文章编号:2096-1472(2023)08-0001-05
DOI:10.19644/j.cnki.issn2096-1472.2023.008.001

浅析元宇宙中区块链技术的应用

王 迪

(中国西南电子技术研究所,四川 成都 610036)
✉ di_wang0227@foxmail.com

摘 要:为探索元宇宙中应用区块链技术的必要性与具体方式,分别从元宇宙的发展内涵与区块链的技术特点进行归纳总结,研究元宇宙去中心化、去信任的必要性,指出区块链技术不仅可以为元宇宙提供开放自由的去中心化基础设施,而且可以为其构建公开透明的社会规则与可信金融生态。它还是分布式身份与数字资产实现的基础,是实现元宇宙不可或缺的部分。同时,阐述了通过区块链技术构建元宇宙面临的挑战,提出多学科融合的元宇宙体系建设方向。

关键词:元宇宙;区块链;去中心化;去中心化金融;智能合约
中图分类号:TP399 **文献标志码**:A

Application of Blockchain Technology in Metaverse

WANG Di

(*Southwest China Institute of Electronic Technology, Chengdu* 610036, *China*)
✉ di_wang0227@foxmail.com

Abstract: In order to explore the necessity and specific ways of applying the blockchain technology in the Metaverse, this paper proposes to study the necessity of decentralization and de-trust in the Metaverse, based on a summary of the development connotation of the Metaverse and the technical characteristics of blockchain. It points out that blockchain technology can not only provide open and free decentralized infrastructure for the metaverse, but also build open and transparent social rules and credible financial ecology for it. It is also the basis for the realization of distributed identity and digital assets, and an indispensable part of the realization of Metaverse. At the same time, the challenges of building Metaverse through blockchain technology are explained, and the direction of building a Metaverse system with multidisciplinary integration is proposed.

Key words: Metaverse; blockchain; decentralization; decentralized finance; smart contract

0 引言(Introduction)

计算机科学与技术的创新与发展不断地改变与丰富着人类社会的交流、互动和交易行为。元宇宙作为下一代具有变革潜力的普适性计算范式,旨在通过融合价值互联网、沉浸式体验与虚拟现实技术,创造出一个全新的虚实结合的环境。同时,元宇宙作为新的文明形态,必将在未来的全球格局中引发新的“文明之争”,是未来全球新的社会体系和经济秩序重组的关键[1]。

区块链技术作为支撑元宇宙的核心技术,是达成共识,实现元宇宙次序,形成元宇宙体系的关键。本文对元宇宙构成要素与区块链技术特点进行分析,探索了基于区块链技术实现元宇宙基础设施、社会规则、身份与金融生态建设的技术特点与应用的必要性,并对当前的主流技术进行了介绍,指出构建自适应、自循环、自发展的元宇宙生态仍充满挑战,需多学科融合与支撑。

收稿日期:2023-02-08

1 元宇宙概述(Overview of Metaverse)

目前,对于元宇宙尚缺乏一个公认的定义,从其特征来看,元宇宙是一个持久的多用户环境,构建了一套新的经济、社会系统,是现实世界在虚拟世界的映射,脱胎于现实世界,又相互影响[2]。元宇宙融合了虚拟现实、数字经济与人工智能等,是一个高度开放、复杂且巨大的生态系统,包含用户沉浸式、低延迟的感官体验,虚拟化的身份、资产,开放式创造的环境、社交与安全有序的经济系统。社交媒介公司 Gamer DNA 的创始人 Jon Radoff 曾经列出构成元宇宙的七层要素,描述了元宇宙的实现从底层技术到生态应用所需要的七个层面,如图 1 所示,其中包含以通信技术、芯片、传感器与仿生材料构成的基础设施层,以移动终端、交互传感器构成的人机交互层,以数字孪生技术、区块链技术、边缘计算与微服务等构成的去中心化层与空间计算层,还有为应用产品及运营生态的布局所构建的创作者经济层、发现层及体验层[3]。每一层均关系着相应的技术发展、进步与融合[4]。

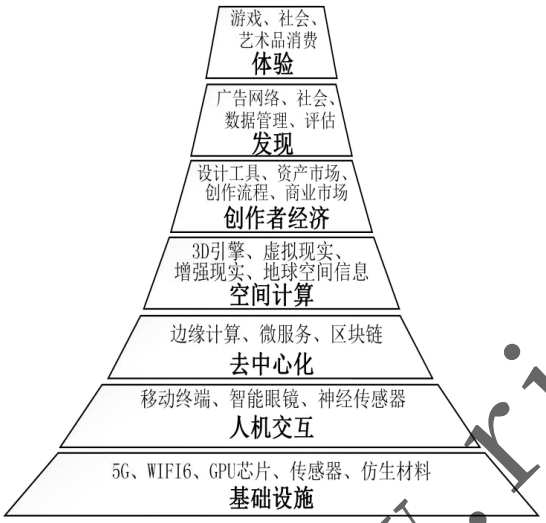

图 1 元宇宙七层架构

Fig. 1 Seven-layer architecture of Metaverse

上述七层要素构成了元宇宙的主要要素,由此可见,元宇宙是多种新兴技术相融合而产生的新型虚实相融的具备社会形态的互联网应用,它不能简单地等同于电子游戏,也不等同于虚拟世界,它基于数字孪生技术与虚拟现实技术提供类似真实世界的沉浸式体验,通过区块链技术构建元宇宙中的经济体系,将现实世界与虚拟世界的身份、金融、社交进行关联与融合,同时为用户提供生产、创作的能力。

目前,元宇宙及其相关技术已应用于游戏、虚拟社区、电子商务等领域。未来,元宇宙的落地应用还将不断扩展,有望在社交、商业、教育、医疗与军事等领域取得进一步的发展。通过元宇宙,可以为用户提供身临其境的社交与商业行为,实现虚拟的教学活动、健康咨询与疾病诊治行为。同时,元宇宙技术的应用可以为军队在训练、作战决策、情报侦察、联合作战等方面带来更多的创新和优势。

当前,元宇宙正处于起步阶段,仍面临着伦理与道德、安全与隐私、技术限制等问题,需要推进技术的创新和发展,建立和完善相应的技术规范和监督管理机制,促进元宇宙的健康发展。

2 元宇宙中相关技术(Related technologies in Metaverse)

从科学角度来看,元宇宙中的相关技术均不是新兴技术,而是多学科融合的结果[5]。元宇宙中的相关技术如图 2 所示,主要包含区块链技术、交互技术、建模与渲染技术、人工智能技术、网络及运算技术与物联网技术。

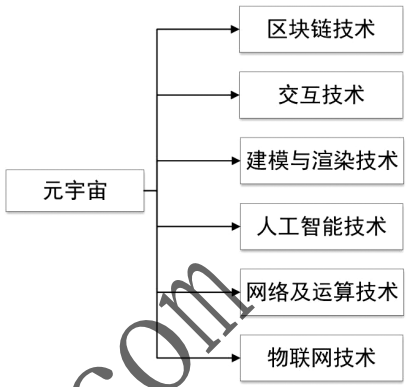

图 2 元宇宙技术构成

Fig. 2 Composition of Metaverse technology

区块链技术具有分布式、去中心化、去信任、共识与智能合约等特点,是元宇宙中建立信任、维持经济体系的重要基础。元宇宙建立的核心一定是去中心化、去信任的,只有不依赖任何中心化实现的身份认证、资产确权,才能形成庞大的经济体系,才能保障价值归属、传递与流转。通过区块链技术中的同质化资产(Fungible Token,FT)与非同质化资产(Non-Fungible Tokens,NFT)、分布式自组织(Decentralized Autonomous Organization,DAO)、智能合约(Smart Contract)与去中心化金融(Decentralized Finance,DeFi)等技术的应用,激发创作者经济模式与海量内容的创新,实现元宇宙经济体系运行的稳定性、透明性、高效性和确定性,促进元宇宙社会的自促性发展。

交互技术包含前端信息处理、声纹识别、语音识别、情感识别、人机交互与语音合成等技术,是让用户从心理和情感层面完全沉浸的关键,也是制约当前元宇宙体验的瓶颈所在,人机交互技术包含传感与体感技术,包括虚拟现实显示器、触觉、痛觉等体感技术与位置、力量、速度传感器等相应的传感技术。此外,更为复杂先进的脑机交互技术,也是交互技术的下一个发展目标。

建模与渲染技术目前主要是利用游戏引擎相关的三维建模与实时渲染,也包括在虚拟空间中实现映射的数字孪生技术,是元宇宙中逼真呈现丰富数字场景的重要技术支撑。

人工智能技术包含计算机视觉技术、机器学习技术、自然语言处理技术与智能语音技术等,通过上述技术,为元宇宙中的系统与虚拟角色提供超越人类的学习能力,同时赋予其语言识别、理解与交流的能力。

元宇宙对延时与实时渲染的要求极高,需要支持大规模用户同时在线、接入与计算,因此对元宇宙的网络性能与运算能力提出了更高的要求,目前 5G、6G、Wi-Fi 7 与边缘计算、GPU 集群技术的发展,为元宇宙提供高速、低延时、规模化接入的传

输通道，为用户提供了更实时、流畅的体验。

物联网技术为元宇宙物联网设备感知物理世界万物的信号和信息来源提供技术支撑，承担了物理世界数字化的前端采集与处理职能，同时作为媒介为虚实共生的元宇宙搭建起了虚拟世界与物理世界的桥梁。只有在实现真正的万物互联的基础上，元宇宙才能实现真正的虚实共生。物联网技术的发展，使得元宇宙中将每个现实世界的“事物”连接起来成为可能，为虚拟世界提供现实世界信息感知的能力与数据的供给。

3　元宇宙中区块链技术（Blockchain technology in Metaverse）

区块链技术是通过链式数据结构存储数据，利用分布式数据库与共识算法产生与追加数据，利用密码学技术保障交易、传输与数据存储的安全，利用公开透明且可自动化执行的智能合约，共同构建了全新的分布式基础架构与计算范式。区块链技术结合计算机科学、密码学、社会学与经济学，具备去中心化、开放性、自治性、不可篡改性与匿名性等特点，区块链本身的特点使其在身份认证、金融服务、数据协同、供应链管理等方面具有较大的应用价值。

目前，有部分学者对如何在元宇宙中利用区块链技术进行了相应的研究。YANG 等[6]研究了区块链与人工智能如何与元宇宙融合，深入探讨了元宇宙组建、数字货币等在虚拟世界的应用。郭亚军等[7]研究了元宇宙场域下的虚拟社区知识共享模式，阐述了用户在元宇宙场域下的虚拟社区进行知识共享的基本流程。GADEKALLU 等[8]从数据获取、数据存储、数据共享、数据互操作性和数据隐私保护等方面讨论了基于区块链实现元宇宙数据交互的方法。NGUYEN 等[9]指出元宇宙必须克服大量资源需求、互操作性、安全和隐私等挑战，并利用 Stackelberg 博弈论开发了一种激励机制。虽然上述研究中都提及了需要利用区块链技术实现元宇宙，但是并未对元宇宙中使用区块链技术的必要性与应用方向进行归纳阐述。

既然元宇宙的终极目标是打造一个所有人都参与其中的虚拟世界，那么就得解决所有人对这个虚拟世界的信任问题，对于该虚拟世界中的身份、资产、交易等的真实性与所有权有着绝对的信任，并且不依靠任何所谓的“可信”第三方；而区块链特有的去中心化、去信任、多方共识、不可篡改等特点，天然地成为元宇宙可信底层构建的关键技术。区块链账本间通过时间戳与哈希算法技术，为元宇宙底层数据提供了不可篡改性、可追溯性等特点；区块链的共识机制，解决了分布式网络中的信任与数据一致性问题，实现了去中心化的模式下各节点的相互证明与账本一致；区块链分布式网络构成了元宇宙的整个经济系统运行的核心基础与保障，依托智能合约自动化、可编程、易验证的特点，为元宇宙中的价值交换提供了公开、透明的执行流程与可信验证，可以在不需要任何可信第三方作为中介的情况下，实现链上的可信交互；区块链提供了定义与确权资产的技术基础，例如 NFT，作为一种元宇宙中新的价值承载物，为元宇宙中的稀有属性、稀有资产提供证明和确权，从而为实现数据内容的价值流转提供基础。因此，区块链技术所具有的安全性与隐私性、抗抵赖性和可审查性、透明性和匿名性、可扩展性和互操作性、公平性和平等性等特征可以更好地促进元宇宙的发展，解决了元宇宙中信任、资产、经济等方面问题[10]。在元宇宙中的应用价值具体体现为如下五个部分。

3.1　去中心化基础设施

区块链通过对等网络技术将所有节点连接在一起，基于分布式账本实现链上数据的分布式存储，使用共识机制与智能合约使链上各方在不需要可信第三方的基础上建立信任机制，并使用广播或多播的方式传播交易信息[11]。

P2P 网络：区块链网络中各节点采用点对点（P2P）的组网方式，各节点间处于对等的地位且具备相同的功能，无主从之分，每个节点均会参与区块链网络中消息分发、交易验证、共识等工作，并通过 Kadelima、Gossip 协议等实现节点的发现。

分布式账本：一种在区块链各节点间共享、复制和同步的分布式数据库，区块链在分布式数据库技术的基础上构建了一种以区块为单位的链式存储结构，运用密码学与时间戳等技术实现区块的串联并保障其难以被篡改。

共识算法：共识算法是维护区块链分布式账本数据一致性的核心机制，在区块链分布式网络中，通过信息交换识别恶意节点和伪造数据并达成共识，靳世雄等[12]在《区块链共识算法研究综述》中，按照主节点产生方式将共识算法分类为竞争类、选举类、随机类和其他类。①竞争类：所有参与共识的节点通过约定的竞争方式，争夺记账权，该类算法以比特币、以太坊的 POW 共识算法为代表。②选举类：节点通过投票的方式选择出主节点进行记账，选举类共识算法以 PBFT（实用拜占庭容错算法）、RAFT（容错一致性复制算法）等为代表。③随机类：通过特定的随机算法选择共识节点作为主节点进行记账。④其他类：以 Ripple 联盟链中的 RPCA（瑞波协议共识算法）、分片共识算法、基于 DAG（有向无环图）的共识算法为代表。

广播机制：区块链节点收到交易后，需要将交易进行广播，尽可能地使交易到达更多的节点，从而对交易进行验证与背书，新产生的区块也通过广播机制进行确认，从而进行全网同步，区块落盘。

只有基于去中心化构建的元宇宙，才是安全、自由和永恒的，应用区块链技术，为元宇宙带来了去中心化的网络技术、去中心化的经济体系及去中心化的虚拟世界，实现数据、存储、计算与网络传输的去中心化，使得元宇宙不是被一个或几个主体所掌控的服务器或信息系统所承载，使元宇宙中的数据、资产与身份等都属于用户个人，不会出现元宇宙被他人随意篡改、支配或破坏的情况。

3.2　公开透明的规则

区块链去中心化的特点，构建了可信的存储环境与执行环境，而智能合约则为区块链提供了可信的执行逻辑。智能合约是 20 世纪 90 年代由密码学家尼克·萨博提出的理念，他指出“智能合约的设计目标是执行一般的合同条件，最大限度地减少恶意和意外的状况，最大限度地减少使用信任中介”。随着区块链技术从数字货币到去中心化自治组织（Decentralized Autonomous Organization，DAO）的发展，智能合约在区块链技术中发挥着越来越重要的作用，智能合约为区块链平台提供了可编程性，区块链又为智能合约提供了公开、透明的执行环境。目前，智能合约已在众多区块链系统中实现，名气较大的如以太坊（Ethereum）、超级账本（Hyperledger Fabric）、Fisco Bcos 等。

以太坊中的智能合约代码是图灵完备的，基于以太坊虚拟机(Ethereum Virtual Machine，EVM)部署和执行智能合约代码，以太坊用户通过 Solidity 编程语言编写智能合约，并转换为“操作码”(Opcodes)运行。Solidity 编程语言是一种面向合约的高级编程语言，它通过 EVM 编译、部署并执行，语法类似于 JavaScript，支持强类型、继承、库以及用户自定义类型[13]。但是，Solidity 也有其特有的语言特性，包括用于定义账户的数据类型 Address，将存储类型分为内存型(Memory)与持久型(Storage)，使用关键字 Payable 定义函数是否可支持以太币或其他数字货币的收付款操作，并支持可回滚的异常处理机制等。

超级账本中的智能合约称为 Chaincode，是图灵完备的，通常用 Golang 语言编写，也支持 Java、Nodejs 等编程语言。超级账本通过“世界状态”存储当前的账本值，避免频繁地通过“遍历”区块获得想要的数据，而区块链账本本身则是记录了形成当前“世界状态”的事务日志。超级账本中的智能合约通过账本数据操作方法间接地对“世界状态”进行操作。超级账本中的智能合约代码由 Golang 语言实现，因此具有代码简洁、支持高并发、支持内嵌 C 语言与支持自动垃圾回收等特点。

Fisco Bcos 是国内企业主导研发且开源的区块链底层平台，同样支持图灵完备的合约语言，包括 Solidity(以太坊智能合约语言)、Liquid(流体模板语言)与预编译合约机制等。Liquid 由 Fisco Bcos 团队自行研发并开源，支持使用加密原语对上链数据进行隐匿，从而确保数据的安全性与隐私性；支持智能合约的安全检测，从而增强逻辑鲁棒性；支持基于 DAG 的合约并行执行技术，提升区块链平台交易的效率。预编译合约是一种使用 C++语言编写合约的方法，将合约逻辑编译至区块链平台底层中，可直接访问本地数据库，有着更好的性能表现与并行处理能力。

“代码即法律”是区块链智能合约一个显著特点。由于区块链网络本身的公开、透明及分布式的特性，使得在区块链平台运行的智能合约具备公开、透明、可验证、可自动触发等特性，智能合约一旦部署，便可以自动执行，当触发了规则所设定的条件后，就能按照设定执行相应的操作，这也是对“代码即法律”的诠释，在不需要可信第三方的基础上即可进行可信交互。如果将元宇宙中的金融系统、社会规则、法律法规构建于区块链之上，那么智能合约则可将社会运行的逻辑与规则以程序化、可信任、可验证的方法构建，从而极大地减少社会系统中存在的人为干涉等问题，可广泛应用于元宇宙中的社会自治、金融市场、交易合约等领域。

3.3 身份标识与认证

区块链中的身份标识与认证是基于区块链应用中资产确权与交易流转的基础，包含对身份的创建、恢复、认证等全生命周期的管理。区块链中的身份管理主要包括三个方面的内容，即身份标识、身份认证和身份隐藏[14]。其中，身份标识是构成链上资产权属标记和支付确权的基础，身份认证是实现交易行为权限校验的核心，身份隐藏则是链上隐私保护的重要体现。

身份标识是区块链系统中实体身份唯一性与关联性的标志，大多基于密码学协议实现，例如比特币、以太坊等公链中，身份标识即基于用户公钥经过一定规则的变换，成为用户链上的钱包地址，也是该用户的链上身份标识。在联盟链中常常基于数字证书实现用户标识，例如在超级账本中使用了 MSP(Membership Service Provider)在联盟链中进行数字证书的颁发、授权、认证与管理，MSP 基于公钥基础设施(Public Key Infrastructure，PKI)实现，通过定义身份、身份管理、身份认证为超级账本网络中的用户、组织与联盟提供服务。W3C DID(Decentralized Identifier)工作组成立于 2019 年 9 月，它定义了一种分布式身份标识规范，具有全局唯一性、高可用性、可解析性和加密可验证性等特点，可用于标识人员、组织和事物，并具备多种安全和隐私保护特性。

区块链中身份认证可分为匿名认证与实名认证，例如比特币、以太坊等公链采用无准入机制的网络架构和基于公钥、私钥的交易验证机制，为用户提供匿名认证，用户通过打包交易、利用自身私钥签名并全网广播宣布对私钥对应账户的所有权，从而实现身份认证。实名认证则需要接入证书的签发机构(Certificate Authority，CA)，通过线上或线下的身份核实与证书颁发实现对实体的身份认证。

身份隐藏主要利用隐私保护技术实现对链上用户身份的隐匿与难追踪，在加密货币中具有代表性的是门罗币，它基于 CryptoNote 底层协议实现，利用环签名、混淆地址与环机密交易，分别实现对交易发送方的不可追踪，交易接收方的不可追踪与交易金额的隐匿。在联盟链中对于身份隐私的保护常常采用密码学技术，例如盲签名、群签名、环签名、同态加密或零知识证明等，实现对交易与用户身份的隐藏或混淆。

元宇宙中实体身份的标识与认证依赖于实体发送交易上链过程中对身份合法性、签名正确性和数据完整性等信息进行校验，其中包括口令认证、密钥体制的认证与生物特征认证[15]。元宇宙中一切资产、交易与行为均建立在身份认证的基础上，区块链通过密码学机制实现的身份认证，确保“你的账号归属于你，你的身份数据归属于你，你的身份对应的资产属于你”，用户在元宇宙中的一切认证、交易行为均依赖于密码学技术，用户可以真正地享有资产的所有权，任何第三方都无法伪造、夺取或销毁它们，这是对元宇宙中数字资产确权的根本。同时，依赖于区块链中现有的隐私保护技术又可以实现对元宇宙中身份、行为信息的隐匿。

3.4 可信金融生态

近几年，去中心化金融概念的提出与发展，推动了分布式技术与金融产业的融合，DeFi 常是指基于区块链金融智能合约与分布式应用程序(Decentralized Application，DApp)所构建的数据资产金融市场，简单来说，它是建立在区块链上的金融协议与软件。DeFi 除通过数字货币作为重要组成部分外，主要通过智能合约实现自动化交易，加上其可组合性，创造出具有更多功能的金融产品，目前的去中心化金融产品包括去中心化稳定币、去中心化借贷、去中心化交易所等。

如果货币的价值时刻在剧烈地波动，就无法作为一个用于日常交易和支付的稳定货币，就如目前的数字货币，暴涨与归零比比皆是，甚至是宣称将加密货币与法定货币美元挂钩的泰达币(USDT)，因为无法公开审计，所以常常被人们质疑其超发。去中心化稳定币通过智能合约与抵押数字资产发行，当抵押数字资产到智能合约，合约通过从各大交易所获取抵押资产的加权平均价值，发行一定比例且低于抵押率的稳定币资产。去中心化稳定币通过超额抵押与目标利率反馈机制确保其价

值的相对稳定。这里分为两种情况,如果抵押资产升值,意味着更高的抵押率,这不会对系统带来风险,但如果抵押资产贬值,如资产价值下降到一定值,并且原抵押人没有追加抵押物或偿还稳定币,则合约会自动启动清算。

去中心化借贷可分为 P2P(点对点)模式、稳定币模式、流动池模式,均基于区块链智能合约实现。P2P 模式将借贷双方撮合在一起,通过智能合约约定借贷条款与抵押物,当借款人无法还款时,智能合约自动执行清算。稳定币模式就如上述的去中心化稳定币的发行,广义来讲也是一种去中心化的借贷模式。流动池模式中借贷双方通过流动的数字资产交易池进行交易,而不是直接与交易对手进行点对点匹配,每笔交易的利率与收益由交易池的流动性大小确定。

去中心化交易所本质是通过智能合约实现资产托管、撮合交易、资产清算等功能,实现了去信任的交易机制,杜绝了交易所的运营、道德与安全风险,但去中心化交易所中所有的交易均会记录上链,受当前公链交易速率影响,不能处理大并发实时交易。

经济系统的高效、持久与稳定将会成为元宇宙大规模运行的关键,而区块链技术天然具有的去中心化、去信任、可信价值流转的特征将为元宇宙提供可信、高效且自动运行的金融生态系统,交易双方或多方无须依赖可信第三方,仅依赖区块链网络中的智能合约与共识即可实现信任的传递,使得元宇宙中不会再出现银行间结算、对账所带来的消耗,使得元宇宙中的人们可以以更低的成本和更快的速度进行交易。

3.5　数字资产管理

纵观整个人类发展史,交易都是社会属性中非常重要的一环,资产数字化是元宇宙中的又一关键特点,元宇宙社会中需要一种安全、可靠、可追溯、透明的数字资产定义与交易方式,从根本上保证用户的自由。元宇宙无中心、自成体系的经济系统,需要在去中心化的场景下实现资产价值的描述与确权,通过区块链与智能合约技术构建的同质化资产与非同质化资产为元宇宙中的资产进行合理、高效与可靠的定义,使元宇宙中资产数字化成为可能。

目前,具有代表性的基于区块链的资产协议为以太坊开发的 ERC-20 与 ERC-721。

ERC-20 为同质化资产协议,它所描述的代币(Token)的价值与属性一致,可实现拆分与完全等价的互换,在 ERC-20 中描述了如何铸币、如何传输代币、批准交易与抵押以及用户如何查看代币数量与总量等,为元宇宙中货币的定义提供了技术基础与规范。

ERC-721 为非同质化资产协议,是一种基于区块链技术的数字化凭证,它具有唯一、不可分割、可验证与可追溯的特点,可以用来描述特定资产并标识其所有权,因此非常适合对具有唯一性且不可分割的权益或资产进行定义,并可以实现自由交易和转让,为元宇宙中房产、艺术品等虚拟资产的定义与使用提供了标准。

基于区块链实现的同质化资产或非同质化资产在确权、交易与可信度等方面,有着其他技术不能比拟的优势,可满足元宇宙中资产数字化的要求,为元宇宙社会、经济的发展提供基础。

4　区块链构建元宇宙生态挑战(The challenges of building Metaverse ecosystem with blockchain)

元宇宙依托区块链技术构建去中心化的网络模式,使元宇宙中各实体形成彼此交织的生命,构建复杂有序的经济模式、纷至沓来的社会与井然有序的群体,就比如蜂群。凯文·凯利[16]在《失控——全人类的最终命运和结局》一书中所提到"蜂群思维"的神奇之处在于蜂群思维是一种集体思维,单只的蜜蜂并不能控制蜂群,但是每只蜜蜂作为独立单元通过"连接"构建了这样一个蜂群系统。蜂群中没有强制的中心控制,蜜蜂高度自治又相互连接,依赖不可见的群体规则达成目标,当蜜蜂大量聚集,则会形成质变,蜂群的特性就会从单个蜜蜂中显现出来。这就像是区块链中的分布式网络,不依赖于强大的中心化机构,网络中各成员有自治的倾向性和组织方式,成员间通过点对点的关系而非线性的关系组建网络,这正是区块链技术的初衷和效用。目前,公链最为成功的应用场景——数字货币,就如"蜂群",有着高度自治的倾向性。每位"矿工"为了自己利益拼命争夺记账权利,同时利用相应规则巧妙地解决了区块链双花、恶意攻击等问题,极大地维护了账本的安全性。

在区块链技术的创世论文"Bitcoin-A Peer-to-Peer Electronic Cash System"中提到,解决双重记账消费问题的方案,来自采信最长的链,最长的链不仅证明了事件发生的顺序,而且证明了它来自最大的算力池[17]。这里面有一个隐含的非技术的"利益"问题,"矿工"为了自己能够获得记账权和交易费,会选择最长的链进行计算,因为短的链大概率会被丢弃,同时不能获得收益,这样的选择反过来又保障了比特币网络的安全性。但是,对于区块链系统,它验证不了任何系统自身之外产生信息的真实性,同时系统内的信息脱离系统也毫无意义。

基于区块链技术构建的元宇宙,它应该是分布式的、封闭的、自治的与利益统一的,元宇宙中基于区块链技术构建的金融体系与社会生态就如现实世界一样,具备自适应、自循环、自发展的特性,最终达成稳态,但这又是极其困难的。就如 1991 年美国为模拟人类生态环境打造的生物圈 2 号,虽然投入巨大,但是最终以失败告终。

因此,如何基于区块链或其他现有技术构建这样一个复杂封闭的系统,如何建立一种高度自治、利益统一的群网络,如何实现自循环、自发展,推动元宇宙社会就如同人类社会一样的不断发展与进步,是目前应用区块链技术构建元宇宙的难点,也是区块链技术本身真正落地的鸿沟,这不仅是技术的问题,还涉及博弈论、社会学等学科领域。

5　结论(Conclusion)

本文从元宇宙技术构成与区块链技术在元宇宙中的应用必要性与应用方式进行了阐述,指出区块链技术可极大地杜绝中心节点的作恶,实现去中心化、去信任与开放性,真正实现规则公开透明、信息不可篡改、资产与身份归属个人,是构建元宇宙基础设施与经济体系不可或缺的部分,是元宇宙稳定、高效、透明和确定性运行的保障。同时,对构建元宇宙提出思考,如何通过区块链技术结合博弈论、社会学等学科,打造自循环、自发展的元宇宙生态,仍是当前构建元宇宙生态和区块链技术落地面临的挑战。

(下转第 10 页)