姚前：Web3.0，渐行渐近的新一代互联网

文/新浪财经意见领袖专栏作家 姚前

互联网是人类通信技术的重大革命，对人类社会产生了极其深远的影响。随着当前各类信息技术的迭代创新，互联网正呈现向下一代互联网演进的趋势。这一演进或将引发新一轮的信息革命，进一步深刻改变人们的生活、工作以及社会的方方面面。

在 Web1.0 问世前夕的 1993 年，美国克林顿政府出台“国家信息基础设施”战略计划，大力建设信息时代的“高速公路”，从而获得 Web1.0 和 Web2.0 的全球领导地位。

互联网经过 30 年的发展，如今正处在 Web2.0 向 Web3.0 演进的重要时点。加强 Web3.0 前瞻研究和战略预判，对我国未来互联网基础设施建设无疑具有重要意义。本文拟结合国内外互联网发展实践和技术演变趋

势，分析 Web3.0 的可能形态并进行相关思考。

Web3.0 是用户与建设者拥有并信任的互联网基础设施

科技创业者兼投资人克里斯·迪克森（Chris Dixon）把 Web3.0 描述为一个建设者和用户的互联网，数字资产则是连接建设者和用户的纽带。研究机构 Messari 研究员江下(Eshita)把 Web1.0 到 Web2.0 再到 Web3.0 描述成为：Web1.0 为“可读”（read），Web2.0 为“可读+可写”（read+write)，Web3.0 则是“可读+可写+拥有”（read+write+own)。

Web1.0 是早期的互联网，用户只能被动地浏览文本、图片以及简单的视频内容，是内容的消费者，互联网平台提供什么就看什么。在 Web2.0 时代，用户不仅可读而且可写，尤其是随着移动互联网以及 Youtube、Facebook、微信等网络平台的发展，用户可以在平台上创造和传播自己的内容(包括文字、图片、视频等)，并与其他用户交流互动。但无论是 Web1.0 还是 Web2.0，用户的线上活动都依赖于特定的互联网平台；即使在 Web2.0 阶段，用户可以是内容的生产者，但规则依然由互联网平台制定，用户缺乏自主权。

一是用户数字身份缺乏自主权。用户只有在互联网平台上开了账户，才能有参与相应线上活动的数字身份，一旦销户则失去权限。每开一次户，用户都要反复填写个人信息。不同互联网平台企业建立不同账户体系，各账户体系规则不尽相同，用户需要管理诸多账户和密码。不同账户体系相互独立，容易形成“孤岛”，不利于互联网生态发展，还衍生出垄断、不

正当竞争等问题。近年来，联邦化身份管理（Federated Identity Management，FIM）模式逐渐流行起来。虽然该模式减少了用户重复开户次数，给予用户一定的身份自主体验感，但也并没有从根本上改变互联网平台身份管理模式的弊端。数字身份仍捆绑在互联网平台的具体账户上。

二是用户个人数据缺乏自主权。在大型互联网平台面前，用户个体相对弱势。在“要么同意，要么不服务”的条约下，用户只能同意个人数据被采集甚至过度采集。如今，互联网平台高度渗透到社会方方面面，向用户提供通信、社交、网购、资讯、娱乐等各类服务。为了获取这些服务，用户不得不让渡数据主体权利。大量用户数据集中于互联网平台，一旦泄露，将对用户隐私造成极大损害，如 Facebook 就发生过类似案例。一些互联网平台还可能滥用技术上的优势，引导劝诱用户，在用户不知情的情况下收集和使用数据，并利用技术手段规避法律约束。

三是用户在算法面前缺乏自主权。算法是互联网平台的核心。通过“千人千面”的用户画像，可以形成独特的客户洞察，成为网络经济的制胜法宝。但近年来，算法滥用、算法作恶等问题日益突出。比如，利用大数据“杀熟”，同样的商品或服务，老客户的价格反而比新客户要贵；只推荐能带来潜在商业利益的产品甚至假冒伪劣产品，而不是对用户最适合、最恰当的商品；滥用人性弱点，过度激发、劝服、诱导用户消费，使人习惯于“被喂养”，不自觉地对算法投放的产品沉迷上瘾；算法的具体原理和参数只有运营企业的少部分人才能知道，易引发利益侵占问题；还有一些

平台甚至利用算法作恶，推送低级庸俗的内容或耸人听闻的虚假信息以扩大流量。

Web3.0 以用户为中心，强调用户拥有（own）自主权。一是用户自主管理身份（Self-Sovereign Identity，SSI）。用户无需在互联网平台上开户，而是通过公私钥的签名与验签机制相互识别数字身份。为了在没有互联网平台账户的条件下可信地验证身份，Web3.0 还可利用分布式账本技术，构建一个分布式的公钥基础设施（Distributed Public Key Infrastructure，DPKI）和一种全新的可信分布式数字身份管理系统。分布式账本是一个严防篡改的可信计算范式，在这一可信机器上，发证方、持证方和验证方之间可以端到端地传递信任。

二是赋予用户真正的数据自主权。Web3.0 不仅赋予用户自主管理身份，而且打破了中心化模式下数据控制者对数据的天然垄断。分布式账本技术可提供一种全新的自主可控数据隐私保护方案。用户数据经密码算法保护后在分布式账本上存储。身份信息与谁共享、作何种用途均由用户决定，只有经用户签名授权的个人数据才能被合法使用。通过数据的全生命周期确权，数据主体的知情同意权、访问权、拒绝权、可携权、删除权（被遗忘权)、更正权、持续控制权得到更有效的保障。

三是提升用户在算法面前的自主权。智能合约是分布式账本上可以被调用的、功能完善、灵活可控的程序，具有透明可信、自动执行、强制履约的优点。当它被部署到分布式账本时，程序的代码就是公开透明的。用

户对可能存在的算法滥用、算法偏见及算法风险均可随时检查和验证。智能合约无法被篡改，会按照预先定义的逻辑去执行，产生预期中的结果。契约的执行情况将被记录下来，全程监测，算法可审计，可为用户质询和申诉提供有力证据。智能合约不依赖特定中心，任何用户均可发起和部署，天然的开放性和开源性极大地增强了终端用户对算法的掌控能力。

四是建立全新的信任与协作关系。在 Web1.0 和 2.0 时代，用户对互联网平台信任不足。20 年来，爱德曼国际公关公司（Edelman Public Relations Worldwide）一直在衡量公众对机构（包括大型商业平台）的信任。2020 年的调查结果发现，大部分商业平台都不能站在公众利益的立场上考虑自身的发展，难以获得公众的完全信任。而 Web3.0 不是集中式的，没有单一的平台可以控制，任何一种服务都有多家提供者。平台通过分布式协议连起来，用户可以通过极小的成本从一个服务商转移到另一个服务商。用户与建设者平权，不存在谁控制谁的问题，这是 Web3.0 作为分布式基础设施的显著优势。

Web3.0 是安全可信的价值互联网

在计算机世界，若没有可信机制，由电子信息承载和传送的价值（Value）很容易被随意复制和篡改，引发价值伪造与“双花”（Double Spending）问题。Web1.0 和 Web2.0 仅是信息网络，虽然可以传播文字、图片、声音、视频等信息，但缺乏安全可信的价值传递技术支撑，因此无法像发邮件、发短信一样点对点发送价值（如数字现金），只能依赖可信机构的账户

系统，开展价值的登记、流转、清算与结算。分布式账本的出现则创造了一种高度安全可信的价值传递技术。它以密码学技术为基础，通过分布式共识机制，完整、不可篡改地记录价值转移（交易）的全过程。其核心优势是不需要依赖特定中介机构即可实现价值的点对点传递，使互联网由 Web1.0 和 Web2.0 的信息互联网向更高阶的安全可信的价值互联网 Web3.0 转变。

在 Web3.0 登记和传递的价值可以是数字货币，也可以是数字资产。分布式账本技术为数字资产提供了独一无二的权益证明。哈希算法辅之以时间戳生成的序列号保障了数字资产的唯一性，难以复制。一人记录、多人监督复核的分布式共识算法杜绝了在没有可信中间人的情况下数字资产造假和“双花”问题。数字资产还能做到不可分割（Non-fungible），如 NFT 可以完整状态存在、拥有和转移。

除了链上原生，数字资产还可来自链下实物资产，如一幅画、一幢房子。如何保障链上数字资产和链下实物资产的价值映射是关键。可考虑通过射频识别标签（RFID）、传感器、二维码等数据识别传感技术以及全球定位系统，实现物与物相连，组成物联网（Internet of Things，IoT），与互联网、移动网络构成“天地物人”一体化信息网络，实现数据自动采集，从源头上降低虚假数据上链的可能性。

Web3.0 一方面能够实现用户侧自主管理身份，另一方面也可实现网络资源侧的自主管理地址，真正做到端到端访问过程的去中介化。传统互

联网作为全球化开放网络，其资源访问依赖于中心化管理的域名系统（Domain Name System，DNS）。DNS 作为互联网最根本的基础设施，虽然从 IPv4 到 IPv6 进行了系统扩展和优化，但仍有可能被操控。Web3.0 作为全新的去中心化的价值互联网，需要全新的去中心化的 DNS 根域名治理体系。这在技术上可以通过分布式账本实现，资源发布方自主注册和管理域名，用户自主查询和解析域名。不仅可以支持传统互联网信息资源，还可以对更广泛意义的数字资产资源、数字实体、区块链等进行命名和解析，从而使得智能合约可以对数字资产以更为方便和可读的方式进行操作，使得 Web3.0 可以更好地实现数字空间与现实空间互动。

例如，以太坊域名服务（Ethereum Name Service，ENS）就是一种 Web3.0 域名服务。它是一个基于以太坊区块链的分布式、开放和可扩展的命名系统。ENS 的工作是将可读的域名（如“alice.eth”）解析为计算机可以识别的标识符，如以太坊地址、内容的散列、元数据等。ENS 还支持“反向解析”，这使得将元数据（如规范化域名或接口描述）与以太坊地址相关联成为可能。与 DNS 一样，ENS 是一个层次结构的域名系统，不同层次域名之间以点作为分隔符，我们把层次的名称叫做域，一个域的