计算机科学
COMPUTER SCIENCE

元宇宙中区块链技术的应用、挑战和新策略

孙力

引用本文

孙力. 元宇宙中区块链技术的应用、挑战和新策略[J]. 计算机科学, 2024, 51(7): 373-379.

SUN Li. Application,Challenge and New Strategy of Block Chain Technology in Metaverse[J]. Computer Science, 2024, 51(7): 373-379.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230800072

元宇宙中区块链技术的应用、挑战和新策略

孙　力
江南大学江苏省“互联网+教育”研究基地　江苏 无锡 214122

摘　要　近年来,虚拟现实、人工智能等技术的发展,催生出了以沉浸式互联网为核心的元宇宙系统框架。在分析架构元宇宙环境核心技术所面临挑战的基础上,分析了融入区块链技术对元宇宙系统及其相关核心技术的作用,指出了现有区块链运行机制对其在元宇宙环境中应用带来的延迟性和扩展受限等问题。运用分片机制和斯塔克伯格博弈理论,提出了一种新的基于区块链的元宇宙应用策略,设计了相应的用户激励方案,并通过数值实验验证了该方案的有效性。最终,通过分析该策略的优势和面临的问题明确了后续的研究方向。

关键词:元宇宙;区块链;智能合约;分片机制;斯塔克伯格博弈
中图分类号　TP311

Application,Challenge and New Strategy of Block Chain Technology in Metaverse

SUN Li
Research Base of Internet+ Education,Jiangnan University,Wuxi,Jiangsu 214122,China

Abstract　In recent years,with the development of virtual reality,artificial intelligence and other technologies,metaverse system framework with immersive Internet as the core has emerged. Based on the analysis of the challenges faced by the core technologies of metauniverse environment,this study proposes the role of integrating blockchain technology on the metaverse system and its related core technologies,and points out the delays and scaling limitations of the existing blockchain operating mechanism on its application in the metaverse environment. Using sharding mechanism and Stackelberg game theory,this study proposes a new blockchain-based metaverse application strategy,designs the corresponding user incentive scheme,and verifies the effectiveness of the scheme through numerical experiments. Finally,based on the advantages and problems of this strategy,the future research direction is clarified.

Keywords　Metaverse,Blockchain,Smart contract,Sharding mechanism,Stackelberg game

1　引言

元宇宙概念的起源可以追溯到1992年,指的是下一代互联网应用程序,旨在创建实体对象,包括用户和应用程序,通过数字化身进行交互的虚拟3D环境[1]。由于未来互联网的巨大潜力,元宇宙吸引了研究者极大的关注。

元宇宙环境架构的核心技术主要包括:(1)通过专门的传感器,从各类物联网设备中收集数据,作为与现实世界数据接口的物联网技术;(2)通过实时数据形成与实际世界同步的用户模型,并能在用户进入元宇宙环境之前预测他们的需求[2],把现实世界镜像到虚拟世界中去的数字孪生技术;(3)自动分析用户画像,并渲染成元宇宙中用户数字表征的人工智能技术;(4)应对元宇宙中从客户服务到数据分析的数据更多样化、数据量更大、产生速度更快等特征,提升用户的数据收集、处理和组织能力的大数据技术;(5)利用传感器结合现实世界的物体,实现虚拟和物理对象的实时表示,使用户能够同时沉浸式地体验真实和虚拟世界的扩展现实技术,包括VR和AR等。

这些核心技术的综合应用带来了新的需求,比如:(1)物联网技术带来的非结构化和实时的数据分析需求,物联网设备在虚拟世界中跨平台的数据共享能力和跨不同虚拟世界的数据存储方式提升等[3];(2)数字孪生模型为了提高准确性,实现相互之间在不同虚拟世界中的交互、连接和协作,检测并响应虚拟世界的变化,而带来的对于数据高质量、消除僵尸网络和其他恶意软件对数据安全影响的需求[4];(3)降低不法分子利用人工智能技术参与元宇宙交互以非法盗取资源,或者人工智能本身犯错的可能性;(4)元宇宙中近乎翻倍并仍在继续增长的数据量,以及各种应用程序生成数据的异构性,将给大数据技术带来的巨大挑战;(5)用户能够同时沉浸式地体验真实和虚拟世界,要求元世界必须保证敏感信息的私密性,用户应用程序之间必须随时访问、交换和传输这些数据。同时,当各种利益相关者和第三方参与到数据共享过程中时,元宇宙

到稿日期:2023-08-14　返修日期:2024-01-15
基金项目:国家自然科学基金(61972182)
This work was supported by the National Natural Science Foundation of China(61972182).
通信作者:孙力(lisun@jiangnan.edu.cn)

必须使数据透明。以上需求可以归纳为:大规模计算资源,超低延迟要求,应用程序之间的互操作性,大规模数据存储,数据高质量,以及用户和数据的安全隐私问题等。

为了应对元宇宙世界新的需求,区块链是一个有前景的解决方案[1]。它的智能合约机制[5],使得其可以自动管理元宇宙环境中各类实体之间,比如元宇宙服务提供商(Metaverse Service Provider,MSP)、元宇宙用户(Metaverse User,MU)和数字内容创作者之间的复杂交互;它的防篡改和可追溯等特性[6],可以提高数据质量,保护元宇宙应用程序中的数字资产;它的非对称密钥加密和数字签名机制[6],可以增强用户的隐私和匿名性。

然而,区块链在元宇宙环境中的应用也面临着各种挑战[1]。目前典型的区块链网络采用的共识机制,如工作量证明(PoW)和权益证明(PoS),延迟现象较为明显。另外,共识机制使得区块链网络的可扩展性受到限制。

由于区块链在元宇宙中的应用刚刚开始,目前的研究大多关注环境资源的分配,尚未涉及到应用区块链促进元宇宙中的各类互动、数字资产交易以及服务销售等行为,对延迟现象的研究相当有限[7];区块链的可扩展性问题在当前的研究中也均未见到解决方案[8]。这两个问题将会成为元宇宙环境中区块链的应用瓶颈。本研究的目的是在梳理元宇宙及区块链的基本概念和主要特征的基础上,分析区块链在元宇宙环境中的应用前景及所面临的挑战,并提出相应的解决策略。

2 区块链融入元宇宙的前景及挑战

2.1 区块链综述

典型区块链的架构、相应功能、关键技术以及与元宇宙之间的相关性如表1所列。

表1 区块链的分层结构

Table 1 Hierarchical structure of blockchain

层次	功能	关键技术	与元宇宙的相关性
应用层	提供应用场景	可编程货币、金融、社会	支撑并有序管理元宇宙经济体系
合约层	定义约束条件	脚本代码、算法机制、智能合约	为参与实体提供可信赖环境,实现价值交换
激励层	鼓励节点参与	发行机制、分配机制	增强元宇宙系统可扩展性
共识层	对区块数据有效性达成共识	PoW,PoS,Dpos	解决元宇宙交易信用问题
网络层	节点间信息交互	P2P网络、数据传输和验证机制	为系统数据的传输、校验提供网络支持
数据层	安全实现数据存储、账户交易	数据区块、链式结构、非对称加密、时间戳、哈希函数、Merkle树	为用户提供数据的可追溯性和保密性

2.2 区块链在元宇宙中的应用前景

融入区块链对于元宇宙环境的作用如下所述。

2.2.1 确保数据隐私和安全

元宇宙环境在运行过程中会收集大量数据,相关组织或应用程序需要这些数据来形成服务系统,以此为用户提供服务体验。区块链通过身份验证、访问控制和共识机制等手段为用户提供对其数据的完全控制,从而保护用户的数据隐私;通过非对称加密和哈希函数,确保元宇宙中数据的传输安全。

2.2.2 确保数据质量

元宇宙环境从多个应用程序中收集数据,对应的人工智能模型依靠这些数据为用户做出关键决策。决策质量的高低依赖于真实世界中用户共享的数据质量。区块链提供的交易全流程跟踪和相关的用户验证,将提高元宇宙中的数据质量。

2.2.3 实现无缝和安全的数据共享

元宇宙通过AR和VR设备,形成一个互联和沉浸式的环境。元宇宙的优势在于它对数字和物理对象的融合,而融合的成功取决于AR和VR数据的无缝共享。区块链的数据编码系统使元宇宙的数据共享无缝且安全。

2.2.4 增强数据互操作性

元宇宙中的用户需要访问和持有多个虚拟世界中的数字资产,同时使用各种应用程序。由于构建多个虚拟世界的环境不同,因此它们之间的数据互操作会受到影响。区块链的互操作性,可以通过跨链协议实现在不同虚拟世界中的两个或多个区块链上交换数据。

2.2.5 确保数据完整性

元宇宙中的数据必须保持一致和准确。数据完整性受损,会影响用户对元宇宙应用的信心。区块链的不可篡改性确保了元宇宙数据的完整性。

区块链的去中心化、数据加密、匿名性、防篡改、可追溯和自动执行等特性同时也可赋能元宇宙的核心技术。

(1)赋能元宇宙中的物联网技术

元宇宙中的物联网设备能够通过跨链网络进行数据通信,产生虚拟世界中不可篡改的交易记录,在多个虚拟世界中安全地共享和存储真实数据,所有的交易都会被记录和验证。元宇宙应用程序和用户能够在去中心化的情况下共享、跟踪和访问区块链分类账户中的物联网数据。

(2)赋能元宇宙中的数字孪生技术

真实世界对象将数据存储在区块链上,并使用智能分布式账本同步到元宇宙中的数字孪生模型。同时,将数字孪生部署在区块链上,将区块链与人工智能系统合并,跟踪传感器数据。数字孪生体的每一个动作都将被记录为区块链上一次不可篡改的交易。如此形成的数字孪生模型将是高效、精确和抗攻击的。

(3)赋能元宇宙中的人工智能技术

人工智能系统通过区块链技术获取、存储和使用高质量的真实数据进行渲染建模,保证所建立的模型不受损害。通过零知识证明,用户可以使应用程序确定某些数据是准确的,而无需再使用这些数据进行人工智能建模训练。区块链分类账户提供的审计跟踪,使得元宇宙中发生的所有交易的责任易于确定,使用户能够在元宇宙中识别关键要素,同时保护他们的隐私,保证其资源不被人工智能产生的虚假化身所盗用。

(4)赋能元宇宙中的大数据技术

区块链将有助于确保元宇宙中的数据流具有较高的质量,包括从可信数据源收集数据,减少无用或有害数据的

数量,保证数据所有者对数据的完全控制,限制第三方的数据操作等。同时,使元宇宙中的数据处理保持高效的沟通和协作,降低实现数据分类和为分析应用程序创建数据集等的时间和成本,以及数据污染的风险。

(5)赋能元宇宙中的扩展现实技术

区块链的分布式账本、零信任机制和跨链技术,将支持AR/VR应用程序的记录验证、错误数据来源追踪,以及不同虚拟世界之间安全的数据共享。区块链的共识机制能保证数据的防篡改,使数字资产核查和所有权转移透明,确保AR/VR利益相关者之间的信任。

2.3　区块链在元宇宙应用的挑战

2.3.1　巨大的算力需求

元宇宙环境中拥有大量用户,他们在虚拟世界中频繁交易,同时使用各种元宇宙环境之内或之间的应用程序。在元宇宙环境中工作的区块链节点,至少是承担验证任务的节点,这些节点要处理大量交易,因此需要在本地存储所有历史交易,这将给这些节点带来巨大的数据处理负担和算力资源需求。

2.3.2　事务处理的延迟性

满足人类习惯的互联网应用程序的端到端延迟通常在几十毫秒到几百毫秒之间;形成沉浸式体验的、基于三维显示和交互的元宇宙应用程序需要在10 ms内保持稳定,以避免产生眩晕现象。区块链共识过程的巨大算力需要,将导致元宇宙环境中基于区块链的交易确认过程与当前的比特币和以太坊等典型区块链网络相仿。采用工作量证明(PoW)的比特币每秒只能确认7～10笔交易[6],采用权益证明(PoS)的以太坊每秒交易不超过15笔[8],显然无法满足元宇宙事务对低确认延迟的要求。

2.3.3　元宇宙环境的扩展性限制

典型的区块链共识机制,比如PoW或PoS,其验证节点的产生依赖于节点算力或权益的竞争,这样会阻碍包括计算机、服务器和算力资源在内的更多资源快速地加入区块链网络,限制了元宇宙环境的可扩展性。

2.3.4　其他挑战

区块链在元宇宙架构中的应用面临的挑战是:如果分类账户上的智能合约存在非法性,区块链的匿名性和智能合约自动执行会使元宇宙中所有非法服务交易的追踪变得困难。此外,要使人工智能系统能够适应构建在不同区块链上的元宇宙环境,还需要实现跨链转换功能。再者,如果在新的区块链平台中不能有效地解决增强的人工智能技术带来的深度伪造问题,将妨碍VR/AR技术在智能手机和电脑中的应用普及。

综上所述,融入区块链技术将有益于应对元宇宙环境架构本身以及相关核心技术应用带来的挑战。但是,现有的区块链共识协议和机制带来的巨大算力需求、延迟和扩展限制等问题,阻碍了区块链在元宇宙中应用的发展,需要新的共识协议和机制来满足元宇宙交易的严格要求。

3　基于区块链的元宇宙应用新策略

为了应对以上挑战,本研究提出一种新的基于区块链的元宇宙应用策略。该策略可以促进元宇宙环境中元宇宙服务提供商(MSP)和用户(MU)之间的各种交互;根据应用需求有效管理资源;鼓励MU向区块链和元宇宙应用程序贡献算力资源,为MSP和MU带来利益。它的优势是不需要通过可信任的第三方,而是通过智能合约机制,使得MSP和MU之间的各种交互自动实现。它的创新之处在于引入分片机制[9],将区块链划分成更小的独立单元——分片,分片的数量和大小依据元宇宙应用的实际需求决定,允许MSP动态分配资源,有效解决了元宇宙应用大量数据处理带来的延迟性问题。另外,元宇宙应用需要大量计算资源,本研究基于斯塔克尔伯格博弈(Stackelberg Game)理论[10],设计了一种激励机制。MSP可以利用MU的贡献资源来支持区块链运营以及满足元宇宙应用需求;同时,由于其贡献可获得奖励,将会吸引更多用户加入元宇宙,有效解决扩展性限制问题。

3.1　策略概述

该策略的系统架构分为3层,如图1所示。

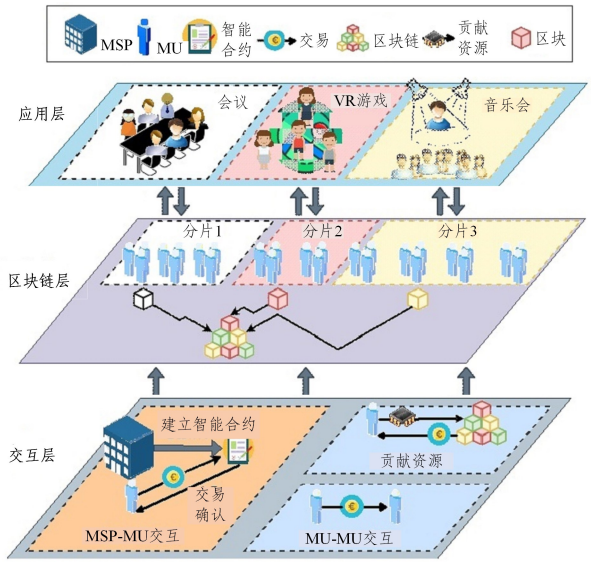

图1　元宇宙区块链应用系统架构

Fig. 1　Architecture of meta-universe blockchain application

最上层是应用层,包括元宇宙环境中MSP向MU提供的各类应用程序或服务。中间层是区块链层,由MSP管理的、引入了分片机制的区块链作为MSP和MU之间、MU之间以及MU向元宇宙应用贡献计算资源等所有交互的平台,这些交互都以交易形式记录在区块链中。同时,每个MU在系统中都有一个账户和相应的数字资产,例如代币和服务使用权限,其资产的变化也以交易形式记录在区块链中。最底层是交互层,交互活动包括MSP和MU之间应用或服务信息的交流,MU向MSP支付费用,获得对相应应用或服务的使用权限;MU向区块链贡献计算资源以获得MSP的奖励;MU之间进行的数字资产的转移和交换等。

3.2　应用层

元宇宙环境中包含了各种可以在虚拟环境中运行的应用和服务,例如虚拟会议、VR游戏和虚拟音乐会等。每一种应用程序或服务都有不同程度的数据处理需求,同时有不同数量的用户参与。例如,虚拟会议通常有比游戏更多的参与用户数,同时也有较大的数据量产生;而虚拟音乐会一般会有

更多的用户参与，也意味着有更多的数据处理需求。尤其是，在诸如虚拟会议等应用中，用户的需求可能会根据时间和地理位置大幅波动。例如，当欧洲会议正在进行时，东亚的大多数用户都在睡觉。应用或服务的用户数和数据量将是后续处理交易的区块链的分片依据。

3.3 区块链层

本策略将区块链网络划分为更小的子网络，即分片；每个分片都通过独立的共识过程，创建新的区块；新区块的创建速度将比没有分片的区块链网络成倍提升。随着应用需求的增长，可以划分更多的分片，以确保为用户提供高质量、低延迟的服务。

依据网络分片、交易分片和状态分片这 3 种主流的区块链分片方式[9]，本策略采用基础的网络分片，同时依据交易事务处理能力和算力需求两个方面的实际情况，根据应用、服务或用户的实际需求来创建大小不同的分片。例如，每个应用或较大应用的每个用户区域创建一个分片。MSP 可以根据需求将其计算资源适当地动态分配给每个分片。

在一个应用或服务结束后，将依据实际情况的变化进行分片重配置，这样既能允许新用户的加入，又能保证分片后区块链网络的安全性。本策略的分片策略主要依据应用和用户区域而定，相对较为固定；目前主流分片重配置方式[9]中，二次全随机重配置虽然安全性最好，但用户组合的随机性带来的交易验证时延问题显然是不合适的；针对应用/服务和用户的特征和变化，可以采用部分重配置或自由选择重配置的方法。例如：对用户活跃度要求较高的虚拟会议，可以采用部分重配置方法；针对用户加入/退出较快而活跃度要求不高的虚拟音乐会，可以采用自由选择重配置方法。

分片后，区块链的交易共识过程分为片内共识和跨片共识两个进程[9]。片内共识以同一分片内的各个节点为交流单位，依据所在分片的共识协议完成共识过程。片内共识协议主要分为基于 BFT 和基于 PoW：对于用户数量比较固定但即时数据处理要求较高的应用，比如虚拟会议，一般采用基于 BFT；对于用户数量变化较大而即时数据处理要求不高的应用，比如虚拟音乐会，一般采用基于 Pow。跨片共识以区块链上的各个分片为交流单位，执行共同的跨片协议实现共识。交易原子化、交易集中化和类路由协议是跨片共识的主要方式[9]。对于规模较小，即分片数量较少的元宇宙环境，一般采用交易集中化；对于规模较大，即分片数量较多的元宇宙环境，一般采用类路由协议。

3.4 交互层

3.4.1 MSP 与 MU 的交互

MSP 和 MU 之间的交互基本通过区块链完成，这有助于保证用户的隐私和匿名性，同时实现交互的自动化。例如，MSP 可以依据预先定义的智能合约，在区块链上广播其元宇宙会议服务的费用和其他选项，比如人数和主题；MU 向智能合约发送各种指定选项（例如参与者和时间）的交易；如果支付满足预设条件，智能合约将被触发自动执行，向相关参与者发送交易确认信息，这些信息后面将作为进入虚拟会议室的凭证。

3.4.2 MU 之间的交互

除了实现以上自动化的交互，区块链还可作为一个不可篡改的数据库来存储用户的数字资产。另外，该策略还支持用户无需通过第三方信任机构，进行相互之间数字资产的转移和交换。例如，购买了虚拟音乐会门票但无法参加的用户可以将其转售或赠送给另一个用户。该策略可以通过智能合约或区块链交易，以安全和透明的方式支持此类交互活动。

3.4.3 MU 贡献资源

元宇宙应用最显著的特点是巨大的算力需求。尽管用户端设备能力的快速发展可以部分规避这一问题，但仍有一些应用需要用户在统一的运行环境中相互交互，比如会议和游戏。这就需要来自区块链以外的算力资源的支持，比如用户。而 MSP 又不能直接将 MU 自身资源分配给区块链分片，因此元宇宙管理策略应该鼓励 MU 将自身的算力资源贡献给元宇宙应用，同时换取代币或指定元宇宙应用使用权限等数字资产作为奖励。MSP 根据每个分片的实际需求，设置奖励总额度。MU 可以根据其算力资源贡献的实际情况，按照预先制定的奖励分配规则，例如份额分配制[11]，获得奖励。

然而，MU 是理性的，其目标是利益最大化。他们可能会将资源集中在奖励额度较高的分片上。如果依据按份额奖励的原则，一个分片加入的 MU 越多，单个 MU 获得的奖励就越少，MU 之间存在利益冲突。因此，激励机制应当在 MSP 奖励额度确定的前提下，既使 MU 获得最佳收益（获得奖励-贡献成本），又使 MSP 获得最佳收益（获得贡献-奖励代价）。

在区块链分片结构下设计节点资源贡献的激励机制，目前尚未见公开的研究成果。Cai 等为了鼓励用户延迟蜂窝网络业务转而接入 WiFi 网络，运用斯塔克博格（Stackelberg）博弈，设计出了可以有效降低包括蜂窝网络拥塞和奖励用户代价在内的运营商总代价的激励机制[12]；Wang 等在基于实用拜占庭机制的区块链分片架构下，应用契约理论，设计了实现区块链使用者包括服务收益、可靠性和预算代价在内的效益最大化的激励机制[13]。以上研究成果为本研究提供了可行性依据。

4 用户资源贡献的奖励方案

4.1 系统描述与表征

本研究设计的系统是一个按照元宇宙应用的数量分成 M 个分片的区块链，以数列 $M=(1,\cdots,m)$ 表示，数列 $N=(1,\cdots,n)$ 表示将为元宇宙应用程序贡献资源的 N 个用户，每个用户具有的资源贡献能力以数列 $R=(R_1,\cdots,R_n)$ 表示，用户 n 为分片 m 贡献的资源量用 r_n^m 表示，用户 n 贡献资源的单位成本用 C_n 表示，MSP 为每个分片设置的用户贡献资源奖励额度用数列 $P=(P_1,\cdots,P_m)$ 表示。

在实际运营中，MSP 首先确定并公布每个分片的奖励额度 P，随后 MU 将决定为每个分片贡献资源的量。因此，MSP 与 MU 之间的交互可以用单主（Leader-MSP）多从（MUs）的 Stackelberg 博弈模型 G 表示[12]。在 G 中，首先 MSP 宣布对分片 m 的奖励策略 P_m，然后用户将决定贡献多少资源。S_n 表示用户 n 的所有可能资源贡献策略的集合，s_n^* 表示它的最佳对策，即在 MSP 奖励策略 s_L 给定的情况下，

用户 n 获得最佳奖励的资源贡献策略。

用户 n 的收益函数为：

$$U_n(s_n^*, s_L) \geqslant U_i(s_n', s_p), \forall s_n' \in S_n \tag{1}$$

MSP 基于 MU 最佳对策 s_n^* 的 Stackelberg 博弈策略表示为：

$$s_L^* = \arg\max_{s_L = P} U_L(s_L, s_n^*) \tag{2}$$

其中，$U_L(s_L, s_n^*)$ 是 MSP 的收益函数。Stackelberg 模型解可以用元组 (s_L, s_n^*) 定义，其对应的收益元组 (U_p^*, U_i^*) 是博弈模型 G 的 Stackelberg 均衡。G 可以分为两个阶段的子博弈，第一阶段 G_L 表示 MSP 公布奖励策略；第二阶段 G^F 表示 MU 根据 MSP 的奖励策略来决定自己的对策。我们基于向后归纳分析法[12]来确定 G 的 Stackelberg 均衡。

4.2　用户的子博弈 G^F

在上述系统中，用户 n 向分片 m 贡献的资源为 r_n^m，$m \in M$，则用户 n 对整个区块链的资源贡献策略为：$r_n^* = \sum_{m=1}^{M} r_n^m \leqslant R_n$。MSP 公布的对分片 m 的奖励额度为 P_m，若按每个用户的资源贡献份额进行奖励，则用户 n 由于向分片 m 贡献资源 r_n^m 而获得的奖励表示为：

$$U_n^m = \frac{r_n^m}{r_n^m + \sum_{i \in N_{-n}} r_i^m} P_m \tag{3}$$

其中，N_{-n} 是除用户 n 以外的所有用户集合。用户 n 在分片区块链中的收益函数为其获得的奖励扣除运行成本后的多余部分，表示为：

$$U_n = \sum_{m=1}^{M} U_n^m = \sum_{m=1}^{M} \frac{r_n^m}{r_n^m + \sum_{i \in N_{-n}} r_i^m} P_m - C_n \sum_{m=1}^{M} r_n^m \tag{4}$$

4.3　MSP 的子博弈 G_L

MSP 的收益函数为 MSP 获得所有 MU 的资源贡献去除给予 MU 奖励后的剩余部分，表示为：

$$U_L = \sum_{m=1}^{M} (\alpha_m \ln(\sum_{n=1}^{N} r_n^m) - P_m) \tag{5}$$

其中，α_m 是优先系数，表示 MSP 在每个分片资源分配的优先级，分片的资源需求越大，其 α_m 越高；ln 函数可以防止一个分片的用户资源贡献过度集中。MSP 的最优策略 s_L^*，即能够给予最大贡献的 MU 最高奖励的奖励策略，可以表示为：

$$s_L^* = \arg\max_{s_L = P} U_L(s_L, s_n^*) = \sum_{m=1}^{M} (\alpha_m \sum_{n=1}^{N} r_n^{*m} - P_m) \tag{6}$$

4.4　Stackelberg 均衡的存在性和唯一性

由于篇幅限制，Stackelberg 均衡的存在性和唯一性证明简述如下：

(1)根据向后归纳分析法，如果 S_n 是一个紧凸集，$u_n(\forall n \in N)$ 是拟凹函数时，则至少存在一个纳什均衡[12]。本研究中 S_n 明显是紧凸的，通过求 U_n^m 的二阶导数，发现它总是负的，因此 U_n 是严格凹的，由此证明了均衡的存在性。

(2)根据罗森定理[14]，若能证明 $[\boldsymbol{G}(s,\omega) + \boldsymbol{G}^{\mathrm{T}}(s,\omega)]$ 对于一个固定的 ω 是负定的，则可证明均衡的唯一性。类似于文献[15]中定理 4 的证明，可以将 $\boldsymbol{G}(s,\omega)$ 和 $\boldsymbol{G}^{\mathrm{T}}(s,\omega)$ 重写为一个负半定矩阵和一个负定矩阵的和，则 $[\boldsymbol{G}(s,\omega) + \boldsymbol{G}^{\mathrm{T}}(s,\omega)]$ 是负定的，由此证明了均衡的唯一性。

4.5　算法设计

为了找到给定模型 G 的 Stackelberg 均衡，本研究设计了如算法 1 所示的迭代算法。

算法 1　寻找 Stackelberg 均衡的迭代算法

```
repeat
max←0, Pm ←1, m∈M, P* ←P
CALCULATEUL(P, max)
for i := 1 to M do
P_i ←P_{i+1}
CALCULATEUL(P, max)
end for
until Stopping criteria
function CALCULATE UL(P, max)
repeat
for n : 1 to N do
Find rn *
end for
until No follower changes strategy
if UL>max then
max ←UL, P* ←P
end if
return max
end function
```

算法分为两部分，描述如下：

(1)依据式(3)－式(6)，设计函数 $CALCULATE\ U_L(P, max)$，其中 P 为 MSP 的奖励策略，max 作为 MSP 最佳收益的存储变量。

①函数的输入为 MSP 的奖励策略 P。

②循环开始，固定除 n 以外其他用户的资源贡献策略，通过 matlab 的 $fmincon$ 函数，获得用户 n 的最佳贡献策略 r_n^* 和收益 U_n。

③固定用户 n 的策略，继续获取其他用户的最佳策略和收益。

④当没有用户更新策略时，循环终止。

⑤计算 MSP 在当前奖励策略 P 时的收益 U_L，如果 U_L 大于存储变量 max，则更新 max。

(2)对于给定的分片架构区块链，通过迭代算法，找出 MSP 的最优收益 U_L 和对应的奖励策略 P^*，以及用户的最优贡献策略和最优收益。

①变量初始化。设定每个分片的奖励为 1，获得 MSP 奖励策略的初始值 P，存储变量 max 为 0。

②调用函数 $CALCULATE\ U_L(P, max)$，计算 MSP 在当前奖励策略 P 时的收益 U_L。

③循环计算当每个分片奖励额度增加 1 时，相应的 MSP 收益 U_L。

④当一个新的最优收益 U_L 出现时，记录 U_L 和对应的各类策略。

⑤当出现 Stackelberg 均衡收敛时，算法结束。

⑥获得相应 MSP 的最优收益 U_L 和对应的奖励策略 P^*，以及各用户的策略 r_n^* 和收益 U_n。

5　奖励策略的数值实验及结果

本研究以 MATLAB 为实验环境，设定系统有 4 个用户

和一个有 2 个分片的区块链系统，用户的资源贡献能力为 $R=[100,200,300,500]$，贡献资源的单位成本为 $C=[0.2,0.1,0.3,0.2]$，分片优先级为为 $\alpha=[4,6]$。通过上述设计的算法来分析用户的对策变化以及对 MSP 策略和收益的影响。实验中首先考查一个用户的收益函数，并给出了当其他用户和 MSP 的策略固定时，该用户的最优对策。其次，使用函数 $CALCULATEU_L(P;max)$，显示用户对策如何向唯一的G^F的 Stackelberg 均衡收敛的过程。最后，利用设计的迭代算法模拟博弈过程，得到 MSP 的收益函数和 Stackelberg 均衡。

在其他用户和 MSP 的策略都固定的情况下，用户 n 的收益函数U_n趋势和最优策略如图 2 所示。在本例中，MSP 的奖励额度固定为 $P=[1\,000,2\,000]$，用户 n 的资源贡献能力 $R_n=100$。可以看到，当用户 n 向分片 1 的资源贡献 $r_n^1=41.42$和向分片 2 资源贡献$r_n^2=46.41$时，它的最优收益$U_n^*=121.68$。值得注意的是，$r_n^1+r_n^2<R_n$，用户 n 并没有贡献其所有的资源，这是由于在达到一定的阈值后，贡献更多的资源所带来的回报就会低于所产生的成本。这个阈值取决于用户 n 的单位成本 C_n 以及 MSP 和其他用户的策略。

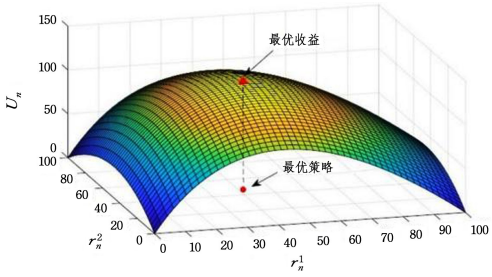

图 2 用户收益函数趋势

Fig. 2 Trend of user revenue function

图 3 显示了各用户的资源贡献策略随着迭代次数的增加而向均衡状态收敛的情况。在本例中，我们将 MSP 对分片的奖励策略固定为 $P=[100,200]$。

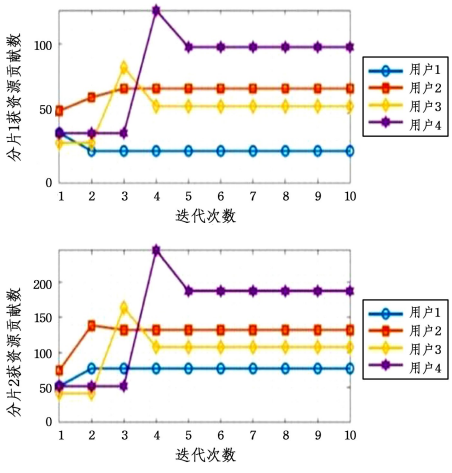

图 3 用户策略向均衡收敛的趋势

Fig. 3 User policies converge towards equilibrium

可以看到，在 5 次迭代后，用户的资源贡献策略趋向均衡。在均衡状态下，所有用户对奖励高的分片 2 的贡献均高于奖励低的分片 1；同时，用户 1 和 2 将它们所有的资源都贡献给了分片 1 和 2，而用户 3 和 4 则没有。原因是用户 1 和 2 的单位成本较低，它们可以从单位资源贡献中获得更多的收益。同时，由于单位成本的差异，尽管用户 2 资源贡献能力低于用户 3，但它实际贡献的资源多于用户 3。

图 4 显示了 MSP 的收益函数U_L和策略 $P(P_1,P_2)$的对应变化情况。可以看到，当 MSP 设置分片 1 的奖励策略 $P_1=4$，分片 2 的奖励策略$P_2=6$ 时，它的最优收益达到$U_L=20.35$，此时 MSP 最优策略$P^*=[4,6]$。由于设置的分片优先系数 $\alpha=[4,6]$较小，用户对分片的资源贡献不够充分。从图 5 可以看到，当将分片的优先系数提升到 $\alpha=[10,15]$时，MSP 最优策略$P^*=[11,15]$，最优收益可以增加到原先的 3 倍以上。由此可见，由区块链分片方案决定的 α，对于 MSP 调控每个分片需获得用户的资源贡献量和给予用户的奖励之间的关系，是一个非常有效的参数，即区块链的分片方案不仅可以有效地解决数据处理的延迟性问题，同样可以有效地吸引用户贡献算力资源，解决元宇宙环境的扩展性问题。

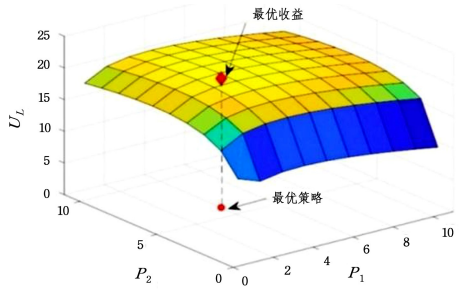

图 4 MSP 收益函数 1

Fig. 4 MSP income function 1

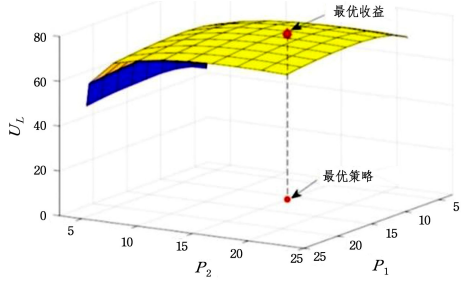

图 5 MSP 收益函数 2

Fig. 5 MSP income function 2

结束语 元宇宙是互联网的下一个发展阶段。相对于第一代互联网的互联互通，第二代互联网的随时随地，元宇宙又增加了沉浸、参与以及虚实互联与共融等新的关键要素。元宇宙＋传统行业应用将比现有的互联网＋传统行业应用更加精彩纷呈。

本研究分析指出，在元宇宙环境中应用区块链技术具有提高数据质量和安全性，增强数据互操作性，确保数据完整性以及实现数据无缝、安全共享等优势；以及支撑元宇宙架构核心技术应对挑战的能力。同时，现有的区块链共识协议和机制将无法满足拥有大量用户和数据处理任务的元宇宙应用所要求的低延迟性，并影响其可扩展性等。

据此，本研究提出了一种新的应用策略。该策略通过分析 MSP 与 MU 的行为，运用分片机制，将区块链网络依据搭载的元宇宙应用实际情况分成更小的子网络。该策略相比现有区块链在元宇宙中的应用优势可以归纳为：(1)沿袭了区块链的

固有优势，可以实现单 MSP 和多 MU 之间的智能化和可信任的交互行为；(2)分片策略可以实现各区块链子链的并行处理，实现更高的数据吞吐量，有效地满足元宇宙应用的低延迟性需求；(3)分片策略使区块链能够适应更多的用户和交易。

同时，依据 Stackelberg 博弈理论，本研究提出了一种帮助单 MSP 依据元宇宙应用实际算力需求，有效地激励和配置用户资源的经济模型，模型的有效性通过 MATLAB 环境中的数值实验得到了验证。该模型可以激励用户向元宇宙应用程序贡献自身计算资源，既可缓解元宇宙环境的巨大算力需求，也可吸引更多用户加入。同时，分片技术使得每个节点只需存储和处理其所属分片的数据，而不是整个区块链，这降低了运行节点的硬件要求。以上两点可以有效地提升元宇宙环境的可扩展性。

然而，分片技术也带来了新的挑战。首先，分片都是独立的，分片间的相互通信要通过增加跨分片的通信机制来实现，这会增加整个区块链的复杂性，降低网络效率。解决方案是通过分片策略和状态通道的结合，即通过用户之间建立双方或多方的双向通信通道，用户之间的交易都在链下，主区块链仅验证和记录交易状态，使用户能够在链外执行复杂的交易和智能合约互动；也可以通过合理平衡状态归约和多轮验证回滚，设计新型的处理跨分片交易方法来解决[16]。

其次，分片后，每个分片组成的节点数少于原先整个区块链，造成区块链子链算力降低，而区块链算力是恶意攻击抵御力的重要依据。攻击某个分片所需的算力将低于对整个区块链的攻击，节点数最少的分片将成为最不安全的分片，导致整个区块链的安全性降低。因此，可以在充分综合考虑节点算力和行为特征的基础上，引入一种可信机制随机调整分片组合[17]，既确保子链算力的均衡性，又避免恶意节点的聚集，从而提高分片区块链的安全性。

本研究的后续方向是研究多 MSP 和多用户的 Stackelberg 博弈模型，最终实现多 MSP 和多用户之间更为复杂的互动活动。

参 考 文 献

[1] LEE L H, BRAUD T, ZHOU P, et al. All one needs to know about Metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda[J]. arXiv: 2110.05352, 2021.

[2] PAN Y H, QU T, WU N Q, et al. Digital Twin Based Real-time Production Logistics Synchronization System in a Multi-level Computing Architecture[J]. Journal of Manufacturing Systems, 2020, 58: 45-51.

[3] ZHANG L, LI F, WANG P, et al. A Blockchain-Assisted Massive IoT Data Collection Intelligent Framework[J]. IEEE Internet of Things Journal, 2021, 9(16): 14708-14722.

[4] DL A, SANG H, NM A, et al. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects[J]. Automation in Construction, 2021, 127: 603-688.

[5] LUU L, CHU D, OLICKEL H, et al. Making smart contracts smarter[C]// Proc. of the ACM SIGSAC Conference on Computer and Communications Security. 2016: 254-269.

[6] NGUYEN C T, HOANG D T, NGUYEN D N, et al. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities[J]. IEEE Access, 2019, 7: 85727-85745.

[7] HAN Y, NIYATO D, LEUNG C, et al. A dynamic resource allocation framework for synchronizing Metaverse with IoT service and data[J]. arXiv: 111.00431, 2011.

[8] NG W C. Unified resource allocation framework for the edge intelligence-enabled Metaverse[J]. arXiv: 2110.14325, 2021.

[9] YU G, WANG X, YU K, et al. Survey: Sharding in blockchains[J]. IEEE Access, 2020, 8: 14155-14181.

[10] HAN Z, NIYATO D, SAAD W, et al. Game Theory in Wireless and Communication Networks: Theory, Models, and Applications[M]. Cambridge University Press, 2012: 63-65, 88-91.

[11] ROSENFELD M. Analysis of bitcoin pooled mining reward systems[J]. arXiv: 1112.4980, 2011.

[12] CAI S J, XIAO L M, WANG J, et al. Incentive Mechanism Design for WiFi Offloading with Users' Mobility[J]. Journal of Electronics & Information Technology, 2015(10): 2431-2437.

[13] WANG S M, TAN B H, YU R. Blockchain Sharding and Incentive Mechanism for 6G Dependable Intelligence[J]. Computer Science, 2022, 49(6): 32-38.

[14] ROSEN J B. Existence and Uniqueness of Equilibrium Points for Concave N-Person Games[J]. Econometrica, 1999, 33(3): 520-534.

[15] NGUYEN C T, HOANG D T, NGUYEN D N, et al. Blockchain-based Secure Platform for Coalition Loyalty Program Management[C]// 2021 IEEE Wireless Communications and Networking Conference (WCNC). Nanjing, China, 2021: 1-6.

[16] WANG D X, LI Z H, CHEN Y H, et al. Multi-round Verification Scheme Using State Reduction to Process Cross-shard Transactions[J]. Computer Systems & Applications, 2022, 31(5): 304-315.

[17] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning[J]. IEEE Communications Letters, 2019, 24(6): 1279-1283.

SUN Li, born in 1966, Ph.D, professor. His main research interests include online education system construction, smart education and application of big data technology.

（责任编辑：柯颖）