元宇宙架构及其安全性问题分析

赵亚洲[1]，兰舒琳[2]，杨晨[3*]，王力翠[4]，祝烈煌[3]

1. 北京理工大学计算机学院，北京，100081

2. 中国科学院大学经济与管理学院，北京，100190

3. 北京理工大学网络空间安全学院，北京，100081

4. 瑞典皇家理工学院生产工程系，瑞典斯德哥尔摩，10044

摘要：元宇宙自诞生之初就在全球范围内引起了广泛关注，展现出推动人类社会实现美好愿景的巨大潜力，被称为是“互联网的终极形态”。但目前元宇宙的发展仍处于起步阶段，对相关系统架构和理论技术的研究还远未成熟。因此，本文首先基于元宇宙发展现状，从元宇宙构成要素、运行体系、角色和交互模式等方面研究提出了元宇宙架构，探讨了标识解析技术在元宇宙虚实交互场景中的应用。然后，文章重点分析了元宇宙存在的安全性问题，包括虚实交互使敏感数据和隐私问题面临的形势更加严峻，开放自由的环境成为滋生各类焦点问题的温床，虚拟经济系统与现实经济系统的相互影响，自动化算法和模型的大量应用导致不公平、歧视等伦理问题突出等。最后，本文分析了元宇宙仍面临着难以实现与现实世界之间的发展平衡，缺乏对元宇宙中技术、法律和经济层面焦点问题的有效治理手段，赋能生产生活的步伐缓慢等挑战性问题。

关键词：元宇宙架构；安全；标识解析；隐私；虚实交互；公平；歧视

Metaverse Architecture and Security Issues

Zhao Yazhou[1], Lan Shulin[2], Yang Chen[3*], Wang Lihui[4], Zhu Liehuang[3]

1.School of Computer Science, Beijing Institute of Technology, Beijing, 100081

2.School of Economics and Management, University of Chinese Academy of Sciences, Beijing, 100190

3.School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, 100081

4.Department of Production Engineering, KTH Royal Institute of Technology, Stockholm, Sweden, 10044

Abstract: Metaverse has attracted widespread attention all over the world since its birth, showing great potential to achieve a better vision of promoting human society. It is regarded as “the ultimate form of the Internet”. However, the development of the metaverse is still in its infancy, and the research on the relevant system architecture and theoretical technology is far from mature. Therefore, based on the current situation of metaverse development, this paper proposes a metaverse architecture from the aspects of the constituent elements, operation system, roles and interaction modes, and discusses the

基金项目：国家重点研发计划项目 2021YFB1715700、国家自然科学基金项目 62103046、中央高校基本科研业务费专项资金资助。

作者简介：赵亚洲，男，北京理工大学计算机学院硕士研究生，主要研究方向为智能物联网及安全。

通讯作者：杨晨，男，北京理工大学网络空间安全学院副教授，主要研究方向为工业互联网、云制造、智能系统及安全，E-mail：yangchen666@bit.edu.cn。

application of identifier resolution technology in the metaverse on the interaction between the reality and the virtual space. Then, the security issues of the metaverse are analyzed, including: the synergy of the reality and the virtual space makes sensitive data leak and privacy problems more serious; the open and free environment has become a hotbed for all kinds of hot issues; the virtual economic system and the real economic system influence each other; the massive application of automated algorithms and models brings prominent ethical problems such as unfairness and discrimination. Finally, this paper identifies the challenging problems that the metaverse still faces, such as the difficulty of achieving the balanced development with the real world, the lack of effective governance means for the key issues in the technical, legal and economic aspects of the metaverse, and the slow pace of empowering production activities and living.

Keywords: Metaverse Architecture; Security; Identifier Resolution; Privacy; Synergy Between the Reality and the Virtual World; Fairness; Discrimination

引言

“元宇宙”一词最早出现在美国作家尼尔史蒂芬森 1992 年的科幻小说《雪崩》[1] 中，小说描述未来人们的生活场景——戴上耳机和目镜，找到连接终端，就能够以虚拟分身的方式进入由计算机模拟的电子世界，在这个世界里可以完成很多现实世界中不能完成的事情。2021 年 3 月 10 日，罗布乐思（Roblox）上市，带火了元宇宙概念。2021 年 12 月，Facebook 在“Facebook Connect 2021”增强现实和虚拟现实发布会上，正式宣布改名为“Meta”，自此元宇宙在世界范围内掀起一股热潮，各大互联网头部企业争先布局，以期抢占元宇宙发展先机。

目前，元宇宙的发展仍处于概念阶段，大部分应用集中于娱乐领域，在智能制造等实体经济生产领域的应用较少。因此元宇宙是否在炒作概念、操纵收割资本市场，最终能否塑造人类社会生活的新形态，仍存在诸多不确定因素。结合当前元宇宙和新兴信息技术的发展现状，本文第一部分从元宇宙的构成要素、运行体系、角色和交互模式等方面，研究提出元宇宙的多维架构；第二部分基于元宇宙架构，重点分析元宇宙存在的安全性问题；第三部分探讨元宇宙面临的挑战性问题；最后总结了本文对元宇宙的研究。

1 元宇宙架构

元宇宙带来的全新的视听体验和娱乐方式正潜移默化地影响着我们的生活方式，元宇宙的具体定义也随着元宇宙的发展在不断丰富，目前业界对元宇宙尚无统一的定义。陈刚等 [2] 认为元宇宙可定义为：利用科技手段进行链接与创造的，与现实世界映射与交互的虚拟世界，具备新型社会体系的数字生活空间。元宇宙是整合多种新技术而产生的新型虚实相融的互联网应用和社会形态，它基于扩展现实技术提供沉浸式体验，以及数字孪生技术生成现实世界的镜像，通过区块链技术搭建经济体系，将虚拟世界与现实世界在经济系统、社交系统、身份系统上密切融合，并且允许每个用户进行内容生产和编辑 [3]。Ning 等 [4] 定义元宇宙是一个人、物和数字世界相混合的，具有沉浸式、超时空、持续连接特点的三元虚拟共享空间。元宇宙也被认为是继 web2.0 和移动互联网之后的下一代互联网的重要演变范式。

元宇宙架构是研究元宇宙各类问题的基础，已有学者从不同的角度和层面提出并分析了元宇宙架构。Duan 等 [5] 提出元宇宙三层架构，

包括基础设施层、交互层和生态系统层。Lee 等 [6] 分别从技术和生态系统两个角度，提出了包括用户交互、XR、计算机视觉、人工智能 / 区块链、机器人 / 物联网、云边计算、网络、基础设施等 8 方面的技术内容和替身、内容创作、虚拟经济、社会责任、安全和隐私、信任和责任等 6 个方面的生态系统构成部分。Lim 等 [7] 从基础设施、元宇宙驱动引擎、虚拟世界和现实世界等四个方面，系统分析了元宇宙从底层硬件，通过支撑技术驱动，构建虚拟世界，最终实现虚拟世界和现实世界的有机交互。然而到目前为止，大部分关于元宇宙架构的研究内容缺少对元宇宙构成要素、角色和交互模式等重要组成部分的研究分析。因此，本文综合元宇宙的构成要素、运行体系、角色及虚实交互模式等内容，通过构建多维度、逻辑一体的元宇宙架构，探讨元宇宙如何成为一个现实世界与虚拟世界高度融合交互的新世界。

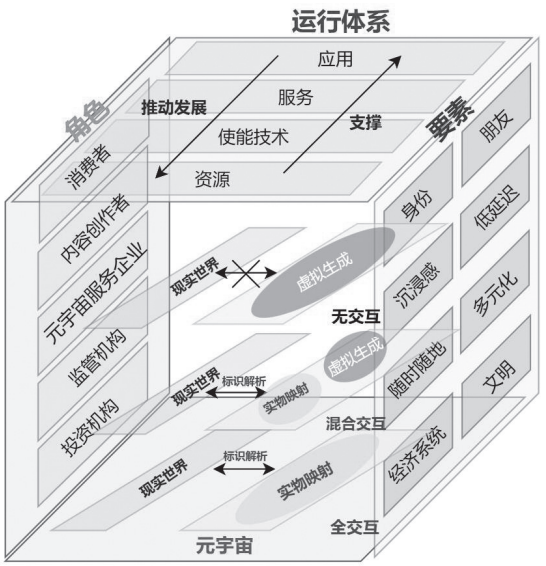

图 1　元宇宙架构

1.1 元宇宙要素

2021 年 3 月，被称为元宇宙第一股的罗布乐思（Roblox）正式在纽约证券交易所上市，Roblox 公司在其招股书中给出的元宇宙包括八大要素：身份、朋友、沉浸感、低延迟、随时随地、多元化、经济系统和文明 [8]。本文将这八大要素划分为三部分，第一部分包括身份、朋友。第二部分包括沉浸感、低延迟、随时随地。第三部分包括多元化、经济系统和文明。

元宇宙最初始的应用领域集中于游戏和社交，而“身份”和“朋友”也是进入元宇宙开展社交和游戏活动的基础。在元宇宙中，大致存在两类“玩家”，一类“玩家”是具备现实人的全部或部分属性的“数字替身”，这些“数字替身”集合了全部或部分个人信息和隐私数据，因此具备一定现实人的“身份”。另一类是基于建模仿真与人工智能技术，为维持元宇宙运行环境而创建的虚拟玩家，这类“玩家”通常与现实人不存在关联关系，类似于现在游戏中的非玩家角色（NPC）。具备不同“身份”的“玩家”在元宇宙中进行社交、游戏、工作等活动的过程中，逐渐形成了“朋友”群体。因此“身份”和“朋友”是元宇宙中密切联系的两个要素，也是元宇宙中各类活动的基础要素。

“沉浸感”、“低延迟”和“随时随地”是为支持现实中的人在元宇宙中开展各项活动而提出的技术要求。“沉浸感”的实现主要是通过 VR、AR、MR 等技术和设备让用户在视觉、听觉和触觉上达到身临其境的感觉，这是元宇宙不同于传统互联网应用的一个重要特征。“低延迟”是通过高速网络，例如高速 WIFI、5G 和 6G 等技术，来保证人在接入元宇宙后，在元宇宙中进行各项活动的实时性和流畅性。“随时随地”指可以让用户不受地理位置和物理设备的限制，能够实现随时持续进入元宇宙，从而实现更高层次的虚实交互。但目前受限于 VR、AR、MR 等技术和设备的短板约束，这一要求在短期内难以实现突破性发展。

“多元化”、“经济系统”和“文明”是元宇宙发展到一定阶段的产物。“多元化”的形成是因为元宇宙中有大量的内容创作者。他们作为用户在享受元宇宙带来各项服务的同时，也为

元宇宙的各类内容输出提供了巨大贡献。内容创作者结合用户对元宇宙的发展期望，自定义创造出一个个不同价值观、不同社会形式、不同经济体系、不同规则制度的小世界，助推元宇宙走向多元化；元宇宙的“经济系统”不仅是虚拟世界中资产流通和管理的基石，推动元宇宙生态建设，还可以与现实世界经济体系互联。例如通过区块链技术打造的 NFT 和虚拟货币在全球范围内备受追捧。随着元宇宙中虚拟经济的不断成熟与完善，虚拟经济必将作为实体经济的有力补充，推动社会经济发展；“文明”可能成为元宇宙发展的更高阶段。现实世界的文明是人类社会不断发展形成的，元宇宙中文明的发展也亦是如此。不同的是，元宇宙文明的起源于现实人在元宇宙的“数字替身”，在现代科技的加持之下，这些“替身”在元宇宙中通过各类社会活动快速形成一定规模的社会群体。随着这些社会群体规模的不断扩大，如何确保群体的稳定发展成为重点，于是一系列规则和制度被制定用来约束元宇宙中社会群体活动，最终经过一系列持续改善和变革形成了元宇宙的文明。因此，人作为现实世界文明的缔造者和主宰者，也将推动人类从现实社会文明迈向未来的元宇宙文明。

1.2 运行体系

元宇宙的运行体系从下至上主要分为资源、使能技术、服务和应用等四个层面，下层为上层提供支撑，上层推动下层不断完善和发展。

资源是构建元宇宙基础设施的集合，主要包括存储设备、计算设备、通信传输设备、数据采集设备和其他辅助设备等。元宇宙环境的构建包括大量的虚拟内容生成、实物映射和数据交互，这些任务需要强大算力、存储和数据传输能力作为保障。同时，为了实现人的持续接入运行，还需要大量的数据采集和辅助设备，捕捉人的各类生物信息，优化数据双向连接，实现元宇宙的虚实交互。

使能技术决定元宇宙未来的发展潜力。这些技术主要涉及交互技术、数字孪生、AI、物联网、区块链等。扩展现实（XR）作为交互技术的核心，是从现实世界进入元宇宙的入口。它包括虚拟现实技术（VR）、混合现实技术（MR）和增强现实技术（AR）[5]。XR 技术的目标是使人通过相关设备，如可穿戴式头戴设备，可以最大程度地沉浸于虚拟世界中，体会身临虚拟世界带来的极佳视听感受。脑机接口也是元宇宙交互技术的关键要素，通过将个人的大脑信号解码成计算机设备可识别的命令，将人类的神经世界和外部物理世界连接起来[9]。脑机接口技术的应用，打破了人的物理躯体的阻碍，使脑神经信号直接跨越肢体动作，让所想即所得成为现实。未来随着更高程度的脑机接口技术发展，人类将以更高的程度融入虚拟世界，达到更高水平的虚实结合；数字孪生是现实世界的物体或系统的在虚拟世界中高度真实的数字克隆[10]，针对元宇宙这种包含大量虚实交互和虚实映射任务的应用场景，数字孪生技术可以实现对各要素的全周期、全流程动态管理；人工智能（AI）技术将加速元宇宙的生态系统建设。近年来，人工智能在图像识别、自然语言处理等领域取得了快速进步，这些领域的研究成果可以移植到元宇宙的生态系统建设中。元宇宙的应用场景中包含大量的虚拟环境生成任务，通过人工智能技术可以自动化地生成自定义场景并有组织地呈现给用户[11]，这有助于元宇宙生态系统的建设。同时在元宇宙中还包括一些数据分析任务和推荐算法，如社交关系分析和个人喜好分析，这些都离不开人工智能技术的支持；物联网是元宇宙的重要的网络基础设施。物联网在工业制造领域得到了广泛应用[12]，提高了工业制造智能化水平。同时物联网也为元宇宙万物连接及虚实共生提供了可靠的技术保障，只有实现了万物互联，元宇宙中的虚实共生才真正有了可能[11]。元宇宙中大量运用传感器和智能设备实现元宇宙与现实世界的连接，有了物

联网技术的加持，元宇宙距离虚实共生的愿景就更近了一步；区块链技术是元宇宙中虚拟经济系统的基础。区块链技术主要包括点对点传输、数字加密技术、分布式存储、共识机制和智能合约等[13]，这些技术特点使得区块链技术被普遍认为是元宇宙经济系统的唯一解决方案，它为元宇宙提供一套确权和交易体系，以支撑跨圈层、跨生态的价值交换。元宇宙中的数字资产也因为有了区块链技术才有交易的可能。

服务是元宇宙内容建设及生态系统构建的基础。服务的主要作用是为元宇宙各类环境和内容创建提供功能高度集成的接口和技术支撑，因此元宇宙中的服务主要包括提供内容创作平台、虚拟环境生成平台和虚拟经济体系等。内容创作平台主要为内容创作者提供一系列创作集成工具，让其可以通过简化的变量描述或利用丰富的创作模板快速完成元宇宙内容的构建和开发，从而大大减少元宇宙内容创作的工作量，有助于提高内容创作者的热情，加快元宇宙生态建设；虚拟环境生成平台主要利用数字仿真技术、数字孪生技术和人工智能技术完成元宇宙虚拟环境的自动化构建，包括现实世界到元宇宙的自动化映射和元宇宙环境的自定义生成等。虚拟环境生成平台大大提高了环境构建效率和准确性，也将人从繁重的环境构建工作中解放出；虚拟经济体系主要用于支撑元宇宙中的经济行为活动，包括虚拟数字资产、加密货币和交易规则等内容。与现实中的经济体系不同的地方在于，虚拟经济体系主要利用区块链技术实现其中心化的目标，使得现实世界中的“垄断”、超发货币等现象在虚拟经济系统中不复存在。因此，虚拟经济体系可能成为更加公平的经济体系，也是元宇宙生态发展繁荣的驱动力。

应用是元宇宙构建的目标。元宇宙的应用主要集中在娱乐、工作、教育、医疗和工业生产等领域。通过基于日常生产生活需求打造的各类定制化应用，一方面利用元宇宙带来的沉浸感，丰富并改变人类的娱乐生活方式；另一方面通过虚拟世界与现实世界的深度融合，赋能工业生产和生活，提高工业生产效率，改变人类的生活方式。

1.3 元宇宙角色

元宇宙未来要走向规模化应用并产生持续经济效益，必须要建立完善的生态系统。而元宇宙生态系统的不断完善也将加速元宇宙建设力量分工，使得元宇宙生态建设更加高效专业。目前针对元宇宙中的角色大致可分为消费者、内容创作者、元宇宙服务企业、监管机构和投资机构等。

消费者是元宇宙中的主体，也是元宇宙发展的动力。一个没有消费者的市场，是无法持续的。根据中商产业研究院发布的《中国元宇宙行业市场前景及投资机会研究报告》，“十四五”期间，要发展战略性新兴产业，国家层面重视人工智能、虚拟现实、移动互联网、物联网等产业发展，国家层面及各省市“十四五”规划纲要多次提到相关行业，促进了元宇宙相关产业的发展。政策支持下，中国元宇宙产业迎来发展新机遇，预计 2027 年元宇宙市场规模将达 1263.5 亿元。由此可见，消费者是元宇宙产业发展的重要推动力量。

内容创作者是元宇宙生态系统中内容的提供方，相当于实体经济的生产者，承担输出元宇宙商品的角色。不同于现实世界，元宇宙中不存在实体物品，所有的东西都以虚拟的形式存在。内容创作者通过创作头像、艺术品、元宇宙土地、游戏卡、域名等方式实现交易变现，在提供虚拟数字物品，丰富元宇宙生态的同时，还传达着多元化的价值观。

元宇宙服务企业的主要任务是为用户、内容创作者、技术人员等各类人群提供了一个集消费、娱乐、创作、教育、工作、金融等活动于一体的平台。元宇宙服务企业既可以是提供元宇

宙接入设备和基础设施的硬件厂商，也可以是提供元宇宙应用开发平台的软件企业。

监管机构主要由政府相关职能部门组成，主要任务是实现对元宇宙的有效监管。任何一个领域或产业如果没有监管，将很难保持健康、持续发展。元宇宙作为一个新领兴域，各方面技术尚未成熟，相关的法律约束仍不完善。因此，在布局元宇宙产业发展的同时，要同步规划好政府职能部门的监管制度设计，确保元宇宙发展依规、合法、健康、可持续。

投资机构是元宇宙产业发展的出资方，是元宇宙架构中非常重要的角色。元宇宙产业落地需要大量的资金投入，用于推广元宇宙应用、开发元宇宙市场、建立元宇宙生态系统。元宇宙近年来迅猛的发展势头也得益于各大互联网巨头和投资机构的青睐，大量的投资源源不断为元宇宙产业的发展输送新鲜血液，元宇宙也因此一直保持着居高不下的发展热度。

1.4 元宇宙交互模式及关键技术

对于元宇宙未来的发展阶段展望，许多研究者都做了分析。王海龙等 [14] 将元宇宙发展演变依次划分为数据创生、数字仿生、虚拟镜生、虚实共生四个阶段，并阐述了各阶段特征及对应形态。Lee 等 [6] 概括元宇宙包括三个发展阶段数字镜像、虚实交互和超现实阶段。本文认为元宇宙的各个发展阶段是基于元宇宙不同的交互模式而变化的。元宇宙的交互模式是对现实世界与元宇宙交互的方式及程度的描述，主要分为三个层面，分别是无交互、混合交互和全交互。无交互构成的数字空间严格意义上来说不能称作为是元宇宙。无交互意味着在元宇宙内所有的人、物和环境与现实世界是不存在映射关系，这样的元宇宙是一个相对独立、封闭的虚拟空间，虽然具备高度开放和创造性的特点，但存在脱离现实的问题，难以对现实世界发展起到指导作用。混合交互在未来很长一段时间应该是元宇宙的主流应用模式，因为混合交互既保证了现实世界与元宇宙存在一定程度的交互，也保留了部分虚拟创作空间，在确保元宇宙现实应用意义的同时，也在时空维度提高了元宇宙的可扩展性。全交互的思想是在元宇宙中复制一个与现实世界完全一致的数字空间，这个数字空间里包括现实世界所有涉及的人、物和环境。数字孪生为全交互的实现提供了技术支撑，文章 [15][16] 研究了数字孪生技术在智能制造领域的应用，这些研究成果对数字孪生技术在元宇宙中的应用具有深刻的借鉴意义。显然全交互模式的优点是可以通过相关交互技术实现对元宇宙和现实世界的实时双向控制，在对现实世界影响最小的情况下实现对其有效指导。但缺点也很明显，过于全面的交互不利于元宇宙创造性和开放性特点的潜能释放，同时过多的交互也会导致资源浪费和网络攻击隐患增大的问题。

未来，随着元宇宙应用范围及规模的扩张，越来越多的物理实体和资源将实现与虚拟世界的交互，如何实现对如此庞大数量的实物和虚拟资源的高效管理将制约元宇宙的未来发展潜力。工业互联网领域的标识解析技术通过标识码为实体和虚拟的对象赋唯一的身份码，这个身份码能够记录和追溯虚拟或实体对象的全生命周期信息，从而更好地实现全寿命周期管理。工业互联网标识解析体系的对象是机器、产品等物理实体和算法、工艺等虚拟制造资源，标识解析系统根据标识查询网络位置，从而实现人与物、物与物之间的通信寻址，或者直接查询物的相关信息 [17]。因此，标识解析技术可应用于满足未来元宇宙中大规模虚实映射带来的实体和虚拟资源的管理需求，可以作为关键技术来实现对元宇宙中实体或虚拟对象的全寿命周期管理。针对元宇宙的特点，结合标识解析技术的应用。元宇宙中的标识解析技术要具备如下特点：

首先，拥有健壮的标识解析体系架构。元宇宙拥有数量庞大的物理实体和虚拟资源，这

些物品之间存在复杂的映射或关联关系，同时这些物理实体和虚拟资源在地域分布上十分广泛，因此基于元宇宙的标识解析体系必须具备极高的容错性能，这就要求标识解析体系架构要足够健壮，从而确保元宇宙的虚实交互的稳定性。如图 2，元宇宙的标识解析体系架构区分国际节点、国家顶级节点、二级节点和企业节点等，通过分层的架构设计，实现物理实体和虚拟资源的注册、接入、管理和解析等操作，大大拓展元宇宙中虚实结合能力和抵御故障风险的鲁棒性。

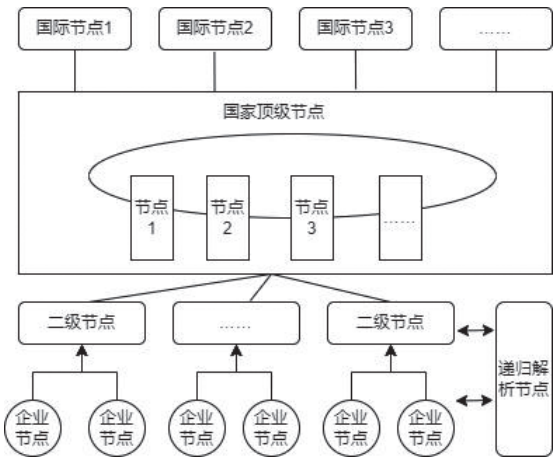

图 2　标识解析体系架构

其次，要有安全的身份认证。元宇宙虚实交互过程中存在一个极薄弱的风险点位，就是虚实映射关系容易被攻击并篡改，映射关系一旦被篡改意味着攻击者可以通过现实世界的“傀儡”潜入元宇宙中的任何位置或者成为任何人，这从网络安全防护角度是无法接受的。身份认证通过协议约束或加密等手段能够保证双方建立安全联系，确保双方在交互期间的真实对应关系。因此，对于元宇宙的标识解析体系来说，身份认证是其安全运行基础，没有身份认证，就不能保证标识解析的过程安全，元宇宙安全也就无从谈起。

此外，具备快速的溯源能力。元宇宙随时随地、低延迟的要素要求其网络支撑技术必须具备极高性能以维持连续和实时的体验感。一方面通过引入高速 WIFI、6G 等高速网络实现基础设施的改善。另一方面在现有网络基础设施之上，利用云边端计算 [18] 等新技术实现潜力挖掘。然而网络环境在不断改善的同时，元宇宙大量的虚实交互不可避免地会导致网络拥堵等问题，从而导致一些连带问题。快速的溯源能力有助于及时发现问题，解决问题。因此，针对元宇宙的标识解析体系要具备快速的溯源能力，从而提高元宇宙抵御风险能力。

2 元宇宙安全性问题分析

元宇宙复用了部分传统互联网的技术和基础设施，所以它同样面临着传统互联网的安全问题，包括网络渗透攻击、软硬件漏洞利用、木马病毒攻击等在内的各类网络安全和数据安全问题。但由于元宇宙交融性和文明性的特征 [19]，元宇宙的安全问题呈现出新特点，具体表现如下。

2.1 虚实交互使敏感数据和隐私问题面临的形势更加严峻

虚实交互是元宇宙的各类应用基础，但大量的虚实交互势必导致敏感数据泄露和隐私侵犯问题，因为虚实交互的过程进一步拓宽了非法网络活动的攻击面。目前，这类问题主要集中于两个方面，第一方面是元宇宙的社交功能本身带来的隐私问题。元宇宙社交的第一步需要将现实人的各类信息映射到虚拟世界的“替身”之上，于是“替身”就成为个人隐私信息汇聚的集合体，攻击者可以通过社会工程手段或者网络攻击技术手段完成对个人隐私信息的窃取。同时，“替身”在元宇宙的一些行为活动也在不经意间泄露大量敏感信息，包括在工作和娱乐等方面的行为数据，甚至是财产交易过程中的金融数据 [20]。针对这方面的问题，用户既可以通过创建多个替身迷惑并阻碍攻击行为，也可以创建单独的空间副本，实现与周围环境

隔离，从而实现风险规避和管控。第二个方面是元宇宙中大量的信息采集设备增加了数据泄露和滥用的隐患。为了提升元宇宙中用户体验，实现更高层次的虚实交互，元宇宙中的应用利用 VR、AR 及配套设备大量采集用户的指纹、声纹、面部、脑波等生物特征信号。对这些敏感数据的存储、传输及应用都是潜在的风险点。针对这一方面问题，要确保采集数据的保密性、匿名性、隐蔽性和无关联性 [21]。

2.2 开放自由的环境场景成为滋生各类焦点问题的土壤

第一，高度沉浸式和自定义化的场景使得不法活动展现出新形式。在元宇宙中，人们可以高度自定义周围环境、场景甚至是规则，这打破了现实世界性别、种族、年龄、地理位置和法律约束的界限。由于过于拟真的虚拟环境，使得元宇宙的参与者在特定的环境下丧失对真实情况理性的判断，这意味着传统的间谍、社会工程和诈骗等活动在元宇宙中将会变得更难以分辨，因此不法分子的实施违法犯罪活动的成功率将变得更高。同时，由于元宇宙与现实世界的割裂，使得不法分子可以在世界的任意角落对同一目标实施攻击，但溯源工作和取证量刑工作将难以开展。

第二，元宇宙可能成为人们释放压力、放纵欲望、打破现实世界伦理约束的精神场所。元宇宙高度虚拟化特点，可以让参与者完成许多在现实世界中无法完成的事情，这给暴力、色情、精神毒品等危害因素泛滥提供了温床。因此元宇宙极有可能沦为新式“精神”鸦片，未成年人或是自制力差的成年人如果过度沉溺其中，将不利于人的成长和全面发展，甚至他们会将元宇宙中的危害转嫁到现实世界，成为社会的不稳定因素。在现实世界，由于法律法规的约束，各类违法犯罪活动得到极大的抑制，但在元宇宙中，实现世界的法律并不完全适用。同时，由于元宇宙是近年来新兴领域，针对其的法律法规约束还不完善，所以，元宇宙可能成为各类新式违法犯罪的聚集地。

2.3 虚拟经济系统和现实经济系统将荣祸共生

去中心化作为元宇宙经济系统的一个重要特征，能够促进人类在元宇宙中实现同工同酬的美好愿景。但其存在一个不可忽视的弊端——不可监管。如果无法实现对虚拟经济的系统的有效监管，那么代币集资、虚拟货币非法交易等经济犯罪行为将会泛滥，进一步影响现实经济，这将大大制约元宇宙的生态系统和相关配套的发展。

NFT 作为元宇宙中经济体系中重要的组成部分大有成为元宇宙经济基石的趋势。NFT 标记了数字资产的唯一性及所有权，正因为其唯一性的存在使得 NFT 的数字产品在元宇宙中拍出天价。2022 年 2 月，一家区块链技术初创公司的首席执行官以 8000 以太币，约合 2370 万美元的价格购得 CryptoPunk #5822。这款像素风格的数字藏品之所以拍出如此高的价格，一方面确实由于它的稀缺性使然，另一方面众人的投机炒作也助推了这一乱象。然而一般现在这些数字藏品的社区通常由去中心化的组织自治运营，因此未来可能存在不受监管和法律约束的情况，这些项目在一定程度上面临违约的风险 [22]，而由此导致的经济问题也会转嫁到现实经济中。

目前来看，元宇宙和现实世界仍然是两个相互平行的世界，两个世界之间的经济交流一般通过比特币和以太坊等实现。但仅仅这有限的交流也导致了经济问题在双方之间的相互传导。2022 年北京时间 5 月 10 日早上 8 点左右，比特币短时跌破 3 万美元，最低至 29735 美元，24 小时内跌幅逾 10%。这是自去年 11 月 10 日，比特币登顶 6.9 万美元最高点后，首次跌破 3 万美元。而导致这次比特币暴跌的原因就是美

国的加息政策，也就是说现实世界的经济活动已经影响到元宇宙中的虚拟经济。未来，随着现实世界与元宇宙的更深度的融合，经济领域的相互影响将更加密切，虚拟经济系统和现实经济系统将成为不可分割的整体。

2.4 自动化算法和决策模型的大量应用导致伦理问题突出

元宇宙作为集合了各类前沿技术的互联网新领域，汇聚了大量自动化算法和模型。而这些算法模型大部分以人工智能技术为基础且代码数量庞大，所以这不可避免地带来一些算法层面的问题。第一个问题就是元宇宙应用的各类算法和决策模型的可解释性变差。试想如果人们不能解释算法或模型做出决策的依据，那意味着人们默认这些决策是正确的、公平的、客观的。然而事实并非如此，以人工智能为基础的算法和模型正不断导致伦理问题的发生，因此提高算法和模型的可解释性有助于改进算法和模型的缺点。以图像分类为例，人工智能模型或算法的输入是每个像素点颜色的 RGB 数值，这对于人类来说是很难理解的。同时随着深度神经网络的层数的增加，算法设计者也无法准确了解模型得出结果的过程。针对可解释性，文章 [23] 给出了文本和图像可解释的模型——LIME，通过词包和超像素的概念增加算法和模型的可解释性。但元宇宙涉及的数据格式种类更加多元，也包含更大数量级的数据交融，实现对多元、大量数据的解释几乎变得不可能。同时由于受限于技术和设备，未来的可解释性工作需要探索新的可解释模型从而满足元宇宙复杂庞大的应用需求。

第二个问题就是元宇宙中产生的不公平、偏见和歧视问题。元宇宙打破了种族、肤色、年龄和性别等因素的限制，因此在现实世界中常见的伦理问题将在虚拟世界中得到放大。产生这个问题的原因一方面是元宇宙虚拟的环境和较少的法律约束导致这些行为可以一定程度免受道德和法律的制裁。另一个重要的方面是元宇宙的支撑算法或模型存在伦理性问题。以往人们对于算法模型的主观印象就是客观、公正。然而随着人工智能技术大量用于决策，“信息茧房”“种族歧视”“性别歧视”等越来越多的伦理问题指向了原本“公平公正”的算法和模型，人们也开始重新审视人工智能技术给元宇宙带来的影响。为什么原本客观公正的算法或模型会存在伦理问题？这主要集中于两部分原因。一是由于市场上存在追逐利益、精致利己的企业和道德意识淡薄的算法设计师，通过收集隐私信息，设计带有歧视、偏见的不公平算法，从而取得不正当收益，这种算法自设计伊始就打上了伦理问题烙印。针对此类算法的问题，通过算法审查、白盒测试等手段就能够实现问题算法及模型的判断。另一方面随着深度神经网络的广泛应用，大量的数据用于训练模型，如果训练数据中夹杂这类问题数据，最终的训练模型也会具有伦理问题。针对这种非主观人为因素，可以通过类似于监督学习的方式实现对算法模型的全面评估。

3 挑战性问题

结合上文对元宇宙架构和安全性问题分析，元宇宙仍存在着诸多挑战性问题亟待解决。

3.1 如何实现元宇宙发展和现实世界发展之间的平衡

现阶段，元宇宙的未来发展前景并不明朗，业内针对关于元宇宙究竟是炒作概念的还是未来的技术高地的争论一直持续不断。随着全球互联网头部企业扎堆进军元宇宙同时，也有不少声音唱衰元宇宙的未来发展前景。我们要辩证地看待元宇宙是否具备实现超现实 [24] 的现实条件，既不能因为忌惮元宇宙可能会给现实世界带来的问题而过分打压元宇宙发展，也不能

因为科技巨头对元宇宙的热烈追捧而放任其自由发展。为什么产生截然不同的两种声音？首先，元宇宙去中心化的思想对主权国家构成了挑战。元宇宙发展到一定阶段后将形成与现实世界相互平行，甚至对立的多元化文明，这些文明在政治、经济、文化等方面的去中心化思想与现实世界主权国家追求集中统一的观念存在严重的矛盾和分歧，这对于一个国家来说是不可接受的。例如，以比特币为代表的加密货币在一定程度上与国家的主权货币形成了激烈竞争[22]，因此一些国家对虚拟加密货币的态度十分谨慎。其次，元宇宙带来的全新的生产生活方式，使人们在理论上可以脱离现实世界在元宇宙中长期生活。除了像吃饭、睡觉等正常的生理需求之外，人类可以在元宇宙娱乐、工作、接受教育，这对于现实世界的影响是不可想象的。由于人们几乎可以在元宇宙中成为任何想成为的样子，做到任何想做的事情，获得极佳的优越感，因此可以预见，未来越来越多的人会选择长期生活在元宇宙中，那意味着现实世界生产生活的参与者将会越来越少，与实体经济相关的各类产业就会萧条，最终可能导致无法挽回的后果。因此，对于元宇宙未来的发展，我们必须慎之又慎，综合衡量利弊，同时也不能因噎废食，要以更高的站位推动元宇宙的发展。

3.2 如何实现对元宇宙中焦点问题的有效治理

首先，从技术层面实现元宇宙的有效治理仍存在短板。针对元宇宙中通过信息采集设备等硬件设备导致的隐私数据泄露和通过新型社会工程、间谍活动实现敏感数据窃取等各类问题，还缺乏有效的技术手段实现及时、精准的安全防护；针对元宇宙涉及算法和模型产生的歧视、偏见和不公平等伦理问题，由于数据的多元和庞大，也难以短期从技术手段实现有效治理。

其次，从法律层面实现对元宇宙的有效治理仍存在诸多问题。第一是元宇宙的虚拟的环境使得法律约束的范围受限且适用性不强。例如在元宇宙中，当用户离线之后，为了维持元宇宙的持续运行，元宇宙中会有大量的算法替代用户做决策。假设在高度拟真的环境中，有用户因为这个自动决策产生轻生的行为，由此产生的后果由谁承担，算法设计者还是用户本人。类似的伦理问题在元宇宙中并不鲜见。所以，针对元宇宙中的类似问题很难通过法律实现有效治理。第二是元宇宙快速迭代发展的特性使得法律的滞后性的特点缺陷突出。元宇宙是一个瞬息万变的虚拟环境，这意味着针对元宇宙的约束规则需要随着元宇宙环境的变化而不断调整。然而法律从立法到实施需要经历一系列标准而漫长的流程，这大大削弱了法律对元宇宙的约束。甚至元宇宙可能通过利用法律的这个缺陷和自身的特性逃避法律约束。

此外，从经济层面实现对元宇宙的有效治理仍缺乏手段。现阶段，元宇宙和现实世界的融合远未达到预期水平，两者之间的经济交流也受到诸多限制，因此通过经济手段调控现实世界来影响元宇宙中的虚拟经济产生的效果十分有限。同时，元宇宙中的虚拟经济也因其去中心化的特点，使得现实世界中传统的经济调控手段在元宇宙中无法实施。如果元宇宙面临经济危机，可能会由于缺乏可用的经济调节手段，产生灾难性的后果并波及现实世界的经济体系。

3.3 如何加速元宇宙应用从社交游戏等娱乐领域向人类生产生活全方位应用的过渡

目前大部分的元宇宙应用集中于游戏、社交等娱乐领域，其主要目的是满足人类的娱乐消遣活动，但这种应用趋势将不利于元宇宙的持续、健康发展。一方面，过于集中于娱乐领域将不利于元宇宙在推动生产力的变革和改变生产生活方式方面的潜力释放。另一方面，元宇宙的娱乐应用在吸引大量的用户的同时，也使得大部分开发者蜂拥而至，导致元宇宙应用开

发力量失衡。虽然目前针对工作、教育等非娱乐领域的元宇宙应用开始陆续出现，但可能会由于需求市场萎靡，加之传统的替代应用强大的用户粘滞性，使元宇宙全面迈向改变人类的生产生活方式的步伐大大减缓，这不利于元宇宙的全面发展。

4 结语

元宇宙之所以成为众多行业巨头重金押注的未来，是因为它集合了包括交互技术、人工智能、区块链技术等在内的众多先进科技成果，向人类展示了构建一个虚实共生的“大同世界”的可能性。本文从元宇宙构建要素、运行体系、角色和交互模式出发，系统论述了元宇宙架构，重点分析了元宇宙中存在的安全性问题。然而目前要客观地认识到，元宇宙的发展还远未成熟，要以此为契机，超前部署元宇宙系统架构及安全设计，充分考虑并统筹规划元宇宙存在的诸多问题及解决方案，元宇宙也将助推人类社会实现数字化、智能化的终极目标。

参考文献

[1] Stephenson N. Snow crash: a novel[M] [S.l.]:Spectra, 2003.

[2] 陈刚 . 北京大学学者发布元宇宙特征与属性 START 图谱 [EB/OL]. 光明网 (2021-11-19)[2021-11-22]. https://view.inews.qq.com/a/2021111A02CIJ00.

[3] 胡喆 , 温竞华 . 什么是元宇宙？为何要关注它？[N]. 新华每日电讯 , 2021-11-21(004). DOI:10.28870/n.cnki.nxhmr.2021.008968.

[4] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, “A survey on metaverse: the state-of-the-art, technologies, applications, and challenges,” arXiv preprint arXiv:2111.09673, 2021.

[5] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, “Metaverse for social good: A university campus prototype,” in ACM International Conference on Multimedia (MM), Oct. 2021, pp. 153–161.

[6] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui, “All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda,” arXiv preprint arXiv:2110.05352, 2021.

[7] W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang, “Realizing the metaverse with edge intelligence: A match made in heaven,” arXiv preprint arXiv:2203.05471, 2022.

[8] Lin X. Metaverse: What? Why? When? [EB/OL]. Solactive (2021-12-20) [2022-01-03]. https://www.solactive.com/metaverse-what-why-when/

[9] Zhang X, Yao L, Wang X Z, et al. A survey on deep learning based brain computer interface: Recent advances and new frontiers[J/OL]. arXiv preprint (2021-10-12) [2022-01-15]. https://arxiv.org/abs/1905.04149.

[10] Y. Wu, K. Zhang, and Y. Zhang, “Digital twin networks: A survey,” IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13 789–13 804, 2021.

[11] 户磊 . 元宇宙发展研究 [J]. 电子产品可靠性与环境试验 ,2021,39(06):103-106.

[12] Yang C, Shen W M, et al. The Internet of Things in Manufacturing: Key Issues and Potential Applications[J]. IEEE Systems, Man, and Cybernetics Magazine, 2018.

[13] Zhai S P, Yang Y Y, Li J, et al. Research on the application of cryptography on the blockchain. J Phys: Conf Ser, 2019, 1168:032077.

[14] 王海龙 , 李阳春 , 李欲晓 . 元宇宙发展演变及安全风险研究 [J]. 网络与信息安全学报 , 2022, 8(02):132-138.

[15] Lin T Y, Jia Z, Yang C, et al. Evolutionary digital twin: A new approach for intelligent industrial product development[J]. Advanced Engineering Informatics, 2021, 47(2):101209.

[16] Lin T Y, Shi G, Yang C, et al. Efficient container

virtualization-based digital twin simulation of smart industrial systems[J]. Journal of Cleaner Production, 2020, 281(4):124443.

[17] 谢家贵 , 齐超 , 朱佳佳 . 工业互联网标识解析体系架构及部署进展 [J]. 信息通信技术与政策 , 2020(10):10-17.

[18] Yang C, Wang Y C, Lan S L, et al, Cloud-edge-device collaboration mechanisms of deep learning models for smart robots in mass personalization[J], Robotics and Computer-Integrated Manufacturing, Vol 77, 2022, 102351.

[19] 方凌智 , 沈煌南 . 技术和文明的变迁——元宇宙的概念研究 [J]. 产业经济评论 ,2022(01):5-19. DOI:10.19313/j.cnki.cn10-1223/f.20211206.001.

[20] 陈辉 , 闫佳琦 , 陈瑞清 , 沈阳 . 元宇宙中的用户数据隐私问题 [J/OL]. 新疆师范大学学报 (哲学社会科学版),2022(05):1-9[2022-06-02]. DOI:10.14100/j.cnki.65-1039/g4.20220412.001.

[21] J.A. De Guzman, K. Thilakarathna, et al. Security and privacy approaches in mixed reality: A literature survey, ACM Computing Surveys (CSUR), 2019(6).

[22] 王陈慧子 , 蔡玮 . 元宇宙数字经济 : 现状、特征与发展建议 [J]. 大数据 ,2022,8(03):140-150.

[23] Ribeiro M T, Singh S, Guestrin C. "Why Should I Trust You?": Explaining the Predictions of Any Classifier[C]/ the 22nd ACM SIGKDD International Conference. ACM, 2016.

[24] Wang, Y. Su, Z. Zhang, N. Liu, D. Xing, R. Luan, T.H. & Shen, X.S. "A Survey on Metaverse: Fundamentals, Security, and Privacy," arXiv, preprint arXiv:2203.02662, 2022.