, Shutong Chen, and Zongpeng Li. 2018. A truthful and efficient incentive mechanism for 绿色数据中心的需求响应。IEEE 并行分布系统汇刊 31, 1 (2018), 1–15。

[103] 朱烈皇,董晖,沈萌,盖可可。2019. 基于区块链的医疗数据共享的 Shapley 值激励机制。IEEE 第五届云端大数据安全国际会议（BigDataSecurity 19）、IEEE 高性能智能计算国际会议（HPSC 19)和 IEEE 智能数据与安全国际会议（IDS 19)论文集。IEEE，113–118。

[104] Yevhen Zolotavkin、Julian Garcia 和 Joseph K. Liu。2019 年。工作量证明加密货币中的时间相关决策和去中心化。IEEE 第 32 届计算机安全基础研讨会 (CSF 19) 论文集。IEEE,108–10813。

收到日期:2021 年 3 月 15 日;修订日期:2022 年 4 月 8 日;接受日期:2022 年 5 月 13 日