中国联通
China unicom

中国联通

面向下一代互联网 Web3.0

可信数字身份基础设施白皮书

（2024 年）

中国联合网络通信有限公司研究院

2024 年 8 月

版权声明

目录

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”，“新质生产力是创新起主导作用，摆脱传统经济增长方式、生产力发展路径，具有高科技、高效能、高质量特征，符合新发展理念的先进生产力质态”。

互联网诞生时间约为 50 年，对促进信息交流、资源共享、商业创新、政府管理和公共服务、社交互动等方面起到了巨大推动作用。新理念、新架构、新技术、新应用不断涌现，如何引导下一代互联网促进、激活新质生产力，如何利用网络数字基础设施保护数字权属、促进智力协作创新，是本白皮书编制动机。

本白皮书得到青岛大学、中钞区块链技术研究院、联通华盛通信有限公司、浪潮计算机科技有限公司、中国电子科技网络信息安全有限公司、合肥安永信息科技有限公司、Metopia Technology（區塊城科技）和香港 Web3.0 協會大力支持，获得詹立东、平庆瑞、张钰雯、张波、雷志斌、刘扬、衣莉莉，王海涛、李亚荣、金晶、李汪红、毕磊、王培帆等专家帮助，特此衷心感谢。

编写组成员（排名不分先后）：

马红兵、唐雄燕、贾雪琴、曹畅、史可、张岩、刘永生、王立文、王施霁、马力俊、曹云飞。

一、当前互联网数据互联面临的挑战

互联网从诞生起经过五十多年的发展，如今已成为一个全球性网络，是有史以来最成功的人类基础设施之一。

互联网在我国经历了 30 年发展，取得了辉煌成就：从 1994 年的 10 万网民增长到 2023 年的 10.5 亿，互联网普及率达 73%，位居世界第一；建成全球规模最大的光纤宽带网络，5G 网络建设也处于世界领先水平。互联网基础设施更加完善，网络连接更加高速、稳定。2023 年，中国数字经济规模达 49.3 万亿元，占 GDP 比重为 39.8%，位居世界第二。电子商务、在线支付、网络金融等新业态蓬勃发展，互联网经济成为经济发展的新引擎。

互联网为全球主机互联提供了网络连接基础，随着 ICT 技术的不断进步，尤其是移动互联网、大数据、云计算、物联网和人工智能等新兴技术的发展，数据互联的能力和范围得到了极大的扩展。这些技术不仅促进了数据的快速生成和流通，也为数据的分析和应用提供了强大的工具。

互联网数据互联已经成为推动社会经济发展、促进科技创新、提升公共服务效率的重要力量，但在数据互联方面还面临着某些技术瓶颈。

（一）星型连接架构，造成“中心化平台主导的围墙花园”困境

互联网的数据互联主要采用 Web 技术。

Web 架构缺陷越来越明显：互联网最初设计时旨在解决跨局域网（LAN）连接机器的问题，通信双方只能知道所连接的机器的地址，而无法了解任何有关使用机器进行通信的人、组织或事物的信息。由于传统互联网协议不支持操作主机的主体身份验证，一切重要网络活动（如支付、合同等商务活动）均需依赖于平台（即中介），所有的客户端须以星型方式连接服务器、两个客户端之间需要通过服务器（平台）才能互相交互，这造成了中心化平台主导的围墙花园困境如图 1 所示。

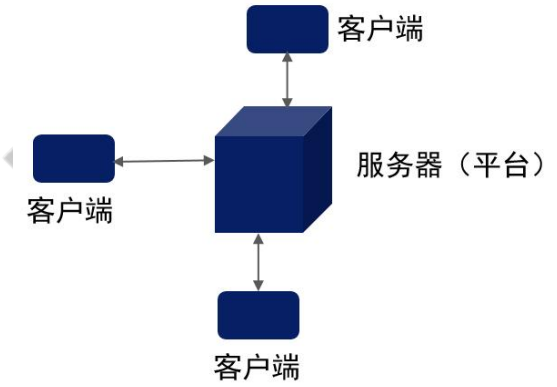


图 1 现有互联网数据互联的星型架构

中心化平台主导的围墙花园模式正为互联网带来越来越不能忽略的问题：从互联网治理角度，中心化平台的不断发展将形成互联网平台寡头，导致缺乏竞争、信任和民主稳定性，造成世界各地的隐私

侵犯、权力集中和数字鸿沟问题；从技术发展角度，这些中心化平台的规模正变得足够庞大后，管理它们的挑战也随之大大增加，会大大限制互联网应用发展。

（二）缺乏语义支持，难以支持数据跨中介（平台）互联

由于互联网 Web 采用客户端-服务器星型链接架构，现有互联网应用之间的数据交互局限于“一跳交互”模式，即：

- 向数据使用方提供数据时，数据提供方需将数据提供给中介（平台）；
- 当数据使用方需要获取数据时，需要从中介（平台）获取数据提供方的数据。

这种依赖中介（平台）的互联网数据交互模式，在互联网上形成了以中介（平台）为中心的“语义孤岛”。由于中介（平台）之间缺乏可共同遵循的互联网语义标准和相关的语义接口和协议，“语义孤岛”之间的数据语义不能互通（见下图 2），这是现有互联网的数据难以跨中介（平台）互联的重要原因之一。

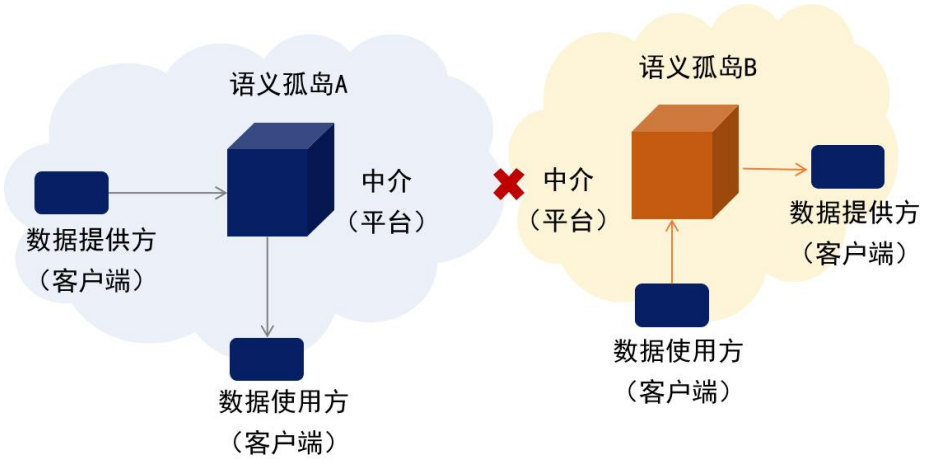


图 2 现有互联网的“语义孤岛”

上世纪 90 年代，创建万维网的蒂姆·伯纳斯-李（Tim Berners-Lee）为 Web 的演进提出了语义网（Semantic Web）的理念。该理念的核心是：通过给万维网上的文档（如: HTML）加上可被计算机所理解的语义（Meta data），使整个互联网成为一个通用的知识交换媒介。这是解决互联网数据跨中介（平台）互联的合理思路。

但实际情况是，如果不深入研究互联网核心语义互通需求和语义网基础设施架构，互联网语义空间会过于庞大、繁杂且难以工程实现。因此，迄今为止，语义网并未大规模发展起来。

（二）依赖第三方中介建立可信关系，不支持跨中介的可信数据互操作

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，当前互联网是通过可靠的第三方中介为数据提

供方和使用方建立信任关系。注：可靠的第三方中介除了为数据提供方和使用方提供中立、安全的数据存储、处理和交换服务，还提供接入验证、数据操作确权和授权的机制，确保数据的合法使用和流通。这种机制有助于解决数据接入和操作的权限问题。

由于数据提供方、数据使用方的数据操作依赖于通过第三方中介建立的可信关系，这导致互联网形成了以中介为核心的信任域。由于中介与中介之间缺乏构建信任的基础设施，导致信任域之间无法为跨中介的数据提供方和数据使用方提供“信任链”，从而形成了“信任孤岛”，如下图 3 所示。

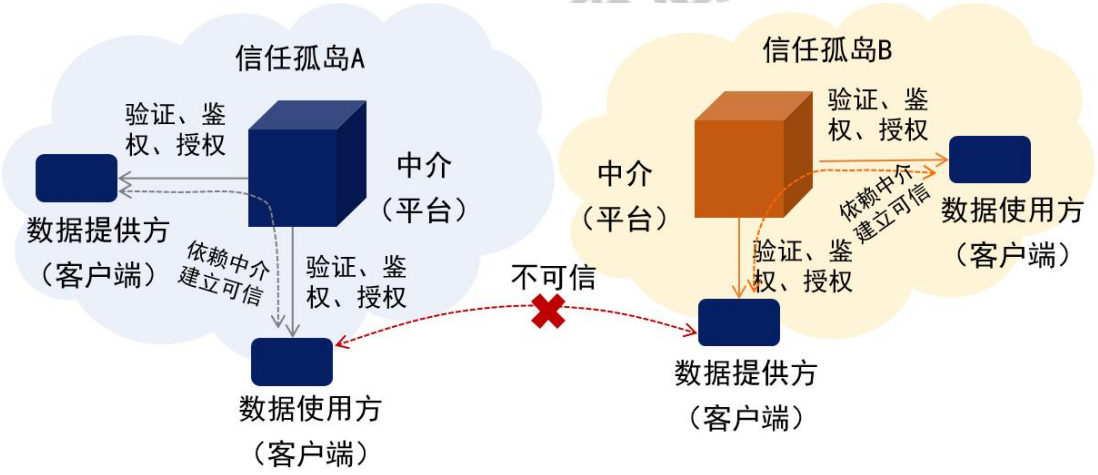


图 3 现有互联网的“信任孤岛”

此外，“信任孤岛”内部也存在问题。尽管第三方中介在增强数据可信度和隐私保护方面发挥着重要作用，但它们的建设和运营也面临着一系列挑战。例如，如何确保中介机构自身的安全性和可信度，避免成为单点故障或遭受恶意攻击；如何平衡数据的开放性和保护性，

既促进数据的流通和利用，又防止数据泄露和滥用；以及如何建立有效的法律和监管框架，规范中介机构的行为，保护数据主体的权益等方面也面临的挑战。

总之，不依赖第三方中介为数据提供者和使用者提供可信的数据互联基础设施是 Web3.0 的愿景之一，需要各方面的合作和努力。

（三）数据权属机制缺乏，妨碍下一代互联网数字资产发展

由于互联网数据权属机制缺乏，绝大部分互联网数据尚未形成“数字资产”。

参考维基百科，数字资产是指任何具有价值、建立所有权并可被发现的数据。数字资产的数据类型包括摄影、徽标、插图、动画、音频/视觉媒体、演示、电子表格、数字绘画、文字文档、电子邮件、网站以及多种其他数字格式及其各自的元数据。

现在，人们在通过互联网交流和共享数字数据时，并没有有效手段保护数字所有权。数据交易过程伴随的权利转移和收益也如互联网数据互联架构一样，为“单跳”形式，即（参考图 4）：

数据提供方将数据提供给中介（平台），由于缺乏技术手段保护数据权利，这意味着数据相关的专利也被转移到中介（平台）；

数据使用方从中介（平台）通过交易获得数据，数据相关的专利也从中介（平台）转移到了数据使用方。

在上述过程中，由于缺乏技术手段保护数据提供方的数据权利，

即使中介（平台）向数据使用方提供的数据是来自于数据提供方的数据，但是中介（平台）很可能不会将获得的收益分享给数据提供方。这降低了数据作为生产要素流动的活力。

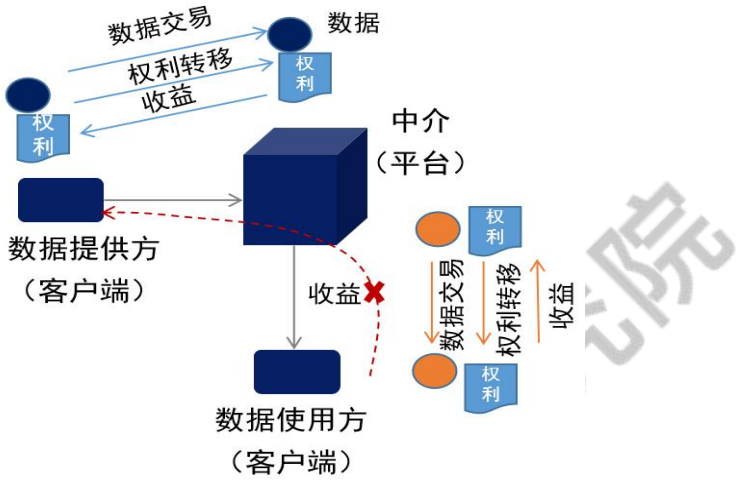


图 4 数据交易、权利转移与收益模型

如果具有技术手段为数据所有权和权益提供保护，互联网上的很多数据都可以被归类为数字资产。注：数字所有权包括访问、创建、修改、打包、获利和销售数据等权利。

总之，在现有互联网数据互联的星型架构上形成的数据交易、权利转移与收益模型不利于下一代互联网软件和算法等数字资产的交易，也很难支持隐性知识类数字资产交易，比如知识想法、观点和经验/方法等，然而这些数字资产的交易对下一代互联网中 AI/ML（人工智能/机器学习）、大模型、元宇宙等新兴技术和业务的发展具有重要作用。

二、Web3.0 的理念及典型应用

（一）Web 技术的演进

上世纪 80 年代中后期，以 TCP/IP 为代表的互联网协议蓬勃发展，促成了全球主机广域互联。

在主机互联的基础上，Web 技术进入发展阶段：以统一资源标识符（URI）、超文本标记语言（HTML）、超文本传输协议（HTTP）构成 web 文本超级链接基础，实现全球主机数据互通。

上世纪 90 年代至本世纪初为互联网 Web1.0 时代，其支持的应用特征可概括为：Web1.0 的页面为静态页面，能够对信息进行简单管理。在这一时代，由主机产生内容、主机产生权利。互联网信息来自于平台、存在于平台服务器上，平台拥有信息的控制权。Web1.0 能够向互联网用户提供的功能非常有限：互联网用户只能通过静态网页，获取平台企业提供的信息，无法向互联网贡献智慧以从互联网直接获得收益。代表性的平台有雅虎、新浪、网易等。

2010 年左右，互联网进入 Web2.0 时代。与 Web1.0 相比，Web 2.0 提供动态页面，为互联网用户参与互联网应用互动提供了可能。Web2.0 通过平台向互联网用户提供了信息上传/发布能力、用户组建群组等能力，互联网舆论力量形成，对社会消费起到一定影响（包括销售渠道、产品流通等环节）。在这一时期，Web2.0 为互联网用户提供了参与互联网应用的技术基础，用户的智力贡献对消费

环节产生影响力（如淘宝电商、抖音网红等），可直接从互联网平台（如淘宝、抖音）获得收益。在这一时代，因 Web 只支持客户端-服务器单跳连接，互联网商贸活动依赖中介式的平台，平台掌握了用户数据，用户数据的控制权以及相应的价值分配权由平台主导，即互联网用户所产生的价值由平台制定协议来分配。

如图 5 所示，突破 Web1.0、Web2.0“客户端-服务器”单跳业务连接限制，促进互联网数据在多个平台间多跳协同，是 Web3.0 技术演进的重要方向。在此基础上，去中心化可信、数据权属与价值分配管理机制也是业界正在探讨的重要问题。

Web3.0 将促进互联网从主机互联、“客户端-服务器”单跳互联到全球数据可信互联和数据价值公平分配，这意味着互联网将不仅是消费互联网，而更是可促进全球劳动者、劳动资料、劳动对象及其优化组合的产业互联网，从而助力形成无与伦比的巨大新质生产力。

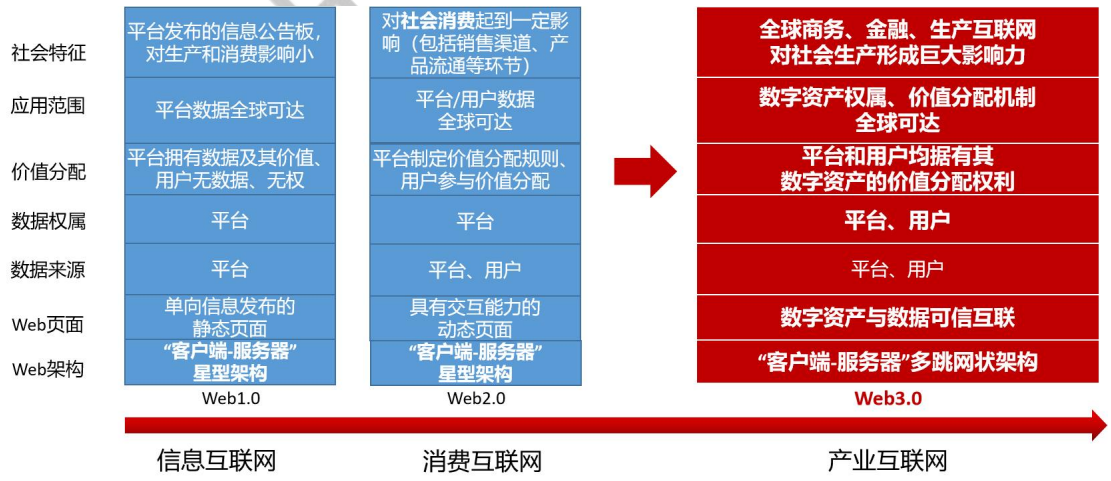


图 5 互联网 web 技术演进

（二）Web3.0 的基本理念

本节总结了编者对 Web3.0 基本理念的理解。

1. 去中心化数据互联架构

从当前互联网数据互联面临的挑战来看，最根本的问题是采用了“客户端-服务器”这种星型数据连接架构。该架构不仅形成了“语义孤岛”、也造成了“信任孤岛”，此外还无法保障数据提供方合理享有权益、公平享有数据资产收益。因此，数据互联架构是 Web1.0、Web2.0 的最根本问题。

Web 3.0 旨在实现不同应用程序、平台和数据源之间的无缝互操作性。这涉及架构、协议、数据格式和应用程序接口的标准化，以促进不同系统之间的通信和数据交换。互操作性可加强各种服务之间的连接和整合，从而形成一个更具凝聚力和互联性的网络生态系统。

Web3.0 的核心理念之一在于“去中心化”，这意味着需要摒弃以服务器为核心的数据互联理念，转而采用一种能够支持互联网应用之间自主、直接建立连接的全新理念，如图 6 所示。

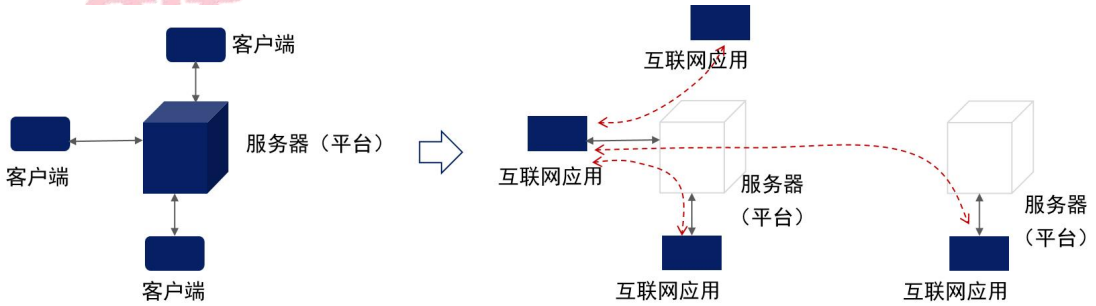


图 6 Web3.0 VS Web2.0 数据互联理念

2. 语义互联

语义网是 Web 3.0 中的一个关键概念，其核心在于利用元数据和语义注释来丰富互联网数据互联能力，从而实现更智能、更能感知上下文的互动。通过以机器可读的格式构建数据，并在不同信息之间建立有意义的关系，语义网显著提升了互联网上的数据搜索、发现、知识表示、数据融合等能力。

基于去中心化数据互联架构，采用本体、知识图谱等语义技术有望解决 Web1.0、Web2.0 的语义孤岛问题（参考图 7）：

- 数据提供方无需将数据提供给中介（平台），并按照中介（平台）的语义规则定义数据；
- 数据使用方可直接从数据提供方获取数据（无需经过中介（平台）），也无需按照中介（平台）的语义规则定义数据。

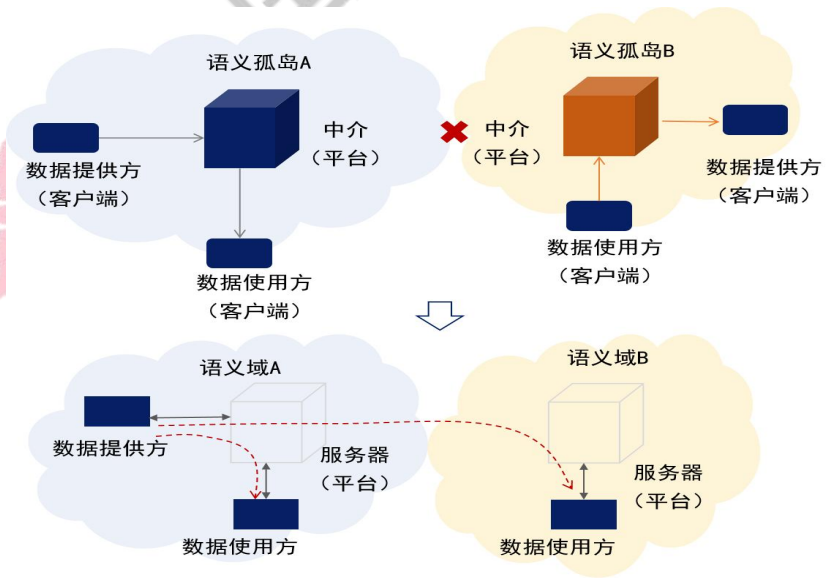


图 7 Web3.0 VS Web2.0 语义互联模式

3. 自主建立可信关系

Web3.0 强调要构建一个更加安全、可信的网络环境。这一理念的核心在于利用区块链等分布式技术，实现数据的去中心化存储和传递，从而提高数据的安全性和透明度。

数据的去中心化存储与传递依赖于数据的提供方和使用方具备自主建立可信关系的能力。

去中心化身份是一种新兴的身份管理方式，正逐步成为构筑可信关系基石的核心技术。它的核心思想是将身份验证从中心化的机构转移到数据提供方和数据使用方手中，从而实现可信身份的自主管理和数据的隐私保护。

在 Web3.0 的框架下，数据提供方和数据使用方不再是单纯依赖中介（平台）建立可信关系，而是能够自主建立可信关系，能够在确保数据隐私保护的同时，实现数据的流通和价值交换，如图 8 所示。

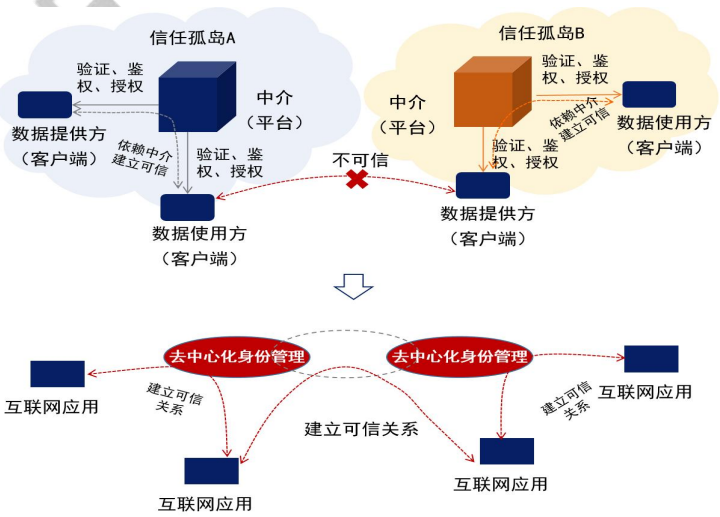


图 8 Web3.0 VS Web2.0 可信关系模型

4. 权属保护与价值分配公平

Web 3.0 的核心原则之一是去中心化，这一原则不仅体现在数据互联过程中力求减少或消除中介的介入，而且体现在深入至数据权属层面，旨在将数据的所有权和控制权从图 9 所示的传统中介（如平台）中彻底剥离出来，归还给数据的拥有者。

Web 3.0 显著强化了用户对其个人数据及数字身份的核心所有权与控制力。分布式可信身份认证机制、加密技术和隐私保护技术使用户能够在参与在线活动的同时，确保个人隐私安全无虞。这种向以用户为中心的数据所有权转变，不仅提升了数字生态的隐私保护水平，还增强了整体安全性与透明度。在此过程中，区块链技术、分布式账本技术（DLT）以及点对点（P2P）网络作为关键技术支柱，正引领着去中心化趋势的深入发展。它们不仅赋予了网络应用程序和服务前所未有的弹性和抗审查能力，还促进了信息流通的民主化与高效性，为构建更加健康、互信的互联网环境奠定了坚实基础。

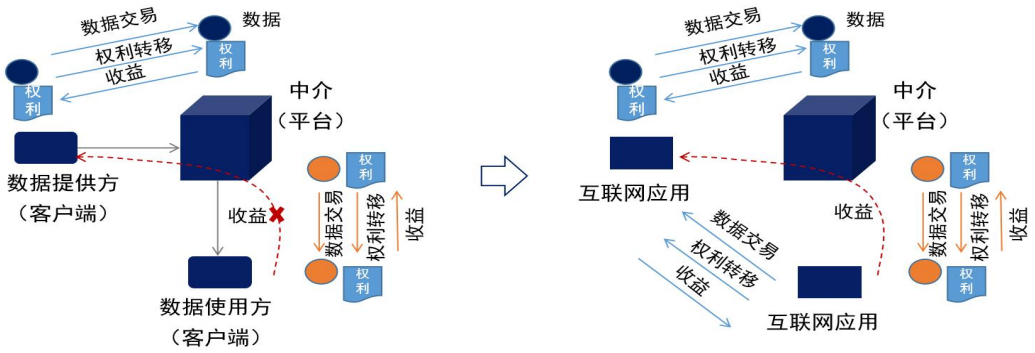


图 9 Web3.0 VS Web2.0 数据交易、权利转移与收益模型

（三）Web3.0 的典型应用

1. 去中心化自治组织（DAO）类应用

去中心化自治组织（Decentralized Autonomous Organization，DAO）是一种基于区块链技术的组织形式，它通过智能合约和基于代币的治理机制来实现自主运作，无需传统的管理层结构或中央控制。DAO 的核心特点在于其决策过程是分布式的，所有成员共同参与决策，推动组织朝着共同的目标或目的前进。

在面向下一代互联网的 Web3.0 支持下，DAO 类应用具有区别于 Web2.0 应用的独特特征：基于语义技术，协作各方可在互联网范围内通过智能合约约定的规则进行协作（不局限在事先设定的利益相关方范围内）、进行资源提供与收益分配匹配等，这可大大降低协作各方的沟通和建设成本。

应用场景举例：

生产资料提供方期望通过互联网锁定生产资料使用方，并寻找物流公司、融资机构产业链上下游合作方。传统方式下，需要各方通过展会、熟人介绍等各种方式寻找潜在合作伙伴，然后再通过招投标等方式确定合作企业。

在面向未来网络的 Web3.0 支持下，DAO 类应用可将供需信息发布到互联网上，然后通过自定义的智能合约规则，实现上下游合作企业的适配、合同签约以及履约认定。这将大大促进社会生产协作。

新冠疫情早期，由于互联网中心化平台主导的围墙花园阻隔了企业间信息的流动，企业间自行进行生产协同较为困难，当时如果具有 Web3.0 的支持，无纺布生产企业、口罩生产企业、消毒湿巾生产企业可按 DAO 类应用方案快速在互联网范围内有效协作迅速补足应急物资缺口，解决社会防疫应急需求。

2. 元宇宙类应用

元宇宙是以人为中心的、沉浸式、实时永续、具备互操作性的互联网新业态，将催生 3D 虚实融合的数字体验，是新一代信息技术集成创新和应用的未来产业，是数字经济与实体经济融合的高级形态，将创造由数字“比特”与人类“原子”深度融合的新型社会景观。

一种观点认为，元宇宙是一个通用的数字平台（即单元宇宙），而另一种观点，是多个平台构成元宇宙（即多元宇宙）。不论是单元宇宙还是多元宇宙，都是指在一系列 ICT 技术的支持下，与现实世界密切联系和互动的虚拟世界，相关 ICT 技术包括人工智能、物联网、数字孪生和 Web3.0 等。

Web3.0 的去中心化数据互联架构为元宇宙数字“比特”跨平台互通提供了基础；Web3.0 的语义互通能力不仅可帮助元宇宙中智能数字体理解网络上的内容，而且使得虚拟世界中的信息能够被智能地处理和推理；Web3.0 的去中心化可信与权属保护可为元宇宙的创新活力和繁荣发展提供必要的保障。

场景举例：元宇宙数字人与多虚拟场景的融合

元宇宙是一个融合了增强现实、虚拟现实和其他技术的三维数字空间，它支持用户以数字人为代理在虚拟环境中进行社交、工作和娱乐等活动。

数字人，作为元宇宙中的关键元素，是由计算机技术创造的具有人类特征的虚拟形象。数字人不仅能够具有个性化特征，还能与教育、商业营销、虚拟演出和智能办公等多种元宇宙虚拟场景进行互动。

Web3.0 可为数字人、不同元宇宙虚拟场景提供身份确认、权属验证、数据互通、权益保护等重要技术保障。

3. 数字资产类应用

Web3.0 之前，数字资产主要指的是传统数据资产，例如：数字文件，数据库，软件，网站及域名等。传统数据资产通常由中心化机构拥有和控制，例如公司、政府或其他组织。传统数据资产的特点是：数据存储于机构的服务器中，数据所有者缺乏相应的技术手段保护其对数据的所有权和控制权，这使得一旦数据发送给其他方，原有的所有者会失去对这些数据的一切所有权和控制权。

为了建立数字资产以及相应的交易系统，Web3.0 需要为数字资产的所有者、买方、卖方等角色提供必要的技术支持，包括但不限于：

任何数字资产的所有者都必须通过在私有/公共存储库中注册来声明数字资产的所有权。与专利一样，未注册的数字资产不被视为具

有所有权。Web3.0 的去中心化数据互联架构可支持多种/多个私有/公共存储库数据互通。

数字资产所有者必须遵循一定的注册流程，以检查是否违反了任何法律法规，包括检查该数字资产是否是非法复制得到的数字资产。Web3.0 的语义互联技术可支持数字资产的语义互通，从而支持买方以及相关机构对数字资产合法性的查验。

为了出售数字资产，数字资产的卖方必须披露交易条款，包括价格等。如果买方想要检查数字资产的内容或质量，则必须能够对数字资产进行有限的访问。卖方需要将数字资产的所有权证明披露给买方。需要有中立机构能够核实数字资产买方的所有权。Web3.0 的可信技术可支持中立机构的灵活构建。

此外，针对数字资产，还需解决数字资产是否只是消费类数字资产，还是可以转售给他人，或者在购买后，买方可以如何使用它们（如是否可以在一定范围内分享给其他人）等问题。

典型应用场景举例：

- 数字艺术品市场：艺术家可以直接向消费者出售数字作品，并获得收益保护（如防止数字作品被买家再次销售）。
- 游戏类资产：玩家可将游戏中的独特资产，如角色、装备、土地等分享/销售给其他玩家，增强了游戏的可玩性和经济价值。
- 知识产权保护：针对音乐、文学、服装设计等作品的进行数字

产品销售和版权保护。

- 数字交易仲裁：针对数据共享等数字交易全过程进行可信存证保护，在发生数据安全纠纷时可取证仲裁。
- 数据隐私保护：数据拥有方的高价值数据在本地计算后共享计算结果，进行可用不可见的多方协同计算隐私保护。

总之，Web3.0 是构建数字资产基础设施的关键技术，随着 Web3.0 技术的发展和应用，数字资产的时代将来临。

4. 算力互联

算力互联是一个含义广泛的概念，它涉及到将分布在不同地理位置的计算资源通过网络连接起来，实现资源共享和协同工作。这种互联可以提高计算效率，优化资源分配，并支持大规模的数据处理和复杂的计算任务。

Web3.0 可为算力互联的构建、基于算力互联的服务等提供重要技术支持。

应用场景举例：

为了对算力资源进行管理，算力互联需要对不同域（即网内域、网间域和服务域）的资源进行注册、标识和认证。传统方法，参考图 10，采用在不同域按照不同域的管理要求进行标识管理；各域需要建立自己的算力注册、标识分配以及算力认证等能力。由于各域自行

管理，会造成相关机制异构、数据难以互通、算力互联互操作成本高等问题，对算力互联造成障碍。

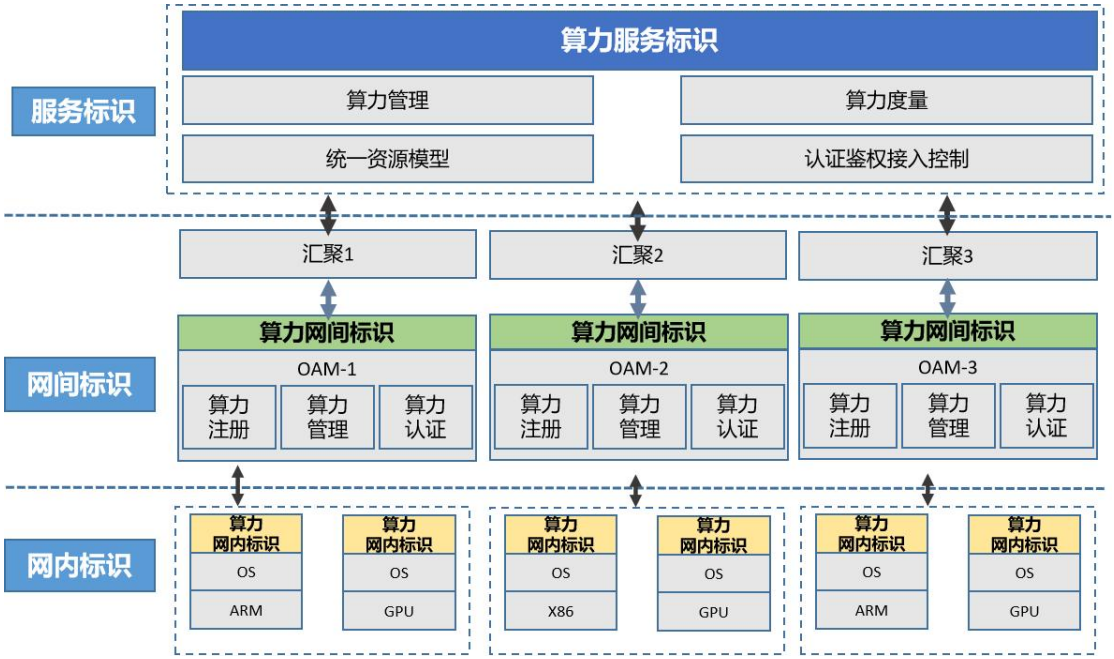


图 10 传统算力互联

Web3.0 的去中心化架构、语义互联、自主可信等特性为算力互联提供了有力支持。

参考图 11，算力网内标识、算力网间标识、算力服务标识可统一采用 Web3.0 的去中心化标识符（DID）、可验证凭证（VC）等技术。在 DID 机制下，各域的算力资源标识、算力身份注册可由算力注册机构负责；各域算力资源的 claims（即算力资源对自身相关信息的申明）可灵活地由不同的机构背书（即可支持不同域下的不同机构为相应算力资源提供背书）；算力资源的 claims 可在区块链、可验

证凭证（VC）、可验证表达（VP）等相关技术的支撑下对相关背书进行可信性验证。

Web3.0 的语义互联对各域算力资源的身份、claims 数据语义互通等至关重要，可灵活支持各域对于算力资源身份、claims 断言的差异性表达和一致性理解。

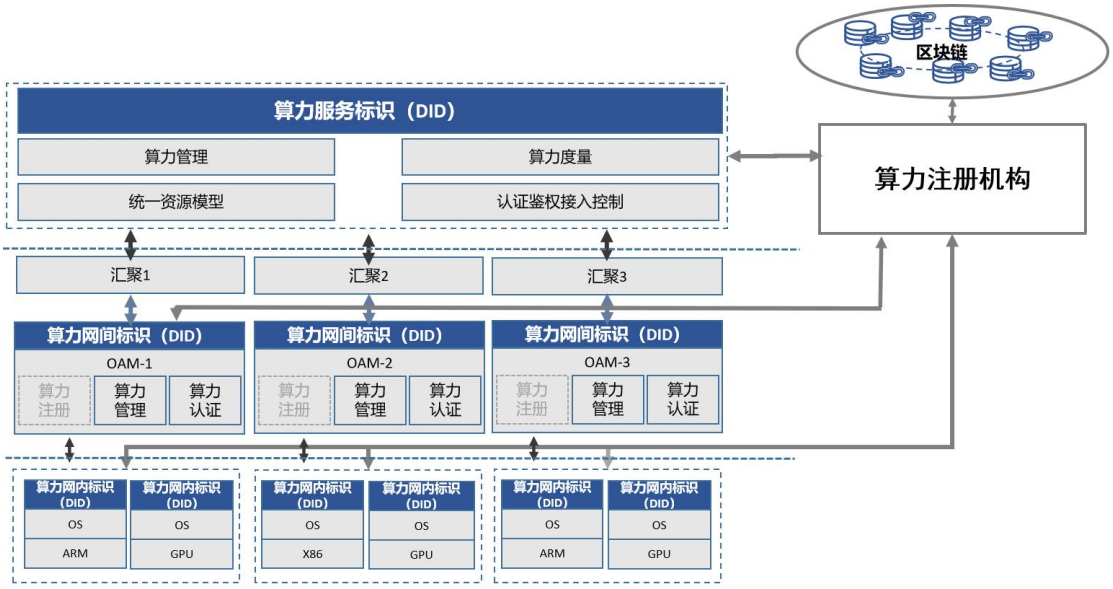


图 11 基于 Web3.0 的算力互联

总之，Web3.0 相关思想和技术可支持算力互联具备可扩展性、灵活性、语义互通性、可信性等特性，可有效保障算力互联各参与方的权益，同时可大大降低算力互联核心业务系统的复杂性和成本，有利于算力互联业务快速发展。

三、面向下一代互联网 Web3.0 的可信数字身份基础设施关键技术

（一）数字身份

根据数字身份管理架构的不同，可以把数字身份分为三类，如图 12 所示，分别是：中心化身份、联盟身份以及去中心化身份。

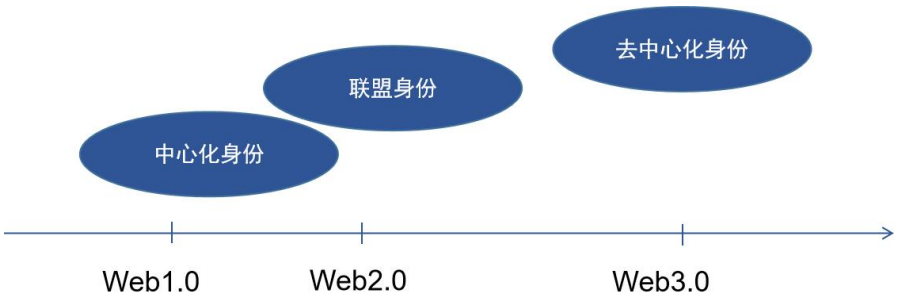


图 12 三种类型的数字身份

中心化身份是由单一的权威机构进行管理和控制的，现在互联网上的大多数应用 APP 的身份管理是中心化身份。

联盟身份的出现解决了中心化身份中身份数据零碎混乱的弊端，此种身份是由多个机构或者联盟进行管理和控制的，用户的身份数据具备了一定程度的可移植性，因此在 Web2.0 时代被广泛应用，例如用户登录某个微信的第三方小程序时，可以通过微信账户直接进行身份验证从而无缝登录该第三方小程序。

联盟身份是在中心化数据互联架构基础上，大型互联网平台公司以中介的方式为小型互联网应用公司以及消费者提供的中心化身份发行和身份验证服务。由于中心化的限制，互联网应用的发展受制于

大型互联网平台公司的用户规模以及互联网平台之间的跨平台合作。但大型互联网平台公司的跨平台合作，不仅涉及到技术异构还涉及到敏感的商业问题。

去中心化身份是支持下一代互联网应用突破平台（中介）限制的重要基础性技术，是 Web3.0 互联网应用繁荣发展、区别 Web2.0 应用的标志性核心技术之一。

（二）Web3.0 去中心化身份基本原理

每个主体（如自然人、法人、机器人、AI 应用等）在不同环境下针对不同用途，可以有多个数字身份。如图 13 所示这些数字身份分别对应着在不同环境下和不同用途下，有关交易主体身份的一组固定的、有限的属性。这些身份属性信息只能在特定的、有限的环境中使用。

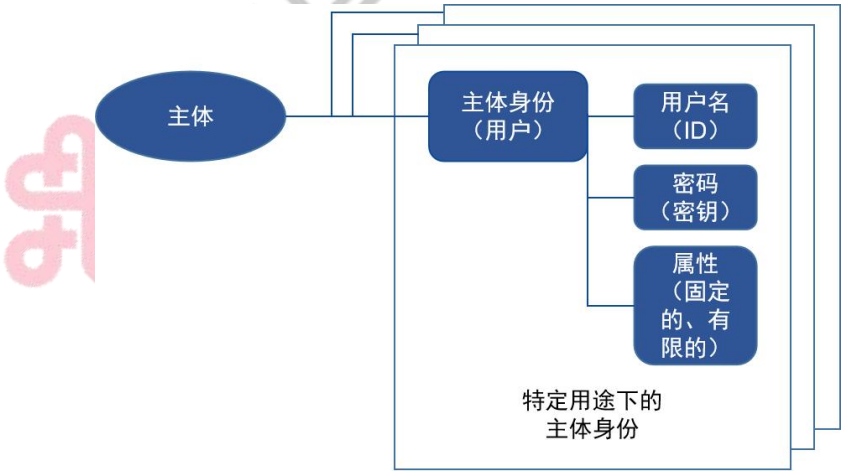


图 13 主体与主体身份

因为主体身份中含有关于主体身份的固定信息，因此在数字化世

界中，围绕主体的一切活动都需要基于主体的数字身份。

如图 14 所示互联网上主体身份的形成主要依赖于三方，即，身份发行方、身份验证方以及身份持有方。

图 14 身份发行发、身份验证方以及身份持有方

“身份发行发（issuer）”：基于用户名（ID）和密码（密钥）标记注册用户并依据相关证明材料，形成注册用户的身份属性，并针对该身份属性为身份持有方发行相应的凭证。

“身份验证方（verifier）”：依据注册用户提供的信息，为其进行身份验证；

“身份持有方（holder）”：是身份属性对应的主体，持有可证明主体与身份属性相对应的凭证。

基于不同的互联网架构设计理念，围绕以上三者之间的不同关系，形成了中心化身份系统和去中心化身份系统。

以Web2.0/Web1.0客户端-服务器架构为基础的传统数字身份系统是中心化身份系统，如图 15 所示，其特点是身份发行方与身份验证方紧耦合，即身份发行方与身份验证方可视为一体：身份发行方发出的主体身份凭证是由身份发行方验证，即身份发行方同时扮演了身份验证方的角色。

图 15 中心化身份系统概念图

中心化身份系统下，身份发行方与身份验证方紧耦合，适用的环境和用途有限，不同身份系统中的身份属性很难整合在一个主体下为多个环境和用途使用。到目前为之，身份管理系统都是对具体情境身份的解决方案。现实世界里，不会有一个单一的数字身份适用于身份主体的所有关系，故彻底解决数字身份问题需要构建比过去一次性的、特定于上下文的身份系统更抽象和通用的身份系统。

相比较中心化身份系统，Web3.0 去中心化身份系统将身份发行方与身份验证方解耦，支持主体在身份发行方处构建身份、主体自主进行身份凭证传递、并可支持他方（身份验证方）对身份凭证进行可信验证，见图 16。

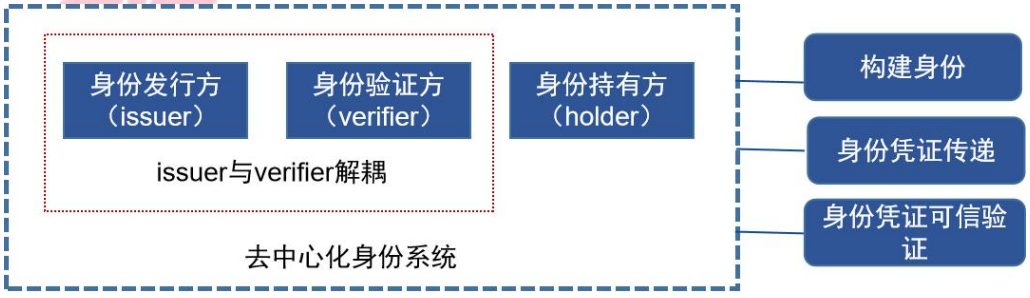


图 16 Web3.0 去中心化身份系统概念图

构建在去中心化身份系统之上的每个身份凭证交换系统都代表

了为特定场景所创建的具体身份系统。人们可以为不同的目的定义凭证，且同一个身份主体的不同身份属性可支持选择性重构和可移植性使用。

（三）Web3.0 可信数字身份基础设施关键技术

1. 关键技术框架

下一代互联网去中心化身份的落地实现依赖于互联网软硬件的演进升级。

为了实现 Web3.0 去中心化身份系统，需要 Web3.0 可信数字身份基础设施的支持。

如图 17 显示了 Web3.0 可信数字身份基础设施需要具备必要的核心关键技术，包括：

- 去中心化标识
- 可验证凭证
- 标识解析
- 区块链
- 数字钱包与可信载体

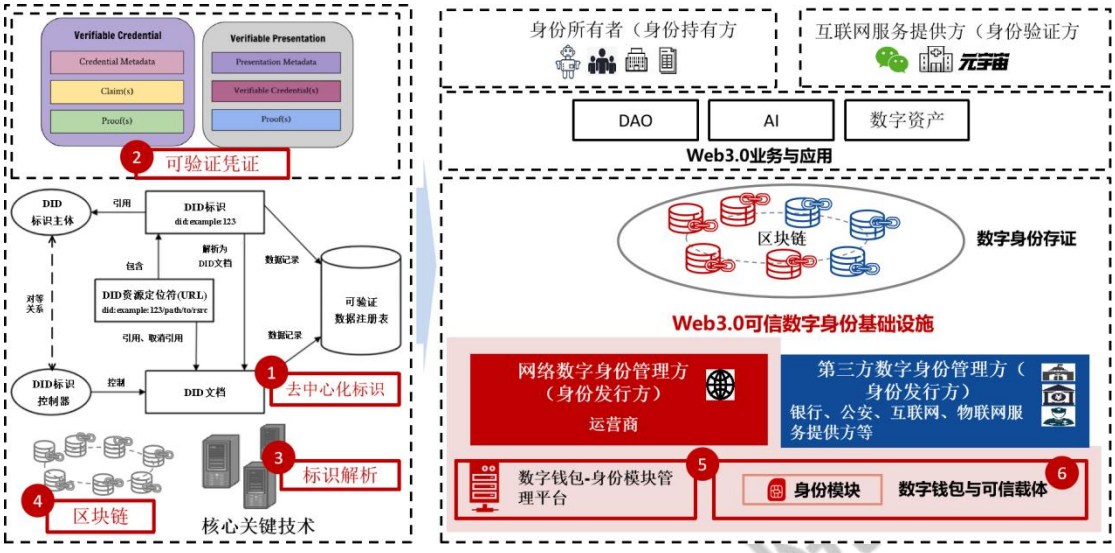


图 17 Web3.0 可信数字身份基础设施核心关键技术

2. 去中心化标识符 DID

2019 年 11 月 7 日，W3C 分布式标识符工作组发布去中心化标识符（Decentralized Identifier，DID）技术框架。

DID 对应着基于区块链技术的去中心化数字身份解决方案。它允许个人或组织在不需要中心化机构的情况下，创建、管理和验证自己的数字身份。

DID 具有唯一性、可验证性和安全性等特点，可以确保身份信息的真实性和可信度。

DID 核心要素及交互关系如图 18 所示，包括 DID 文档、DID 标识符、DID 主体、DID 控制器。

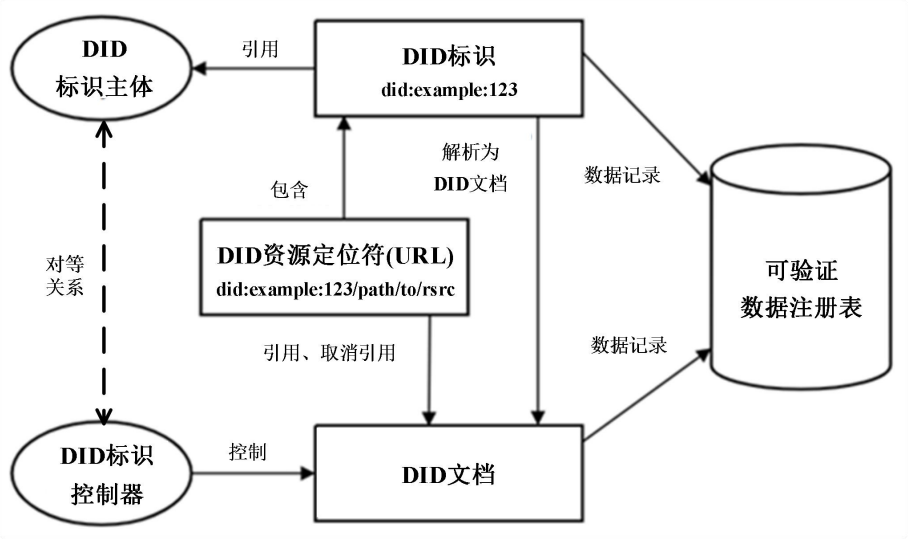
DID 文档用于描述主体的相关信息，通常包括基本身份情况及个人属性等。

DID 标识符用于指引上述 DID 主体信息，通过 DID 标识解析器，

可将 DID 标识符解析为 DID 文档。

DID 主体表示 DID 标识所指向的具体物理实体或虚拟实体，如人、机器、电子文档、AI 程序代码等。

DID 控制器表示实际控制 DID 标识及其 DID 文档的实体。大部分情况下，DID 控制器与 DID 主体相同，但在部分情况下也可以指代不同的实体（例如，当父母控制一个对其孩子进行标识的 DID 时，主体是孩子，但控制器是父母）。



来源：根据网上公开资料整理

图 18 分布式数字标识核心要素关系图

DID 的应用场景非常广泛，包括金融、医疗、教育、电子政务等多个领域。比如，在金融领域，DID 可以用于身份认证和交易验证，提高金融服务的效率和安全性。在医疗领域，DID 可以保护患者隐私，实现医疗数据的共享和互操作。在教育领域，DID 可以帮助学生和教

师建立可信的数字身份，促进教育资源的共享和交流。在电子政务领域，DID 可以用于身份认证和电子签名，提高政务服务的便捷性和安全性。

3. 可验证凭证（VC）与可验证表达（VP）

可验证凭证（Verifiable Credential，VC），是一个 DID 主体向另一个 DID 主体的属性做背书而发出的带有数字签名的描述性声明，用以证明这些属性的真实性，可以认为是一种数字证书。

VC 的数据结构如图 19 所示，其中：

凭证元数据（Credential Metadata）为 VC 的元数据；

断言（Claim）为 VC 包含的针对主体的声明。比如，学历证是学校颁发给学生（主体）的 VC，声明的内容包含学生姓名、学历等级、学制、发证机构等信息；

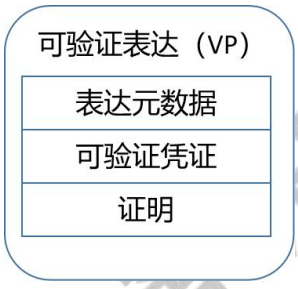
证明（Proof）通常是发证者的数字签名，以确保该 VC 可以被验证，包括支持验证 VC 内容是否被篡改以及验证 VC 颁发者。

来源：根据网上公开资料整理

图 19 VC 的数据结构

可验证表达（Verifiable presentation，VP）是 VC 持有者向验证者表明自己身份的数据。一般情况下，VC 持有者直接向验证者出示 VC 全文即可，但是在某些情况下，出于隐私保护的需要，只希望选择性披露某些属性，或者不披露任何属性，只需要证明某个结论即可。VP 可满足这些需求。

VP 的数据结构与 VC 类似，如下图 20 所示。



来源：根据网上公开资料整理

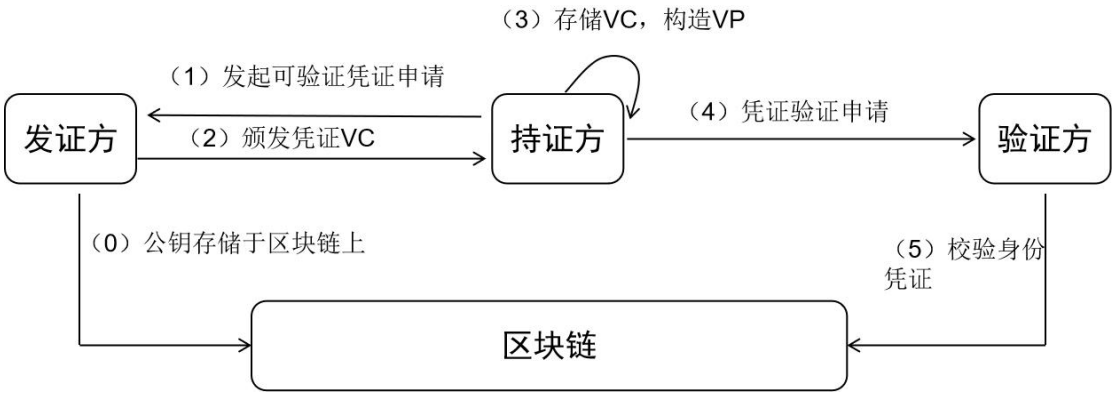
图 20 VP 的数据结构

表达元数据（Presentation Metadata）为 VP 的元数据，主要包含了版本，本 JSON 对象的类型等信息；

可验证凭证（Verifiable Credential）为要对外展示的 VC 的内容，如果是选择性披露或者隐私保护的情形，可能就不包含任何 VC；

证明（Proof）为 VP 持有方对本 VP 的签名信息。

可验证凭证工作原理，参考图 21：



来源：根据网上公开资料整理

图 21 VC/VP 工作流程

（0）前置条件：发证方将自己的公钥存储于区块链上。

（1）持证方在填写必要的申请信息后，向发证方发起可验证凭证申请。

（2）发证方根据用户的信息以及用户提交的 DID 进行审核，满足条件则为用户生成 VC，并将该 VC 关联到用户提交的 DID。发证方使用私钥对 VC 进行签名，之后将签名后的 VC 发送给持证方。

（3）持证方将收到的 VC 存储到本地。一个持证方可以拥有多个发证方颁发的 VC。

（4）当持证方需要出示凭证证明时，可选择相应身份对应的 VC，并可按照验证方的格式要求构造凭证的证明（VP）。然后将凭证（VC）或者凭证的证明（VP）发送给验证方。

（5）验证方收到 VC/VP 后，去区块链查询发证方的公钥进行 VC/VP 验证，从而可以确认该 VC/VP 是否为发证方颁发的凭证。

4. 标识解析

标识解析是 Web3.0 可信数字身份基础设施中不可或缺的重要功能，主要作用是将复杂的标识信息转换为可读的、有意义的数据，使得不同的实体能够相互理解、交互和操作。

解析流程通常包括：识别出需要解析的标识；根据预设的规则或协议，对标识进行解码或转换；将解析后的信息呈现给相应的实体或系统，以便进行进一步的处理。

由于 Web3.0 架构支持去中心化特性，标识的生成和管理将不再依赖于单一的权威机构，而是由网络中的多个节点共同维护。这大大提高了标识的安全性和可信度。

Web3.0 下的标识与标识解析技术具有广泛的应用场景。例如，在数字身份领域，通过唯一标识，我们可以实现去中心化的身份验证和授权，保护用户的隐私和数据安全。在供应链管理领域，标识与标识解析技术可以帮助企业实时追踪货物的流向和状态，提高供应链的透明度和效率。此外，在物联网、大数据等领域，标识与标识解析也发挥着重要的作用。Web3.0 时代的标识与标识解析技术提供了一种全新的方式来管理、访问和操作各种网络资源。通过唯一标识和智能的解析机制，用户能够实现更高效、更安全的数据共享和互联互通。

5. 区块链/分布式账本

区块链/分布式账本技术是一种基于分布式计算和密码学技术的

新型账本管理技术。在 Web3.0 中，分布式账本实现了去中心化的数据存储和传输，保证了数据的可靠性和安全性。与传统的中心化账本不同，分布式账本将账本数据分散存储在多个节点上，每个节点都可以验证账本数据的正确性。当有新的交易数据加入到账本中时，需要通过共识机制来验证这笔交易的合法性，并将交易数据打包成区块，最终形成一个不可篡改的区块链。这种去中心化的结构使得数据更加安全，因为每个节点都参与验证和存储，且没有单点故障的风险。

去中心化技术则是相对于传统中心化网络模式而言的新型内容生产过程。在传统中心化网络中，数据一般集中存储在一个或几个核心节点上，这种模式容易出现单点故障，数据易受损且难以恢复。而去中心化技术将数据分散存储在区块链网络中的多个节点上，每个节点都是中心，都可以连接并影响其他节点。这种扁平化、开源化并且平等化的结构极大地提高了数据的安全性和可靠性。

在 Web3.0 中，分布式账本与去中心化技术相结合，形成了一种高效、安全、透明的数据存储和传输方式。通过利用密码学、共识机制等技术手段，Web3.0 确保了数据在传输和存储过程中的完整性和真实性。同时，由于数据分散存储在多个节点上，黑客攻击的难度也大大增加，从而有效保护了用户的数据安全。此外，分布式账本与去中心化技术还为 Web3.0 提供了许多其他优势。例如，它们可以简化复杂的业务流程，降低交易成本，提高处理效率。同时，这些技

术还有助于实现更加公平和透明的数据共享和交换，促进不同实体之间的互信和合作。分布式账本与去中心化技术有望共同构建了一个高效、安全、透明的未来网络环境。

6. 数字钱包与可信载体

从狭义上看，数字钱包（或电子钱包）是一种可在任何具有网络连接能力的设备上运行的金融交易应用程序。它最核心的能力是可安全的存储、管理主体的身份凭证，并能利用身份凭证参与主体的相关数字化交易活动。

因为涉及到主体身份，数字钱包对安全性的要求是毋庸置疑的。一方面，数字钱包需要采用高级加密技术保护用户的财务信息和交易安全，另一方面可采用可信载体等硬钱包技术，即基于安全芯片、智能卡等安全硬件技术实现数字钱包相关功能，这样能大大提高数字钱包的安全性和可靠性、确保钱包的存储和交易安全。

通用集成电路卡（UICC）是一种能够安全、可靠地存储、传输和处理数据的可信载体，是适用于 Web3.0 下一代互联网应用的理想的底座型数字钱包技术。

UICC 是在全球移动通信系统中使用的智能卡，目前主要用于存储用户信息、鉴权密钥、短消息、付费方式等信息，还可以包括多种逻辑应用，例如用户标识模块（SIM）、通用用户标识模块（USIM）、IP 多媒体业务标识模块（ISIM）、以及其他如电子签名认证、电子钱

包等非电信应用模块。UICC 中的逻辑应用可以单独存在，也可以多个同时存在，如下图 22 所示。

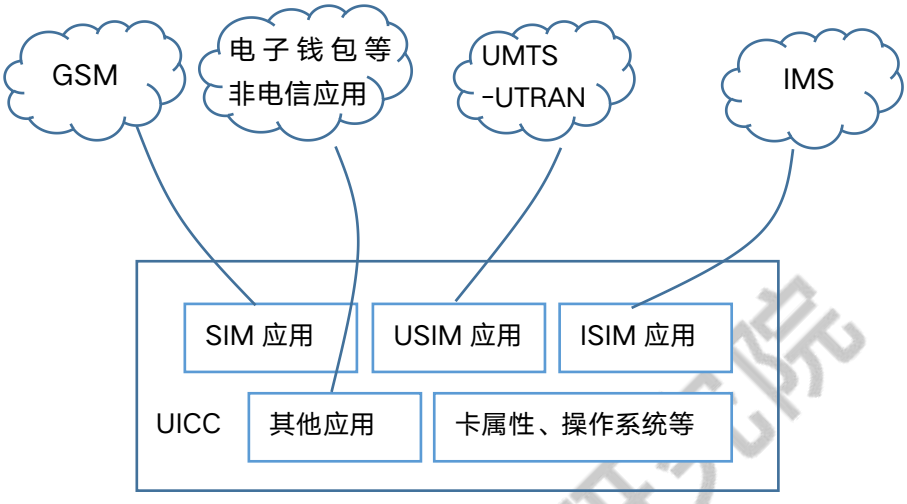


图 22 UICC 及其卡应用

UICC 能够确保卡数据的完整性和安全性，通常可以容纳几百千字节。除了卡应用，UICC 还可以提供电话簿和其他应用程序的存储。

UICC 相关标准主要由 ISO/IEC、3GPP、ETSI、GSMA 等组织制定。UICC 相关标准与标准化组织/联盟的对应关系见图 23。

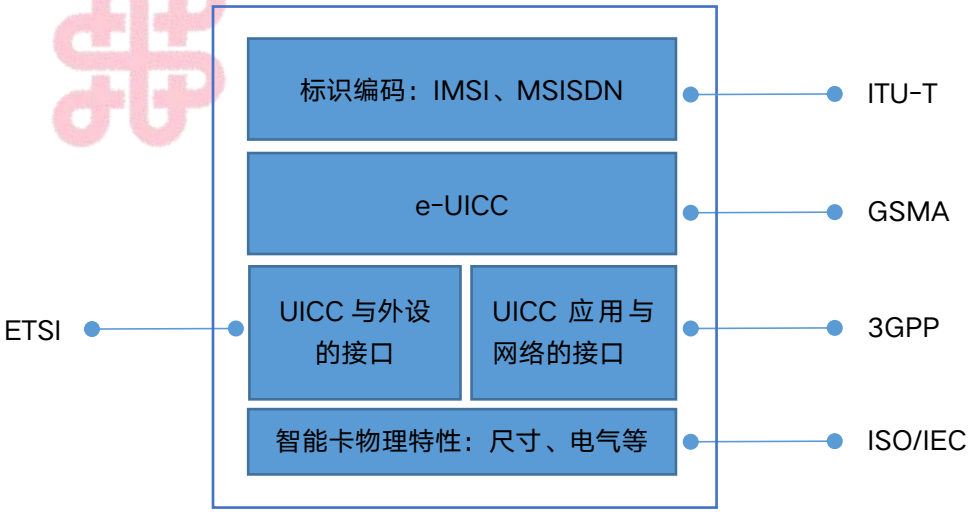


图 23 UICC 相关标准及其标准化组织

ISO/IEC 7816-1（1987）、ISO/IEC 7816-2, 1988 分别定义了标识集成电路卡的物理特性、物理尺寸和触点位置，关注智能卡的物理电气层面，是 UICC 标准的规范性引用文件之一。

ETSI UICC 系列标准主要关注 UICC 与终端的接口，包括 UICC 应用可编程接口、UICC 终端接口、卡应用工具包一致性、SIM 应用工具包等。

3GPP 制定 SIM、USIM 以及智能卡测试规范、终端与 SIM/USIM 的测试规范等。

GSMA 主要制定 eUICC 及其管理平台的规范。

ITU-T 制定了 UICC 可承载的全球移动用户编码 IMSI、MSISND（即电话号码）等编码规范等。

四、相关标准化活动

（一）ITU-T

ITU-T，全称为国际电信联盟电信标准分局（ITU-T for ITU Telecommunication Standardization Sector），是国际电信联盟（ITU）管理下的专门制定电信标准的分支机构，负责研究和制订除无线电以外的所有电信领域的标准。

此外，在 ITU-T 还有大量的与分布式账本/区块链相关的标准，这些标准化工作为 Web3.0 基础设施发展提供了基础。

1．SG13

ITU-T SG13 是未来网络和新兴网络技术研究组。

ITU-T SG13 已开始进行可信数字基础设施的研究工作，于 2022 年 11 月成立了“新兴 Web 时代的未来 ICT 演进”ad-hoc 组 (Web3-adhoc)，是 ITU-T 研究可信数字基础设施技术的先锋。目前在研的技术报告包括《Network enhancement for supporting emerging Web technologies (Web3.0)（中文：支持新兴 Web 技术的网络增强（Web3.0））》、《Trustworthy Data Infrastructure for Web 3.0（中文：Web3.0 可信数字基础设施）》。

除此之外，在 ITU-T SG13 与可信数字身份基础设施相关的关键技术主要是区块链，相关标准（包括已发布和在研）如下表所示。

表 1 ITU-T SG13 与可信数字身份基础设施相关相关标准

Work item	Question	Timing	Approval process	Subject / Title
Y.2342 (ex Y.NGNe-BC-reqts)	Q2/13	2020-10	AAP	Scenarios and Capability Requirements of Blockchain in Next Generation Network Evolution
Y.3530 (ex Y.BaaS-reqts)	Q17/13	2020-Q4	AAP	Cloud computing - Functional requirements for blockchain as a service
Y.2247 (ex Y.frd)	Q1/13	2022-11	AAP	Framework and Requirements of Network-oriented Data Integrity Verification Service based on Blockchain in Future Network
Y.3081 (ex Y.SCid-fr)	Q22/13	2022-Q2	AAP	Self-Controlled Identity based on

Work item	Question	Timing	Approval process	Subject / Title
				Blockchain: Requirements and Framework
Y.2086 (ex Y.DNI-fr)	Q2/13	2021-07	AAP	Framework and Requirements of Decentralized Trustworthy Network Infrastructure
Y.MDRM-DLT-reqts	Q2/13	2024-12	AAP	Requirements and framework of multi-dimensional resource matching of NGNe based on DLT
Y.NRS-DLT-arch	Q2/13	2023-12	TAP	Functional architecture of network resource sharing based on distributed ledger technology
Y.NRS-DLT-reqts	Q2/13	2023-03	AAP	Scenarios and requirements of network resource sharing based on distributed ledger technology
Y.SNICE-DLT-reqts	Q2/13	2024-12	AAP	Requirements and framework of distributed S-NICE based on DLT
Y.3082 (ex Y.MNS-DLT-fr)	Q22/13	2022-Q4	TAP	Mobile network sharing based on distributed ledger technology for networks beyond IMT-2020: Requirements and framework
Y.ICN-DLT	Q22/13	2023-Q2	AAP	Requirements and Functional Framework of Information Centric Networking to support Distributed Ledger Technology in IMT-2020 and beyond
Y.FMSC-DLT	Q23/13	2023-Q4	AAP	Distributed Ledger Technology for fixed, mobile and satellite convergence in IMT-2020 network and beyond
Y.energy-brokerage	Q16/13	2023-02	AAP	Framework of trusted electricity brokerage for distributed energy resources

2．SG16

目前在 ITU-T SG16 与可信数字身份基础设施相关的关键技术主要涉及到区块链，相关标准（包括已发布和在研）如下表所示。

表 2 ITU-T SG16 与可信数字身份基础设施相关相关标准

Work item	Question	Timing	Approval process	Subject / Title
F.751.1 (ex F.DLT-AC)	Q22/16	2020	AAP	Assessment criteria for distributed ledger technology (DLT) platforms
F.751.2 (ex H.DLT)	Q22/16	2020	AAP	Reference framework for distributed ledger technologies
HSTP.DLT-RF	Q22/16	2019	Agreement	Distributed ledger technology: Regulatory framework
HSTP.DLT-Risk	Q22/16	2022	Agreement	DLT-based application development risks and their mitigations
HSTP.DLT-UC	Q22/16	2019	Agreement	Distributed ledger technologies: Use cases
F.751.3 (ex F.DLT-CHM)	Q22/16	2022	AAP	Requirements for change management in DLT-based decentralized applications
F.751.4 (ex H.DLT-INV)	Q22/16	2022	AAP	General framework for DLT-based invoices
F.751.5 (ex F.DLT-DMPG)	Q22/16	2022	AAP	Requirements for distributed ledger technology-based power grid data management
F.751.6 (ex H.DLT-PAM)	Q22/16	2022	AAP	Performance assessment methods for distributed ledger technology platforms
F.751.7 (ex H.DLT-FAM)	Q22/16	2022	AAP	Functional assessment methods for distributed ledger technology platforms
F.751.8 (ex H.DLT-TFR)	Q22/16	2022	TAP	Technical framework for DLT to cope with regulation
F.DLT-DPT	Q22/16	2022	AAP	Application Guideline for DLT-based

Work item	Question	Timing	Approval process	Subject / Title
				Distributed Power Trading
F.DLT-FIN	Q22/16	2023	AAP	Financial distributed ledger technology application guideline
F.DLT-TRICI	Q22/16	2024	AAP	Technical requirements on inter-chain interoperability for permissioned distributed ledger technologies
H.DLT-AGFAS	Q22/16	2025	AAP	Application guideline for authorization services based on distributed ledger technology
H.DLT-AMMSP	Q22/16	2024	AAP	Assessment methods for DLT management service platform
H.DLT-DAS	Q22/16	2024	AAP	Technical framework for distributed ledger technology based multi-media data asset service
H.DLT-DCS	Q22/16	2024-01	AAP	Technical framework of DLT-based digital collection services
H.DLT-DE	Q22/16	2023	AAP	Digital evidence services based on distributed ledger technologies
H.DLT-DST	Q22/16	2024	AAP	Technical framework for permissioned distributed ledger technology based on sharing technology
H.DLT-EMDGP	Q22/16	2023	AAP	General architecture for DLT-based energy metering data sharing platform
H.DLT-ESSS	Q22/16	2024-12	AAP	Framework of distributed ledger technology-based energy storage sharing systems
H.DLT-FMD	Q22/16	2023	AAP	Framework for fast message delivery for DLT-based services
H.DLT-GTI	Q22/16	2023	AAP	DLT governance and technical interoperability framework
H.DLT-MMPA	Q22/16	2025	AAP	Maturity model of permissioned

Work item	Question	Timing	Approval process	Subject / Title
				distributed ledger technology application
H.DLT-PTS	Q22/16	2025	AAP	Performance test suite for distributed ledger technology system
H.DLT-RECT	Q22/16	2024-12	AAP	Reference architecture for information tracing of renewable energy consumption based on distributed ledger technology
H.DLT-RFMSP	Q22/16	2024	AAP	Reference framework for DLT management service platform
H.DLT-SCLMR	Q22/16	2024	AAP	Smart contract lifecycle management requirements for distributed ledger technology systems
H.DLT-SGDRF	Q22/16	2025	AAP	Framework of distributed ledger technology-based smart grid demand response
H.DLT-TEE	Q22/16	2022	AAP	TEE-based confidential computing on distributed ledger technology system
H.DLT-TFI	Q22/16	2022	AAP	Technical Framework for distributed ledger technology (DLT) Interoperability
H.DLT-VERI	Q22/16	2023	AAP	Formal verification framework for smart contract on distributed ledger technology
F.DLT.HC	Q24/16	2024	AAP	Requirements of distributed ledger technologies (DLT) for human-care services
F.DLT.PHR (ex F.DLT.SM.PHR)	Q24/16	2024	AAP	Service models of distributed ledger technologies (DLT) for personal health records (PHRs)

3．SG17

ITU-T SG17 负责安全方面的标准化。

ITU-T SG17 的主要研究领域聚焦于利用信通技术提供安全保障，并确保信通技术自身的安全性。保护个人身份信息，如数据保护的技术和操作方面，以确保个人身份信息的保密性、完整性和可用性等都属于 SG17 的职责范围。

与文本关键技术相关的，目前在 ITU-T SG17 有大量区块链相关标准（包括已发布和在研）如下表所示。

表 3　ITU-T SG17 与可信数字身份基础设施相关相关标准

Work item	Question	Timing	Approval process	Subject / Title
X.1400 (ex X.dlt-td)	Q14/17	2020-09	AAP	Terms and definitions for distributed ledger technology
X.1401 (ex X.sct-dlt)	Q14/17	2019-09	AAP	Security threats of distributed ledger technology
X.1402 (ex X.sra-dlt)	Q14/17	2020-03	AAP	Security framework for distributed ledger technology
X.1403 (ex X.dlt-sec)	Q14/17	2020-03	TAP	Security guidelines for using DLT for decentralized identity management
X.1404 (ex X.sa-dlt)	Q14/17	2020-09	AAP	Security assurance for distributed ledger technology
X.1405 (ex X.str-dlt)	Q14/17	2021-04	AAP	Security threats and requirements for digital payment services based on distributed ledger technology
X.1407 (ex X.srip-dlt)	Q14/17	2021-09	TAP	Security requirements for digital integrity proofing service based on distributed ledger technology
TR.qs-dlt	Q14/17	2023-09	Agreement	Technical Report: Guidelines for quantum-safe DLT system
X.1409 (ex	Q14/17	2022-05	AAP	Security services based on

Work item	Question	Timing	Approval process	Subject / Title
X.ss-dlt)				distributed ledger technology
X.sc-dlt	Q14/17	2023-09	AAP	Security controls for distributed ledger technology
X.srscm-dlt	Q14/17	2023-09	AAP	Security Requirements for Smart Contract Management based on the distributed ledger technology

4．SG20

ITU-T SG20 是物联网和智慧城市研究组。

2023 年 4 月，中国联通、中国信息通信研究院正式向 SG20 提出发起去中心化物联网课题组的建议。该建议已经在 SG20 下一个研究期筹备会议中进行了多轮讨论，目前 SG20 已将该课题组建议提交 TSAG 会议。

除此之外，在 ITU-T SG20 与可信数字身份基础设施相关的关键技术主要是区块链，相关标准（包括已发布和在研）如下表所示。

表 4 ITU-T SG20 与可信数字身份基础设施相关相关标准

Work item	Question	Timing	Approval process	Subject / Title
Y.BC-SON	Q2/20	2023-Q3	AAP	Framework of blockchain-based self-organization networking in IoT environments
Y.IoT-BC-reqts-cap	Q2/20	2023-Q4	AAP	IoT requirements and capabilities for support of blockchain
Y.dec-IoT-arch	Q3/20	2023-Q3	AAP	Decentralized IoT communication architecture based on information centric

Work item	Question	Timing	Approval process	Subject / Title
				networking and blockchain
Y.IoT-BoT-peer	Q3/20	2023-Q3	AAP	Capability and functional architecture of peer of blockchain of things
Y.4476 (ex Y.IoT-rf-dlt)	Q3/20	2021-Q2	AAP	OID-based resolution framework for transaction of distributed ledger assigned to IoT resources
Y.IoT-DES-fr	Q3/20	2023-Q1	AAP	Framework of decentralized service by using DLT and edge computing technologies for IoT devices
Y.4464 (ex Y.IoT-BoT-fw)	Q4/20	2019-Q4	AAP	Framework of blockchain of things as decentralized service platform
Y.4560 (ex Y.DPM-BC-ES)	Q4/20	2020-Q3	AAP	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities
Y.4561 (ex Y.DPM-BC-DM)	Q4/20	2020-Q3	AAP	Blockchain-based Data Management for supporting Internet of things and smart cities and communities
Y.Suppl.62 to ITU-T Y.4000 series (ex Y.Sup-DPM-OBC)	Q4/20	2020-Q3	Agreement	Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
Y.4560-rev	Q4/20	2023-Q1	AAP	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities
Y.DPM-alm-fra	Q4/20	2024-Q4	TAP	Functional requirements and

Work item	Question	Timing	Approval process	Subject / Title
				architecture of blockchain-based activity logs management for IoT data processing and management
Y.4052 (ex Y.blockchain-terms)	Q5/20	2022-Q2	AAP	Vocabulary for blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects
Y.4907 (ex Y.SSC-BKDMS-arc)	Q7/20	2020-Q4	AAP	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities

（二）IEEE SA IC

IEEE（The Institute of Electrical and Electronics Engineers，电气和电子工程师协会）是电子信息领域的权威国际学术组织，也是全球范围内排名头部的非营利性专业技术组织，致力于电气、电子、生物医学、计算机工程和与科学有关的领域的开发和研究。IEEE SA（STANDARDS ASSOCIATION）是 IEEE 的标准协会，是 IEEE 下支持技术研究与标准化的平台。IEEE SA IC（Industry Connections）是 IEEE 为行业提供标准、产品和业务孵化的平台。

2023 年香港科技大学、中国联通等机构联合在 IEEE SA IC 发起了“面向 6G 时代的可信去中心化网络”研究组。该组关注 Web3.0、区块链、隐私计算等技术赋能 6G 时代的可信去中心化网络并研究网

络资源共享、智能城市、数字金融等重要的 6G 时代应用。

2022 年中国信息通信研究院在 IEEE SA 发起了“信任科技全球推进计划”，在该计划下目前有多个草案在研，包括下一代网络可信标识体系、数字身份与数据共享的信任基础等多个重要技术方向。

五、展望

数字身份对于促进下一代互联网数字经济发展至关重要。面向下一代互联网 Web3.0 的可信数字身份基础设施将优化互联网数据要素的产权关系、安全流通及价值分配等关键环节，帮助明确数据权属、保护个人隐私、促进数据的可控共享、实现数据在不同数字化活动间的合规流转。

本白皮书对可信数字身份基础设施阶段性的技术研究结果进行了归纳总结，希望促进电信运营商、软硬件设备提供商、金融机构、研究机构等进一步加强合作、就可信数字身份基础设施的本质和发展方向形成一定共识，充分利用已有基础、发挥各自优势，共同打造整个生态共赢的下一代互联网 Web3.0 底层基础设施，赋能数字产业转型升级，促进基于下一代互联的新质生产力发展。

缩略语

缩写	英文全称	中文名称
AI	Artificial Intelligence	人工智能
DAO	Decentralized Autonomous Organization	中心化自治组织
DID	Decentralized Indentifiers	去中心化标识符
DLT	Distributed Ledger Technology	分布式账本技术
eUICC	Embeded UICC	嵌入式通用集成电路
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 Communication Technology	信息通信技术
ID	identification	身份标识号码
IP	Internet Protocol	网络之间互连的协议
ISIM	IP Multimedia Service Identity Module	IP 多媒体服务身份模块
LAN	Local Area Network	局域网
P2P	peer-to-peer	点对点
SIM	Subscriber Identity Module	用户识别模块或用户身份模块
TCP	Transmission Control Protocol	传输控制协议
UICC	Universal Integrated Circuit Card	通用集成电路卡
URI	Uniform Resource Identifier	统一资源标识符
USIM	Universal Subscriber Identity Module	全球用户识别卡
VC	Verifiable Credential	可验证凭证
VP	Verifiable presentation	可验证表达

参考文献

[1] 中国联通，中国联通算力网络白皮书（2019）

[2] 中国联通研究院，算力网络架构与技术体系白皮书（2020）

[3] Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/2022/REC-did-core-20220719/

[4] Verifiable Credential, https://www.w3.org/TR/vc-data-model-2.0/#what-is-a-verifiable-credential

[5] Verifiable presentation, https://www.w3.org/TR/vc-data-model-2.0/#verifiable-presentations

[6] 中关村区块链产业联盟，区块链+数字标识技术与应用研究报告（2023）

[7] 中国信息通信研究院,全球 Web3 技术产业生态发展报告(2022)

[8] 中国信息通信研究院，区块链基础设施研究报告（2023）

[9] IEEE SA IC, https://ieee-sa.imeetcentral.com/trusteddecentralizednetworkingtowards6gera/folder/WzIwLDE3MzQzNTkzXQ/WzIsODU4Njc5MDId/

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院致力于提高核心竞争力和增强核心功能，紧密围绕联网通信、算网数智两大类主业，按照 4+2+X 研发布局，开展面向 C3 网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国建设，大力发展战略性新兴产业，加快形成新质生产力。联通研究院现有员工 700 余人，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话：010-87926100
邮编：100176

中国联通研究院

中国联通泛终端技术