DOI：10.61189/304718qrovcm

·专家述评·

# DID在元宇宙医学中的应用探索

高承实*
安徽栈谷科技有限公司，池州 247100

［摘要］ 随着元宇宙医学的发展，患者身份管理、数据隐私保护及跨机构数据共享成为亟需解决的核心问题。去中心化身份（decentralized identity，DID）作为一种基于区块链的身份管理方法，为元宇宙医学提供了可信、可验证且可自主可控的身份体系。本文系统分析了DID的技术原理、架构模式及在医疗场景中的应用实践，梳理了国际、国内的探索案例，并对技术、法律、伦理和产业层面的风险与挑战进行了深入讨论。在此基础上，提出了未来发展方向，包括DID与隐私计算、数字孪生和AI医疗助手的融合，全球虚拟医院身份互认体系的构建，多方协作治理模式以及学科交叉研究的必要性。研究表明，DID在解决“身份可信性、隐私可控性与数据共享性”三重矛盾方面具有显著优势，为元宇宙医学的安全、合规与高效发展提供了关键支撑。

［关键词］ 去中心化身份（DID）；隐私保护；数据共享；跨机构互操作性；数字孪生；多方协作治理
［中图分类号］ R-0　　［文献标志码］ A

**Exploration of the application of did in metaverse medicine**

GAO Chengshi*
Anhui Stack Alley Technology Co., Ltd, Chizhou 247100, Anhui, China

［**Abstract**］ The emergence of metaverse medicine has introduced critical challenges in patient identity management, data privacy, and cross-institutional data sharing. Decentralized identity (DID), a blockchain-based identity framework, provides a verifiable, trustworthy, and user-controlled solution for these challenges. This paper presents a systematic analysis of DID's technical principles, architectural designs, and applications in healthcare, reviewing both international and domestic implementations. It further examines associated risks and challenges across technical, legal, ethical, and industrial dimensions. Future directions are discussed, including the integration of DID with privacy-preserving computing, digital twins, and AI healthcare assistants, the development of globally interoperable virtual hospital identity systems, multi-party governance models, and interdisciplinary research initiatives. The findings indicate that DID effectively addresses the triad of identity trustworthiness, privacy control, and data shareability, offering foundational support for the secure, compliant, and efficient advancement of metaverse medicine.

［**Key Words**］ decentralized identity (DID); privacy protection; data sharing; cross-institution interoperability; digital twin; multi-party governance

随着虚拟现实（VR）、增强现实（AR）、区块链以及人工智能等技术的迅速发展，医学正快速迈入元宇宙医学时代。元宇宙医学不仅包括沉浸式的医学教育、虚拟手术模拟和远程康复训练，还涵盖了跨地域协作、数字孪生人体、虚拟医院等新型医疗形态。然而，在这一过程中，身份管理与隐私保护成为绕不开的核心难题。

首先，医学数据具有高度敏感性。患者的病历、基因数据、影像资料往往涉及个人隐私乃至家族风险，一旦泄露可能造成严重的社会与法律后果。因此，元宇宙医学中的任何交互场景，无论是医生资质验证、患者远程诊疗，还是跨机构病历共享，都必须建立在可信的身份识别与隐私保护基础之上。

其次，现有的医疗身份体系存在显著局限。一方面，大多数医院和医疗机构依赖于本地或区域性的电子病历（EMR/EHR）系统，导致数据难以跨机构、跨区域互操作，患者就医过程中往往需要重复检查和信息录入。另一方面，传统的身份验证机制高度中心化，例如依赖医院内部的账户体系、政府颁发的身份证号或医保卡号。这种模式在虚拟空间中难以直接套用，且容易产生身份伪造与数据滥

［收稿日期］ 2025-09-12　　［接受日期］ 2025-09-25
［作者简介］ 高承实，博士，副教授.
*通信作者（Corresponding author）.Tel: 13838001036. E-mail: 13838001036@163.com

用的风险。

此外，远程医疗与虚拟医院的兴起，对身份信任体系提出了更高要求。在跨国界、跨区域的虚拟医疗服务中，医生如何证明其真实身份与执业资质？患者如何在不暴露全部隐私信息的情况下获得诊疗服务？医疗设备、虚拟人体（数字孪生）又该如何建立与现实世界的一一对应关系？这些问题都凸显了传统身份管理体系的不足。

在法律与合规层面，全球主要国家和地区均在加强医疗数据的隐私保护。例如，欧盟的《通用数据保护条例》（GDPR）[1]、美国的《健康保险可携性与责任法案》（HIPAA）[2]、中国的《个人信息保护法》[3]均对医疗数据的收集、存储、处理和跨境传输提出了严格要求。这些法规不仅强调了“最小化收集”和“知情同意”的原则，也对身份识别和授权机制提出了要求。在元宇宙医学环境中，身份认证与数据访问更加复杂，如何在合规的同时实现高效的医疗服务，是亟待解决的难题。

## 1 去中心化身份（DID）的基础与原理

在此背景下，去中心化身份（decentralized identifier，DID）逐渐进入研究者与产业界的视野。与传统身份体系不同，DID倡导“用户自主管理身份”，通过密码学与分布式账本技术实现身份标识的可验证与不可篡改。更重要的是，DID能够结合可验证凭证（verifiable credentials，VC）等机制，在不暴露完整信息的前提下，向验证方证明“我是谁”或“我具备某种资质”[4]。例如，患者可以仅证明自己“已年满18岁”而无需泄露出生日期，医生可以证明自己“拥有某项手术执业资质”而不必公开全部执业信息。这种特性为元宇宙医学中的身份与隐私管理提供了新的解决思路。

1.1 DID的概念与发展背景 去中心化身份（DID）是指一种无需依赖中心化身份提供者，由用户自主管理的身份体系。与传统身份体系（如政府身份证、医院账户或第三方认证系统）不同，DID的设计理念是“用户主权”，即用户能够自主管理自己的身份信息，并选择性地向验证方披露数据[4]。

DID概念源于分布式账本技术的发展。随着区块链在金融、供应链、物联网等领域的应用，研究者逐渐认识到，分布式账本天然具备数据不可篡改、可追溯、去中心化信任的特性，可以用来构建跨域、无需中心化机构管理的身份体系。W3C在2022年发布了DID 1.0标准，定义了DID的核心结构、解析方法及与可验证凭证的交互规范[4]。

在元宇宙医学背景下，DID的价值尤为突出。它不仅可以保护患者隐私，实现数据可控共享，还可以用于验证医务人员资质、保障医疗设备的可信性，为数字孪生与虚拟医院提供可信身份基础。

1.2 DID的核心要素 根据W3C DID标准及相关研究，DID主要由以下三个核心要素组成[4-5]。

一是DID标识符（decentralized identifier）。DID是一种全局唯一的标识符，用于标识一个身份主体（个体、组织、设备、数字孪生等）。DID的格式通常为“did:方法名:标识符”，例如“did:example:123456789abcdefghi”。“方法名”指定了DID的解析和注册规则，而“标识符”唯一标识了身份主体。

二是DID文档（DID document）。DID文档是存储在区块链上或分布式存储系统中的JSON或JSON-LD数据结构。DID文档包含公钥、服务端点、验证方法等信息，用于支持身份验证和加密通信。通过DID文档，验证方可以获得与DID关联的公钥，从而完成身份认证与消息加密。

三是去中心化验证机制。DID的可信性依赖于分布式账本或去中心化网络，而非单一机构。用户持有私钥，通过签名证明自己对DID的控制权。验证方使用公钥验证签名，从而确认身份的真实性。

通过上述三个要素，DID实现了身份的自主管理、可验证以及不可篡改。

1.3 可验证凭证 DID本身只提供身份标识，但医疗场景经常需要证明某种属性或资质，例如“医生具备心脏手术资质”或“患者已完成疫苗接种”。此时，可验证凭证（VC）成为关键机制[4]。

VC的核心思想是，发行方颁发凭证，持有者保存凭证，验证方验证凭证。在元宇宙医学中，VC的应用示例，首先是对医务人员进行资质验证，医院或专业机构作为发行方，颁发医生执业凭证（VC），医生将凭证存储在个人DID钱包中，参与远程手术或虚拟诊疗时，可向虚拟医院验证资质而无需泄露完整信息。之后对患者健康状态进行证明。疫苗接种、慢病管理、检验结果等证明可作为VC颁发给患者，患者可选择性披露某些信息，例如仅证明“已完成疫苗接种”，而无需公开具体接种日期或个人敏感信息。

通过VC，DID可以实现“数据可用不可见”，这是元宇宙医学中身份与隐私管理的核心优势。

1.4 DID与传统身份体系的比较 传统EMR/EHR与医保电子凭证以“机构—平台”为中心，患者账号受限于院端或国家库，跨院需重复注册、调阅依赖接口开放，存在数据孤岛与隐私泄漏风险。DID将身份与

凭证拆分为患者自持的加密钥匙与可验证凭证，跨院、跨省无需新建账户，通过链上信任注册表即可秒级验证，真正实现“我的数据我做主”。在落地层面，DID可复用现有EMR/EHR的数据出口与医保结算通道，医院继续按HL7/FHIR保存完整病历，仅将摘要、授权与状态写入VC，既保留集中系统的大容量、高性能，又获得去中心化网络的互操作性和隐私保护，二者互补形成“链上身份+链下数据”的新型医疗数字底座。DID与传统中心化身份的比较及其在元宇宙医学中的意义如表1所示。

**表1　DID与传统中心化身份的比较及其在元宇宙医学中的意义**

| 特性 | 传统中心化身份 | DID（去中心化身份） | 元宇宙医学意义 |
|---|---|---|---|
| 管理主体 | 政府、医院、第三方平台 | 用户自主管理 | 患者/医生可自主控制信息披露 |
| 数据存储 | 中心化数据库 | 分布式账本/联盟链 | 跨机构互操作，防篡改、可追溯 |
| 信任模式 | 信任中心化机构 | 密码学+分布式共识 | 虚拟医院、远程诊疗环境中无需单点信任 |
| 隐私保护 | 受限，中心化平台可访问 | 可选择性披露，结合零知识证明等 | 保护患者敏感信息，实现合规数据共享 |
| 可扩展性 | 跨机构复杂，互操作差 | 方法可扩展，可支持多种医疗场景 | 支持数字孪生、虚拟医院、远程诊疗等新场景 |

从表1可以看出，DID在患者数据主权、医务人员资质验证、跨机构互操作性和隐私保护方面具有显著优势，这也是本文后续分析其在元宇宙医学中应用的理论基础。

1.5　*DID的技术优势与医学应用价值*　DID在元宇宙医学中具有多重优势和价值。首先是身份自治，患者和医务人员可完全控制自己的身份信息，不依赖中心化平台。其次是数据可控共享，通过VC或零知识证明，允许有限信息披露，实现跨机构医疗数据共享。三是防篡改与可追溯，利用分布式账本技术，所有身份操作均可记录、验证和追溯。四是跨平台互操作性，DID体系基于开放标准，可与不同医院系统、虚拟医疗平台和国际标准（如HL7 FHIR）对接。最后还支持数字孪生与虚拟设备绑定，每个数字孪生或IoT设备均可通过DID绑定身份，实现可信的虚拟—现实对应关系。

综合来看，DID不仅是一种技术机制，更是元宇宙医学中身份治理与隐私保护的基础设施，为后续的应用场景分析和技术实现提供了理论支撑。

## 2　医学应用场景分析

DID在元宇宙医学中的典型应用场景，涵盖了患者健康身份管理、医务人员资质认证、虚拟医院与远程诊疗，以及医疗设备与数字孪生体身份。上述场景中的应用，揭示了DID的实际价值与潜在应用路径。

2.1　*患者健康身份管理*　在元宇宙医学环境中，患者健康信息的跨机构共享和隐私保护是核心问题。传统医疗体系下，患者的病历信息分散在不同医院、实验室和健康管理平台，跨机构访问往往依赖纸质病历或中心化系统授权，效率低且存在隐私泄露风险。通过DID与可验证凭证（VC）的结合，患者可以实现自主管理健康身份，同时支持可控共享。具体应用包括以下几个方面。

一是个人健康档案（PHR）管理。患者通过个人DID钱包管理电子健康档案；医疗机构可通过验证患者DID与VC来确认身份及健康状态；支持选择性信息披露，例如仅提供过敏史、免疫接种记录或慢病管理状态，而不泄露全部病历信息。

二是跨医院病历整合。利用DID进行患者身份统一识别，确保不同机构的病历信息可溯、可验证。结合零知识证明，可在不透露敏感数据的前提下，实现数据可信共享。例如患者在虚拟医院接受远程诊疗时，医生只需验证关键健康信息即可制定治疗方案，而无需访问完整历史病历。

三是动态授权与隐私控制。患者可根据不同场景动态授权数据访问，例如一次性授权、限时授权或按功能授权。权限变化通过区块链记录，实现操作可追溯，防止滥用。

通过以上应用，DID为患者提供了“自主可控、可验证、跨机构互操作”的健康身份管理，实现了元宇宙医学中身份与隐私的双重保护。

2.2　*医务人员资质与执业认证*　在虚拟医疗环境中，医生和护理人员的身份验证与资质确认尤为关键。传统认证模式依赖中心化机构颁发的纸质证书或电子认证，这种证书或认证存在以下局限：跨境远程手术或远程会诊难以实时验证资质；纸质或单一数字证书易被伪造或篡改；不利于虚拟医院、远程诊疗等新型医疗模式的扩展[6]。

DID与VC提供了一种新的解决方案。在资质颁发与存证环节，医疗监管机构或医院作为VC发行方，将医生执业资质、手术权限等信息颁发给其

DID;VC数据通过区块链或分布式账本存储,保证不可篡改。在动态验证与使用场景环节,医生在虚拟手术、远程诊疗或学术交流中,可通过VC向医院或患者验证资质,而无需公开完整信息,并且支持动态更新,例如手术许可到期、培训更新等。在跨境与跨机构互操作环节,DID体系支持全球标准化解析,使医生资质在不同国家或地区的虚拟医院互认,减少跨境医疗服务的身份信任壁垒,提高远程医疗效率。

通过这种方式,DID体系不仅确保医务人员身份的真实性,也为虚拟医疗场景提供了安全可信的资质管理机制。

2.3 *虚拟医院与远程诊疗* 随着VR/AR技术的发展,虚拟医院和远程诊疗逐渐成为元宇宙医学的重要组成部分。在此场景下,身份验证与隐私保护面临更高要求。一是双向的身份验证,患者DID与医生DID的双向验证可以确保双方均为真实、授权的主体。结合零知识证明技术,患者可在不泄露全部个人信息的前提下完成身份确认。二是虚拟诊疗流程设计。患者通过DID钱包提交必要健康信息;医生通过VC验证执业资格;虚拟医院系统通过区块链或联盟链验证双方身份及权限,完成安全诊疗。三是数据隐私与合规,所有身份与权限操作均可链上记录,实现可追溯性。结合加密存储、访问控制和隐私计算,满足GDPR、HIPAA等法规要求。四是跨平台互操作性。支持多种虚拟医疗平台和远程诊疗系统的身份互认,便于实现患者健康数据和诊疗记录的跨平台共享。

通过上述机制,DID为虚拟医院与远程诊疗提供了身份可信、数据安全、隐私可控、跨平台互操作的技术基础。

2.4 *医疗设备与数字孪生体身份* 在元宇宙医学中,医疗设备及数字孪生体的身份管理同样关键。医疗IoT设备的DID化,使得每个智能医疗设备(如可穿戴设备、监测仪器)均可注册DID,这样既确保了数据来源可信,也防止了数据伪造或篡改。

一方面是数字孪生身份绑定。患者的数字孪生体可通过DID与真实个体绑定,实现虚拟与现实的可信对应。结合区块链记录,确保数字孪生体操作和数据可溯源。另一方面是跨设备协作与数据整合。多种医疗设备数据通过DID与患者DID关联,实现统一身份管理。支持智能诊疗系统进行数据分析、AI辅助诊断,而不暴露敏感信息。通过对设备与数字孪生体的身份治理,DID不仅保障了数据可信性,也为虚拟医疗环境中复杂实体的管理提供了标准化方法。

综上所述,DID在元宇宙医学中呈现出广泛的应用价值。在患者健康身份管理方面,实现了跨机构、跨场景的数据可信共享与隐私保护;在医务人员资质管理方面,保障远程医疗与虚拟手术的身份真实性与资质可验证性;在虚拟医院与远程诊疗方面,支持双向身份验证、隐私计算与合规管理;在医疗设备与数字孪生方面,确保数据来源可信、操作可追溯、虚拟实体与真实个体一致性。这一系列应用场景为元宇宙医学中的身份与隐私治理提供了可行路径,也为后续技术实现和案例分析提供了具体实践依据。

## 3 技术实现与系统架构

DID在元宇宙医学中的技术实现路径和系统架构设计,涵盖了DID注册与解析、可验证凭证(VC)管理、身份验证流程、隐私保护机制以及与现有医疗信息系统的集成。

3.1 *DID注册与解析* DID的技术实现首先依赖于身份的注册与解析机制,这一过程确保了每个身份的全局唯一性和可验证性[7]。

DID注册。用户或设备在注册时生成一对公私钥,通过公有链或联盟链发布DID文档。DID文档包含公钥、服务端点、验证方法等信息,用于后续身份认证和数据交互。在医学场景中,患者、医务人员及医疗设备均可注册DID,实现统一身份标识。

DID解析。验证方在需要确认身份时,通过DID解析机制获取DID文档。解析方法依赖于具体的DID方法(method),如did:example、did:ethr、did:indy等,不同方法对应不同的底层账本和解析规则。在元宇宙医学中,解析过程必须保证高可用性和低延迟,以满足虚拟诊疗和实时交互需求。

链上与链下存储结合。DID文档可存储在公链、联盟链或分布式存储系统中(如IPFS、Arweave),保证数据不可篡改与可溯源。对于敏感信息(如患者病历、医疗设备参数),可采用链下加密存储,并在DID文档中存放索引或加密指针,兼顾安全性与性能。

3.2 *可验证凭证(VC)管理* 在DID架构下,可验证凭证(VC)用于证明身份属性和资质,是元宇宙医学中隐私保护与信任建立的核心机制。

VC的颁发。医疗监管机构、医院或实验室作为VC发行方,为患者、医务人员或设备颁发凭证,凭证内容可以是执业资质、疫苗接种记录、病历摘要、设备认证信息等。VC使用发行方私钥签名,确

保证书的真实性与完整性。

VC 的存储与管理。用户通过 DID 钱包或客户端存储 VC，并可在不同虚拟医疗平台携带和使用。支持多重凭证管理，如按场景、按时间、按角色进行分类存储。

VC 的验证与隐私保护。验证方使用发行方公钥验证 VC 的真实性。结合零知识证明（ZKP）技术，可以在不泄露全部属性的前提下验证特定资质。例如，患者可证明“已接种疫苗”而不泄露具体时间或品牌。这种机制在跨医院、跨地区、跨平台的远程诊疗中尤为关键。

3.3　*身份验证与访问控制流程*　在元宇宙医学中，身份验证流程需同时满足安全性、效率性与隐私性。在身份认证流程中，患者或医务人员通过 DID 钱包发起认证请求；系统解析 DID 文档，获取公钥及验证方法；使用签名或加密挑战—响应机制完成身份验证。

在授权与访问控制环节，用户基于 VC 授权访问特定资源（如病历、影像、设备数据），授权信息通过智能合约或链上策略存储，保证不可篡改和可追溯。支持细粒度权限控制，包括按角色、按时间、按功能授权。

在多方协作场景中，比如在虚拟手术或远程诊疗中，患者、医生、设备均可通过 DID 完成身份互认证，系统根据 VC 和访问策略动态控制数据流向，保证隐私保护和合规性。

3.4　*隐私保护与安全机制*　DID 在元宇宙医学中的隐私保护依赖多种技术手段。一是加密存储与通信。患者数据、VC、设备信息均采用对称或非对称加密存储；通信过程使用 TLS 或端到端加密，防止数据在传输中泄露。二是零知识证明（ZKP）与选择性披露。ZKP 技术允许用户证明某一属性的真实性，而无需公开具体信息。例如，患者可证明“血糖水平在安全范围”而不泄露具体数值。支持 VC 的选择性披露，实现最小化信息共享原则。三是链上审计与可追溯性。所有身份操作、凭证颁发和访问授权均记录在区块链公有链或联盟链上；审计日志可用于合规检查和事件追溯，防止滥用或身份冒用。四是防篡改与防重放攻击。利用区块链不可篡改特性保证身份数据及 VC 的完整性，签名和时间戳机制防止重放攻击，确保身份验证安全可靠。

3.5　*系统架构设计*　结合前述技术实现，元宇宙医学中 DID 系统的典型架构可分为五层，如图 1 所示。

身份层（DID 层）管理患者、医生、设备及数字孪生体的 DID，提供身份注册、解析和公钥管理服务；凭证层（VC 层）颁发、存储、验证 VC，支持选择性披露与零知识证明，提供跨平台、跨机构的资质与健康状态认证；访问控制与策略层基于智能合约或链上策略进行权限管理，支持动态授权、时间/角色/功能控制和多方协作；应用服务层支撑虚拟医院、远程诊疗、数字孪生交互、医疗 IoT 数据管理等具体应用，提供身份验证接口、VC 验证接口及安全通信服务；数据存储与隐私保护层用于链上存储 DID 文档和策略信息，链下加密存储敏感数据，实现数据可溯源、不可篡改，同时保证隐私保护。

通过该架构设计，DID 系统可以在元宇宙医学中实现身份可信、数据安全、隐私可控、跨机构互操作的技术目标。

## 4　案例与实验探索

本节将以实际案例和实验为基础，分析 DID 在元宇宙医学中的落地尝试，包括国际探索和国内探索。通过对比不同实践经验，可以为未来在国内外医疗场景中推广 DID 提供参考。

4.1　国际探索

4.1.1　*欧盟 EBSI 在医疗身份管理上的尝试*　欧洲区块链服务基础设施（European Blockchain Services Infrastructure，EBSI）是欧盟委员会与成员国联合建设的跨境区块链基础设施，明确将 DID 与 W3C 可验证凭证（VC）作为其“数字信任基建”核心组件之一。EBSI 提供了专门的 DID 方法规范（did：ebsi / 针对自然人与法人不同的 DID 方法）、DID 注册/解析（DID Registry API）、以及面向 VC 的数据模型与工具链（钱包、解析库、issuer registry 等），并在教育、职业证书与若干公共服务场景开展跨境试点。

就健康医疗方向，EBSI 的治理与技术栈支持将凭证颁发方（issuers）列入“可信发行者名单”，凭证以加密/选择性披露方式在持有者钱包中保存，验证时通过 DID 文档和信任注册表完成验证与状态检查，从而在合规（GDPR）约束下实现跨国凭证互认。若干学术/行动研究也用 EBSI 做了跨境凭证验证的实证（教育/证书领域的试点经验对医疗凭证设计具有直接借鉴意义）。EBSI 的医疗身份管理探索主要包括以下几个方面[8]。

一是去中心化身份（DID）与医疗凭证。EBSI 推出了基于 DID 的可验证凭证（VC）框架，支持医疗从业者资质、患者健康信息和疫苗接种记录的数字化。在试点项目中，患者可通过 DID 钱包存储健康凭证，并在不同欧盟成员国的医疗机构之间共享，

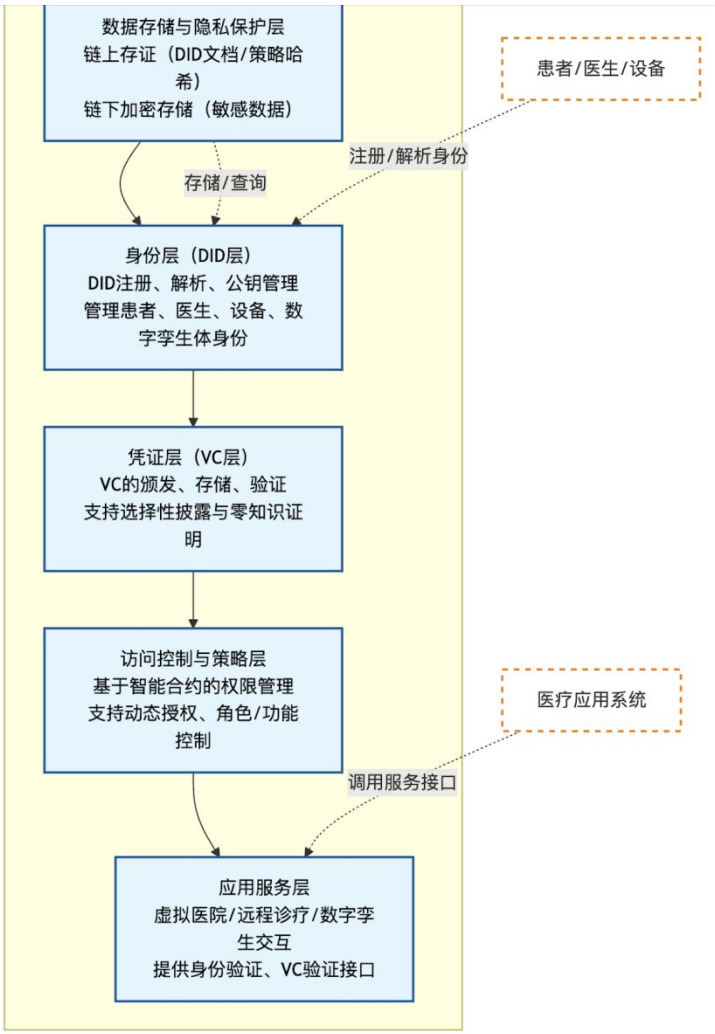


**图1 元宇宙医学中DID系统的典型五层架构**

实现跨境互认。

二是跨机构互操作性。EBSI利用统一的DID方法和链上服务端点，实现医疗机构之间的身份互认与数据共享。支持GDPR合规，凭证数据采用加密存储和选择性披露，确保患者隐私。

三是试点成果与挑战。初步试点显示，使用DID与VC可有效减少跨机构病历验证时间。该试点尚未大规模进入生产环境，仍属Pre-Production阶段，在试点场景下能够显著提高医疗服务效率。面临的主要挑战包括，不同成员国法规差异、现有医疗信息系统兼容性、用户教育和数字素养。

欧盟EBSI统一DID方法当前版本为did:ebsi v2.0，支持在Polygon与Hyperledger Fabric双链部署，而非单一公链。上述工作表明，EBSI已把DID/VC从概念推进到可操作的跨境基础设施与试点工具，技术细节（DID方法、DID Registry、VC data models、issuer registry、resolver libraries等）均在官方hub文档中公开[9]。

4.1.2 美国MediLinker基于Hyperledger Indy/Aries的医疗DID/VC原型与可用性评估

MediLinker是由美国大学研究团队（以德州奥斯汀Dell Medical School等机构为主）开发的患者中心化身份管理原型，采用Hyperledger Indy + Hyperledger Aries实现去中心化标识与凭证交换，前端为用户钱包（可持有多类VC：健康ID、保险、药物清单、疫苗/COVID-19状态、研究同意等）。该项目包括技术设计论文（阐述DID/VC模式、链上保存DID与凭证schema，链下/离线数据用FHIR标准互操作）和以模拟就诊场景的可用性/功能性测试。

公开论文报告，在30人的模拟测试中29人完成全部活动，系统在七类临床场景（签到、共享凭证、撤销授权等）中均能实现预期功能；后续的可用性调查显示大多数受访者愿意采用该类患者自主管理的凭证模型（论文中披露了具体的完成率与用户反馈）。这些论文清晰记录了实现栈（Indy/Aries、钱包、凭证类型、与FHIR的接口说明）与测试结果，

表明 Hyperledger Indy/Aries 在“医疗场景的原型/POC”中已具备可操作性，但仍处于实验/小规模试点与用户测试阶段，而非大规模生产部署[10]。

4.1.3　美国 MITRE 与 Mayo Clinic 分布式身份实验　美国 MITRE 和 Mayo Clinic 开展了针对分布式身份在医疗领域的实验，重点探索患者和医疗从业者的可信身份管理。

MITRE 基于 Hyperledger Indy 和 Aries 框架，构建了实验性的医疗 DID 系统。支持患者对病历、实验室结果和疫苗记录的自主控制，并可选择性分享给医生或保险机构[11]。

Mayo Clinic 将 DID 与远程诊疗平台结合，医生和患者通过 DID 钱包完成身份验证。实验显示，使用 DID 与 VC 可以显著提升远程诊疗的安全性和用户信任度，同时在试点场景下减少重复验证步骤，降低中心化身份管理成本[12]。

美国相关实验给我们的关键启示是，分布式身份在医疗场景中可增强信任、保障隐私，但对系统性能、用户操作便捷性和合规性提出了高要求。

4.2　国内探索

4.2.1　医保电子凭证与健康码的潜在对接　中国的医保电子凭证和健康码体系已广泛应用于日常就医和公共健康管理，其与 DID 的对接具有潜在价值。在医保电子凭证方面，电子凭证已实现患者身份验证和医疗费用结算数字化，但仍依赖中心化机构管理。如果引入 DID，患者可自主控制凭证授权，增强跨机构、跨省就医的便利性。在健康码与疫情防控数据方面，健康码记录的个人健康状态和疫情相关信息，可通过 DID 与 VC 的方式实现可验证共享。患者可选择性披露健康状态，兼顾隐私保护和防疫要求。

4.2.2　医疗联盟链案例　国内部分医疗联盟链也在探索去中心化身份的应用，杭州、深圳等地具备联盟链基础设施，学者已提出引入 DID 的框架[13]，但尚未公开落地试点，技术路径可参考欧盟 EBSI 与国际 MITRE 经验。相应的应用实践可以包括医院间病历信息共享、医务人员资质验证、远程会诊身份确认均可通过 DID 实现。初步研究显示，DID 有助于降低身份管理复杂度，提高数据共享效率，同时兼顾隐私保护。

通过国际、国内的案例可以看出，DID 在元宇宙医学中具有以下特点。一是身份可信、跨机构互操作。DID 可统一患者、医生和设备身份，实现跨平台和跨机构的数据共享。二是隐私可控、选择性披露。结合 VC 与零知识证明技术，患者可自主管理数据共享范围。三是实践成熟度差异明显。欧盟和美国在实验性应用上更为成熟，而国内在联盟链与电子凭证层面逐步探索。这些案例为后续技术标准制定、系统部署和政策规划提供了经验和借鉴，同时也揭示了跨国法规、技术兼容性和用户接受度等未来挑战。

## 5　风险与挑战

随着去中心化身份（DID）在元宇宙医学中的应用逐步推进，尽管其在身份可信、隐私可控和跨机构互操作性方面展现出显著优势，但在技术、法律、伦理及产业层面仍面临诸多风险与挑战。

5.1　技术层面的挑战　可扩展性问题。元宇宙医学涉及海量患者、医疗机构及设备数据。DID 系统需支持高并发身份注册、凭证颁发和验证。因此，首先面临的挑战就是链上性能限制。大部分 DID 方法依赖区块链或联盟链存储 DID 文档或索引，链上吞吐量直接影响注册和验证效率。当前公链如 Ethereum 每秒可处理交易数有限，可能无法满足大规模医疗场景需求。其次是链下存储与计算压力。为保障隐私，敏感信息通常在链下采用加密存储，链上仅存索引或哈希。大规模医疗数据的加密、解密及访问控制可能导致系统计算压力增加，影响响应速度。

跨链互操作性。元宇宙医学必然涉及不同区块链网络、联盟链和医疗信息系统，不同 DID 方法的底层账本不一致，导致解析、验证和凭证共享复杂化。Cosmos IBC 与 Polkadot DID 模型为医疗凭证跨链提供了现成的底座，IBC 轻客户端可让医院联盟链在分钟级内同步患者 DID 文档与 VC 状态，无需新建网关即可与区域健康链互通；Polkadot 平行链架构则允许医保、药监、科研三条异构链各自运行专用 DID 方法，通过中继链共享信任根，实现“一键跨域”授权。借助跨链 DID，患者在国内就诊后，可将疫苗 VC 通过 IBC 实时传递至海外旅行保险链，自动触发保障生效，真正将“链上健康护照”融入全球医疗生态。但跨链互操作目前仍缺乏统一标准，需要协议层协调、智能合约桥接和中继机制支持。

用户友好性。DID 钱包和 VC 管理对非技术用户仍存在一定门槛。医疗场景中，患者和医务人员操作复杂度过高可能影响接受度和使用体验。需要设计简单、易操作的身份管理客户端，同时保证安全性。

5.2　法律与合规层的挑战　隐私法规冲突。欧盟

GDPR强调数据主体控制权和数据最小化原则，而中国《个人信息保护法》在数据存储和跨境传输上有不同要求。跨境医疗数据交换过程中，DID系统需兼顾不同法律框架，确保合法合规。

责任认定与审计。去中心化身份系统去除了单一中心化机构，这导致在发生数据泄露或身份滥用时，责任归属复杂。必须结合链上审计和可追溯机制，明确医疗机构、平台和用户各方责任。

5.3 伦理层的挑战 数据自主权与公共利益平衡。DID提供患者对数据的完全控制权，但在公共卫生、疫情防控等场景中，过度自主可能影响公共利益。如何在保护隐私的同时，确保必要的公共健康数据共享，是伦理层面亟需解决的问题。

信息不对称与数字鸿沟。不同患者在数字素养、设备获取能力上存在差异。高技术门槛可能导致部分群体难以获得虚拟医疗服务，增加社会不平等。

信任与透明度。虽然区块链和DID技术本质上增强透明性，但复杂的加密和零知识证明机制可能令用户难以理解验证过程。如何提升用户信任，同时保证技术复杂度不影响可用性，是伦理设计的重要考虑。

5.4 产业层的挑战 基础设施建设。医疗DID系统需要高可靠的链上节点、存储系统和安全通信通道。对医院、远程诊疗平台和虚拟医疗企业而言，部署和维护成本较高。

商业模式可持续性。虚拟医疗和元宇宙医疗场景中，DID系统的盈利模式尚不明确。如何在保证数据隐私与安全的前提下，实现系统的商业可持续发展，是产业化推广的关键问题[7]。

标准化与生态建设。缺乏统一标准和规范可能导致各平台DID和VC无法互操作。医疗元宇宙生态中，标准化工作、跨机构合作和行业联盟建设亟需推进。

技术、法律、伦理与产业层面的挑战相互交织。技术层面，可扩展性、跨链互操作性和用户友好性仍需优化。法律与合规层面，跨境法规差异和责任认定问题影响系统推广。伦理层面，需平衡数据自主权与公共利益，同时关注信息不对称和信任问题。产业层面，基础设施投入、商业模式和标准化建设是推广关键。这些挑战表明，元宇宙医学中DID的广泛落地仍需技术优化、政策引导、伦理审视及产业协同，以实现真正安全、可信、可持续的数字身份管理。

## 6 未来展望

随着去中心化身份(DID)在元宇宙医学中的探索不断深入，技术成熟度、产业应用和政策环境均呈现加速发展趋势。未来，DID将不仅是身份管理工具，更可能成为元宇宙医学可信体系的核心支撑。

6.1 技术融合 未来元宇宙医学将呈现多技术融合的趋势，DID将与隐私计算、数字孪生及AI医疗助手深度结合。

首先是DID + 隐私计算。隐私计算技术(如同态加密、联邦学习、多方安全计算)可在保证数据不泄露的前提下进行跨机构分析。与DID结合后，患者数据可以安全参与算法训练或远程诊疗，同时保持身份不可伪造和隐私可控。

其次是DID + 数字孪生。每位患者的数字孪生体可以与DID绑定，实现虚拟医疗环境中的个性化互动。数字孪生体不仅承载病历和健康状态，还能在虚拟诊疗、手术模拟、康复训练中充当可信代理。

再次是DID + AI医疗助手。AI医疗助手依托DID认证和VC验证，能在虚拟诊疗场景中为患者提供个性化建议，同时确保交互数据的安全性。结合智能合约，AI助手的诊疗行为和决策可被链上审计，提高可追溯性与合规性。

技术融合将进一步提升元宇宙医学中身份管理的可信度、安全性和效率，同时为远程诊疗、虚拟医院及健康数据分析提供基础保障。

6.2 产业走向 未来元宇宙医学的产业发展将趋向全球化和平台互操作化。全球虚拟医院身份互认体系将满足跨境医疗、远程诊疗及国际科研合作的需求，将推动全球虚拟医院建立统一的身份互认体系。基于DID和VC，患者身份、医疗从业者资质和设备认证可以实现跨国、跨平台互认，从而打破地域限制。

产业链延伸与商业模式创新。DID作为基础设施，可延伸至医疗保险结算、药品供应链、健康管理服务等环节。企业可基于DID提供增值服务，如虚拟健康档案管理、个性化健康推荐、数字孪生手术训练平台。

标准化与生态建设。全球虚拟医疗生态需要统一身份标准、协议规范和数据互操作标准，以推动产业健康发展。标准化可降低跨平台应用成本，提升系统可靠性和用户接受度。

6.3 治理模式 DID在元宇宙医学中的应用将促使治理模式由单一机构管控向多方协作转变。

首先是多方协作治理。政府、医疗机构、技术平台和患者共同参与 DID 系统管理。智能合约和链上策略可保证治理过程透明可审计，确保各方权责明确。

其次是动态授权与策略管理。随着医疗场景的多样化，访问权限和数据使用策略将动态调整。DID 系统结合 VC，可实现按角色、按时间、按功能的精细化权限控制，提高治理灵活性和合规性。

最后是合规与标准监管。去中心化身份的推广必须在法律法规框架内开展，结合区块链审计机制实现监管与隐私保护的平衡。跨国应用场景下，需要建立国际协作的治理机制，协调不同国家隐私法规的差异。

6.4　学科交叉　未来元宇宙医学中的 DID 研究将成为多学科交叉的前沿领域。医学提供临床需求和应用场景，定义患者、医生及医疗设备身份管理的功能和规范。计算机科学负责 DID、VC、零知识证明、隐私计算、数字孪生和智能合约等技术的研发与优化。法律研究跨境数据流通、患者隐私保护和责任认定等法律问题，为 DID 落地提供合规依据。伦理学探讨数据自主权、公共利益、数字鸿沟与信任等问题，为系统设计提供伦理指引。

通过学科交叉合作，可形成技术、法律和伦理的有机统一，推动元宇宙医学身份管理系统在安全、合规和可持续方向发展。

未来展望显示，DID 在元宇宙医学中的应用前景广阔。在技术层面，DID 与隐私计算、数字孪生和 AI 医疗助手的融合将显著提升身份可信度和医疗服务效率。在产业层面，全球虚拟医院身份互认体系和标准化生态建设将推动跨境虚拟医疗发展。在治理层面，多方协作治理模式、动态权限管理和合规监管将成为新趋势。在学科交叉方面，医学、计算机、法律与伦理的深度融合将为技术落地提供全面支撑。

DID 将不仅是身份管理工具，更是元宇宙医学可信生态的核心支撑，为未来虚拟医疗服务的安全、合规与高效提供坚实基础。

## 7　结　论

本研究系统梳理了去中心化身份（DID）在元宇宙医学中的理论基础、技术架构、应用场景及实际案例，并对风险、挑战和未来发展进行了深入分析。通过前文的探讨，可以得出以下主要结论。

7.1　DID 在元宇宙医学中的核心价值　DID 通过提供自主、可信、可验证的身份标识，为元宇宙医学中的各类参与主体建立了统一的身份基础。其核心价值主要体现在三个方面。一是身份可信性。DID 采用分布式账本和加密算法，使患者、医生及医疗设备的身份可被安全验证，防止伪造和冒用。通过可验证凭证（VC），医疗从业者资质、患者健康信息及数字孪生均可在虚拟环境中得到可信确认。二是隐私可控性。患者数据通过选择性披露、零知识证明等技术实现自主管理。数据使用、访问范围和共享对象均可由数据主体自主控制，有效保护隐私，同时满足医疗和科研的合规要求。三是跨机构共享性。DID 提供统一身份体系，支持不同医院、虚拟诊疗平台及跨境医疗机构的数据互操作。医疗信息可以在保持隐私的前提下进行安全交换，为远程诊疗、全球虚拟医院及医疗科研提供基础支撑。

7.2　解决“身份 + 隐私 + 共享”三重矛盾　元宇宙医学面临的核心矛盾，一是身份可信性与去中心化。传统中心化身份管理存在单点失效风险，而 DID 在分布式账本上实现身份验证与可追溯。二是隐私保护与数据共享。患者隐私与医疗数据共享需求存在天然冲突，DID 与 VC、隐私计算结合可实现选择性共享与最小化数据暴露。三是跨机构互操作性与安全性。多机构、多平台协作要求身份和数据互操作，同时保证安全合规，DID 提供可验证的身份锚点，为安全数据交换提供支撑。

因此，DID 在元宇宙医学中实现了身份可信、隐私可控与跨机构数据共享的平衡，为解决这一“三重矛盾”提供了可行路径。

7.3　未来研究与政策建议　基于本文分析，未来研究与政策可从以下几方面推进。

在技术优化方面，提升 DID 系统的可扩展性和跨链互操作性，优化链上链下协同存储与计算机制；改进用户界面和交互体验，降低非技术用户操作门槛。在产业生态建设方面，推动全球虚拟医院身份互认体系和标准化协议建设，形成跨境、跨平台的医疗身份生态；鼓励初创企业和科研机构探索创新商业模式，实现技术落地与可持续发展。在法律与合规指导方面，协调不同国家和地区的隐私法规差异，建立跨境数据流通合规框架；明确去中心化身份的责任归属与审计机制，为监管提供依据[5]。在伦理与社会研究方面，平衡数据自主权与公共利益，关注数字鸿沟和信息不对称问题；探索医学、计算机、法律与伦理交叉的多学科研究，为系统设计提供指导。

通过技术、政策、伦理及产业的协同推进，DID 有望在元宇宙医学中发挥核心作用，促进可信、隐

私友好和高效的医疗服务发展。

总的来看，DID在元宇宙医学中的应用不仅是身份管理手段，更是虚拟医疗生态可信体系的基石。它为患者自主控制数据、保障隐私安全、实现跨机构数据共享提供了技术支撑；同时，也对法律合规、伦理规范和产业模式提出了新要求。未来，随着技术优化、标准化推进和多学科协同，DID将在全球虚拟医疗体系中发挥越来越重要的作用，为元宇宙医学的可持续发展提供坚实保障。

**伦理声明** 无。

**利益冲突** 所有作者声明不存在利益冲突。

**作者贡献** 高承实：选题，撰写、修改论文。

## 参考文献

[1] 欧洲议会与理事会. 欧盟通用数据保护条例(General Data Protection Regulation, GDPR)[S]. (2016-04-27)[2025-09-01]. https://gdpr-info.eu/

[2] U. S. CONGRESS. Health Insurance Portability and Accountability Act of 1996 (HIPAA)[S]. Washington, D. C.: U. S. Government Printing Office, 1996.

[3] 全国人民代表大会. 中华人民共和国个人信息保护法[S]. (2021-08-20)[2025-09-01]. http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html

[4] SPORNY M, LONGLEY D, CHADWICK D, 等. 去中心化标识符(DID)v1.0：核心架构、数据模型与表示法[EB/OL]. (2022-07-19)[2025-09-01]. https://www.w3.org/TR/did-core/.

[5] ALLEN C. The Path to Self-Sovereign Identity [EB/OL]. (2016-04-26)[2025-09-02]. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

[6] ZHUANG Y, ZHANG W, NI J, 等. 基于区块链的医疗数据共享去中心化身份管理研究[J]. 工业信息化学报, 2022, 18(12): 9292-9301.

[7] 葛 锐, 廖方宇, 姜 文, 等. 分布式数字身份及其在科学数据共享中的应用前景[J]. 数据与计算发展前沿, 2023, 5(5): 46-59.

[8] European Commission.. Application and Exploration of the European Blockchain Services Infrastructure (EBSI) in Healthcare Identity Management [EB/OL]. (2025-07-09)[2025-09-02]. https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

[9] European Commission. What is EBSI? [EB/OL]. Digital Building Blocks, (2025-07-01)[2025-09-25]. https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/590447955/What%2Bis%2BEBSI

[10] KHURSHID A, HOLAN C, COWLEY C, et al. Designing and testing a blockchain application for patient identity management in healthcare[J]. JAMIA Open, 2021, 4(3): ooaa073.

[11] M P V, QURASHI S N, SOBIA F, et al. Decentralized identity management using blockchain for healthcare systems[C]//2024 IEEE Silchar Subsection Conference (SILCON 2024). November 15-17, 2024, Agartala, India. IEEE, 2024: 1-6.

[12] Mayo Clinic. Distributed identity for remote telehealth: Joint POC with MITRE [EB/OL]. (2021-06-30)[2025-09-25]. https://newsnetwork.mayoclinic.org/discussion/mayo-clinic-platform-and-mitre-explore-distributed-identity-for-telehealth/.

[13] 王 伟, 李 娜. 医疗联盟链中去中心化身份(DID)的应用研究[J]. 中国医疗信息化, 2022, 28(3): 45-49.

**引用本文**

高承实. DID在元宇宙医学中的应用探索[J]. 元宇宙医学, 2025, 2(3): 1-10.

GAO C S. Exploration of the application of did in metaverse medicine[J]. Metaverse Med, 2025, 2(3): 1-10.