未来网络发展大会
FUTURE NETWORK
DEVELOPMENT CONFERENCE
NANJING · CHINA / 中国 · 南京

未来网络技术发展系列白皮书（2025）

面向Web3.0的数字实体互联白皮书

第九届未来网络发展大会组委会

2025年8月

版权声明

编写说明

主要编写单位：

中国联合网络通信有限公司研究院

青岛大学数字社会研究所

中钞数字信息科技（北京）有限公司

紫金山实验室

主要编写人员：

贾雪琴、詹立东、平庆瑞、曹畅、唐雄燕、张岩、史可、王立文、曹云飞、王施霁、霍如、刘辉、王志浩

前　言

2024 年 1 月 31 日，习近平在中共中央政治局第十一次集体学习时强调“高质量发展需要新的生产力理论来指导”。传统的 ISO/OSI 等经典网络理论，虽然涵盖了联网设备之间，从物理连接、数据传输、会话管理到应用服务的完整通信功能，但并未纳入网络用户交互所需的身份识别、行为交互、数据解析等能力。针对当前互联网在数据互联互通中面临的架构性与基础性瓶颈，本白皮书在参考借鉴 OSI 网络七层模型的基础上，通过在网络传输层之上构建新型互联协议，提出一种面向 Web3.0 的数字实体网络创新技术路径。

本白皮书[1]首先分析了网络中的数据对象，探讨了网络发展与数据传输的本质、现有架构的局限性以及下一代网络的关键突破方向；其次梳理了现有 Web3.0 技术演进路径；在此基础上，提出了“数字实体互联网络”的概念与内涵，并阐述了其核心价值、关键技术要素及相关标准化情况；最后对未来发展进行了展望。

[1] 本白皮书得到国家重点研发计划资助（编号：2022YFF0610300）。

目　　录

一、网络发展与数据传输

（一）网络发展历史回顾

网络技术的发展经历了半个多世纪的演进，从最初的 ARPANET（1969 年）开始，网络技术已经完成了多次质的飞跃。ARPANET 最初的设计目标是为了实现计算机之间的资源共享，其核心思想是分组交换（Packet Switching），这一思想彻底改变了信息传输的方式，奠定了现代网络的基础。

20 世纪 70 年代，TCP/IP 协议族的提出（1974 年由 Vint Cerf 和 Bob Kahn 提出）标志着网络技术进入了一个新阶段。TCP/IP 采用分层架构：IP 等网络层协议负责将数据分组从源主机以尽力而为（best-effort）的方式送达目的主机；TCP 等传输层协议则专门负责进程（端）到进程（端）的可靠数据段传输服务，即，将数据交付从两台主机扩展到了两台主机上的进程。这种分层设计使得网络各组件能够独立演进，极大地促进了数据传输的扩展性和适应性。

20 世纪 90 年代，Tim Berners-Lee 发明的万维网（World Wide Web）将互联网从学术和研究工具转变为全球信息基础设施，其主要贡献是在网络应用层采用超文本标记语言 HTML 将主机中的信息进行结构化表达和采用超文本传输协议 HTTP 进行浏览器与服务器之间的通信，以传输 HTML 文件、图像、视频等信息。HTML 协议、HTTP 协议以及浏览器等技术使得主机中的信息能够被普遍访问和相互链接，这创造了全新的信息交互范式。这一时期，网络互联的对象从主机互联延伸到了超文本互联。

万维网出现之后（1995 年左右开始），互联网的商业化进程开始提速，网

络技术的普及和应用创新蓬勃发展。电子商务、搜索引擎、社交媒体等新型应用不断涌现，网络处理的对象和交互模式变得更加多样化。21 世纪前二十年，移动互联网与云计算技术成为全球信息技术发展的主导趋势：智能手机等移动终端的普及把网络应用扩展到移动视频、移动多方会议、实时定位、传感器智能协同等；云计算则重新定义了计算资源的获取和使用方式，降低了用户数据处理和存储的成本，大大缩短了应用建设周期。这一时期，互联网应用层协议栈经历了重要演进，如 HTTP/2（2015 年）、QUIC（2012 年提出，后成为 HTTP/3 基础）等新协议的出现，旨在解决传统 TCP/IP 在高延迟、移动环境下的性能问题。

随着全球数字化转型、国际贸易、数字金融等业务的发展，相关技术正处于快速迭代演进阶段。本白皮书主要针对全球文本互联 Web2.0 之后的下一代数据互联技术架构展开思考与探究。

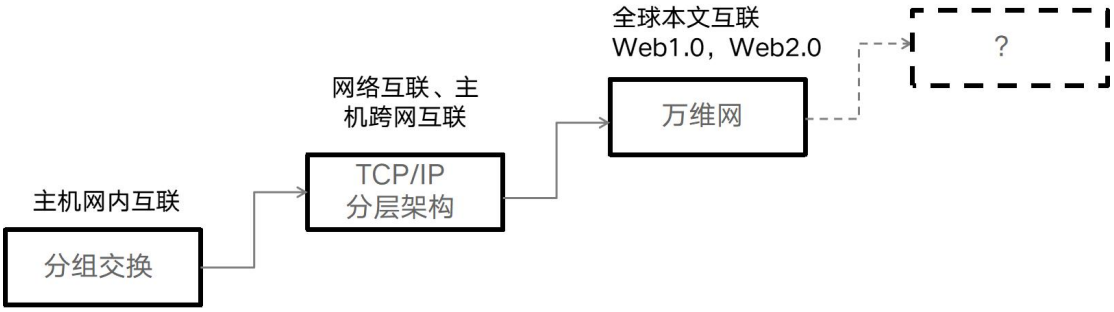

图 1 网络技术的演进

（二）网络传输设计思想

1) 网络分层的核心思想

OSI 七层模型和 TCP/IP 四层模型都体现了网络设计的核心思想：分层抽象。每一层为其上层提供服务，同时屏蔽下层的实现细节。这种设计使得网络各组件可以独立发展和优化，而不影响整体架构。

在网络分层架构中，各层的处理对象有所差异：“数据链路层”（如以太网、Wi-Fi）负责物理设备间的数据帧传输；“网络层”（如 IP）负责主机到主机的数据包路由；“传输层”（如 TCP、UDP）提供端到端的通信服务；“应用层”（如 HTTP、FTP）则实现具体的应用功能。

2) 网络传输的实质：状态与信息的传递

从本质上看，网络传输的本质可以归结为“状态变更和信息流动”，网络通信的核心机制始终围绕着信息的端到端传递以及传输过程中状态同步的实现。无论是早期的文件传输，还是现代的视频流媒体，在传输过程中均需保持信息的完整性。信息完整性（Data Integrity）是一个严格的技术概念，特指数据在采集、处理、存储和传递过程中保持完整且未被篡改、遗漏或损坏的特性， 这一特性主要通过校验和（Checksum）、数字签名（Digital Signature）等密码学机制予以保障。

近年来，除了信息的完整性，ICT 技术在追求的另一个重要特性是信息的时效性。时效性指信息在特定时间段内具备使用价值的特性，其核心在于信息能否在需要时及时传递并发挥作用。时效性直接影响信息的决策价值——过时的信息如同“失效的药品”，即使内容完整准确，也可能导致判断失误或机会丧失。

互联网基于"尽力而为"（best-effort）的数据传输机制，能够满足大多数常规信息传输需求，例如电子文档传输、门户网站新闻资讯等典型的 Web1.0 和 Web2.0 应用场景。然而，特定类型的信息对传输时效性具有严格要求，超出时限将导致信息价值丧失。以工业控制系统为例，执行器的传感器状态信息若未能及时传输，将造成控制时序错乱；金融交易场景中，买卖报价瞬息万变，信息传输延迟会直接影响成交价格。这类场景下，信息的时效性成为其使用价值的决定

性因素。

3) 网络处理对象

网络分层思想的核心之一是在每一层网络把信息对象进行合理的抽象，并针对该抽象专注于处理该层的任务功能。如图 2 所示，具体说明如下：

物理层（也被称为一层网络）的处理对象是物理介质上的比特流，主要功能包括：定义物理接口标准（如网线接口规格、信号编码方式）、确定传输速率（如 10Mbps、100Mbps）、处理信号的传输方式（全双工/半双工）、屏蔽物理设备的差异，以为数据链路层提供统一传输服务。

为确保比特流传输的可靠性，数据链路层（也被称为二层网络）将需要处理的对象抽象为数据帧，主要功能包括：将比特流封装成帧（包含源/目的地址）、差错检测与纠正（循环冗余校验等）、流量控制（避免网络拥塞）、介质访问控制（解决多设备共享同一传输介质的冲突）等。

为了实现数据能跨二层网络传输，网络层（也被称为三层网络）将数据抽象为数据包（Packet），主要功能包括：基于 IP 协议进行逻辑寻址（如 IP 地址）、路由选择（确定最佳路径）等，实现跨网络通信。三层网络与具体的网络介质无关，极大扩展了网络互通的范围。

三层网络解决多个二层网络互联互通的问题，作为通信终端的主机之间的传输质量保障需要传输层（也被称为四层网络）解决。传输层将三层网络的 Packet 封装为段（Segment），针对段进行连接管理、流量控制及错误校验（如 TCP 的可靠性保障或 UDP 的实时性传输），并使用端口号区分主机上的应用进程，实现主机之间的信息通信。

传输层之上，OSI 模型中的会话层（负责建立、管理和终止会话）、表示层

（处理数据编码、加密等）和应用层（处理应用程序数据）在实际 TCP/IP 实现中往往被统称为应用层。

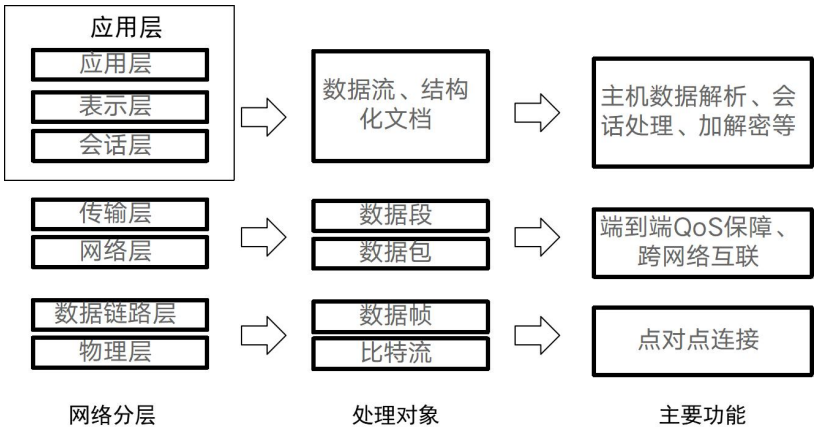

图 2 网络分层、主要功能与处理对象

（三）当前网络的局限性

1) 处理对象存在局限

OSI 七层模型主要解决异构网络互通问题，并非针对语义数据互联：OSI 标准化工作的主要动机是解决 IBM SNA 体系等私有网络结构互不兼容的问题，为此，ISO 于 1977 年设立专门委员会，启动网络通信体系的标准化工作。1984 年，ISO 正式批准并发布 OSI 参考模型标准（ISO/IEC 7498）。

作为现代网络协议的基础架构，OSI 七层模型虽然涵盖了物理连接、数据传输、会话管理到应用服务的完整通信流程，但是受限于领域特定数据与网络公用性的矛盾问题，传统的 ISO、TCP/IP 等经典网络理论主要定位在异构网络通信层面，数据互联所需的身份识别、行为交互、数据语义解析等需求被当做应用层问题由“客户端-平台（服务器）”交互模型解决。

2) 缺乏对数据的合理抽象

OSI 七层模型主要针对异构网络互联，这使得当前网络基础设施主要面向"

数据管道"角色，但缺乏对数据进行合理抽象以剥离个性化语义/知识与通用概念，同时缺乏网络原生能力支持数据之间的共性交互模型。这造成了当前互联网之上的数据交互高度依赖于平台，形成了以中心化平台主导的围墙花园模式。这种模式助长了互联网平台寡头的形成，引发了数据垄断、交互受限、缺乏竞争等问题，并影响信任和治理的稳定性，加剧了世界各地的隐私侵犯、权力集中和数字鸿沟问题。

3) 数据表示的碎片化

数据表示的碎片化已成为现代网络架构的核心挑战。由于各类应用采用不同的自定义数据格式（JSON、XML、Protobuf 等），系统间互操作必须依赖专门的应用层转换，不仅增加了 15-30%的计算开销，还形成了紧密耦合的集成架构。更关键的是，这种碎片化导致两个根本性问题：一是缺乏对数据语义的标准表达方式，造成约 30%的系统集成错误源于数据理解偏差；二是中间网络设备（如 CDN、防火墙）因无法理解应用层数据内容，只能进行基于 IP 和端口的浅层优化，导致缓存命中率等性能指标下降 40%以上。这种现状与 OSI 模型标准化的初衷形成鲜明对比，亟需在网络架构中引入统一的数据抽象层，在保持格式灵活性的同时实现语义互操作，从而突破当前"数据管道"式传输的局限性。

4) 跨平台数据可信保障技术缺乏

数据的流通和利用面临着可信、隐私保护和数据安全等多重挑战。为了确保数据的可信，当前互联网通过平台为数据提供方和使用方建立信任关系。平台除了为数据提供方和使用方提供数据存储、处理和交换服务，还提供接入验证、数据操作确权和授权等机制，为数据互通双方提供基本的数据可信背书。

互联网架构缺乏原生的数据信任机制，导致跨平台数据互通必须依赖平台间

的主动协作，形成以平台为中心的数据流通模式。这种模式下，用户数据的流通边界由平台间的技术接口和商业协议决定，而非数据主体的自主意愿。

要实现以用户为中心的跨平台数据可信流通，必须突破现有架构限制，在网络层建立原生的数据信任与授权机制。这一挑战的核心在于：如何在不影响平台独立性的前提下，使数据主体能够自主控制其数据的跨平台流动。

（四）下一代网络的关键突破点

为了应对全球数字化转型和数字经济的快速发展，在 OSI 参考模型和 TCP/IP 架构的基础上，针对数据互联需求，抽象出数字实体（Digital Entity）概念，通过在传输层之上构建网络原生能力，实现数字实体可发现性、属性可获取性、连接自主性、交互真实性与可解析性，这可能是下一代网络发展的关键突破点。

本白皮书基于 OSI 网络七层模型（参考模型）、TCP/IP 模型（实际应用模型），遵循组网完备性原则提出未来网络模型，以支持数字实体互联。参考图 3，该四层模型包括：

一、保留并合并物理/链路层、保留并合并网络/传输层；

二、建构新的“数字实体层”；

三、改造应用/表示层，扩充数字实体的应用及操作接口；

四、将原应用层与数字实体接口组合，重新定义 Web3.0，支持用户去中心化发现与连接、数字交互、可信验证等。

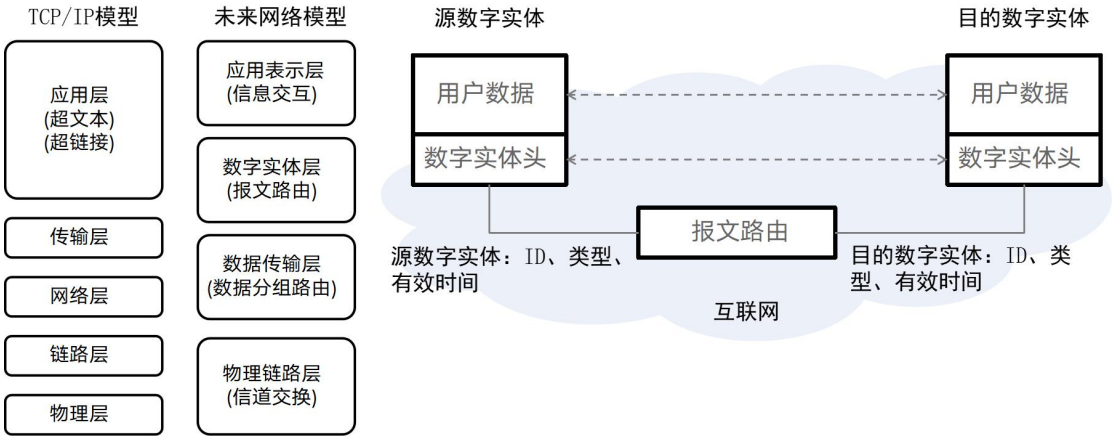

图 3 数字实体互联的突破点

该模型以网络传输层和应用层为突破点，推动网络突破"哑管道"模式，成为能够识别通信实体、理解传输内容、管理交互状态的智能网络，减少中介性平台对互联网数据交互的束缚。

基于未来网络模型，数字实体互联所需的协议框架应支持：

1. 实体中心化：以数字实体为基本通信单元，而非传统的主机或应用；

2. 语义可解析：标准化数据范式携带语义信息，网络设备可进行深度处理；

3. 状态同步原生支持：内置实体状态同步机制，实现不仅仅是数据传递；

4. 安全内建：安全性作为基础属性而非附加功能。

以上模型和协议将能在网络互联、主机互联、文本互联的基础上，支持数字实体在互联网上相互连接组成数字实体网络，这将是 Web2.0 之后的一大进步，见图 4。

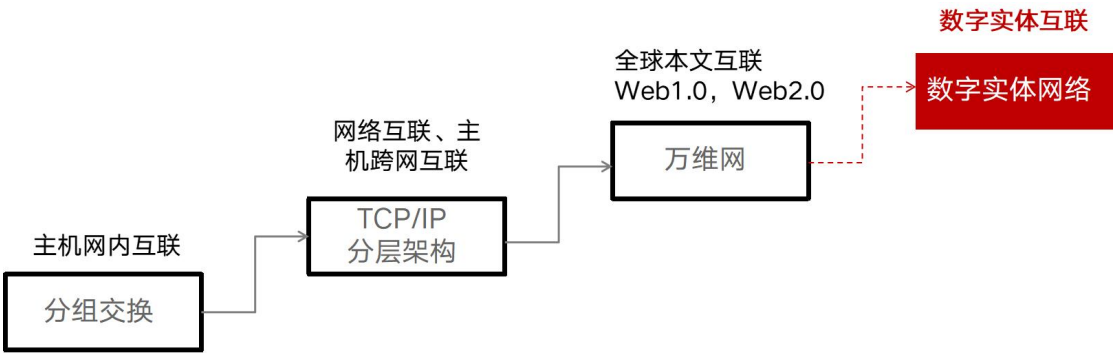

图 4 数字实体网络所处的阶段

二、现有 Web3.0 演进路径

在下一代网络（Next Generation Network，NGN）的演进过程中，语义网（Semantic Web）和 Web3 代表着两条具有深远影响的技术路线。前者致力于解决机器理解网络信息的根本性问题，后者则着眼于重构互联网的信任基础。尽管两者的技术路径存在差异，但在构建智能化、自主化和可信化的数字生态系统方面展现出显著的协同潜力。

（一）语义网构建意义互联的网络空间

1．概念与目标

语义网（Semantic Web）是由万维网联盟（W3C）主导、Tim Berners-Lee 于 1998 年首次提出的网络演进方向。其核心愿景是“让数据不仅可被人类阅读，还能被机器理解和处理”，从而实现更智能、自动化的信息交互。与传统 Web 基于文档链接（HTML 超文本）不同，语义网强调“数据的语义关联”，旨在构建一个全球化的知识网络，使计算机能够自主推理、整合和利用分布式信息。

2．实现思路

语义网的实现遵循知识工程方法论，其核心在于构建多层次的知识表示体系。在实践层面，首先需要将非结构化数据转化为标准化的 RDF 图，这个过程通常涉及实体识别、关系抽取等自然语言处理技术。领域本体（如医疗领域的 SNOMED CT）的构建则需要领域专家与知识工程师的深度协作。推理引擎基于描述逻辑（Description Logic）实现自动化的知识发现。

该架构使机器能够理解"北京是中国的首都"这类陈述中的实体关系，而非仅

将其视为字符串组合，并能从"所有省会都是城市"和"成都是四川的省会"推导出"成都是城市"。

3．主要贡献

语义技术有效应对了信息时代的三大核心挑战：在数据层面，通过 RDF 的统一数据模型解决了传统 ETL 过程中的语义损失问题；在系统层面，本体映射技术（如 OWL:sameAs）实现了跨系统的语义互操作；在应用层面，基于规则的推理支持了智能问答、个性化推荐等高级功能。Linked Data 项目证明，语义网方法可使跨机构数据查询效率提升 40%以上。

4．问题与挑战

语义网的规模化应用面临三重障碍：技术层面，RDF/OWL 等标准学习曲线陡峭，且逻辑推理存在性能瓶颈，难以满足实时需求。生态建设方面，数据标注与应用开发陷入"先有鸡还是先有蛋"的困境，加之现有 Web 内容缺乏平滑迁移路径，导致采用率低迷。架构设计上，过度集中的标准体系难以适应领域需求，且网络基础设施无法利用语义信息，形成应用层与传输层的割裂。这些系统性缺陷严重制约了语义网的规模化落地。

（二）Web3 与公链：构建信任原生的网络结构

1．概念与目标

Web3 是近年来兴起的互联网演进范式，其核心理念是“通过区块链技术重构互联网基础架构，实现去中心化的数字生态”。与 Web1.0（只读）、Web2.0（读写+中心化平台）相比，Web3 强调：

- 用户主权：个人拥有数据、身份和资产的完全控制权

- 去中心化协议：以区块链替代传统中心化平台作为信任基础

- 通证经济：通过加密货币和智能合约实现价值网络化

以太坊联合创始人 Gavin Wood 在 2014 年首次提出 Web3 概念，其愿景是打造"无需信任"(trustless)且"抗审查”的网络基础设施。

Web3 的技术特征如表 1 所示。

表 1 Web3 的主要技术特征

技术方面	Web3 技术特征
核心技术	区块链技术、加密货币等
数据存储	去中心化
交互方式	用户通过加密钱包自主控制
典型应用	去中心化金融 DeFi、不可替代货币 NFT、去中心化自治组织 DAO
侧重点	去中心化、安全性

2. 实现思路

Web3 的技术实现路径采用分层架构设计,各层协同构建去中心化网络生态。在基础层，区块链网络（如以太坊、Solana）通过分布式账本技术建立不可篡改的数据层，IPFS/Arweave 等去中心化存储系统采用内容寻址（CID）替代传统 URL，结合 Libp2p 等 P2P 网络协议实现节点间直接通信。中间件层包含三大核心组件：智能合约平台（如 EVM）提供图灵完备的链上代码执行环境，去中心化身份协议（DID）实现用户自主权身份管理，跨链桥接技术解决异构链互操作问题。应用层则涌现出 DeFi 协议、DAO 治理模型和各类 dApp，形成完整的去中心化应用生态。

关键技术突破包括：1）智能合约实现可编程交易逻辑；2）零知识证明（如 zk-Rollups）平衡隐私与验证；3）PoS/PoH 等新型共识机制提升性能；4）内容寻址（CID）确保数据持久性。这些创新共同推动互联网向用户主权化转型，建立不依赖中心化中介的数字信任体系。

3. 主要贡献

Web3 的主要贡献在于重构了数字世界的信任与价值传递机制。在身份管理方面，基于区块链的 DID 系统（如 ENS）实现了用户自主控制的跨平台身份，打破了传统平台账户体系的垄断。价值传递方面，智能合约将金融逻辑编码为可验证的网络协议，使资产流动实现可编程性。数据存储方面，IPFS 等协议通过内容寻址和分布式存储确保了数据的抗审查性和持久性。这些创新有效缓解了平台垄断、数据确权和跨境结算等传统互联网的痛点。

4. 问题与挑战

Web3 仍面临显著局限。技术层面存在"不可能三角"约束，主流公链的 TPS 难以支撑大规模商用，且私钥管理和 Gas 费用等设计抬高了用户门槛。经济治理方面，通证经济易受投机影响，DAO 治理普遍存在参与度不足问题。架构设计上，链上链下数据协同效率低下，跨链互操作性不足又形成了新的生态割裂。这些系统性挑战制约着 Web3 从金融创新向更广泛场景的拓展。

三、数字实体互联网络

（一）概念与内涵

在传统互联网中，网络通信的端点是“设备”或“应用”，而不是“实体本

身”。下一代网络（NGN）将这一焦点前移，关注网络中“数字实体”（Digital Entities）的直接表达与交互能力，包括人/组织/物数字化形成的数字实体以及算法模型、甚至 AI 智能体等数字实体。

数字实体（Digital Entity）是指网络环境中具有独立身份标识、可独立交互的逻辑单元，它不仅具有唯一身份，还具备自主行为能力和数据主权。其特征包括：

- 自主性：拥有独立的身份标识与自主决策能力
- 交互性：可通过标准化协议与其他数字实体进行可信数据交换与价值转移
- 持久性：其存在与状态不依赖于特定平台或服务
- 可组合性：支持按需功能聚合与解耦

数字实体网络（Digital Entity Network，DEN）是一种新型网络架构，其根本任务从单纯的数据传输转向支持数字实体间的语义互操作与可信协作。这种转变将带来网络技术的范式革命：任何数字实体（包括数字孪生、一项数字化服务、一个虚拟代理还是一个复杂数字系统）都能以标准化方式接入网络，自主发现并关联其他实体，并基于共享协议完成交互，见图 5。DEN 不再仅是数据传递通道，而是成为数字生态的基础协作平台。

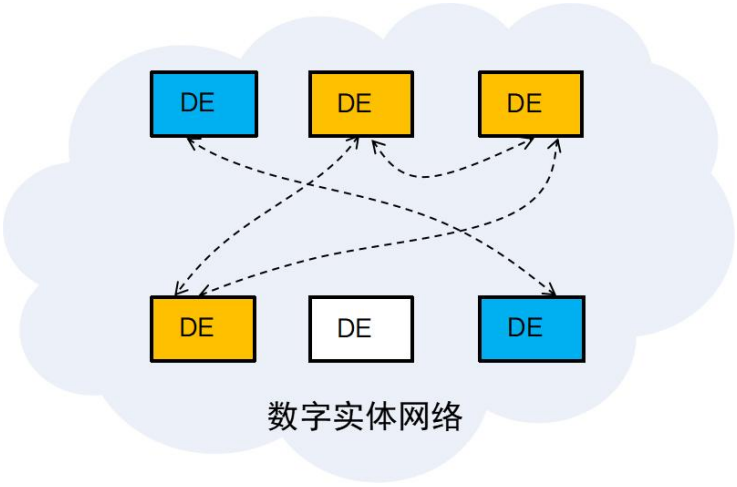

图 5 数字实体网络概念图

（二）核心设想

采用数字实体对网络交互数据进行建模，见图 6：

（1）将数据解构为数据容器和领域知识：数据容器对数据主体及其相关事件的通用方面进行高度抽象，形成可重用的通用软件功能、接口和交互协议；领域知识包含具体主体与事件的元数据信息，其内容与特定应用场景及上下文相关。二者结合构成完整的交互数据表征体系。

（2）采用数字实体头封装数字实体：核心属性包括数字实体 ID、类型、有效时间等。数字实体 ID 确保该数字实体可被识别；类型用于表达数字实体的类型；有效时间表明数字实体的有效生存周期。

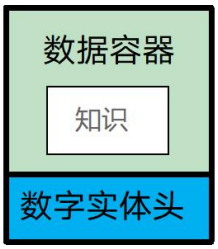

图 6 数字实体的结构

“数字实体网络”的影响可能不亚于从电路交换到分组交换的范式转变。实现这一愿景需要重构网络各层的设计原则，特别是在数据语义化表示、实体自主识别和可信数字交互等基础架构上的创新。

在网络互联 TCP/IP 层之上构建支持数字实体直接交互的数字实体层是数字实体网络的核心思想，如图 7 所示。

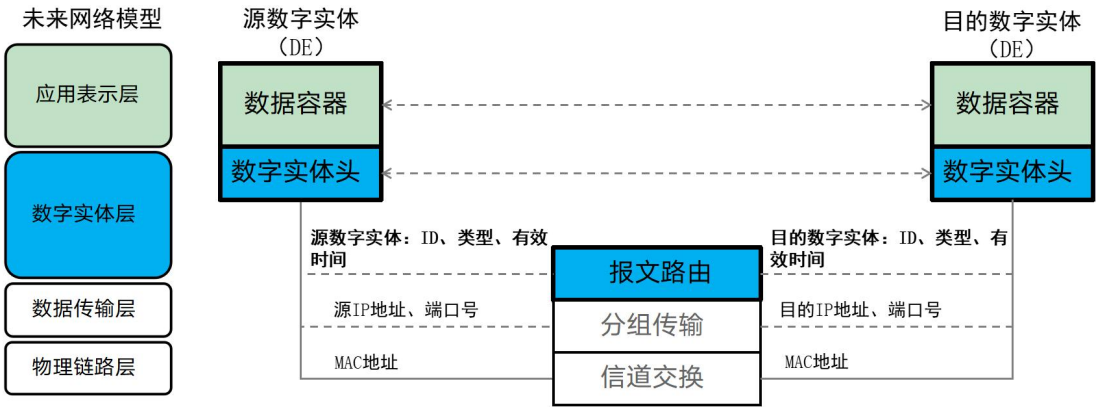

图 7 兼容 OSI 模型的数字实体互联概念图

数字实体层在以下几个核心方面实现突破：

- 以身份寻址替代 IP 寻址：基于数字实体的唯一身份 ID，而非网络 IP 地址进行路由

- 自描述结构化传输数据：所有传输数据基于统一的元数据标准，形成自描述的结构化数据单元

- 基于语义的自动化协同：依托数字实体所处的语义环境，数字实体之间无需依赖中心化平台，通过网络基础设施实现点对点交互。

（三）关键价值

当前数字化进程中，互联网在数据隐私保护、身份管理机制及信任体系构建等方面正面临系统性困境。这些深层次问题不仅制约着社会协同效率，也阻碍了产业协作深化与智能系统发展。在此背景下，构建以数字实体为中心的网络体系成为破局关键 —— 这一新型架构不仅为跨组织协同、智能体交互及用户自主权提供了技术支撑，更对数字经济的可持续发展具有深远影响。

1. 破解数据共享难题

在数据要素市场化进程中，数据共享与数据主权的冲突日益凸显。当前主要面临三重挑战：一是数据孤岛现象突出，各平台数据标准不一、互操作性缺失，导致数据流通效率低下；二是数据权益界定模糊，用户对自身数据的控制权与可审计性严重不足，权益保障机制不完善；三是合规风险居高不下，GDPR 等隐私法规的约束使数据共享的成本与难度显著增加。

针对上述问题，数字实体网络通过制定标准化的数字实体交互协议与数据规范，提供数字实体行为发生的真实性记录与核验服务，确保在交易环境下的参与方以安全、可信且符合隐私保护要求的方式获取所需数据，协同完成业务所需的相关流程。

数据共享与数据主权保护的应用场景包括：医疗健康领域通过隐私计算实现跨院病历协同分析、金融行业借助可验证凭证实现 KYC 信息复用、教育领域则利用分布式存储完成学历资质的跨国核验等。

2. 建立跨组织身份互信

跨组织协作长期受限于三大瓶颈：组织间缺乏天然信任基础，数据互信机制不全；缺乏行为一致性的"协议语言"，流程对接成本高昂；过度依赖第三方身份验证中心，既导致流程延迟，又存在单点故障风险。

针对以上问题，数字实体网络将自主标识符作为组织与个体的身份锚点，可实现跨平台身份自主管理与互通；以数字实体交互协议支撑行为协同，支持动态定义多方参与流程；基于密码学构建分布式信任验证体系，可摆脱对中心化平台的依赖。

跨组织协作应用场景包括：在政务协同中实现跨部门数据的安全核验，在供应链对账中降低多方结算的沟通成本，在企业合约执行中提升条款履行的透明度，在 NGO 协同资助中保障资金使用的可追溯性等。

3. 去平台化自组织协作

当前平台经济模式下，用户权益保障面临双重挑战：账户体系的封闭性导致用户数据、身份与社交关系被 "锁死" 在单一平台，难以跨域迁移；平台中心化平台主导的协作模式中，用户缺乏对自身数字资产的控制权与议价权。

数字实体网络支持身份体系从平台账户向自主权数字身份（Self-Sovereign Identity, SSI）转变，实现身份与行为的数据解耦；培育可携带身份、声誉与价值的 "自主数字代理"，使个体成为协作网络的核心节点；依托 DAO（去中心化自治组织）与 AI Agent 构建去平台化协作生态，重塑价值分配机制。

去平台化协作与用户主权控制的典型应用场景包括：

- 去中心化招聘系统中，求职者可自主管理可验证数字凭证（Verifiable Credentials）并选择性披露给雇主；
- 知识技能市场通过智能合约实现点对点价值交换；
- 去中心化自治组织（DAO）中，成员通过链上治理参与社区规则制定等。

4. 基于 AI 的自动化协同

随着 AI 技术的发展，智能体协同面临新的挑战：现有 AI 系统多以工具形态存在，缺乏独立数字身份标识、明确责任边界与标准化协作协议；智能体间的互动缺乏统一标准化接口与行为溯源机制，制约了大规模协同应用。

数字实体网络为 AI 智能体协同提供了系统性支撑路径：为每个 AI Agent 配置独立数字身份与属性数据集，记录其连接关系与行为日志；基于语义化协议实现智能体间的自动交互与任务协同；利用不可篡改的分布式账本对 Agent 行为进行全程登记与审计。

AI 智能体的自治协同场景包括：智慧城市中，交通、能源等领域的智能体可实现跨系统协同调度；AI 法律助理通过标准化协议完成证据核验与条款比对；科研领域的智能体集群能基于标准化数据接口协同开展数据处理与模型训练，显著提升研究效率等。

数字实体网络在数据主权管理、跨组织协作、分布式协同、AI 代理自主协作等方面展现出的优势，可用表 2 进行归纳说明。

表 2 数字实体网络解决方案与传统方案的对比

问题领域	**传统方案缺陷**	**数字实体网络解决方案**	**提升效果（预测）**
数据共享	所有权让渡或效率低下	使用权精准分离	共享效率提升 3-5 倍
业务协同	中心化平台依赖	去中心化原子协作	对接成本降低 60%+
反垄断	平台数据私有化	个人数据容器+价值透明	用户收益提升 8-12 倍
AI 治理	黑箱操作难追溯	强制注册+交互协议	可审计性提升 4 倍
智能决策	数据延迟与碎片化	实时状态网络+动态实体	决策时效性提升 50%+

（四）核心技术

1. 分布式账本技术（Distributed Ledger Technology, DLT）

分布式账本技术为下一代网络提供价值流转与信任记录的基础设施，其核心在于通过密码学与共识算法构建多方参与的不可篡改账本。技术实现上，DLT 采用区块式或定向无环图（DAG）结构组织数据，通过拜占庭容错（BFT）或权益证明（PoS）等共识机制确保节点间状态同步。智能合约作为可编程逻辑层，支持自动执行预定义规则（如以太坊 EVM、CosmWasm），实现资产转移、条件支付等复杂业务流程。DLT 不仅是加密货币的底层支撑，更为数字实体间的价值交换、权益证明和协作审计提供可信环境。

2. 去中心化身份（Decentralized Identifiers, DID）

去中心化身份体系通过 W3C 标准化的 DID 规范实现身份自主控制。技术实现包含三个层级：标识层（DID URI）、验证层（公钥基础设施）和解析层（分布式账本）。用户生成 DID 后，其对应的 DID 文档（含公钥和服务端点）被写入区块链，形成可验证的身份锚点。身份验证时，依赖方通过解析 DID 文档获取公钥，验证数字签名即可确认身份真实性，无需中心化身份提供商参与。该技术为物联网设备、AI 代理等新型数字实体提供了标准化身份解决方案。

3. 可验证凭证与信任框架（Verifiable Credentials + Trust Graph）

可验证凭证技术基于 JSON-LD 或 JWT 格式构建机器可读的权威声明。其技术栈包含凭证签发（Issuer）、持有（Holder）和验证（Verifier）三个角色，通过数字签名链实现端到端验证。进阶方案如 zk-SNARKs 支持凭证属性的选择

性披露，而 BBS+签名算法实现多凭证的聚合验证，它既支持隐私保护又提供审计能力，形成可扩展的分布式信任体系。

4.隐私增强技术（Privacy-Enhancing Technologies, PETs）

隐私保护技术栈采用密码学前沿方案实现数据最小化使用：零知识证明系统（如 zk-STARKs）通过非交互式证明实现无信息泄露的验证；全同态加密（FHE）允许在加密数据上直接计算（如 IBM HELib）；安全多方计算（MPC）通过秘密分割技术实现多方联合分析（如 SPDZ 协议）。隐私增强技术支持根据不同的需要进行可组合应用。

5. AI 驱动的数字代理（AI-powered Digital Agents）

智能代理技术栈融合多模态感知、知识推理与行动决策能力：自然语言理解模块（如 BERT、GPT）处理用户意图；规划系统（如 PDDL 求解器）生成任务分解策略；记忆网络（如向量数据库）实现上下文保持。知识图谱（如 Wikidata）与领域本体（OWL）提供语义理解基础，而强化学习（如 PPO 算法）优化长期行为策略。这些代理既服务人类用户，也能代表数字实体参与机器间的语义协作。

（五）与现有技术的对比

数字实体网络通过重构网络基础协议，在保留互联网开放性的同时，为数字时代的核心矛盾提供了系统性解决方案。其创新价值不仅体现于技术指标的量化提升 —— 如数据共享效率、决策时效性的显著改善，更在于重塑了数字经济的权力结构：通过技术机制使数据价值回归创造者，让协作信任建立在数学协议而非商业权威之上，最终推动网络空间完成从 "平台主导" 到 "实体共生" 的范式

迁移。

从技术上，数字实体网络与传统网络各维度的对比，见表 3。

表 3 数字实体网络与传统网络对比

维度	传统互联网	语义网	Web3	数字实体网络
基本单元	主机	语义三元组	区块链账户	数字实体
寻址方式	IP 地址	URI	公钥地址	数字实体 ID
数据模型	字节流	RDF 图	交易日志	状态对象
信任机制	CA 中心化	集中式标准	分布式共识	混合验证

- 相对于 Web2.0 的突破性优势

数字实体网络重构了 Web2.0 的中心化交互模式。在传统 Web2.0 架构中，用户数据和服务逻辑被封闭在少数平台的"围墙花园"内，平台同时充当着数据中介和规则制定者的角色。而数字实体网络通过将数字实体作为网络交互的基本单元，实现了三个核心突破：

- 首先，数据以标准化数字实体形式存储与流转，支持跨平台迁移；
- 其次，服务功能被解构为可组合的实体能力，突破单一平台限制；
- 最后，交互规则通过开放协议而非平台政策来定义，削弱了平台垄断的技术依赖性。

这种转变推动网络价值从平台方向实体所有者转移，同时兼容 Web2.0 的交互体验。

- 相对于语义网的实用化改进

语义网虽然提出了机器可理解数据的愿景，但其依赖复杂的 RDF/OWL 标准和集中式本体管理，导致实际应用长期局限于特定专业领域。相比之下，数字

实体网络在继承语义网核心理念的同时，实现了三项关键创新：采用轻量化的结构化数据容器替代繁琐的三元组表示，使语义标注成本降低 90%以上；通过动态本体协商机制，允许实体在交互过程中按需交换语义理解规则，而非依赖全局统一标准；特别是将语义处理能力下沉至网络协议层，使得普通开发者无需深入语义技术栈即可享受智能化红利。这些改进使得语义互联从实验室走向大规模商业应用成为可能。

- 相对于 Web3 的架构革新

Web3 通过区块链实现了价值传输的去中心化，但其"全量数据上链"的设计思想带来了严重的性能局限和生态割裂。数字实体网络采用更务实的架构设计：在身份认证和关键状态存证等核心环节保留区块链的信任价值，而在高频交互场景采用高效的链下验证机制；将全局共识的范围缩小到必要的最小集合，允许大多数实体交互在局部可信域内完成；通过统一的价值-数据融合模型，使数字货币、数字资产与普通数据实体可以在同一协议框架下交互。这种分层设计既保留了 Web3 的数字主权特性，又使其能够支持物联网、元宇宙等实时性要求高的新兴场景，有效缓解了 Web3 面临的可扩展性困境。

综上，数字实体网络代表网络架构的范式级创新，它通过：

1. “实体化抽象” 提升交互直接性

2. “协议层重构” 实现效率突破

3. “混合架构设计” 平衡去中心化与实用性

这种架构既吸收了语义网的机器可理解思想，又继承了 Web3 的数字主权理念，同时通过基础协议创新部分解决了二者的固有缺陷。随着数字实体成为网络交互的首要主体，下一代网络将逐步实现从"连接计算机"到"连接智能体"演进。

四、相关标准化组织及其相关活动

（一）相关标准化组织

许多标准化组织的活动有助于数字实体网络形成与发展，包括但不限于：

W3C：在数字实体的身份与认证、凭证交互等关键技术上发挥核心作用。制定了 Decentralized Identifiers (DIDs) v1.0，为数字实体提供去中心化的唯一身份标识，是数字实体身份体系的重要基础；定义了 DID Document Resolution 机制，实现通过 DID 解析元数据；推出 Verifiable Credentials (VC) 系列标准，包括数据模型、JSON Schema、安全保障等，构建了数字凭证的规范体系；同时，JSON－LD 作为基础数据格式，支撑了这些标准的数据表达与传输，为数字实体网络中身份确立和可信数据交互提供了关键技术标准。网络连接：https://www.w3.org/

Decentralized Identity Foundation (DIF)：致力于推动 DID 生态协议的兼容与代码共享，聚焦于与数字实体身份相关的技术协同。其工作促进了各类去中心化存储系统（如 IPFS/Filecoin/Arweave）与 DID 等标准的结合，可让数字实体数据存储更安全高效；同时，支持 Hyperledger Aries/Indy/Ursa 等开源框架的发展，这些框架基于 DID 标准实现了数字实体间的通信和凭证验证，推动了数字实体网络技术的实际应用。网络连接：https://identity.foundation/

ToIP Foundation：以构建数字实体网络中的信任体系为核心，提出并推广“信任四层架构” 的 Trust Over IP Stack (ToIP)。该架构融合了 DID、VC、ZKP 等关键技术标准，将身份标识、可信凭证、隐私保护等技术整合，形成分

层的信任模型，为数字实体之间建立可信交互提供了全面的技术框架，强化了数字实体网络的信任基础。网络连接：https://toip.global/

国际电信联盟电信标准化部门（ITU－T）旗下的 SG20、SG21、SG13、SG17 分别涉及分布式/去中心化物联网、区块链、可信数据基础设施、数字身份与安全，为数字实体网络相关的通用关键技术和垂直行业应用的国际标准化提供了平台。其官方链接为：https://www.itu.int/en/ITU－T/studygroups/Pages/default.aspx ，在此可获取更多关于 ITU-T 工作的详细动态与研究成果。

ISO/TC 307：专注于区块链与 DID 标准的国际推广和采纳，将区块链技术与数字实体身份技术相结合。通过推动相关标准的国际化，使 DID 等身份标准借助区块链的不可篡改特性得到更好应用，例如促进 Ledger Anchoring 技术在公链上可为数字实体数据打“时间戳”，确保数据可靠性。网络连接：https://www.iso.org/committee/6186257.html

（二）相关标准

1．身份与认证标准

此类标准是数字实体在网络中确立身份、实现可信交互的基础。

• Decentralized Identifiers (DIDs) v1.0：由 W3C 制定，为数字实体提供全球唯一且去中心化的身份标识符，无需中央发行机构，数字实体可自行掌控。通过 DID 能解析出对应的 DID Document，包含用于控制该 DID 的加密材料及其他元数据。具有去中心化、可控性、隐私保护等特性。网络连接：https://www.w3.org/TR/did-core/#did-syntax

• DID Document Resolution：由 W3C 定义，用于通过 DID 解析元数据，为数字实体的身份确立和信息获取奠定基础。当获取到数字实体的 DID 后，通过该机制能解析出对应的 DID Document 中的详细信息。网络连接：https://www.w3.org/TR/did - core/#did - resolution - process

• Decentralized PKI (DPKI)：作为替代传统 CA 的密钥管理模型，通过在 DID 文档中嵌入公钥、撤销列表等机制，强化数字实体身份的安全性和可信度。与 Ledger Anchoring 技术结合，在公链上为数据打不可篡改 “时间戳”。目前无特定单一官方链接，可通过学术数据库或区块链相关技术论坛搜索更多资料。

• Ledger Anchoring：在公链上为数据打 “时间戳”，将数据与区块链不可篡改特性结合，使数字实体的身份信息和相关数据得到更好保护和验证。相关技术细节可在以太坊官网搜索获取：https://ethereum.org/

这些标准相互配合，从身份标识的创建、解析到安全管理，可构建数字实体身份体系的核心框架。

2．凭证与数据交互标准

围绕数字凭证的表达、传输和验证展开，是数字实体间可信数据交换的关键。

• Verifiable Credentials (VC)：遵循 W3C 开放标准的数字凭证，可代表物理凭证信息或无物理对应物的信息，通过加密签名确保防篡改和即时可验证性，生态系统中有发行者、持有者和验证者三方。网络连接：https://www.w3.org/TR/2024/NOTE-vc-overview-20240613/

• Verifiable Credentials Data Model v2.0：定义了 Verifiable Credentials 的核心概念，是其他 VC 相关规范依赖的基础，以抽象方式定义模型，应用通过序列化表达具体凭证，当前多使用 JSON 序列化。网络连接：

https://www.w3.org/TR/vc - data - model - 2.0/

• Verifiable Credentials JSON Schema：当 Verifiable Credentials 以 JSON 序列化时，定义如何使用 JSON - Schema 确保凭证结构被 VC 生态系统所有参与者一致解释，为 VC 在 JSON 格式下的结构规范提供依据。网络连接：https://www.w3.org/TR/vc - json - schema/

• Securing Verifiable Credentials using JOSE and COSE：定义一系列使用 IETF 技术实现的 enveloping proofs，用于保障 Verifiable Credentials 的安全性，通过加密技术封装保护 VC。网络连接：https://www.w3.org/TR/vc - jose - cose/

• Verifiable Credential Data Integrity 1.0：定义 embedded proofs 的通用结构，用于保障 Verifiable Credentials 的数据完整性，在凭证序列化时包含相关证明信息。网络连接：https://www.w3.org/TR/vc - data - integrity - 1.0/

• JSON - LD：基于 JSON 的语义结构化语言，定义上下文概念指定类型和属性词汇表，作为 Verifiable Credentials 等标准的数据表达与传输协议基础格式。网络连接：https://developers.google.com/workspace/gmail/markup/reference/formats/json - ld?authuser = 0000

这些标准共同构成了可靠的数字凭证生态。

3．隐私与信任架构标准

聚焦于保护数字实体隐私并建立网络信任。

• Zero - Knowledge Proof (ZKP)：能让数字实体在不暴露原始数据的前

提下完成验证，如年龄、学历等场景，与 VC 结合增强数据传输安全性和隐私性。虽 W3C 等有涉及相关研究，但无专门标准单一官方链接，可通过 W3C 官网搜索：https://www.w3.org/

• Trust Over IP Stack (ToIP)：由 ToIP Foundation 倡导的分层信任架构，融合 DID、VC、ZKP 等标准，构建数字实体网络中的信任模型，为数字实体间信任建立提供全面框架。网络连接：https://toip.global/

它们与其他隐私保护技术协同，营造出安全可信的数字交互环境。

4．支撑平台与开源框架

基于上述各类标准开发，为实际应用提供技术工具。

• Hyperledger Aries/Indy/Ursa：开源 DID 通信与凭证验证框架，基于 DID 等标准开发，实现数字实体间通信和凭证验证功能。网络连接：Hyperledger Aries [https://hyperledger - aries.readthedocs.io/en/latest/]；Hyperledger Indy [https://hyperledger - indy.readthedocs.io/en/latest/]；Hyperledger Ursa https://github.com/hyperledger/ursa

• SpruceID：支持 DID 解析与 VC 交互，并集成 OAuth，依托 DID 和 VC 等标准实现功能，为数字实体身份识别和可信凭证交互提供便捷解决方案。网络连接：https://spruceid.com/

• Veramo/Trinsic/SSI Kit：开发者工具集，帮助快速集成与部署数字身份，基于 DID 等身份与认证标准，加速数字实体网络应用开发。网络连接：Veramo https://veramo.io/；Trinsic https://trinsic.id/；SSI Kit 可在 GitHub 搜索：https://github.com/search?q = SSI + Kit

• Smart Agents：基于 DID 的 AI Agent 通信协议框架，依赖 DIDComm v2

等实体通信协议，使数字实体中的 AI 代理能遵循标准通信协议交互。目前无单一官方链接，可通过相关技术论坛搜索获取信息。

这些框架降低了标准应用门槛，加速了数字实体相关技术的落地。

5．存储与数据结构标准

为数字实体数据存储和管理提供保障。

• IPFS/Filecoin/Arweave：去中心化存储系统，IPFS 通过内容寻址存储，Filecoin 基于区块链提供激励机制，Arweave 实现数据永久存储，为数字实体数据提供安全存储解决方案。网络连接：IPFS https://ipfs.io/；Filecoin https://filecoin.io/；Arweave https://www.arweave.org/

• Merkle Tree / Merkle DAG：用于构建数据哈希结构，Merkle Tree 形成树状结构，Merkle DAG 在有向无环图基础上应用其原理，为数据快速检索和完整性验证提供高效手段。相关技术细节可在以太坊开发者文档查看：https://ethereum.org/en/developers/docs/data - structures - and - encoding/merkle - trees/

• Content - addressable storage (CAS)：基于内容哈希寻址，确保数据不可篡改与版本控制，根据数据内容计算哈希值进行存储和检索，保证数据完整性和可追溯性。相关技术原理可参考：https://www.distributed - systems - for - fun - and - profit.com/content - addressable - storage.html

它们从存储方式、数据结构到寻址机制，保障数字实体数据的安全存储和高效管理。

6．通信协议标准

保障数字实体之间的有效沟通。

• DIDComm v2：作为实体通信协议，是 Smart Agents 等基于 DID 的 AI Agent 通信协议框架依赖的基础协议，定义了数字实体之间通信的规范和格式，确保安全准确交互。可在 DIF 官方网站搜索详细资料：https://identity.foundation/

它是数字实体网络互联互通的重要支撑。

五、未来发展展望——迈向智能协同的数字实体网络

以语义互操作性为核心基石，以分布式身份与加密体系作为信任底座，以数字实体为协作载体，构建一个支持价值流转、人机协同与跨域合作的数字生态，是面向 Web3.0 数字实体互联网络的总体理念。其目标不仅在于实现数据的可信流动与身份的自主管理，更在于打造一个能够有效处理真实世界复杂性、促进人机智能协同进化的开放系统。这不仅是下一代互联网的发展方向，也是数字文明可持续演进的重要路径。

愿本文为探索语义网络与数字实体交互机制的创新技术路线，提供具有实践价值的参考框架与实施方向。

附：缩略语

AI：Artificial Intelligence，人工智能

ARPANET：Advanced Research Projects Agency Network，阿帕网

BERT：Bidirectional Encoder Representations from Transformers，基于 Transformer 的双向编码器表示

BFT：Byzantine Fault Tolerance，拜占庭容错

CAS：Content-Addressable Storage，内容寻址存储

CID：Content Identifier，内容标识符

COSE：CBOR Object Signing and Encryption，CBOR 对象签名与加密

DAO：Decentralized Autonomous Organization，去中心化自治组织

DAG：Directed Acyclic Graph，有向无环图

DeFi：Decentralized Finance，去中心化金融

DID：Decentralized Identifiers，去中心化标识符

DIF：Decentralized Identity Foundation，去中心化身份基金会

DLT：Distributed Ledger Technology，分布式账本技术

DPKI：Decentralized Public Key Infrastructure，去中心化公钥基础设施

ETL：Extract, Transform, Load，提取、转换、加载

EVM：Ethereum Virtual Machine，以太坊虚拟机

FHE：Fully Homomorphic Encryption，全同态加密

GPT：Generative Pre-trained Transformer，生成式预训练 Transformer

HTML：HyperText Markup Language，超文本标记语言

HTTP：HyperText Transfer Protocol，超文本传输协议

ICT：Information and Communications Technology，信息与通信技术

IPFS：InterPlanetary File System，星际文件系统

ISO/OSI：International Organization for Standardization/Open Systems Interconnection，国际标准化组织 / 开放系统互连

ISO/TC 307：International Organization for Standardization/Technical Committee 307，国际标准化组织 / 第 307 技术委员会（区块链与分布式账本技术）

ITU-T：International Telecommunication Union-Telecommunication Standardization Sector，国际电信联盟电信标准化部门

JOSE：JavaScript Object Signing and Encryption，JavaScript 对象签名与加密

JSON-LD：JavaScript Object Notation for Linked Data，用于关联数据的 JavaScript 对象表示法

MPC：Secure Multi-Party Computation，安全多方计算

NGN：Next Generation Network，下一代网络

NFT：Non-Fungible Token，非同质化代币

OWL：Web Ontology Language，网络本体语言

PDDL：Planning Domain Definition Language，规划领域定义语言

PPO：Proximal Policy Optimization，近端策略优化

PoH：Proof of History，历史证明

PoS：Proof of Stake，权益证明

QUIC：Quick UDP Internet Connections，快速 UDP 互联网连接

RDF：Resource Description Framework，资源描述框架

SPDZ：Secure Multiparty Computation with Oblivious Transfer，基于不经意传输的安全多方计算

TCP/IP：Transmission Control Protocol/Internet Protocol，传输控制协议 / 网际协议

ToIP：Trust Over IP，基于 IP 的信任

VC：Verifiable Credentials，可验证凭证

W3C：World Wide Web Consortium，万维网联盟

zk-Rollups：Zero-Knowledge Rollups，零知识汇总

zk-SNARKs：Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge，零知识简洁非交互式知识论证

zk-STARKs：Zero-Knowledge Scalable Transparent Arguments of Knowledge，零知识可扩展透明知识论证

ZKP：Zero-Knowledge Proof，零知识证明