元宇宙中区块链的应用与展望

宋晓玲，刘勇，董景楠，黄勇飞
（重庆邮电大学计算机科学与技术学院，重庆 400065）

摘　要：元宇宙是虚拟数字世界与真实物理世界无缝融合的新生态，近来引发了各界的广泛关注。区块链、人工智能、虚拟现实/增强现实及传感技术、移动通信及泛在计算等各种新型互联网技术愈发成熟，使元宇宙的进一步发展成为可能。关于元宇宙的研究主要涉及产业项目、基础设施、关键技术、隐私安全等方面，这些研究虽然涉及区块链技术，但未具体指出区块链应用于元宇宙的优势及具体应用方式。区块链技术不仅可以为元宇宙提供开放自由的去中心化环境，而且可以为其提供公平合理的数字资产分配机制。主要从区块链赋能元宇宙中数字身份和数字资产管理的角度出发，分析了元宇宙的发展历程和特征，讨论了元宇宙发展所需核心技术及面临的挑战。同时研究了区块链的关键技术，并从区块链的本质特征及与其他技术融合优势两个方面对区块链应用于元宇宙做可行性分析。进一步提出元宇宙生态体系架构，重点详细分析了基于区块链的自我主权身份管理模型、区块链–非同质化通证（NFT，non-fungible token）工作流程及其在元宇宙中的应用。结合区块链和元宇宙的最新研究进展，从基础设施、通信和计算资源管理机制、监管与隐私保护以及区块链可扩展和互操作性 4 个方面指出区块链应用于元宇宙将面临的挑战和未来的研究方向。

关键词：元宇宙；区块链；非同质化通证；数字身份；去中心化
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.2096−109x.2022045

Application and prospect of blockchain in Metaverse

SONG Xiaoling, LIU Yong, DONG Jingnan, HUANG Yongfei
School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: The metaverse is a new ecology that seamlessly integrates the virtual digital world and the real physical world, and has recently attracted widespread attention from all walks of life. With the maturity of various new IT technologies such as blockchain technology, artificial intelligence technology, VR/AR and sensing technology, mobile communication technology and ubiquitous computing technology, the further development of the Metaverse is possible. At present, research on the Metaverse mainly involves industrial projects, infrastructure, key technologies, privacy and security, etc. Although blockchain technology is covered in these studies, the specific points about the advantages of blockchain applied to the Metaverse are still lacked. Blockchain technology can not

收稿日期：2022−04−18；**修回日期：**2022−06−09
通信作者：宋晓玲，sxllyu@126.com

引用格式：宋晓玲，刘勇，董景楠，等. 元宇宙中区块链的应用与展望[J]. 网络与信息安全学报, 2022, 8(4): 45-65.
Citation Format: SONG X L, LIU Y, DOGN J N, et al. Application and prospect of blockchain in Metaverse[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 45-65.

only provide an open and free decentralized environment for the Metaverse, but also act as a fair and reasonable digital asset distribution mechanism. The digital identity and digital asset management in the Metaverse empowered by blockchain was studied. The development process and characteristics of the Metaverse were analyzed. And the core technologies and challenges faced by the development of the Metaverse were discussed. Meanwhile, the key technologies of the blockchain were studied, and the feasibility of applying the blockchain to the Metaverse was analyzed from two aspects: the essential characteristics of the blockchain and the advantages of other technology integration. The Metaverse ecosystem architecture was further proposed, and the blockchain-based self-sovereign identity management model, blockchain-NFT workflow and its application in the Metaverse were analyzed in detail. Furthermore, combining the latest research progress of blockchain and the Metaverse, it was pointed out that the application of blockchain to the Metaverse will be from four aspects: infrastructure, communication and computing resource management mechanisms, regulation and privacy protection, and blockchain scalability and interoperability. Then the related challenges ahead and future research directions were presented at last.

Keywords: Metaverse, blockchain, NFT, digital identity, decentralization

0 引言

自互联网出现以来，人们对数字空间的探索从未停止，2021 年元宇宙的概念在网络上迅速引起热议，引发了各个行业的广泛关注。在现实需求和建设元宇宙可行性前景的驱动下，国内外互联网知名企业已开始全力布局发展元宇宙，如 Facebook、微软、腾讯及 NVIDIA 都宣布了他们对元宇宙的投资，特别是 Facebook 将自己改名为 Meta，致力于打造未来的 Meta 世界[1]。元宇宙本质是 Web3.0，始于游戏但不终止于游戏，它是互联网发展过程中一次新的转折点，其出现将使人们的生活、体验、价值认知等发生翻天覆地的改变。随着虚拟现实（VR，virtual reality）/增强现实（AR，augmented reality）、人工智能、5G、脑机接口、云计算、区块链等关键技术愈发成熟，元宇宙的发展成为可能。VR 和 AR 提供沉浸式 3D 体验；5G 网络为大规模的元宇宙设备提供高可靠和低时延连接；可穿戴传感器和脑机接口（BCI，brain-computer interface）可使用户在元宇宙中自由交互；人工智能（AI，artificial intelligence）可实现元宇宙中大规模应用的创建和渲染；区块链和非同质化通证（NFT，non-fungible token）将元宇宙中的数据进行资产化并形成新的可信机制和协作模式，在确定数字资产的所有权方面具有重要作用，其去中心化的特征为元宇宙发展提供必要条件。

区块链起源于中本聪提出的比特币，是一个分布式、不可变、允许透明交易的账本[2]。区块链技术是现代密码学、点对点网络、一致性分布式存储和智能合约的结合，可以实现数据交换、处理和存储。共识机制是其关键技术，可以实现元宇宙中匿名和可靠的交易，这些规则和范式与元宇宙是相通的，区块链可以作为元宇宙基础结构体系中必不可少的一块基石。目前，各界对区块链的研究主要涉及系统模型、共识机制、数据安全与隐私、数据存储及性能评价等，同时区块链技术已经被应用于工业互联网、数字医疗、专利保护、资产管理和政府监管等领域。那么，区块链如何赋能元宇宙？元宇宙中的区块链技术主要涉及哪些方面？应用过程中会出现哪些挑战？这些问题将引发各界对区块链技术的进一步思考和研究，这是本文的研究重点。

关于元宇宙有不同方面的研究。Dionisio 等[3]指定了可行的 3D 虚拟世界（或元宇宙）的 4 个特征，即普遍性、真实感、可扩展性和互操作性，并讨论了底层虚拟世界技术的持续改进。Lee 等[4]对实现元宇宙所用到的 8 种技术做了综述研究，通过讨论 6 个以用户为中心的因素来说明元宇宙是一个自我维持、持久和共享的虚拟世界。Ning 等[5]从国家政策、产业项目、基础设施、配套技术、虚拟现实等方面对元宇宙的发展现状进行了介绍。Park 等[6]讨论了元宇宙中涉及的 3 个组件（硬件、软件和内容），并

回顾了元宇宙中用户交互、实施方面的代表性应用程序。Leenes 等[7]从社会和法律角度调查在线游戏《第二人生》中潜在的隐私风险。Wang 等[8]从安全隐私方面分析了元宇宙将会面临哪些安全威胁。除了以上对元宇宙的综合性研究，研究者在医疗健康[9]、零售[10]、教育[11]、社会商品[12]和艺术[13]等社会应用方面也有一定的研究。

同时，研究者在区块链与元宇宙结合方面也有一些研究。Mozumder 等[14]提出了元宇宙中基于区块链的数据用作可追溯数据。Yang 等[15]研究了人工智能和区块链技术在未来元宇宙构建中的应用潜力。Xu 等[16]在区块链的基础上设计了审核元宇宙的访问通信模型。Gadekallu 等[17]通过项目展示了区块链在元宇宙应用程序和服务中的作用，并研究了区块链对元宇宙中关键技术的影响。Nguyen 等[18]针对元宇宙汇总资源需求量大、互操作性强及安全隐私问题设计了基于区块链的新技术框架。虽然以上研究或多或少涉及元宇宙中的区块链技术研究，但并未具体指出区块链应用于元宇宙的优势及与具体应用方式相关的研究。

本文主要对元宇宙进行了概述，讨论了区块链的关键技术，从区块链赋能元宇宙中数字身份和数字资产管理的角度重点分析区块链应用在元宇宙中的可行性及其应用方式。本文的主要贡献包括以下 4 个方面。

1) 讨论元宇宙的发展、特征、核心技术及其面临的挑战。

2) 根据区块链的关键技术特征和元宇宙的挑战，对区块链应用于元宇宙做可行性分析。

3) 提出一个元宇宙生态体系架构，重点分析讨论自我主权身份管理模型、区块链−NFT 工作流程及其在元宇宙中的应用。

4) 总结并指出区块链应用于元宇宙将面临的一些挑战和研究方向，如基础设施、通信和计算资源管理机制、数据安全与隐私等方面。

1　元宇宙概述

1.1　元宇宙的发展

本节从元宇宙的来源出发，从不同的视角分析讨论元宇宙的概念，并阐述其发展所经历的 3 个阶段和发展的必然性。

（1）元宇宙的来源及概念

元宇宙的概念起源于 1992 年出版的科幻小说《雪崩》[19]，这本小说描述了一个人们以虚拟形象在三维空间中跨越不同平台进行沉浸式共享空间体验并可以与各种软件进行交互的世界，小说将此世界命名为 Metaverse，“元宇宙”是单词“Metaverse”的翻译，Metaverse=Meta（超越）+Verse（宇宙的后缀）。元宇宙是一个虚拟的数字世界，更确切地说，元宇宙是未来的虚拟世界。电影《头号玩家》描绘了人们向往的元宇宙的样子，它有可以跨越实体和虚拟数字世界的完整运行的经济体系。所有人不仅可以在这个世界享用已有的设施，而且可以通过自己参与开发、创作等来进行各种数字空间活动。

元宇宙的概念仍在不断发展还没有特别明确标准的定义，本文从不同视角对元宇宙的概念进行阐释。从社会发展的视角，元宇宙是高度数字化、智能化发展下的人类社会体系新形态，将虚拟世界和现实世界的经济系统、社交系统、身份系统进行密切融合，实现人人互联、物物互联、人物互联、关系互联、价值互联、虚实互联和智能互联等多种形态的互联；从经济发展的视角，元宇宙是一个属于用户的、开放的、去中心化且具有连通性的可编辑沉浸式数字经济系统，在此系统中数字资产由用户创造，资产所有权完全归用户所有；从科技发展的视角，元宇宙是科技发展到一定程度融合各种新型技术后出现的一个虚实平行的新形态，将开启信息化发展的新阶段；从互联网发展的视角，元宇宙被认为是继网络和移动互联网革命之后的新一代互联网发展范式，集合了各种各样的虚拟元件，其用户可以开发和探索这个与现实世界平行的数字虚拟世界。从本质上说，元宇宙是一场现实世界与数字世界的接口，抽象的程序界面最终会被沉浸式的体验所代替，现实世界将通过沉浸式体验与数字世界无缝连接。

（2）元宇宙的发展

元宇宙的发展主要包括 3 个阶段：数字孪生、数字原生代、元宇宙[8]，如图 1 所示。

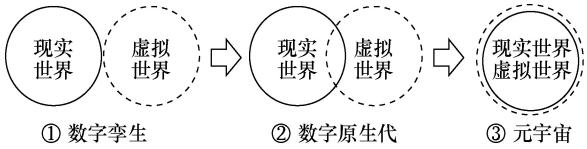

图 1　元宇宙发展的 3 个阶段

Figure 1　Three phases of the Metaverse development

数字孪生阶段是制作一个由高保真的虚拟环境、人和物组成的镜像世界，其目的是为现实世界提供一个生动的数字表示空间。这一阶段涉及的组件和虚拟活动是对现实世界的模仿。数字原生代阶段主要专注于原创内容的创造，数字世界中创造的内容和现实世界中的内容关联部分具有了交集，以虚拟用户为代表的数字原生代可以在数字世界具有自己的见解和创新，但这种状态只存在于虚拟空间并在一定限度上会影响现实世界。元宇宙阶段的数字世界逐渐成熟为一个可以将现实同化为自身的、持续的可自我维护的超现实世界，这一阶段将实现数字世界和现实世界的无缝融合与共生，虚拟数字世界的范围将比现实世界更大，可能会出现现实世界中不存在的场景和活动，因此又可以称之为超现实阶段。

由以上 3 个阶段可以看出元宇宙的出现并不偶然而且符合事物发展规律。从社会发展的角度，元宇宙的实现是整个人类文明的一次竞争，社会发展中的内容载体、传播方式、交互方式、参与感长期缺乏突破，而高沉浸度的元宇宙世界可实现多人实时协作和创造性游玩，这将深刻地改变人类原本的生存方式。从经济发展的角度，元宇宙把虚拟与现实相结合，使用区块链和 NFT 技术构建虚拟经济体系，属于数字经济的一个子集，其虚拟资产市场中的虚拟服装、虚拟土地、虚拟偶像等虚拟商品与现实叠加可以激发更广阔的商业潜能。从技术发展的角度，元宇宙满足 VR/AR、人工智能、脑机接口、5G、区块链等这些新技术的发展，能够模糊虚拟与现实的边界。由此可以看出，探索元宇宙是必然趋势。

1.2　元宇宙的特征

元宇宙虽然还没有一个确切的定义，但其具备一些各界公认的特征，而这些特征是目前任何一个网络或系统都不具备的，本文从 4 个方面概括元宇宙的特征，分别是超时空化、去中心化、自由开放、沉浸交互，如表 1 所示。

表 1　元宇宙的特征

Table 1 The characteristics of the Metaverse

特征	描述
超时空化	元宇宙是虚拟和现实世界的无缝融合且两个世界间相互平行又相互影响，使用户交互摆脱现实世界的约束
去中心化	元宇宙中的节点交互不需要通过某个特定中心节点做认证，并且每个节点都存储系统中所有交互数据的副本
自由开放	元宇宙中的用户可以自由塑造自己的身份角色、创造产品并可以自由活动、交易和制定规则
沉浸交互	元宇宙中的沉浸交互体现在沉浸式情境与沉浸式活动两方面，交互式情境更丰富感知、交互活动更真实

（1）超时空化

元宇宙的超时空化特征主要体现在虚拟数字世界与现实世界的无缝融合并且虚实两个世界之间相互平行又相互影响，可使每个用户实现自身价值的最大化而真正摆脱现实世界的约束。首先，每个人都可以在虚拟数字世界中重塑自我形象和身份体系，使现实身份在虚拟数字世界中得到充分映射，进一步促进现实社区和虚拟社群相融合并壮大崛起。其次，虚拟资产中的数据将成为核心资产并且与现实世界中的真实资产相对应，如现实世界中的艺术品可以在元宇宙中进行拍卖、元宇宙中的房产可以对应现实世界的房产来进行售卖和租用等。同时，现实世界中的资产不仅可以平行到虚拟世界而且用户的数字资产所有权将会得到充分保护，并促进现实世界中价值分配发生新变化。

（2）去中心化

相对于传统互联网中心化的运营机制，元宇宙是一个去中心化系统。元宇宙系统中所有节点交互无须通过某个特定中心节点做认证，而且每个节点都存储系统中所有交互数据的副本。这样节点不仅摆脱强制性的中心控制而且对自己的数据拥有管理权。同时在元宇宙中进行数据交易时，用户是供需互换互动的孪生关系而不再有生产者和消费者的划分，这更加体现了虚拟世界各种交互关系的透明性和公平性。

（3）自由开放

自由开放使元宇宙中的用户不仅可以创造自己想要的身份和角色而且可以随意出入并自由活动，同时各类用户还可以自行去创造自己的作品

并根据自己的需要给创作的内容制定规则。在这个开放的环境中，每个人的创作内容都归自己所有并可以像真实世界一样自由转移买卖。除此之外，多个元宇宙系统之间又是开放的，它们相互开放自己的技术接口，让用户可以自由地编辑内容和自由买卖。这种自由开放式的创造和组织服务关系，将给每个用户带来无限的存在感和自由感。

（4）沉浸交互

沉浸式是当人们在进行某种活动时全部精神都投入当前行为之中而不被其他信息干扰或打断，同时能够产生高度的兴奋和充实感。元宇宙中的高沉浸式主要体现在沉浸式情境与沉浸式活动两个方面。首先，元宇宙交互情境有着比现实更丰富的感知，元宇宙中有着比现实世界更逼真唯美的环境，同时用户在这样的环境中不仅可以自由地来回穿梭而且体验更自由丰富，如可以飞翔或做瞬时地理迁移，这种释放性的体验每时每刻都在发生变化从而使其对这种虚拟情境更加留恋。其次，元宇宙的交互活动可以让用户获得更强的临场感和体验感，与现实世界一样，元宇宙中的每个人都有自己的身份和朋友，同时存在开放的社交文明和经济系统，从而使用户可以一起专注地共处，当用户沉浸在活动交互中时主观的时间感会改变而感觉不到时间的流逝并且对整个交互活动过程具有主控感。

1.3　元宇宙的核心技术

元宇宙发展离不开各种新型技术的支撑，本文将影响元宇宙发展的关键核心技术概括为：区块链技术、VR/AR 及传感技术、人工智能技术、移动通信技术和泛在计算技术。元宇宙的核心技术如图 2 所示，这些技术的综合运用将给元宇宙的建设提供强大保障。

区块链技术的去中心化特质可以将元宇宙中的数据进行资产化并形成新的可信机制和协作模式。其中共识机制和各种加密机制是实现区块链去中心化的关键技术，确保所有参与者无须经过中央权威机构验证而直接进行交互[20]，这符合元宇宙去中心化的特征。智能合约由事件驱动，具有自动化、可编程、不易篡改等特性，能够封装区块链系统中各节点的复杂行为[21]，未来可以作为元宇宙中的智能软件代理机器人。NFT 是链下资产的链上凭证，将成为元宇宙中数字资产确权的令牌，通过 NFT 可实现虚拟资产和现实资产的交互[22]。除此之外，去中心化自组织（DAO，decentralized autonomous organization）、去中心化金融（DeFi，decentralized finance）等区块链应用将进一步激发创作者经济时代，并确保宇宙中的交互具有完整性、透明性和确定性，从而形成一个健康连通的虚拟生态环境。

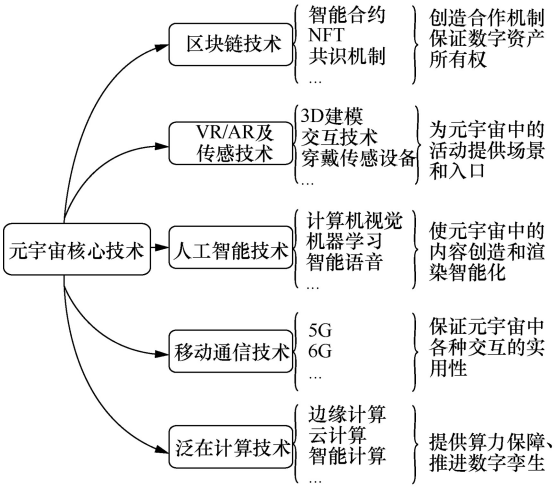

图 2　元宇宙核心技术

Figure 2　Core technology of the Metasverse

从技术演进的角度来看，现阶段元宇宙最有可能依托 VR/AR 来实现。具有代表性的元宇宙应用中[23]，区块链、VR/AR 和人工智能都是其核心技术，如表 2 所示。其中 VR/AR 及传感技术是通往元宇宙的关键接口，AR 可以将数字信息叠加在物理环境上，而 VR 则可以让用户生动地体验数字世界[24]。其中主要涉及的关键技术有：环境建模技术[25-27]、立体声合成和立体显示技术[28-30]、触觉反馈技术[31-32]、交互技术[33-36]等。同时集合 VR 头戴式设备、运动追踪设备、超移动设备等硬件设备可以催生多种应用场景，一定程度上可以增强用户的沉浸式体验，进而改变用户与数字世界的交互方式实现虚实共生。

人工智能可以用智能化的方式广泛联结各领域知识与技术，已成为新一轮科技革命和产业变革的重要驱动力。元宇宙中人工智能将更多地承担辅助内容生产的工作，如机器学习[37]、计算机

视觉[38]、智能语音[39]等技术的应用可以降低用户内容创作门槛，同时加速内容生产和分发进程，丰富元宇宙的内容生态，满足不断发展的元宇宙对优质内容的需求。

表 2 元宇宙的应用

Table 2 The applications of the Metaverse

类型	项目名称	区块链	AR/VR	人工智能
智慧城市	Metaverse Seoul	√	√	√
	Barbados Metaverse Embassy	√	√	√
娱乐	AltspaceVR	√	√	√
	Decentraland	√	√	√
教育	Xirang	√	√	√
办公	Horizon Workrooms	√	√	√
	Microsoft Mesh	√	√	√
医疗	Telemedicine	√	√	√

泛在计算技术是边缘计算[40]、智能计算[41]、云计算[42]等技术的总称，由计算机、服务器、高性能计算集群和各类智能终端来承载。其为元宇宙中无处不在的信息获取、监控、众包、扩增实境、生物识别等提供支持，推进信息化构建模型与现实世界保持适用和同步，保证元宇宙中各种高性能交互对算力的需求。因此，泛在计算是未来元宇宙世界最重要的基础技术资源之一。

5G/6G 具有超容量、低时延等特点，为元宇宙中海量连接和各种低时延高并发交互提供通信保障[43]。这意味着无论在何时何地都将更容易地传输视频、音频等信号，从而模糊物理世界和数字世界之间的界限，进一步助力元宇宙中的沉浸式感官体验。

综上所述，区块链技术、VR/AR 及传感技术、人工智能技术、移动通信技术和泛在计算技术在元宇宙发展建设中都起着举足轻重、不可替代的作用，各种新型互联网技术之间如何无缝融合或许将成为未来探讨的重要方向。

2 区块链技术介绍

区块链是一种利用块链结合式数据结构来存储和验证数据、利用共识算法来生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用自动化脚本代码组成的智能合约来编程和操作数据的全新的分布式基础架构和计算范式。本节主要从区块链的区块结构、共识机制、智能合约 3 个方面来阐述区块链的关键技术。

2.1 区块链的区块结构

区块链上一个完整的存储单元由区块头和区块体组成，被称为区块，其结构如图 3 所示。

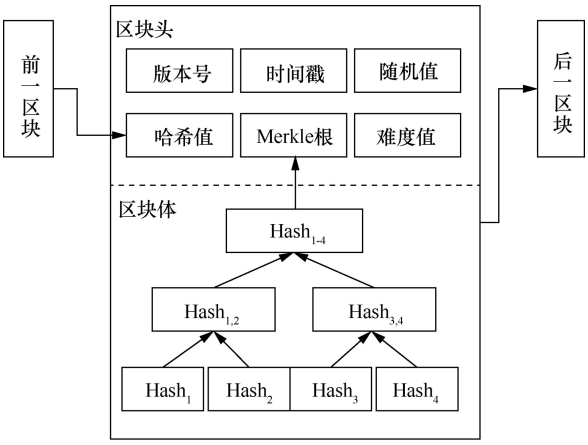

图 3 传统的区块结构

Figure 3 Traditional blocks Structure

区块体存储主要交易内容信息；区块头所占空间一般较小，主要存储当前区块的特征值，包括哈希值、Merkle 根、时间戳、难度值和随机值等，这些字段一般与验证相关。其中哈希值是前一个区块的哈希；时间戳是生成当前区块的时间，可以证明区块的存在，也是链上区块排序的依据；难度值由当前链上共识算法设置，随机值是通过共识算法解出的；Merkle 根是区块链溯源的重要组件，每个区块中的交易会根据时间顺序进行分组哈希，通过递归计算出哈希值并以 Merkle 树的结构形式存储在区块体中，最后生成 Merkle 根存储在区块头中。

由区块结构可以看出区块头里的相关数据决定了区块链中的区块是不可伪造和不易篡改的，保证了去中心化交易的信任度。生成 Merkle 树的哈希函数具有单向性和抗碰撞性，这使区块链的安全性得到充分的保障。另外在区块链上进行交易时还需要签名和认证机制，这些机制采用的是非对称加密技术，很大程度上确保了区块链交易和数据的隐私性。但是，当面对庞大的数据量时，区块链可扩展性方面的能力明显不如中心服务器，因此，很多研究者对区块链的链式结构进行了分析和改进，尝试使用有向无环图（DAG，directed acyclic

graph）结构代替链式结构以提高其存储能力。Cao 等[44]提出了一种基于 DAG 的区块链系统授权框架，并设计了与其相关的两种算法和共识机制，Wang 等[45]对基于 DAG 的 IOTA 网络的特性、功能、性能、安全方面进行了分析，并指出基于 DAG 的模块化设计还有待于进一步研究。Gai 等[46]提出了一个 BlockDAG 模型，并为其设计了一种共识机制，进一步给出了核心算法——BlockDAG 排序算法和块合并算法。Xie 等[47]在给出结合有向无环图和分片的区块链扩展方案的基础上，设计了一种计算效率高的共识算法，提高了资源利用效率。以上研究进一步表明了基于有向无环图的数据结构更适合物联网应用和大数据应用，元宇宙数据时代更需要区块链的高存储，因此对于区块链的扩展性还有待进一步研究。链式结构与有向无环图结构的比较如表 3 所示。

表 3　链式结构与有向无环图结构的比较

Table 3　Comparison of chain structure and directed acyclic graph structure

名称	链式结构	有向无环图结构
区块形式	区块以链式结构连接，每个区块中包含多笔交易	区块以有向无环图结构连接，每个区块中只包含一笔交易
交易速度	每次只能增加一个区块的数据量，交易速度较慢	支持局部处理和并行结算，交易的人越多交易越频繁，速度越快
共识机制	共识机制是为了选举出打包交易的节点，如工作量证明、权益证明等，共识过程有矿工参与	共识机制不是为了选举打包交易的节点，每笔交易由节点自身处理，共识过程无矿工参与
扩展性和改进方案	可扩展性弱，改进方案：增加区块大小、支持，链外通道、节点分级或分片	可扩展性强，扩展方案：使用耦合网络和事务验证，但前提是用户先要处理自己的交易
抗量子攻击	加密算法容易被量子计算机攻击	使用了抗量子攻击的密码算法不易被攻破
交易费用	需要消耗的资源费用高	资源费用消耗很低

2.2　共识机制

共识机制决定了节点是否拥有区块打包权，每个竞争打包权的节点必须遵守这套共识规则，这套规则是系统事先设定好的、每个节点公认的、公平的竞争制度。其本质是共识算法，核心要素是达成一致、公平公正、容错机制、激励机制。接下来通过阐述区块链上的共识交易过程，讨论共识机制的工作原理、分类、改进方法及存在的问题。

2.2.1　共识交易

区块链系统采用点对点的交易形式，与传统的中心化交易不同，整个交易过程不需要第三方验证，系统中所有节点集体监督交易结果，本文将这种交易称为共识交易。共识交易中不存在特殊的中心节点，每个节点既需要验证转发交易又需要维护交易记录。去中心化交易流程如图 4 所示。

交易发起方首先产生一笔交易，然后广播到点对点（P2P，peer to peer）网络中，网络中收到交易的节点会对交易信息进行验证，验证内容包括：发起交易方的身份、双花问题和资产的合理性等。经过一定量的节点验证无误后，此笔交易就会被放入交易池中等待打包入块。此时，网络中的所有节点都在为获得打包块的权利，努力克服一系列难题，最终获得打包权的节点从交易池中按照交易时间顺序打包成区块上链，上链后并再次广播到 P2P 网络中，以致系统中的节点存储新的区块，完成整个交易。

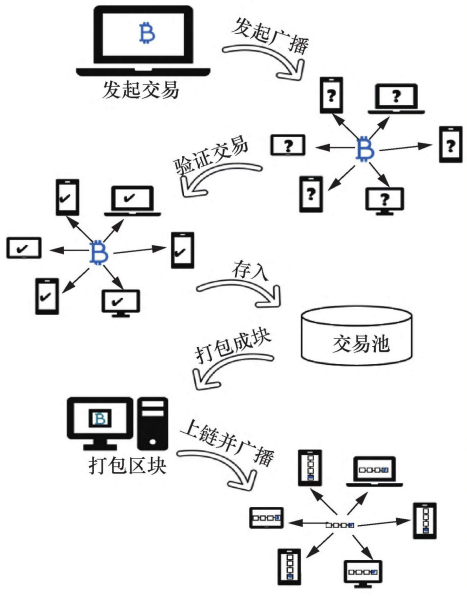

图 4　去中心化交易流程

Figure 4　Process of decentralized transaction

2.2.2 共识算法

在去中心化交易过程中最关键的是共识算法的执行，目前已经有大量研究者对共识算法进行了研究，并从不同的角度进行了分类，如随机类、证明类、选举类和混合类共识算法[22]。共识算法分类如表 4 所示，这些共识算法大部分是基于工作量证明（PoW，proof of work）和权益证明（PoS，proof of stake）的共识，每个共识算法的最终目的都是选出打包区块的节点（又称记账节点）。

表 4 共识算法分类

Table 4 The classification of consensus algorithm

类别	详细	代表算法
证明类	通过证明节点具有的某种特定能力（如算力、权益）较高的方式选出记账节点	PoW[48]、PoS[49]、PoSV[50]、PoB[51]等
选举类	通过“投票选举”的方式选出获得一半以上选票的节点作为记账节点	DPoS[52]、PBFT[53]、DBFT[54]等
随机类	根据某种随机方式（如抽签）选出记账节点	Ouroboros[55]、PoET[56]、Algorand[57]等
混合类	多种共识算法结合使用选出记账节点	PoA[58]等

注：权益流通证明（PoSV，proof of stake velocity）；燃烧证明（PoB，proof of burn）；委托权益证明（DPoS，delegated proof of stake）；实用拜占庭容错（PBFT，practical Byzantine fault tolerance）；授权拜占庭容错（DBFT，democratic Byzantine fault tolerance）；时间流逝证明（PoET，proof of elapsed-time）；活动证明（PoA，proof of activity）。

由于在算法设计上很难克服公平、安全、效率的不可能三角问题，所以已有的对共识算法的研究和改进主要集中在以下几个方面：通过调整工作量难题参数或随机函数类型来优化区块链系统的整体性能；通过权益证明和工作量证明相结合，减少能耗浪费和提高吞吐量；通过共识算法和分片技术相结合，从不同的角度提高区块链的扩展性等。随着研究者不断地对共识算法进行研究和改进，共识算法在性能方面已有了很大的提升，但还存在一些问题：共识效率低，如共识速度；工作量证明共识算法存在算力集中化、选举性能低、资源浪费等，这些问题虽然有了改进，但离实际需求还有一定的距离，同时改进共识算法后也会带来区块容量变大、出块时间加长等；权益证明类共识算法一定程度上解决了资源浪费的问题，但还存在一些安全性问题，如无权益攻击、粉碎攻击等。由此可以看出，共识算法在安全性、能耗、可扩展性、出块速度等方面还需要进一步研究和提高。并且在整个共识过程中获得记账权的节点会得到一些奖励，称与奖励相关的措施为激励机制。激励机制用来激励系统中所有的节点活跃起来竞争记账权，从而确保每一笔交易都可以上链，并缩短上链时间，那么共识算法和激励机制适配结合的研究或许将成为需要关注的一个重要方向。

2.3 智能合约

智能合约可理解为由计算机程序自动执行的智能合同，这份合同需按照预设合约条款拟定并部署到区块链上。其具有可编程性、不易篡改性和去信任等特性，有了智能合约可以在不需要第三方参与的情况下，通过执行合约条款嵌入各种数据、交易资产、管理数字资产等。智能合约具有可编程性和自动执行性，并可以封装区块链网络中各节点的复杂行为，因此可以作为虚拟世界中的智能软件代理机器人。智能合约通常具有以下功能：

1) 使用特定操作自动激活事务，事务在回应他人时传输或在预定的时间自动传输；

2) 支持多重签名的交易，但需要重要参与者全都验证签名后，交易才会被分发；

3) 可以为特定应用程序的数据提供存储空间，类似于成员记录、布尔值或列表状态；

目前对智能合约的研究主要集中在智能合约的开发、安全、漏洞检测等方面，Huang 等[59]从生命周期的角度对智能合约的安全漏洞问题进行了分析总结，并提出在开发智能合约时需要从安全设计、安全实现、部署前测试、监测和分析 4 个阶段检测安全漏洞。文献[60-62]提出了智能合约执行并行模型，以此来提高区块链的吞吐量。Dusdar 等[21]提出了弹性智能合约的参考架构，并在物联网环境下实现多个区块链之间的分析。Cai

等[63]针对区块链智能合约对量子攻击的安全性能，提出了一种基于轻量级量子盲签名的智能合约，给出了智能合约量子盲签名的生命周期和签名规则。元宇宙中的各种交易依赖于智能合约同时会对智能合约提出新的要求，这给智能合约进一步的研究提出新的挑战。

3　区块链应用于元宇宙的可行性分析

通过对区块链的关键技术分析可以看到区块链中的很多规则范式与元宇宙是相通的，本节主要讨论区块链的分类及关键特征和元宇宙发展过程中面临的挑战，从区块链本身特征和区块链与元宇宙中其他技术融合两方面分析区块链在元宇宙中的应用优势。

3.1　区块链的分类及关键特征

根据区块链的开放程度可以分为以下 3 类：公有链、联盟链和私有链[64]。3 类区块链性能的对比如表 5 所示。

表 5　不同类型区块链的对比

Table 5　Comparison of different types of blockchain

名称	去中心化程度	可扩展性	灵活性	共识机制	透明性	可修改性	可追踪性
公有链	完全去中心化	弱	弱	证明类共识算法（PoW、PoS）	全透明	不可修改	可追踪
联盟链	半去中心化	较好	较好	传统共识算法（Raft、PBFT 等）	不透明	部分可修改	可追踪
私有链	中心化	一般	一般	传统共识算法（Raft、PBFT 等）	半透明	可修改	部分可追踪

公有链中任何节点都可以自由进出网络并参与打包新区块和维护区块的内容，网络中不存在任何中心化的服务端节点，是一个全公开的链；联盟链是指定的多个组织机构中的节点可参与的区块链，其数据只允许系统内不同组织进行记录维护，是一个半公开的链；私有链中的节点加入网络需要授权并且各个节点的读写权限都会受到控制，是一个非公开的链。

元宇宙是一个完全去中心化开放自由的虚拟空间，因此通过 3 类区块链性能的对比可以看出公有链应用于元宇宙的可能性最大。

区块链技术是现代密码学、点对点网络通信、一致性分布式存储和智能合约的结合，在数据管理方面具有一些显著的特征，本节主要从去中心化、透明性、不易篡改性、抗抵赖性、可追踪性、持久性、可审核性和匿名性 8 个方面来总结说明，如表 6 所示。

3.2　元宇宙发展的挑战

元宇宙是充分开放自由的虚拟数字世界，虽然现实中一些应用已经具备了元宇宙的某些性能，但距离其成熟仍然还需要一段时间，在这个发展过程中存在着各种各样的挑战。

表 6　区块链的关键特征描述

Table 6　Description of key features of blockchain

关键特征	描述
去中心化	在传统的分布式交易方案中，所有的交易都需要进行身份验证，这不可避免地造成了开销和流量在中心服务器上的使用。在区块链中，主要用共识算法来保持去中心化网络中信息的一致性
透明性	链上所有节点都可以使用并确认参与的交易，因此这些交易信息对于所有用户来说都是透明的，主要体现在溯源数据的获取和共享、数据云存储和决策透明性[65]
不易篡改性	区块链上每个块中都包含前一个块的哈希值，对最后一个块的任何更改都会使所有之前创建的块失效。同时，Merkle 树根哈希存储所有参与交易的哈希，对任何交易的任何修改都会产生一个新的 Merkle 根。因此，任何捏造都很容易被识别出来
抗抵赖性	验证私钥正确性的过程将被用来作为签名放置到事务中，然后该签名由使用等效公钥的其他节点进行确认，因此，以加密方式签名的事务不能被事务发起者拒绝
可追踪性	所有存储在区块链中的交易都是使用时间戳粘贴的，因此，节点可以使用相同的时间戳检查区块信息，等待确定无误后，进一步确认和跟踪历史信息
持久性	区块链中事务经常被快速地验证，正常的矿工节点不会允许无效的事务，不正常的交易几乎不能在区块链内部一次性删除并将被立即纰漏
可审核性	一旦当前交易被存储在区块链中，那么未使用的货币或资产将变为已使用，通过这种方式，可以确认和审核交易
匿名性	节点用户可以使用不泄露个人信息的地址在区块链进行操作，但由于区块链具有一定的局限性，因此它只能进行适当地加密保护

（1）安全与隐私

元宇宙中的安全和隐私问题是阻碍其进一步发展的主要因素。从海量数据流的管理、无处不在的用户活动分析、人工智能算法的不公平结果到物理基础设施和人体的安全，都有可能会出现广泛的安全破坏和隐私侵犯。首先，元宇宙是各种新型技术的集成，这些新技术的弱点和内在缺陷也将被元宇宙继承，如可穿戴设备或云存储被劫持、虚拟“货币”被盗、人工智能制造假新闻等新型技术风险事件层出不穷。其次，在各种技术交织的驱动下，现有威胁的影响在虚拟世界中会被放大并变得更加严重，甚至可能会滋生物理和网络空间中不存在的新威胁，如虚拟跟踪和虚拟“间谍”[7]。特别是元宇宙中为了使用 AI 算法构建虚拟场景，用户将不可避免地佩戴内置传感器的可穿戴 AR/VR 设备，全面收集脑电波模式、面部表情、眼动、手动、语音和生物特征以及周围环境。这些构建真实世界的数字副本所涉及的个人数据将更细粒度地无处不在[66]。此外，用户需要在元宇宙中被唯一识别，这意味着耳机、VR 眼镜或其他设备可以被非法用于跟踪用户的真实位置，甚至黑客可以利用系统漏洞和入侵设备，并将其作为切入点入侵现实世界的设备，以威胁个人安全和基础设施，如通过高级持续威胁攻击家用电器、电网系统、高速铁路系统和供水系统等[57]。

（2）身份认证管理

随着人工智能的发展，人类和机器人之间的区别越来越小，导致深度造假无处不在并且相对容易实施，身份验证和授权问题很容易在元宇宙中升级，因此元宇宙中需要为身份验证提供保障，同时防止黑客攻击其他虚拟角色。

（3）数据激增与滥用

互联网数据增长一直呈上升趋势，元宇宙中将会产生更大量、更多样、更隐私的数据，如通过使用可穿戴传感器和其他智能设备将现实世界的用户基本信息及环境敏感信息等数据输入元宇宙，同时这些数据可能被大量应用程序访问，在存储和使用这些数据时可能会被黑客利用或泄露。

（4）计算智能

为了获得高质量的元宇宙体验，处理数据的能力需要进一步增强，不仅涉及数据操作、传输和存储而且需要支持多用户高并发。云计算需要增加计算能力，同时边缘端设备需要更高的计算智能和效率。

（5）数据结构复杂

元宇宙中为实现用户与虚拟形象/环境之间的交互需要安全融合大量多模式用户敏感的大数据，同时其超时空性极大地增加了信任管理的复杂度和难度。随着现实与虚拟的界限日益模糊，监管和取证更容易混淆现实和虚构，如 Deepfake 事件[68]。

（6）互操作性和扩展性

用户需要在不同场景和模式下自由地并发穿梭和活动，这就需要透明的元宇宙系统和轻量级的、易于访问及可迁移的工具，但目前大型虚拟数字世界使用的几乎都是高度异构的软硬件和通信结构，这限制了元宇宙的互操作性和可扩展性。

3.3 区块链应用在元宇宙中的优势

结合元宇宙发展的挑战，区块链在元宇宙中将是一个很有前途的解决方案[17]，如图 5 所示。区块链的关键优势是去中心化的共识机制，该机制适合元宇宙开放自由地创造和交互，智能合约可以自动化管理元宇宙各种用户之间的复杂交互等。本节主要从区块链本身特征和区块链与元宇宙中其他技术融合两方面阐述区块链在元宇宙中的应用优势。

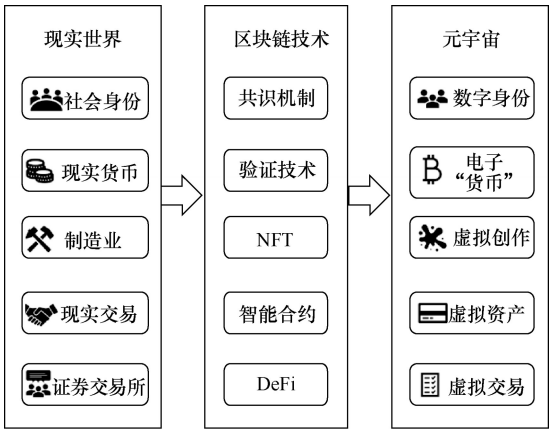

图 5 区块链应用于元宇宙

Figure 5 Blockchain applied to the Metaverse

3.3.1 区块链本身的特征优势

区块链本身的特质使其在金融服务、征信权属管理、资源共享、供应链管理和公共网络服务

方面具有很大的应用价值[69]。区块链本身的关键技术属性符合元宇宙中基本组件的需求，除此之外，区块链具有的一些特征可以促使元宇宙良好健康地发展，主要体现在以下几个方面。

（1）安全性与隐私性

用户信息的安全性与隐私性是元宇宙中用户和服务的关键问题，区块链技术是现代密码学、点对点网络通信、一致性分布式存储和智能合约的结合，可以在没有第三方权威机构认证的情况下保护元宇宙用户和服务提供商的资产和活动[70-71]。首先，用户将自己沉浸在虚拟世界中会产生大量的用户私有数据和内容，如游戏道具、数字收藏品和交互数据等。通过区块链技术将元数据和媒体数据上链存储，这些数据内容成为数字资产，可以使用区块链和 NFT 证明其所有权和唯一性。区块链对链上所有交易信息具有抗抵赖性、不易篡改性，这在一定程度上可以保护元宇宙中交互数据的隐私和安全。其次，在构建和维护元宇宙期间，由物联网设备或传感器支持的虚实同步数据被记录为区块链中的事务。这些与虚拟角色相关的数据和边缘资源可以通过区块链以安全互操作的方式管理。再次，区块链涉及的隐私保护方法主要有：混淆机制、零知识证明、同态加密、环签名、通道隔离、权限限制、承诺方案、基于属性加密[72]及按需披露的隐私保护机制[73]等，并且区块链还可以与隐私计算技术结合，一定程度上减少算力开销，具备良好的信息隐蔽性[74]。

（2）抗抵赖性和可审核性

区块链的抗抵赖性和可审核性是元宇宙去中心化经济系统的基础，元宇宙中的“货币”、商品和转账记录等与交易相关的信息都被永久地记录在区块链中，这些记录不仅防篡改而且可对商品进行追踪审核，为元宇宙中的数字经济提供保障。

（3）透明性和匿名性

区块链中上链的商品和服务信息都具有透明性并且参与的节点都可以开放获取，这解决了传统网络的信息不对称问题，满足元宇宙中各种信息的开放特性。另外，因为区块链上的所有交易都是加密签名且地址属于匿名交易，因此区块链用户的匿名性可最大程度上保护元宇宙中用户的隐私。

（4）可扩展性和互操作性

元宇宙的可扩展性允许大量用户同时沉浸在元宇宙中，同时互操作性允许不同元宇宙用户之间进行无缝交互，因此，区块链中的共识机制和智能合约一定程度上满足可扩展性和互操作性，但对于各应用之间的跨链操作技术，目前还不是特别成熟。

（5）公平性和平等性

区块链的去中心化特质可以使元宇宙中的用户无论其在现实世界中的物理属性是怎样的都可以拥有公平和平等的体验。

（6）数字资产的所有权

创作者经济是元宇宙中经济特征的重要组成部分，元宇宙的所有参与者将成为这个虚拟世界中数字内容的创造者（UGC，user-generated content）[75]，其唯一性和所有权可以通过区块链中的 NFT 来确认和交易。

3.3.2　区块链与其他技术融合

区块链应用于元宇宙除了本身的特征优势外，其与元宇宙中其他关键技术融合也显示出极大的潜力，可以促进构建虚拟世界中各种应用程序和服务的沉浸式体验。本小节主要讨论区块链与 VR/AR 及智能传感技术、人工智能技术和其他技术的融合。

（1）区块链与 VR/AR 及智能传感技术

VR/AR 及智能传感技术通过提供元宇宙中虚拟对象和真实物理对象的实时表示而赋予元宇宙身临其境的真实体验。然而，利用这些技术收集的数据信息来源复杂且可能含有大量与用户隐私相关的敏感数据，同时这些数据在各种传感设备之间交换、传输或共享时可能会有利益冲突或安全威胁，因此这些数据应该具有透明性和可追踪性，那么可以通过建立基于区块链的应用程序记录并追踪数据来源确保数据的合理性和安全性，区块链的共识机制确保各种数据的验证和 AR/VR 利益相关者之间的信任[76]。

（2）区块链与人工智能技术

元宇宙需要通过人工智能技术辅助内容生产和人机交互来满足不断发展的需求，如角色创建、语言处理等。人工智能可以降低内容的生产成本，因此元宇宙会大量使用各种复杂的 AI 应用程序，

但 AI 应用程序有时可能会犯错或出现不公平决策，甚至会出现深度造假和资源滥用的问题[77]，这可能导致用户对元宇宙失去信任。区块链技术可以帮助元宇宙用户在控制自己的私有数据的同时避免深度造假，用户通过零知识证明可以在不透露私有信息内容的情况下给 AI 应用程序提供特定信息。区块链还可以提供审计跟踪来检查元宇宙中所有发生的事务的可靠性，使元宇宙中从粗粒度到细粒度的敏感数据和信息得到更好的保护。

（3）区块链与其他技术

首先，元宇宙中的通信基础设施必须满足前所未有的服务水平要求，如超高的数据速率、通信量等，6G 软件化、虚拟化和云化的运行模式可以促进敏捷高效的管理和网络编排，但同时会导致网络可靠性低、出现安全漏洞、数据隐私性低和多访问控制等安全性问题[78]。区块链技术可以通过共识机制实现去中心化并消除单点故障提高抗攻击能力，同时链上交互存在可追溯性和不易篡改性，因此区块链可以为未来网络提供信任基础。其次，边缘计算和云计算等技术可以保证元宇宙中各种高性能交互对算力的需求，而在实际运行中边缘计算会把云资源和服务扩展到网络的边缘并分布在网络的另一端，存在去中心化管理和安全性低的问题。将区块链和边缘计算集成到一个系统中，可以对分布在边缘的网络、存储和计算进行可靠的访问和控制，从而安全地提供近端大规模的网络服务器、数据存储和有效性计算[79]。

4　区块链在元宇宙中应用

区块链在元宇宙中具有一定的应用优势，本节通过介绍元宇宙生态体系架构来讨论元宇宙生态中各模块之间的协作过程，并重点说明区块链在此生态体系中的作用。从元宇宙交互中涉及的数字身份管理和数字资产管理两个核心方面分析区块链在元宇宙中的应用。

4.1　元宇宙生态体系架构

元宇宙虚拟世界是综合运用多种技术，实现物理空间和数字空间的无缝融合，本文从元宇宙空间交互完整性角度提出一种元宇宙生态体系架构，如图 6 所示。元宇宙生态体系中有现实空间、虚拟空间、核心技术和建设基础 4 个模块，在这个生态中各模块不是独立的而是相互联系相互影响的，虚拟空间和现实空间的内容和事务相互影

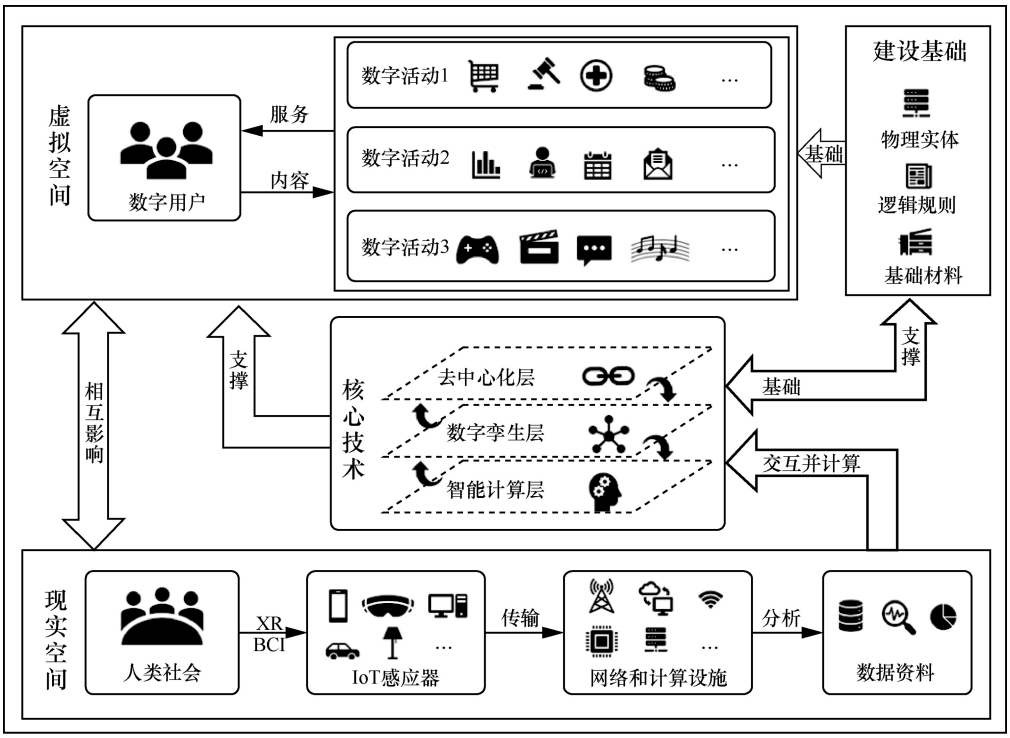

图 6　元宇宙生态体系架构

Figure 6　The ecosystem architecture of Metaverse

响和映射，现实空间中的数据资料需要通过核心技术模块的计算处理传入虚拟空间，同时核心技术模块又是虚拟空间良好运行的技术支撑，建设基础模块不仅是虚拟空间和核心技术的基础，而且离不开核心技术的支撑。

（1）现实空间模块

现实空间主要是现实世界中各种数据要素和资料的产生过程，现实世界中的人主要通过扩展现实（XR，extended reality）或脑机接口技术（BCI，brain computer interface）与物联网感应器（如手机、VR 眼镜、汽车等）进行交互来产生一定的生活数据，如行程数据、数字产品使用偏好等，这些数据将在各种网络中进行传输，同时与服务器相关的计算设施会对这些复杂的数据进行计算分析和分类，从而形成初步的数据资料。很多组织机构将这些数据资料视为不可忽视的财富。首先，这些数据资料经过核心技术模块中智能计算层的分析和计算可以支撑虚拟空间的建设。其次，虚拟空间中的各种数字虚拟活动又会影响到现实人类社会的发展。此模块主要涉及硬件设备的开发、通信设备的建设范式、脑机结构技术的创新、大数据智能分析等新型技术。

（2）核心技术模块

本文把核心技术模块分成 3 个层次：去中心化层、数字孪生层和智能计算层，这 3 层之间互为基础和支撑。首先，去中心化层主要涉及区块链技术，区块链在此不仅为元宇宙提供去中心化的经济交易支持，而且通过智能合约、共识、加密等技术还可以提高各种虚拟数字活动之间的交互性和安全性，通过 NFT 确认数据资产的所有权。其次，数字孪生层主要涉及数字孪生技术，这种技术应用于网络可以创建物理空间的虚拟镜像，即搭建数字孪生网络平台，此平台能够助力网络实现低成本试错、智能化决策和高效率创新，这样通过现实空间和数字孪生技术实时交互、相互影响。最后，智能计算层主要涉及人工智能、云计算、边缘计算等技术，人工智能技术更多地承担辅助内容生产的工作，可以降低用户内容的创作门槛。智能计算主要为虚拟数字空间中无处不在的信息获取、监控、众包、扩增实境、生物识别等提供支持，推进信息化构建模型与现实世界保持适用和同步。此模块主要涉及机器学习、计算机视觉、智能语音、边缘计算、云计算等技术。

（3）虚拟空间模块

虚拟空间是元宇宙生态的基本组成部分，主要由数字用户和数字活动两部分组成，数字用户可以认为是人类在元宇宙中的虚拟化身，是现实人类的映射，数字用户可以通过虚拟数字空间中的各种应用程序创造内容，如购物清单、拍卖记录、办公数据、游戏娱乐偏好等数据资料。这些数据资料会影响到现实空间人类的生活，如在现实空间中可以根据大量的购物清单分析用户的购物喜好，加大对某种商品的生产。虚拟数字空间是数字用户寄生的场所并时刻为每个数字用户提供各种各样的虚拟服务。此模块主要涉及数字用户管理和虚拟应用程序开发技术。

（4）建设基础模块

此模块是虚拟数字空间和核心技术的基础，类似于很多分层框架里的物理层，主要包括物理实体、逻辑规则和基础材料，如光纤、无线通道、各种各样的协议等，主要为数据传输提供信道通路，数据通路可以是一个物理媒体，也可以是多个物理媒体的组成。此模块主要涉及各种接口标准的设定、无线通道的建设、各种传输协议规则的制定等。

4.2　数字身份管理

数字身份是数字世界中节点用户的标识，身份信息分散在各种应用程序中，由多种不同属性信息组合并映射节点用户的真实身份，其属性信息包括交易信息、社交信息、娱乐信息等，属性信息越全面数字身份就越完整。用户实体在虚拟数字世界的行为越来越丰富从而形成一个新的自我，新自我是用户实体在虚拟数字世界的演绎和延续也是一种重生。拥有自主主权的数字身份是在虚拟数字世界活动的必要条件，这符合元宇宙的应用需求。

（1）数字身份定义

数字身份在数字世界中代表一组特定实体的数字序列，是将真实身份信息浓缩为数字标识的一组特定的数字序列代码，是连接物理世界和虚拟数字世界的基础设施，是一张通往虚拟数字活动的通行证[80]。元宇宙中通过签署一个经过验证

的数字身份就可以在其中从事任何形式的活动，如社交、娱乐、投资、买卖等，如同人们在现实活动空间中会使用身份证等有效证件来证明自己或鉴别他人。元宇宙中的数字身份很重要，它代表用户的身份、真实性和所有权[81]。

（2）数字身份形式

数字身份是物理世界到虚拟数字世界的身份映射，如果数字身份散乱，则基于数字身份产生的数据将无法统计和追溯也就无法开展数据治理工作。随着互联网的出现和普及，数字身份的形式经历了 3 个阶段：中心化数字身份、联盟数字身份、去中心化数字身份[82]。3 种数字身份的相关特点、表现形式和存在的问题如表 7 所示。

表 7 3 种数字身份的比较

Table 7 Comparison of three digital identities

名称	特点	表现形式	存在的问题
中心化数字身份	单一机构管理维护	互联网网站独立用户	隐私泄露、互操作性差
联盟数字身份	多个机构联盟管理控制	跨平台登录用户账号	多机构合谋控制
去中心化数字身份	完全个人控制拥有	区块链去中心化用户	未广泛推广使用

（3）去中心化数字身份

去中心化数字身份主要包括：身份标识、身份认证、身份隐藏 3 个要素。其中，身份标识是用户节点身份的凭证是数字资产拥有权的基础，身份认证和身份隐藏为交易中的隐私保护提供有力保障[83]。身份标识证明本人身份的凭证，区块链系统中的身份标识大多基于非对称密码算法来实现，根据区块链系统开放程度的不同，其身份标识方法存在着一定的差异，区块链上使用的身份标识方法主要有三种：公钥身份标识、数字证书身份标识、去中心化身份（DID，decentralized identity）标识。公钥身份标识大多基于公钥密码体系的椭圆曲线密码算法来构建用户。联盟链更关注强监管环境下客户身份识别，采用的是数字证书标识身份，这种身份识别方式是基于数字证书的身份管理机制。DID 标识是一种新的可以支持验证的去中心化数字身份标识方法，具有全局唯一性、高可用性、可解析性和加密可验证性[84]，通常与加密机制关联建立安全通信。

身份认证在区块链系统中通过确认交易者身份的过程来确定该用户是否具有对数字资产数据的访问和使用权限[85]。区块链系统中的身份认证方式有三种：匿名认证、实名认证、可控匿名认证[86]。匿名认证是消息的发送方和接收方都是匿名的，区块链系统通过加密技术隐藏交易双方的地址、金额等内容，以致不能判定交易者的真实身份。实名认证是一种对用户信息真实性进行的验证审核，目的是实现用户的准入控制，认证过程必须符合交易监管要求。目前大多数联盟链要求用户进行实名认证。可控匿名认证是根据实际监管的需求，在保护合理匿名需求的同时可以恢复交易者真实身份的过程，既解决了隐私保护的问题又使整个交易过程监管可控。

身份隐藏主要是交易过程中不透露任何与身份相关的信息，其目的是保护用户身份隐私，区块链中的身份隐藏技术主要有混币机制和无标识交易技术。混币机制是指在交易过程中增加中间环节对多个交易进行混淆，从而增加攻击者的分析难度，保护用户身份隐私[87]。无标识交易技术是指在链上资产的表示，如 UTXO 中不包含资产所有者的身份标识，资产权属变更过程中的交易确认是由用户采用资产表示中的秘密因子进行相应的密码运算来完成的，接收方通过密码运算的结果来判断资产权属和交易的正确性。

（4）自我主权身份应用模型

自我主权身份通常不是一个全局的、绝对的结构，用户通过此身份可以完全控制自己的个人信息并可以根据需要共享自己希望共享的信息[88]。区块链技术的去中心化网络设施，可以帮助节点用户实现一个自我主权身份从而让用户控制自己的信息。基于区块链构建的自我主权数字身份应用模型由 4 部分组成：签发者、持有者、验证者、凭证文档相关信息，如图 7 所示。

模型中的签发者、持有者、验证者可以是任意设备、应用、个人或者组织，他们之间的关系是签发者向持有者签发可验证凭证，持有者向验证者共享出示其身份文档信息。例如，由学生（持有者）、公司（验证者）、学校（签发者）组成的应用模型中，数字身份持有者（学生）拥有自己的简历文档信息，那么学校（签发者）会校验其

简历中学历的准确性，公司（验证者）会根据自己的招聘需求查询学生（持有者）身份凭证信息，判断其是否满足用人需求。模型的整个流程如下：首先，数字身份持有者需要在区块链网络上注册自我主权身份，然后拥有加密的身份凭证数据、加密的可验证凭证和证书凭证；其次，数字身份签发者也需要到区块链网络中注册，然后向持有者签发证书、可验证凭证等声明并同时把这些声明发行上链，并进一步生成可验证凭证；再次，数字身份验证者在区块链上注册后，根据出示的证书和声明来查询区块链网络上存储的相关凭证，从而验证持有者的身份。

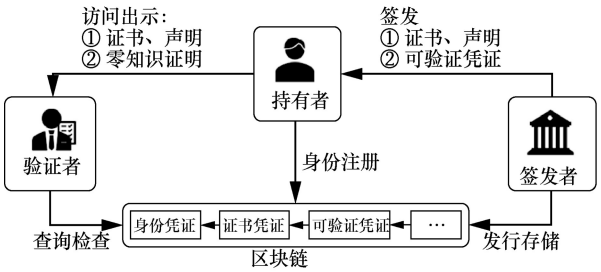

图 7　自我主权数字身份应用模型

Figure 7　Self-sovereign digital identity application model

已有很多研究者对基于区块链的自我主权身份在互联网、物联网、车联网等领域的应用进行了研究，并证明了其在身份认证方面的有效性、可行性和安全性。在互联网环境下，Fan 等[89]对基于区块链的身份安全认证系统进行了仿真分析，分析结果表明：区块链在颁发有效的数字证书后，能够准证输入公钥的用户身份信息，具有系统容错性和安全性。考虑到移动互联网中的个人隐私问题，Xu 等[90]提出了一种基于区块链的身份管理和认证方案，用户使用自我主权身份实现自己的身份由自己控制，并通过实验表明了该方案可降低撤销和通信开销。针对物联网中容易发生单点故障问题，Cui 等[91]研究了基于区块链的物联网多认证方案，实现了各种通信场景下的节点身份相互认证，分析表明该方案具有综合安全性和较好的性能。在边缘和物联网环境下，Ma 等[92]提出了一种基于区块链的去中心化身份认证模型，评估证明了该方案更安全、更可靠且容错性更强。在车联网中针对受信任的权威机构不透明、撤销证书的工作量大、身份验证和消息验证计算开销大的问题，Lu 等[93]提出基于区块链的 VANET 保护隐私认证方案，通过使用新的 MPT（Merkle patricia tree）数据结构提出了一种不带可撤销列表的分布式认证方法，并在 Hyperledger Fabric 平台上进行了性能和有效性的评估。Malik 等[94]提出了一种基于区块链的车辆网络认证与撤销框架，通过减少对可信授权机构的身份验证依赖，不仅降低了计算和通信开销，而且可以快速更新共享区块链分类账本中被撤销车辆的状态。此外，在电网环境下，杨冠群等[95]提出了基于 DID 的身份管理协议，实现了实体身份的自主控制、细粒度访问控制和可信数据交换，通过系统实验和性能分析证明了所设计系统的可用性和有效性。

综上可以看出，自我主权身份在区块链中通过匿名化、数字证书或者可控认证等身份认证方式以及身份标识和身份隐藏技术实现数字身份的完全去中心化管理[96]是有效可行且安全的。同时符合元宇宙的去中心化和自由开放的特征，不仅使用户节点拥有自主可控的数字身份，而且可以为元宇宙中的交互提供用户管理基础。

4.3　数字资产管理

元宇宙是一个属于用户的、具有连通性的、去中心化的沉浸式虚拟数字经济空间，此空间存在原始数据资产、用户创造的数字资产、现实世界平行到虚拟世界的数字资产等各种形式的数字资产。这些数字资产所有权归用户所有。本节从数字资产的定义和所有权形式入手，分析总结了 NFT 的特点以及区块链−NFT 的工作流程。

（1）数字资产的定义

从内容上讲，网络中一切以数字形式存储的内容都可以成为数字资产，如各种业务流程、业务系统、电子表格、文本文件、音频文件等数字化的运营数据都可以被认为是数字资产。从本质上讲，数字资产是数字对象衍生出的一组经济权利的集合体，是原生的、包含全量信息的、以数字形式展现和流转的资产，如数字化后的物流单据、订货合同、发票等。数字资产[97]是数字经济的中心，数字经济是元宇宙中的经济主体，区块链技术将数字资产表达为通证，实现了现实世界的资产在虚拟数字世界的数字化表达，这是元宇宙中数字经济的基础。

（2）数字资产的所有权形式

区块链上的数字资产形式主要有两种：同质化数字资产和非同质化数字资产。同质化数字资产是指资产之间遵循相同的规则，具有可置换性、可分割性、可代替性等特征，如比特币、以太币等数字加密“货币”，这类资产一般具有固定的价值，交易过程中更多关注的是他们的数量而不是他们本身的特性。而非同质化数字资产与之完全相反，非同质化数字资产具有独特性和唯一性，并且不能分割、彼此之间不能自由交换，如虚拟房屋、艺术品、游戏装备道具等，这类资产的价值往往会随着市场和稀缺性而出现浮动。

去中心化交易中同质化数字资产的形式较单一，主要是加密数字货币的形式，非同质化数字资产较丰富，音乐、电影、电视剧、课程、游戏、虚拟设备、虚拟房产、艺术品等经过数字化后，都可以作为区块链上的非同质化数字资产。那么在交易过程中如何保证其“防复制”呢？2017 年，以太坊上发布了一款使用 NFT 的加密猫（Crypto Kitties）游戏[98]，随着这款游戏的火爆，NFT 获得了广泛的关注。

（3）非同质化通证

NFT 是与同质化通证（FT，fungible token）相对应的概念，也被称为非同质化代币。每一个 NFT 在区块链中是独一无二、不可分割、不可替代的，NFT 的 6 个特征以及描述如表 8 所示。

表 8 NFT 的特征描述

Table 8 The characterization of NFT

名称	描述
标准化	NFT 具有通用标准，如铸造标准、流动性标准等。标准中还包括基本的原子操作，如所有权、传输方式和访问控制等
流动性	NFT 没有第三方的干涉，在一定程度上解决了应用程序的排他性问题，使其具有很高的流动性
不变性	NFT 永久记录于区块链中，不可改变只能相互转让，其又是完整不可分割的，就像景区门票不能半张出售一样
唯一性	NFT 所标识数字资产是独一无二的，节点用户可以通过查看 NFT 中的属性了解数字资产的相关信息
可编程性	NFT 由元数据组成并通过智能合约编程来实现其价值，CryptoKitties 和 Axie Infinity 项目[99]都引入了繁育机制
多模态化	NFT 内容形式多样化，可包含图片、视频、音频等，同时具有复合性与多变性，如有些内容是音频和视频的综合体。除了内容形式多模态化以外，其内容的存储位置也不是唯一的，可存于链上或链下

NFT 本质是一种特殊的具有稀缺性的链上数字资产，其用来验证并表达数字资产的所有权，通过智能合约来实现数字资产的转移并在区块链上记录所有权转移的整个过程[22]。NFT 是链下资产的链上凭证，将成为虚拟数字世界数字资产确权的令牌。与普通数字资产不同，NFT 加密资产可以随用随取，也能赋予数字资产所有者真正的所有权。

（4）区块链−NFT 工作流程

元宇宙中的资产主要来自两方面：现实世界中抽象后的数字资产、数字世界固有的和交互中产生的数字资产。NFT 是这些资产的版权凭证，是元宇宙中资产流转必不可少的介质，区块链−NFT 工作流程如图 8 所示。

首先，创作者上传作品到服务器形成 NFT 元数据，这些作品以图片、视频、音频等形式呈现并包含 ID、名称、创作时间等一些关键属性。然后，这些元数据经过区块链上节点共识生成 NFT 凭证并可以通过智能合约进行交易。创作者可以把资产所有权通过 NFT 凭证转让给卖方，那么卖方从链上通过智能合约获取到凭证后就对资产具有拥有权并可以进行交易。如果有买方购买数字资产，可以通过显示设备（如 DAPP）浏览观察资产，一旦交易成功买方将从区块链上得到资产所有权凭证（NFT）同时从服务器获取资产元数据，获取到的元数据会被买方重新存入服务器并赋予新的属性。

目前关于 NFT 的相关研究较少，但基于区块链−NFT 的交易在物联网、能源资产交易等系统中已实现一些具体应用。Karandikar 等[100]提出了一个基于区块链统一能源资产交易的系统，通过使用 NFT 建模实现能源资产价值交换。Sghaier 等[101]引入 ERC721 标准下的 NFT 为物联网设备提供安全的认证和授权，并在基于以太坊的私有链上进行了验证。Arcenegui 等[102]通过使用区块链和 NFT 来确认物联网设备的唯一且不可分割性，实现了物联网设备之间的自动化交易，并保

证了数据和操作的可追溯性。综合以上流程及区块链在各系统中应用可以看出，基于区块链−NFT的资产交易无须通过任何第三方服务认证即可完成，这也符合元宇宙去中心化开放自由的规则，可以为元宇宙中产生的各种数据交互提供保障。

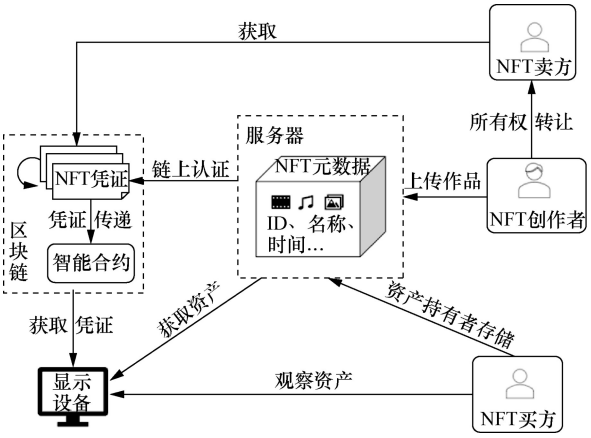

图 8　区块链−NFT 的工作流程

Figure 8　The working process of blockchain-NFT

区块链在元宇宙中的数字身份管理和数字资产管理两方面有着巨大的应用潜力。同时除了这两方面的应用外，区块链在元宇宙中的数据自治、去中心化金融、版权保护、智能软件代理等方面也具有很大的发展空间，值得进一步探究。

5　未来研究方向

区块链可以作为元宇宙建设的核心技术支撑。元宇宙的出现将促进各种新型技术的加速融合，本文从以下 4 个方面讨论元宇宙中这些技术存在的挑战并指明了未来的研究方向。

（1）基础设施

在区块链和多种分布式应用的引领下，互联网正步入下一场革命，去中心化思想正引领着这场革命。元宇宙中应该考虑所有人的基本访问权并将维护网络作为自己的职责，然而，现有网络基础设施的固有特点不可能实现理想的去中心化。因为对于个人来说，访问网络从来都不是自由的，为了使互联网实现理想的去中心化，自由和去中心化的网络接入基础设施的设计和建设将是一个未来研究的方向。

（2）通信和计算资源管理机制

元宇宙中的区块链需要通过多方共识达成一致，这会产生大量的通信和计算资源开销，同时计算资源将被纳入元宇宙资源范围作为元宇宙中的集成资产。以上过程需要解决两个问题：使用区块链构建元宇宙过程中，谁来为大量通信和计算成本买单；如何量化用户或服务提供商使用的通信和计算资源，来确定元宇宙服务的成本和价格。在此基础上，元宇宙的发展可能需要设计新的通信和计算资源管理机制。

未来，元宇宙中的通信应该是基于区块链的分布式网络，加密地址将是元宇宙提供服务的必需信息，这就导致传统的路由协议（如 IPv4/IPv6）可能不再适用，更重要的是不能根据这些加密地址精确地获取节点连接性、链路容量、路径可达性等方面的网络拓扑。因此，设计有效的完全加密的元宇宙本地通信路由方案是一个具有挑战性的问题。同时元宇宙通信系统中可能没有专门的实体负责路由功能。因此，确定由谁以及如何更新、分析、存储与路由相关的数据，从而实现数据传输的低时延和高可靠是一个相当具有挑战性的问题。此外，还有一个实际问题即一些用户节点在交互过程中可能不太愿意帮助其他人转发数据；那么精心设计区块链系统的激励方案来激励用户参与路由相关的活动可能是一个解决方案。

（3）监管与隐私保护

考虑到元宇宙中用户身份的安全与隐私，加密身份框架设计是必不可少的，同时需引发监管层面的关注，即法律应该如何监管这种加密身份。基于区块链的所有信息都被加密并封装到点对点加密隧道中，这意味着执法很难干预并可能成为犯罪活动的“保护罩”而成为执法的障碍。对于这种情况，可以在加密身份框架设计阶段考虑更多的法律因素，实现逐项管制从而避免冲突的发生。元宇宙作为一个全新的领域需要建立自己的法律伦理框架来规范用户的行为，由此从法律和工程的角度来探讨和设计元宇宙的监管规则值得做进一步研究。又由于元宇宙中不仅要对实体资产进行链下监管，还要对虚拟资产进行链上监管。那么链上监管和链下监管如何相互融合进行泛中心化监管可能会成为未来需要解决的问题。

未来基于区块链的加密身份和地址可能会面临量子计算的挑战，特别是区块链中采用的公钥

方案，如 RSA、ECC 等在量子计算机下将丧失所有的安全性。随着基于格的密码学的引入，出现了许多量子证明算法，同时格密码技术被视为下一代公钥的基础，帮助区块链对抗基于公钥的加密身份，防止量子攻击。设计防量子攻击的区块链加密方案将是一个值得探讨的问题。

（4）区块链的可扩展性和互操作性

区块链的可扩展性和互操作性是支持元宇宙广泛连接和交互的基础。然而，区块链的可扩展性和互操作性仍处于起步阶段。一些初始的扩展方案，如脱链、分片和跨链，允许区块链技术提供作为元宇宙基础设施的愿景。然而，仍然缺乏标准化的协议允许区块链的可扩展性和互操作性得到有效利用和开发。标准化的可扩展性和互操作性将允许元宇宙用户更平稳地共享 3D 世界，而不会中断不同区块链系统之间的远程操作。

元宇宙中的应用程序产生的海量数据将给用户和服务提供商带来数据处理与存储的挑战，将这些 UGC 存储在云端和边缘服务器上是潜在的解决方案，因此，将区块链与边缘计算结合，从而设计智能计算框架来处理和缓存接近数据源的 UGC 数据值得做进一步的探讨和研究。

元宇宙中的虚拟经济系统与现实经济系统紧密相连。元宇宙中的用户必须先购买通信和计算资源，才能使用实体货币访问虚拟数字世界，此外，元宇宙的创造者经济允许玩家创造和销售 NFT 来创造收益，用户在元宇宙中所产生的收入可以通过互操作性返回到现实世界的实体经济系统中。上述操作可以使元宇宙的虚拟经济得以维持，同时实体经济系统流通性也将大大增加，因此，探索使用新的区块链技术来安全实时地同步现实和虚拟经济系统是非常重要的。

6 结束语

元宇宙是现实物理世界和虚拟数字世界相互融合的新世界，也是人工智能、泛在计算、移动网络、区块链、VR/AR 等新型互联网技术的综合应用场景。在元宇宙中，区块链具有去中心化、透明性、不易篡改性、抗抵赖性、匿名性等特征，是元宇宙建设必不可少的技术之一。本文主要对元宇宙做了概述，从区块链的关键技术出发，重点讨论区块链应用在元宇宙中的可行性分析及其应用方式，提出了元宇宙生态体系架构，并分析讨论自我主权身份管理模型、区块链–NFT 工作流程及其在元宇宙中的应用，将为今后元宇宙中区块链技术的研究提供理论基础。

通过元宇宙可以看到区块链所展现出来的巨大驱动力，需要进一步研究元宇宙和区块链之间的内在逻辑。总体来说，区块链在元宇宙中的应用还处于初期阶段，元宇宙可能会重新定义区块链并把区块链技术的发展带入一个全新阶段。

参考文献：

[1] FACEBOOK INC. Introducing Meta: a social technology company[EB].

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[3] DIONISIO J D N, III W G B, GILBERT R. 3D virtual worlds and the metaverse: current status and future possibilities[J]. ACM Computing Surveys (CSUR), 2013, 45(3): 1-38.

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

[5] NING H, WANG H, LIN Y, et al. A survey on Metaverse: the state-of-the-art, Technologies, applications and challenges[J]. arXiv preprint arXiv:2111.09673, 2021.

[6] PARK S M, KIM Y G. A Metaverse: taxonomy, components, applications, and open challenges[J]. IEEE Access, 2022, 10: 4209-4251.

[7] LEENES R. Privacy in the Metaverse[C]//IFIP International Summer School on the Future of Identity in the Information Society. 2007: 95-112.

[8] WANG Y T, SU Z, ZHANG N, et al. A Survey on Metaverse: Fundamentals, Security, and Privacy[J]. arXiv preprint arXiv:2203.02662, 2022.

[9] THOMASON J. MetaHealth-how will the Metaverse change health care[J]. Journal of Metaverse, 2021, 1(1): 13-16.

[10] BOURLAKIS M, PAPAGIANNIDIS S, LI F. Retail spatial evolution: paving the way from traditional to metaverse retailing[J]. Electronic Commerce Research, 2009, 9(1): 135-148.

[11] DÍAZ J, SALDAÑA C, AVILA C. Virtual world as a resource for hybrid education[J]. International Journal of Emerging Technologies in Learning (iJET), 2020, 15(15): 94-109.

[12] DUAN H H, LI J Y, FAN S ZH, et al. Metaverse for social good: a university campus prototype[C]//Proceedings of the 29th ACM International Conference on Multimedia. 2021: 153-161.

[13] NEVELSTEEN K J L. Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse[J]. Computer Animation and Virtual Worlds, 2018, 29(1): 1-22.

[14] MOZUMDER M A I, SHEERAZ M M, ATHAR A, et al. Overview: Technology Roadmap of the Future Trend of Metaverse based on IoT, Blockchain, AI Technique, and Medical Domain Metaverse Activity[C]//International Conference on Advanced Communica-

tion Technology (ICACT). 2022: 256-261.
[15] YANG Q L, ZHAO Y T, HUANG H W, et al. Fusing blockchain and AI with metaverse: a survey[J]. arXiv preprint arXiv:2201.03201, 2022.
[16] XU H, LI Z H, LI Z Y, et al.Metaverse Native Communication: A Blockchain and Spectrum Prospective[J]. arXiv preprint arXiv:2203.08355, 2022.
[17] GADEKALLU T R, HUYNH-THE T, WANG W ZH, et al. Blockchain for the Metaverse: a review[J]. arXiv preprint arXiv:2203.09738, 2022.
[18] NGUYEN C T, HOANG D T, NGUYEN D N, et al. MetaChain: A novel blockchain-based framework for Metaverse applications[J]. arXiv preprint arXiv:2201.00759, 2021.
[19] JOSHUA J. Information bodies: computational anxiety in neal stephenson's snow crash[J]. Interdisciplinary Literary Studies, 2017,19 (1): 17-47.
[20] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the artand future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.
[21] DUSTDAR S, FERNÁNDEZ P, GARCÍA J M, et al. Elastic smart contracts in blockchains[J]. IEEE/CAA Journal of AutomaticaSinica, 2021, 8(12): 1901-1912.
[22] WANG Q, LI R J, WANG Q, et al. Non-fungible token (NFT): overview, evaluation, opportunities and challenges[J]. arXiv preprint arXiv:2105.07447, 2021.
[23] XU M, NG W C, LIM W Y B, et al. A full dive into realizing the edge-enabled metaverse: visions, enabling technologies, and challenges[J]. arXiv preprint arXiv:2203.05471, 2022.
[24] KOUTITAS G, SMITH S, LAWRENCE G. Performance evaluation of AR/VR training technologies for EMS first responders[J]. Virtual Reality, 2021, 25(1): 83-94.
[25] LIUBOGOSHCHEV M, RAGIMOVA K, LYAKHOV A, et al. Adaptive cloud-based extended reality: modeling and optimization[J]. IEEE Access, 2021, 9:35287-35299 .
[26] ZHAO H J, WU B. Three‐dimensional face modeling technology based on 5G virtual reality binocular stereo vision[J]. International Journal of Communication Systems, 2022, 35(5): e4651.
[27] BRUMENT H, BRUDER G, MARCHAL M, et al. Understanding, modeling and simulating unintended positional drift during repetitive steering navigation tasks in virtual reality[J]. IEEE Transactions on Visualization and Computer Graphics, 2021, 27(11): 4300-4310.
[28] LU J. Research on optical display technology of virtual reality technology based on optical image[C]//Journal of Physics: Conference Series. 2021, 1802(3): 032011.
[29] TIAN T, SONG G L, CHEN X, et al. Monocular stereo vision of image feature-aware interactive generation[C]//2021 International Conference on Computer Technology and Media Convergence Design (CTMCD). 2021: 281-286.
[30] ZHENG M, TIE Y, ZHU F, et al. Research on panoramic stereo live streaming based on the virtual reality[C]//2021 IEEE International Symposium on Circuits and Systems (ISCAS). 2021: 1-5.
[31] CUI D, MOUSAS C. Evaluating wearable tactile feedback patterns during a virtual reality fighting game[C]//2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct). 2021: 328-333.
[32] SIM D, BAEK Y, CHO M, et al. Low-latency haptic open glove for immersive virtual reality interaction[J]. Sensors, 2021, 21(11): 3682.
[33] HUANG S S, QI D Q, YUAN J B, et al. Review of studies on target acquisition in virtual reality based on the crossing paradigm[J]. Virtual Reality & Intelligent Hardware, 2019, 1(3): 251-264.
[34] YANG L, HUANG J, TIAN F, et al. Gesture interaction in virtual reality[J]. Virtual Reality & Intelligent Hardware, 2019, 1(1): 84-112.
[35] YANG L, W U D, HUANG J, et al. Influence of multi-modality on moving target selection in virtual reality[J]. Virtual Reality & Intelligent Hardware, 2019, 1(3): 303-315.
[36] CUI D, KAO D, MOUSAS C. Toward understanding embodied human-virtual character interaction through virtual and tactile hugging[J]. Computer Animation and Virtual Worlds, 2021, 32(3-4): e2009.
[37] SARKER I H. Machine learning: algorithms, real-world applications and research directions[J]. SN Computer Science, 2021, 2(3): 1-21.
[38] GUO M H, XU T X, LIU J J, et al. Attention mechanisms in computer vision: A survey[J]. Computational Visual Media, 2022: 1-38.
[39] ALAM M, SAMAD M D, VIDYARATNE L, et al. Survey on deep neural networks in speech and vision systems[J]. Neurocomputing, 2020, 417: 302-321.
[40] CAO K, HU S, SHI Y, et al. A survey on edge and edge-cloud computing assisted cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7806-7819.
[41] TONG Z, YE F, YAN M, et al. A survey on algorithms for intelligent computing and smart city applications[J]. Big Data Mining and Analytics, 2021, 4(3): 155-172.
[42] ABDULQADIR H R, ZEEBAREE S R M, SHUKUR H M, et al. A study of moving from cloud computing to fog computing[J]. Qubahan Academic Journal, 2021, 1(2): 60-70.
[43] JIANG W, HAN B, HABIBI M A, et al. The road towards 6G: a comprehensive survey[J]. IEEE Open Journal of the Communications Society, 2021, 2: 334-366.
[44] CAO M R, CAO B, HONG W, et al. DAG-FL: direct acyclic graph-based blockchain empowers on-device federated learning[C]//ICC 2021-IEEE International Conference on Communications. 2021: 1-6.
[45] WANG T Y, WANG Q, SHEN Z Y, et al. Understanding intrinsic characteristics and system implications of DAG-based blockchain[C]//2020 IEEE International Conference on Embedded Software and Systems (ICESS). 2020: 1-6.
[46] GAI K K, HU Z Y, ZHU L H, et al. Blockchain meets DAG: a BlockDAG consensus mechanism[C]//International Conference on Algorithms and Architectures for Parallel Processing. 2020: 110-125.
[47] XIE J, ZHANG K, LU Y L, et al. Resource-efficient DAG blockchain with sharding for 6G networks[J]. IEEE Network, 2022, 36(1): 189-196
[48] LI J R, WOLF T. A one-way proof-of-work protocol to protect controllers in software-defined networks[C]//Proceedings of the 2016 Symposium on Architectures for Networking and Communications Systems. 2016: 123-124.
[49] GANESH C, ORLANDI C, TSCHUDI D. Proof-of-Stake protocols for privacy-aware blockchains[C]//Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2019: 690-719.
[50] REN L. Proof of stake velocity: building the social currency of the

digital age[J]. Self-published white paper, 2014.
[51] KARANTIAS K, KIAYIAS A, ZINDROS D. Proof-of-burn[C]// International conference on financial cryptography and data security. 2020: 523-540.
[52] YANG F, ZHOU W, WU Q Q, et al. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism[J]. IEEE Access, 2019, 7: 118541-118555.
[53] GAO S H, YU T Y, ZHU J M, et al. T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm[J]. China Communications, 2019, 16(12): 111-123.
[54] CRAIN T, GRAMOLI V, LARREA M, et al. DBFT: efficient leaderless Byzantine consensus and its application to blockchains[C]//2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). 2018: 1-8.
[55] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Annual international cryptology conference. 2017: 357-388.
[56] CHEN L, XU L, SHAH N, et al. On security analysis of proof-of-elapsed-time (POET)[C]//International Symposium on Stabilization, Safety, and Security of Distributed Systems. 2017: 282-297.
[57] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th symposium on operating systems principles. 2017: 51-68.
[58] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.
[59] HUANG Y F, BIAN Y Y, LI R P, et al. Smart contract security: a software lifecycle perspective[J]. IEEE Access, 2019, 7: 1.
[60] DICKERSON T, GAZZILLO P, HERLIHY M, et al. Adding concurrency to smart contracts[J]. Distributed Computing, 2020, 33(3): 209-225.
[61] BARTOLETTI M, GALLETTA L, MURGIA M. A true concurrent model of smart contracts executions[C]//International Conference on Coordination Languages and Models. 2020: 243-260.
[62] SARAPH V, HERLIHY M. An empirical study of speculative concurrency in ethereum smart contracts[J]. arXiv preprint arXiv:1901.01376, 2019.
[63] CAI Z Y, QU J, LIU P P, et al. A blockchain smart contract based on light-weighted quantum blind signature[J]. IEEE Access, 2019, 7: 138657-138668.
[64] XU X W, WEBER I, STAPLES M, et al. A taxonomy of blockchain-based systems for architecture design[C]//2017 IEEE international conference on software architecture (ICSA). 2017: 243-252.
[65] 孟小峰, 刘立新. 基于区块链的数据透明化:问题与挑战[J]. 计算机研究与发展, 2021, 58(2): 237-252.
MENG X F, LIU L X. Blockchain-based data transparency: lssues and challeges[J]. Journal of Computer Research and Development, 2021, 58(2): 237-252.
[66] FALCHUK B, LOEB S, NEFF R. The social metaverse: Battle for privacy[J]. IEEE Technology and Society Magazine, 2018, 37(2): 52-61.
[67] HU P F, LI H X, FU H, et al. Dynamic defense strategy against advanced persistent threat with insiders[C]//2015 IEEE Conference on Computer Communications (INFOCOM). 2015: 747-755.
[68] WESTERLUND M. The emergence of deepfake technology: A review[J]. Technology Innovation Management Review, 2019, 9(11).
[69] 章峰, 史博轩, 蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报, 2018, 29(4): 22-29.
ZHANG F, SHI B X, JIANG W B. Review of key technology and its application of blockchain[J]. Chinese Journal of Network and Information Security, 2018, 29(4): 22-29.
[70] ZHENG Z B, XIE SH A, DAI H N, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.
[71] JIANG Y, KANG J W, NIYATO D, et al. Reliable coded distributed computing for metaverse services: coalition formation and incentive mechanism design[J]. arXiv preprint arXiv:2111.10548, 2021.
[72] 王晨旭, 程加成, 桑新欣, 等. 区块链数据隐私保护：研究现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119.
WANG C X, CHENG J C, SANG X X, et al. Data privacy-preserving for blockchain: state of the art and trends[J]. Journal of Computer Research and Development, 2021, 58(10): 2099-2119.
[73] 李少卓, 王娜, 杜学绘. 按需披露的区块链隐私保护机制[J]. 网络与信息安全学报, 2020, 46(3): 19-29.
LI S Z,WANG N, DU X H. Privacy protection mechanism of on-demand disclosure on blockchain[J]. Chinese Journal of Network and Information Security, 2020, 46(3): 19-29.
[74] 刘峰, 杨杰, 李志斌, 等. 一种基于区块链的泛用型数据隐私保护的安全多方计算协议[J]. 计算机研究与发展, 2021, 58(2): 281-290.
LIU F, YANG J, LI Z B, et al. A secure multi-party computation protocol for universal data privacy protection based on blockchain[J]. Journal of Computer Research and Development, 2021, 58(2): 281-290.
[75] LEE L H, LIN Z J, HU R, et al. When creators meet the metaverse: a survey on computational arts[J]. arXiv preprint arXiv:2111.13486, 2021.
[76] KUMAR S, BHARTI A K, AMIN R. Decentralized secure storage of medical records using blockchain and IPFS: a comparative analysis with future directions[J]. Security and Privacy, 2021, 4(5): e162.
[77] HUSSAIN A A, AL-TURJMAN F. Artificial intelligence and blockchain: a review[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(9): e4268.
[78] HEWA T, GÜR G, KALLA A, et al. The role of blockchain in 6G: challenges, opportunities and research directions[J]. 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020: 1-5.
[79] YANG R ZH, YU F R, SI P, et al. Integrated blockchain and edge computing systems: A survey, some research issues and challenges[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1508-1532.
[80] CAMP J L. Digital identity[J]. Technology & Society Magazine IEEE, 2004, 23(3): 34-41.
[81] ALLISON A, CURRALL J, MOSS M, et al. Digital identity matters[J]. Journal of the American Society for Information Science and Technology, 2005, 56(4): 364-372.
[82] GOODELL G, ASTE T. A decentralized digital identity architecture[J]. Frontiers in Blockchain, 2019: 17.
[83] 崔久强, 吕尧, 王虎. 基于区块链的数字身份发展现状[J]. 网络空间安全, 2020, 11(6): 25-29.
CUI J Q, LYU Y, WANG H. The development of blockchain-aided digital identity[J]. Cyberspace Security, 2020, 11(6): 25-29.

[84] AVELLANEDA O, BACHMANN A, BARBIR A, et al. Decentralized identity: Where did it come from and where is it going[J]. IEEE Communications Standards Magazine, 2019, 3(4): 10-13.
[85] LIM S Y, FOTSING P T, ALMASRI A, et al. Blockchain technology the identity management and authentication service disruptor: a survey[J]. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8(4-2): 1735-1745.
[86] 姚前, 张大伟. 区块链系统中身份管理技术研究综述[J]. 软件学报, 2021, 32(7): 2260-2286.
YAO Q, ZHANG D W. Survey on identity management in blockchain. Ruan Jian Xue Bao/Journal of Software, 2021, 32(7): 2260-2286.
[87] YU X Y, WANG Z J, WANG Y L, et al. Impsuic: a quality updating rule in mixing coins with maximum utilities[J]. International Journal of Intelligent Systems, 2021, 36(3): 1182-1198.
[88] FERDOUS M S, CHOWDHURY F, ALASSAFI M O. In search of self-sovereign identity leveraging blockchain technology[J]. IEEE Access, 2019, 7: 103059-103079.
[89] FAN P F, LIU Y ZH, ZHU J Y, et al. Identity management security authentication based on blockchain technologies[J]. International Journal of Network Security, 2019, 21(6): 912-917.
[90] XU J, XUE K P, TIAN H Y, et al. An identity management and authentication scheme based on redactable blockchain for mobile networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 6688-6698.
[91] CUI ZH H, XUE F, ZHANG SH Q, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN[J]. IEEE Transactions on Services Computing, 2020, 13(2): 241-251.
[92] MA Z F, MENG J L, WANG J H, et al. Blockchain-based decentralized authentication modeling scheme in edge and IoT environment[J]. IEEE Internet of Things Journal, 2021, 8(4): 2116-2123.
[93] LU Z J, WANG Q, QU G, et al. A blockchain-based privacy-preserving authentication scheme for VANETs[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2792-2801.
[94] MALIK N, NANDA P, ARORA A, et al. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks[C]//2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). 2018: 674-679.
[95] 杨冠群, 刘荫, 徐浩, 等. 基于区块链的电网可信分布式身份认证系统[J]. 网络与信息安全学报, 2021, 7(6): 88-98.
YANG G Q, LIU Y, XU H, et al. Credible distributed identity authentication system of microgrid based on blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 88-98.
[96] KUBACH M, SCHUNCK C H, SELLUNG R. et. al. Self-sovereign and Decentralized identity as the future of identity-management[C]//Open Identity Summit 2020 - Lecture Notes in Informatics (LNI) - Proceedings. 2020: 35-47.
[97] TOYGAR A, ROHM JR C E, ZHU J. A new asset type: digital assets[J]. Journal of International Technology and Information Management, 2013, 22(4): 7.
[98] Cryptokitties[EB].
[99] Axieinfinity[EB].
[100] KARANDIKAR N, CHAKRAVORTY A, RONG C M. Blockchain based transaction systemwith fungible and non-fungible tokens for a community-based energy infrastructure[J]. Sensors, 2021, 21(11): 3822.
[101] SGHAIER OMAR A, BASIR O. Capability-based non-fungible tokens approach for a decentralized AAA framework in IoT[M]//Blockchain Cybersecurity, Trust and Privacy. Cham: Springer, 2020.
[102] ARCENEGUI J, ARJONA R, BATURONE I. Secure management of IoT devices based on blockchain non-fungible tokens and physical unclonable functions[C]//Proceedings of the International Conference on Applied Cryptography and Network Security. 2020: 24-40.

[作者简介]

宋晓玲（1985– ），女，河南郑州人，重庆邮电大学博士生，主要研究方向为区块链技术及应用，数据安全及隐私保护，网络安全。

刘勇（1978– ），男，重庆人，重庆邮电大学副教授，主要研究方向为区块链、大数据、人工智能。

董景楠（1992– ），男，河南许昌人，重庆邮电大学博士生，主要研究方向为区块链、信息安全、边缘计算、大数据。

黄勇飞（1988– ），男，湖南衡阳人，重庆邮电大学博士生，主要研究方向为区块链技术及应用，量子密码。