

Web3.0前瞻研究报告 (2022年)

可信区块链推进计划
2022年9月



引言

近年来，针对互联网行业发展面临的利益分配失衡、平台资源垄断、个人隐私泄漏等问题，全球兴起了新一轮互联网创新探索热潮，力图通过引入区块链、密码学等技术，来重构互联网发展未来图景，Web3.0 理念应运而生。总体来看，Web3.0 是以分布式技术重新解决互联网数据权属和价值表达的重要创新，有望从技术、产业、经济三方面优化互联网，进而推进生产方式、组织秩序和经济形态创新，但当前 Web3.0 仍存在发展前景备受争议、技术应用不成熟、金融衍生风险等关键问题。建议密切关注 Web3.0 发展动向，包容审慎推动相关技术创新与应用探索，积极稳妥探索我国 Web3.0 发展之路。

为加强我国对 Web3.0 的前瞻研究和战略预判，可信区块链推进计划 (TBI)、大数据技术标准推进委员会 (CCSA TC601) WG6 大数据区块链工作组、中国互联网协会 (ISC) 区块链技术应用工作委员会联合，组织成员单位深入研讨 Web3.0 相关技术细节和应用方向，共同编制研究报告。本研究报告综合分析国内外 Web3.0 政策和产业发展现状，详细介绍了 Web3.0 的关键技术组件和核心应用场景，为我国积极稳妥探索 Web3.0 发展之路提供参考建议。

目录

I 内涵与价值	1
(一) 发展理念	1
(二) 关键需求	3
(三) 概念定义	4
(四) 关键特性	5
(五) 核心价值	7
II 关键技术	9
(一) 技术体系参考架构	9
(二) 关键基础设施	10
1. 开放联盟链	10
2. 分布式存储	11
3. 算力网络	12
(三) 数字资产	13
1. 数字资产	13
2. 数据资产	13
3. 数字资产交易市场	14
4. 数据要素市场	15
(四) 代表性链原生组件	16
1. 非同质化通证	16
2. 分布式金融	20
3. 分布式数字身份	23
4. 分布式自治组织	26
(五) 代表性链外中间件	27
1. 数字钱包	27
2. 预言机	27
3. 跨链	28
4. 隐私计算	32
5. 服务治理	34
6. 链上数据分析	35
7. 安全审计	36
III 产业现状	37
(一) 技术体系逐步成型，产业生态初具规模	37
(二) 国外创业投资活跃，国内聚焦数藏领域	40
(三) 各国推动政策实施，监管举措逐渐升级	42
(四) 应用模式仍需探索，风险挑战不容忽视	43
IV 总结与展望	44
附录 应用案例	46

图目录

图 1: 历代互联网的关键特性演进	1
图 2: Web3.0 的核心价值主张	2
图 3: 从马斯洛层次理论看 Web3.0 关键技术	3
图 4: 历代互联网产生的数字经济规模测算	4
图 5: Web3.0 是开源商业模式的数字化升级	5
图 6: 历代互联网赋予用户的权益变化	6
图 7: 海外 Web3.0 数字原生经济生态	8
图 8: Web3.0 技术与应用参考架构	9
图 9: 联盟链与公有链发展路径对比	10
图 10: 开放联盟链打通 Web2.0 时代“价值孤岛”	11
图 11: Web3.0 价值互联网与数据要素市场的关系	15
图 12: 数字藏品产业生态分层架构	18
图 13: Web3.0 与元宇宙关键技术发展路径	19
图 14: Web3.0 数字资产金融应用演进过程	20
图 15: 基于可信计算的通用跨链交互模型	29
图 16: 基于跨链桥的数字资产双向跨链方法	29
图 17: 基于区块链的 SaaS 服务治理	34
图 18: 2022 年 Web3.0 技术成熟度曲线	37
图 19: 2022 年上半年全球 Web3.0 项目营收规模测算	38
图 20: 2022 年上半年全球 Web3.0 业务营收规模测算	38
图 21: 2022 年海外 Web3.0 生态产业现状	30
图 22: 全球 Web3.0 投资机构投资项目数量规模测算	40
图 23: 2021 全球各地区 Web3.0 投资额度规模测算	40
图 24: 2022 年全球 NFT 交易与我国数字藏品发行规模测算	41

版权声明

本报告版权属于可信区块链推进计划 (TBI)，并受法律保护。转载、摘编或利用其他方式使用本报告文字或者观点的请以下述方式引用本报告: 可信区块链推进计划:《Web3.0 前瞻研究报告(2022 年)》。违反上述声明者，编者将追究其相关法律责任。

免责声明

本报告涉及的各项公有链项目仅用于原理性说明及技术架构分析研究，不构成对任何人的投资建议或市场预测。虚拟资产交易炒作活动扰乱经济金融正常秩序，滋生非法跨境转移资产、洗钱等违法犯罪活动风险。提醒广大消费者，应增强风险意识，树立正确的投资理念，谨防个人财产及权益受损，不参与虚拟货币交易炒作活动，不参与虚假宣传诱导虚拟资产投资，不盲目跟风虚拟资产相关投机行为。

(一) 发展理念

从 Web1.0 到 Web2.0，再到 Web3.0 的演进，反映了互联网发展理念的升级。Web1.0 是以向消费者提供信息服务为理念，其典型应用是以雅虎、新浪、搜狐为代表的门户网站，主要特征是门户网站主导创作并向消费者提供服务，用户只能被动地浏览文字和图片以及简单的视频内容。Web2.0 是以撮合劳动者和消费者为理念，其典型应用是以淘宝、美团、滴滴为代表的中介平台和以微信、微博、抖音为代表的內容社交平台，主要特征是平台作为中间商撮合多边市场，用户不仅是享受服务的消费者，同样可以成为提供服务的劳动者，在平台上交易劳动力、创造内容或者进行线上社交活动。Web3.0 是以去信任、去中介和数字资产化为理念，以区块链为底层关键技术，以数字生产和数字消费为主要经济形态的新一代互联网，其主要特征是利用分布式账本技术对 Web2.0 应用逻辑进行重构，利用区块链的可信协作、分布式执行、数据保护、资产转移等能力进一步整合信息流、业务流和价值流，以更加标准化的、更加简洁的链上智能合约来代替现有互联网应用服务，消除对中心机构的依赖。

来源：可信区块链推进计划整理

互联网演变	Web1.0 (1980s-)	Web2.0 (2000s-)	Web3.0 (2010s-)
入口	浏览器 (Browser)	应用 (App)	钱包 (Wallet)
后端逻辑处理	服务器 (Servers)	云服务 (Cloud)	区块链 (Blockchain)
交互方式	读	读、写	读、写、拥有
经济模式	广告经济	平台经济、广告经济	所有权经济、创作者经济
网络形态	分散式	中心化	分布式、多中心
数据/内容发布者	机构	PGC、UGC	PGC、UGC、DAO
数据/内容所有权	机构	公司及平台	组织及个人、可移植
数字身份系统	用户名密码	平台内数字身份	跨平台、基于私钥数字身份

图 1：历代互联网的关键特性演进

基于区块链的 Web 3.0 概念最早由以太坊的联合创始人 Gavin Wood 于 2014 年提出。

如果用一句话来解释 Web 3.0，Gavin 认为是 Web 3.0 是让互联网“少一点信任 (trust)，多

一些事实 (truth)”。在他眼中, Web 3.0 是利用分布式系统、密码学等技术手段减少用户对互联网中心化机构的“信赖”。Web 3.0 研究机构 Messari Research 在《Web 3.0, 一言以蔽之》一文中, 定义 Web 1.0 的特征是“可读”(read); Web 2.0 的特征是“可读+ 可写”(read+write); Web 3.0 的特征则是“可读+ 可写+ 拥有”(read+write+own)。Coinbase 在《Web3 架构简介》一文中解读“Web 3.0 赋予用户对其创作内容的所有权, 用户通过区块链控制数据和资产的权属”。A16z 合伙人 Chris Dixon 称“Web 3.0 是以数字资产为媒介, 由建设者和用户共同拥有的互联网”。2022 年 3 月, 中国证监会科技监管局局长姚前在《中国金融》发表文章认为“Web 3.0 是用户与建设者拥有并信任的互联网基础设施, 是用户与建设者共建共享的新型经济系统”。

当前 Web 3.0 具有多重定义, 满足不同参与者的价值主张。广义的 Web3.0 是指下一代互联网, 而狭义的 Web3 是指目前全球区块链产业生态。Web3 只是 Web3.0 阶段中诸多技术概念的其中一个, Web3 能否发展成下一代互联网仍有待商榷。Web3 包含两个的核心价值主张: 数字资产化和去中介化。从数字资产化的角度看, Web3 强调价值流通, 认为数字空间中的数字产权可以高效流通, 任何人可以在互联网上创造价值、分享价值、获得价值。从去中介化的角度来看, Web3 强调开发共建, 认为互联网应用服务在技术、数据、知识产权、算法代码、功能接口、金融市场等层面应该足够开放, 普通用户能够参与到互联网应用服务的生产、交换、消费等各个环节当中。

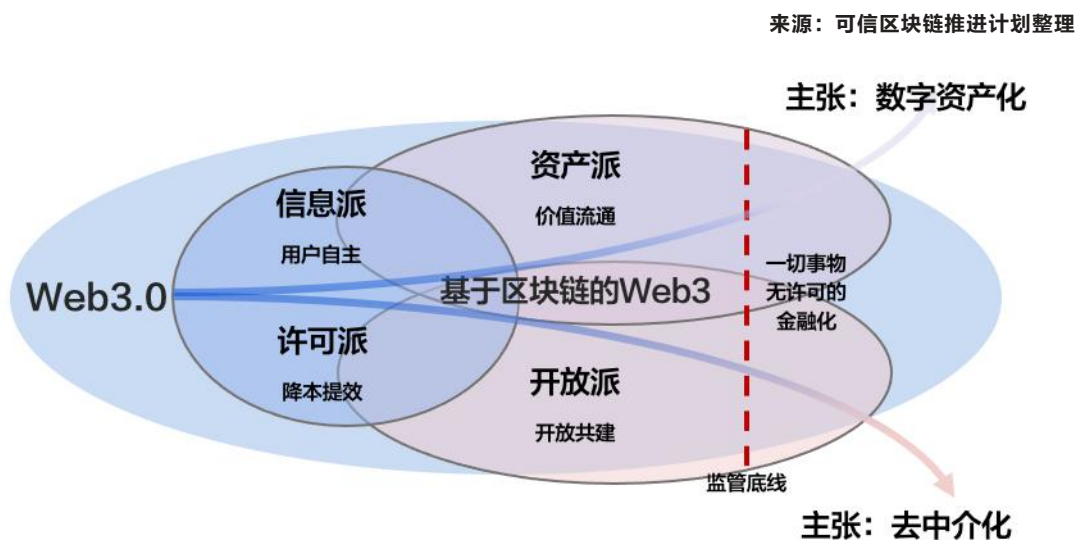


图 2: Web3.0 的核心价值主张

（二）关键需求

Web3.0 概念兴起的底层逻辑是人们对互联网、对数字空间需求的变化。

一是科技向善的需求。Web3.0 是从开源文化、极客精神、加密朋克等文化思潮演变出来以“科技向善”为初心的社会运动。Web3.0 概念兴起的一大推动力是解决目前互联网发展存在的“垄断”和“作恶”问题。极客们希望基于区块链的分布式、不可篡改、公开可验证、代码即法律等特性，创造一个身份自主、数据自主、算法共治、去垄断、去恶性竞争的数字空间。

二是开放共建的需求。随着区块链、人工智能、虚拟现实、数字孪生、人机交互等新一代信息技术不断演进，各项技术独立发展都面临着规模化落地的瓶颈，无法形成闭环的商业生态。而 Web3.0 的出现，为各项技术提供了一个更新、更大、更聚焦的概念和商业模式，以此拉通全产业链的深度融合并进一步促进商业化落地。

三是数字原生的需求。随着经济发展和人民生活水平的提高，互联网用户的需求也不断向高维进阶，人民需求逐渐从物质消费向精神文化消费发展，从满足生理需求、安全需求等基础需求向满足社交需求、尊重和自我实现等高阶需求发展，从实物形态向数字虚拟形态发展，从数字迁移向数字原生发展，未来随着人们的物质匮乏感普遍降低，人类的文化和娱乐需求将迎来新高度，数字原生的商品和服务将成为互联网产业的重要组成部分。

来源：可信区块链推进计划



图 3：从马斯洛需求层次理论看 Web3.0 关键技术

Web2.0 即当今互联网是以信息为核心对象的信息互联网，其核心特征是算法与信息交互，利用算法来生成和分发信息，实现了信息流转趋向于“零边际成本”，实现了以平台经济为核心引擎的数字经济发展模式。**Web3.0 是以数字资产为核心对象的价值互联网**，其核心特征是算法与资产的交互，利用算法来生成和分发数字资产，实现了资产流转趋向于“零边际成本”。Web3.0 通过区块链及智能合约将数字空间的资源标记成数字资产，用户基于数字资产可以拥有互联网的部分数字产权。比如，Web3.0 强调用户对于个人数据具有所有权，对于互联网平台和应用有参与治理的权利。同时，数字资产是一种新型的数字权益凭证。数字资产的引入意味着在互联网上建立了一个内生的新型权益交易市场，用户可以在链上市场中创建、交易、消费自己的数字产权，其带来的数字产权经济将彻底改变数字经济的发展模式。

来源：Folius Ventures，可信区块链推进计划整理

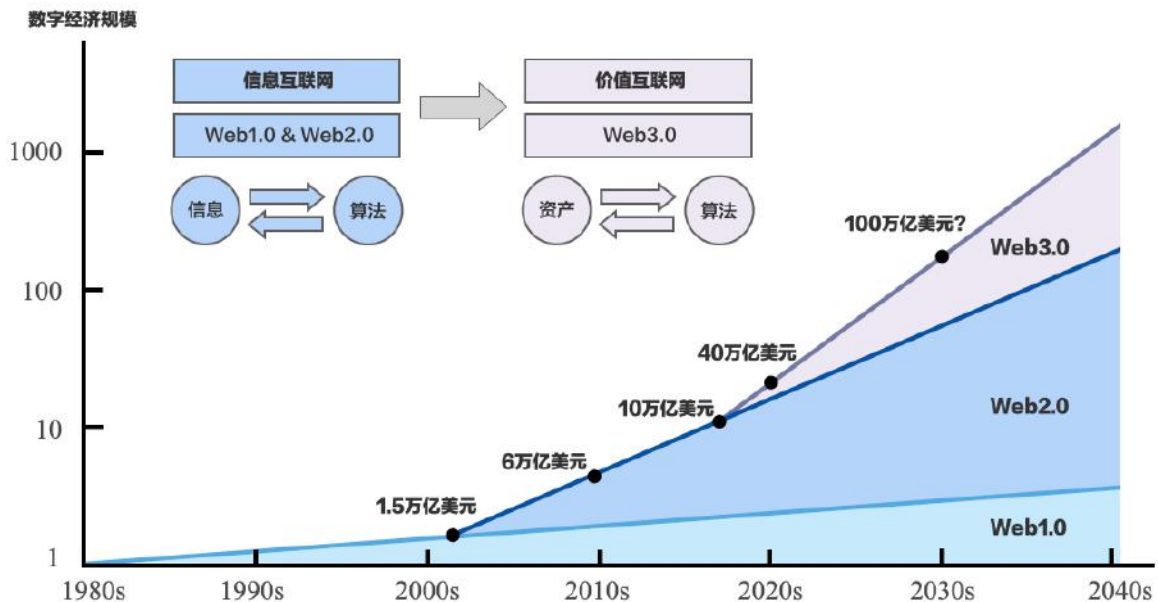


图 4：历代互联网产生的数字经济规模测算

(四) 关键特性

《大教堂与集市》一书中将软件开发模型分为大教堂模型和集市模型。大教堂模式是 Web2.0 中典型的自上而下的闭源商业模式，由顶层的专门团队作为执行领导，用户需要完全信任企业人员来管理资金和执行服务。集市模式则是 Web3.0 典型的分布式的开源开发范式，用户不再信任人，而是信任技术本身。联盟链与公链恰恰是区块链技术在两种模式下的产物，未来两种模式也会衍生出元宇宙的两种流派。两种模式走到最后会是一个趋同的方向，教堂要做大需要用更开放的模式去拓展用户，集市要做大最终还是要形成更严格的准入规则和监管制度。

来源：可信区块链推进计划整理

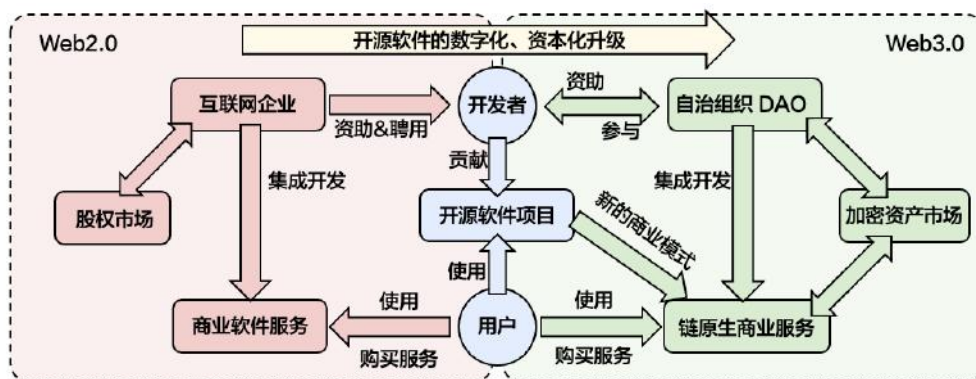


图 5: Web3.0 是开源商业模式的数字化升级

Web3.0 强调建设者与用户开放共建。开源是支撑 Web3.0 开放共建的基础特性。开源实现不仅是对消费者有百利无一害的福利，更是 Web3.0 精神的具现。业界对 Web3.0 的认同感主要来自于它是个开放包容的生态，其技术应用在数据、算法、功能、接口等层面上都是公开透明的。Web3.0 不仅允许用户直接在代码层面检验系统的真实性，为用户提供更彻底的安全验证机制，而且应用程序在生产运行中也完全透明化，充分消除算法“黑箱”造成的负面影响。因为代码开源、治理公开、交易可查等基础特性，所以 Web3.0 才会衍生出一些进阶特性，比如网络的开放共建、算法的可组合性、数据的可移植性等等。

Web3.0 强调赋予用户更多的自主权。密码学是支撑 Web3.0 用户自主权的基础技术。Web3.0 带有一种私有产权保护的价值观，希望把如今被互联网平台控制的数字产权极大地让渡

给用户，这是 Web3.0 发展的一个核心驱动力。Web3.0 从根本的密码学出发，希望通过区块链及智能合约制定一套全新的数字产权制度。通证 (Token) 在技术层面是一种智能合约，本质是一种密码学保障的数字产权管理工具，可以代表数字空间内数字产权的使用规则。

网络的开放共建： Web3.0 将数据、算法、算力等数字资源在区块链上开放共享和数字确权，组织或个体可以自主参与网络的基础设施建设，为 Web3.0 数字空间提供存储、计算、网络带宽、数字内容等资源，并通过密码学保障用户提供的劳动力和资源可以被有效记录和验证。

算法的可组合性： 不同数据、算法、算力、身份、应用之间可相互随意组合，像“乐高积木”搭建在一起。一个应用能成为另一个应用的创作材料，不同应用能融合在一起成为更大的应用。

数据的可移植性： Web3.0 为用户赋予数据的可携带权。用户数据在应用之间可“自由迁徙”、“改门换庭”。如果用户对某个应用不满意，可随时把自己的数据迁移到另一个应用之中。

算法治理的自主权： 通过密码学保障应用规则、数字社会制度的正确运转，用户基于数字权益凭证参与应用业务功能和发展方向的治理，让每位参与者都能掌握算法治理的话语权。

身份数据的自主权： 通过密码学保障用户自我掌控数字身份，自主控制个人数据流转，保护个人隐私信息，有效规避“信息茧房”“二选一”“算法歧视”“大数据杀熟”等乱象。

来源：Fyrfly Venture、可信区块链推进计划整理

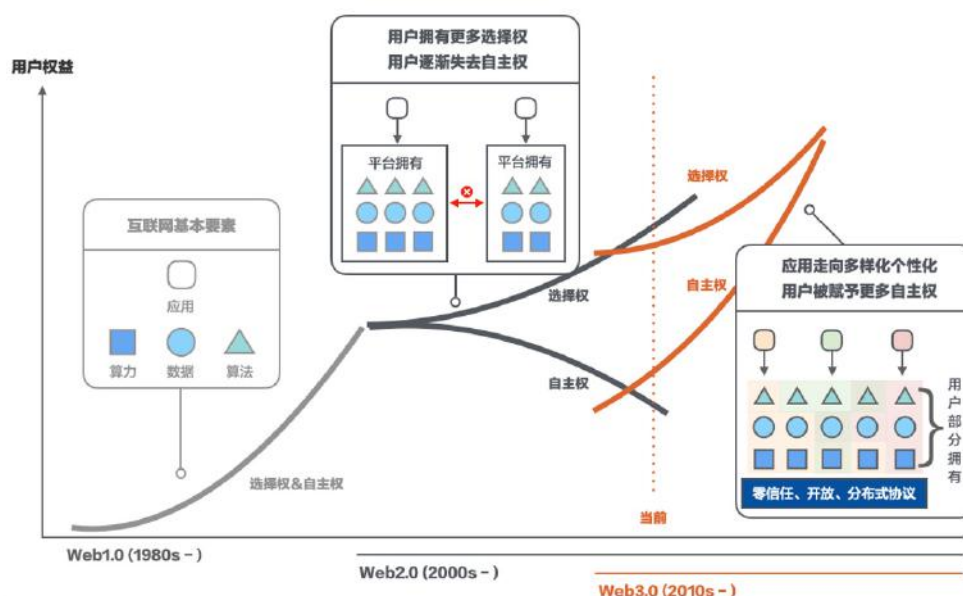


图 6：历代互联网赋予用户的权益变化

（五）核心价值

一是有望塑造互联网技术新体系。Web2.0 的数据收集、存储及使用均以中心化方式为主，存在过度收集并滥用的动机和风险。而 Web3.0 基于开源和密码学的技术治理体系能够有效规避“信息茧房”“二选一”“算法歧视”“大数据杀熟”等乱象。首先，Web3.0 的核心理念是将数据所有权从平台转移给个体用户，基于区块链和密码学技术实现数据确权，保障数据所有者能够自主授权个人数据是否允许他人使用，以此实现从数据滥用到数据自主可控的转变。其次，Web3.0 强调对技术的正确运用并有助于算法开放共治的实现。Web3.0 将算法代码开源，通过密码学建立一种自证清白的信任机制，保障应用按规定正确运转，允许核心团队、独立开发者、用户基于数字权益凭证共同治理应用的业务功能和发展方向，让每位参与者都能掌握算法治理的话语权，以此实现从算法滥用向算法开放共治的转变。最后，Web3.0 将区块链作为互联网逻辑处理和数据存储的公共基础设施，所有基础设施、组件、应用可通过数字钱包访问，彼此之间又可以无障碍地相互沟通、验证和价值交换，这不仅降低了平台对于数据的垄断地位，还为跨应用的数据共享提供了有效解决方案。

二是有望优化互联网发展模式与产业格局。Web2.0 大型互联网平台凭借其技术和渠道优势加剧了资本垄断，主导了经济利益分配的规则制定，并通过规模倍增效应进一步降低边际成本提升话语权，导致市场形成“赢家通吃”局面。而 Web3.0 的去中心化事务处理方式是解决中心平台垄断和利益分配失衡问题的一种尝试。一方面，Web3.0 以多方协同的分布式架构对传统中心化的封闭业务进行重构，通过链上更加透明的商业合作机制形成开放、可互操作、人人可参与的商业生态系统。开放生态中的公共数据积累和多样化应用，会持续赋能技术和应用创新，让更多的中小企业、微组织、独立建设者、创作者从开放生态中获利。另一方面，Web3.0 中的创作者经济将促进数字内容创作和传播以及跨领域的综合利用，形成全球化的数字内容流通市场，开拓互联网产业新的发展方向。发展 Web3.0 有望在做优做强我国文化创新、文化消费、数字文化产业的基础上，助力我国优秀文化出海。

三是有望构建互联网经济新范式。Web2.0 解决了各主体间的信息流通问题，但并未解决在数据流通之上的价值流动问题。Web3.0 依托区块链独创的通证经济体系，在没有第三方信用支

撑的情况下，将数据及资产映射为各类数字化权益凭证，以数字凭证流通的方式实现数据确权、数据交易、数据流转等应用，是用技术手段解决数据价值流通的一种创新性尝试。Web3.0 通过在区块链上建立身份、社区、活动、商品、金融等基本社会要素，形成一套完整的“数字原生社会”运作机理。NFT 的出现为数字原生社会带来数字原生商品，使得数字原生社会的生产和消费形成价值闭环。用户可以在“数字原生社会”中“组织生产—消费—扩大再生产”形成“数字原生经济”体系。Web3.0 能够在做优做强数字经济的基础上，在数字空间创造出经济可自循环的“数字原生经济”市场，拓展数字经济的新空间。

来源：可信区块链推进计划

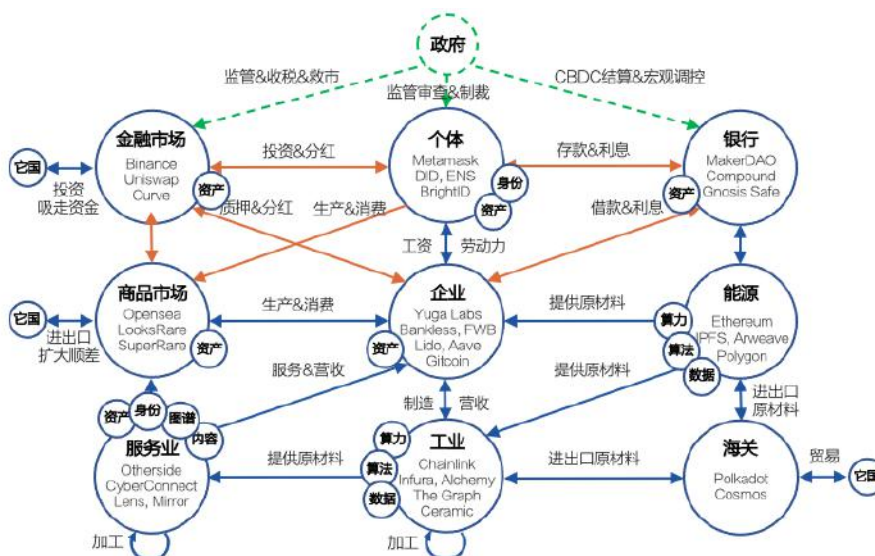
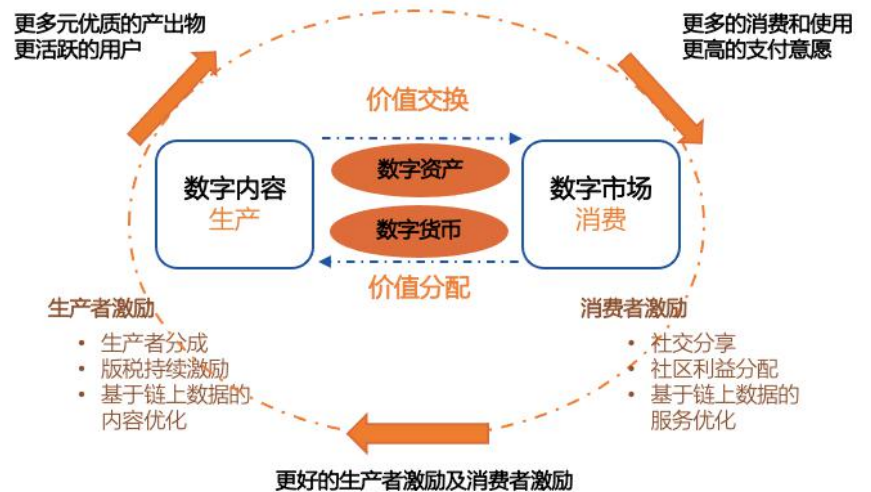


图 7：海外 Web3.0 数字原生经济生态

(一) 技术体系参考架构

Web3.0 技术应用的总体架构可分为基础设施层、组件层和应用层。基础设施层好比构筑大厦的地基，主要包括区块链、分布式存储、算力网络等，区块链平台负责提供多方共识、难以篡改、留痕追溯的数据治理能力，可由不同类型区块链构成：联盟链由小规模可信主体节点构成，通常有明确的运营主体，可管可控，但用户范围与网络规模较小；公链由大规模匿名用户节点构成，面向全球用户，没有上链门槛，但监管困难，容易滋生非法融资等非法金融应用。组件层类似于构建屋舍和装修所需的通用材料，包含基于区块链平台的通证发行和流通、数字资产管理、数字身份、数字钱包、分布式金融等组件，为数字资产交易、应用生态搭建、数据安全保护、应用互操作提供可定制的模块化解决方案，是总体架构的核心部分。应用层相当于大厦中工作生活的各类场所，构建在分布式基础设施和可组合组件之上，为满足下一代互联网新需求而不断丰富应用生态，一方面包括对 Web2.0 迁移而来的应用进行重构，如数据流通、跨境支付、供应链管理、知识产权管理等应用场景，另一方面是伴随 Web3.0 新理念而诞生的数字原生应用形态，如金融、社交、协作、游戏等应用在数字产权回归的背景下体现出来的新型表达模式。

来源：可信区块链推进计划

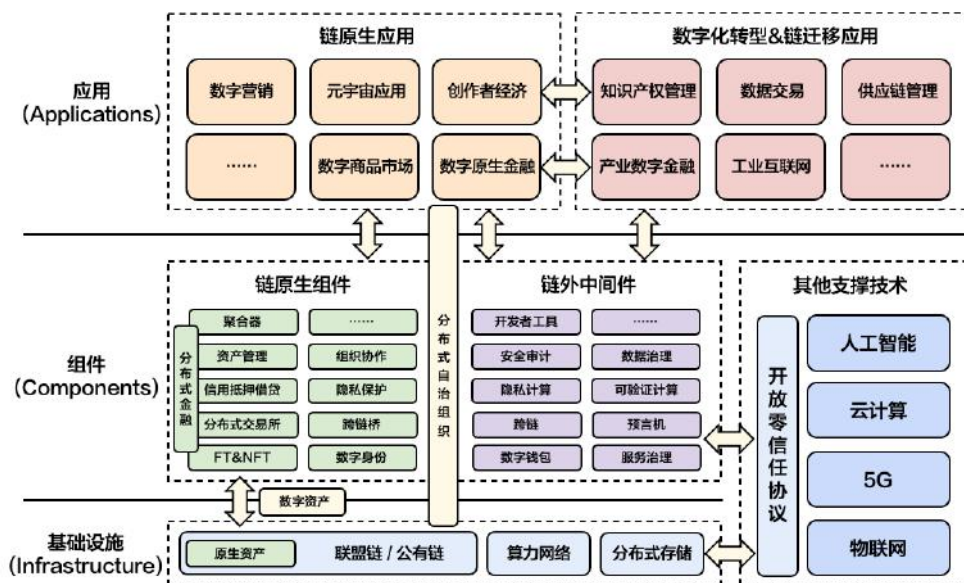


图 8: Web3.0 技术与应用参考架构

(二) 关键基础设施

■ 2.2.1 开放联盟链

区块链技术经过多年的发展，逐渐形成了两条路径：以加密资产为典型应用的非许可链（公有链）和以可信数字协作为驱动的许可链（联盟链）。公有链作为海外区块链的主流形态，其共识协议逐渐由完全去中心化向多中心化发展，相关企业通过牌照准入、实名注册（Know Your Customer, KYC）等方式积极拥抱监管。联盟链作为我国区块链的主流形态，也由单一业务的干系方独立运营逐步扩展为由不同业务或者多个节点服务提供方共同对外提供区块链服务，各区块链厂商逐渐推出不同开放程度的开放联盟链形态。与公链类似，开放联盟链在底层代码、链上数据、API 接口等方面具备一定程度的开放性，其核心共识节点由多家具有行业公信力的机构参与共建，不同应用可同时接入与运转，同时仍要保障联盟链的许可准入、安全审计和监管能力。与传统联盟链相比，开放联盟链不再由单一业务的联盟方组成，同一条联盟链也不再仅支持单一业务的运转；开放联盟链将区块链服务与区块链业务分离，即区块链的联盟方不一定作为区块链服务的使用方，区块链服务的使用方也不一定具有区块链节点。

来源：可信区块链推进计划

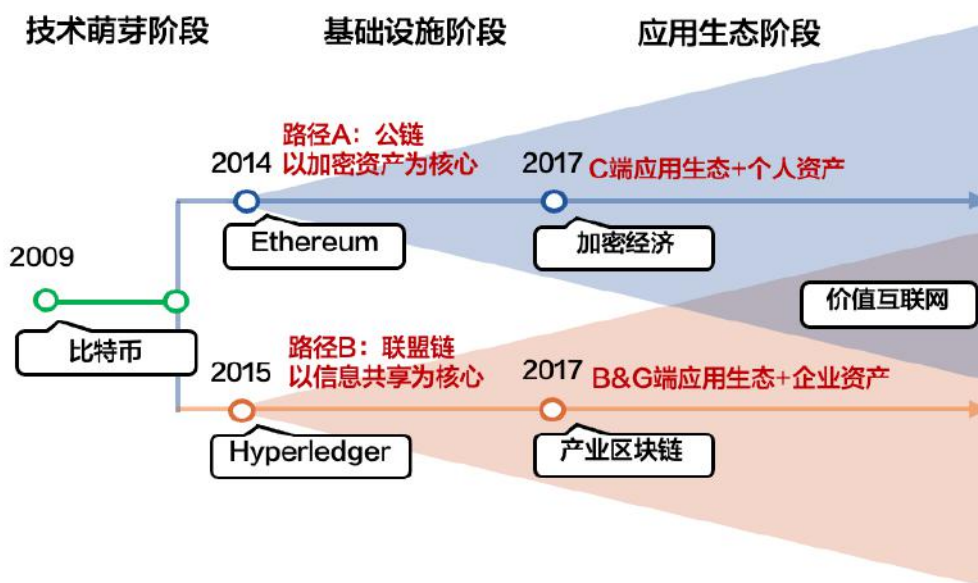


图 9：联盟链与公有链发展路径对比

构建 Web3.0 生态不一定必须基于公链，随着我国联盟链开放程度逐渐增强，也会形成中国特色的 Web3.0 商业生态。 Web3.0 的核心理念并不是技术能力的精尖，而是在理念、制度、产业层面开放程度的转变。例如，公链由于网络开放、数据开放、接口开放等特性，钱包等服务提供商很容易打通所有应用并建立统一入口。然而联盟链接口都是准入的，导致很难进一步建立统一入口，各联盟链平台各自为战仍然是封闭的“围墙花园”，无法形成统一生态。数字身份、跨链、隐私计算等 Web3.0 关键技术同样面临着“互连互通”的问题。所以，如何在金融稳定、数据安全、内容合规的背景下，逐步对外开放联盟链的各项能力，是现阶段我国构建 Web3.0 生态的主要挑战。

随着开放联盟链接入场景增多、规模扩大，各个用户及业务方的数据在链上公开沉淀，不同业务间可实现数据、数字内容、数字资产在链上跨平台互通。用户可授权业务 A 的数据在业务 B 中使用，也可以整合多个业务的数据资产，统一收拢于一个链上区块链账户中。最终实现一个用户的链上数字身份即可打通所有链上应用，用户能以统一数字身份自由穿梭在生态内的各个场景中，进一步推动用户身份、数据、资产真正为用户所拥有、所支配，打破 Web2.0 时代应用与应用之间的“价值孤岛”，真正意义上形成基于 Web3.0 时代的价值流通。

来源：腾讯云至信链



图 10: 开放联盟链打通 Web2.0 时代“价值孤岛”

■ 2.2.2 分布式存储

新型分布式存储解决方案在性能、易用性、激励机制等方面尝试弥补 IPFS 缺陷，逐渐代替 IPFS 存储方案。 Web3.0 分布式存储和 Web2.0 传统存储相比的主要优势在于数据的可验证性

和可用性,但性能较低,一旦决定数据一经上传就不可更改,导致程序的迭代成本较高,机动性不足。当前公链生态的数据存储的主流解决方案是 IPFS/Filecoin、Arweave 和 Ceramic Network。Filecoin 是在 IPFS 之上引入的激励层,激励用户参与并保证数据在约定内可靠存储。Arweave 通过对区块链链式结构创新实现链上数据存储的降本提效。Ceramic Network 提供结构化动态数据存储方案,并通过 W3C DID 标准格式管理数据,旨在解决 IPFS 文件不能实时更新,需要手动保持同步动态,效率低等问题。

■ 2.2.3 算力网络

Web3.0 应用通过对接区块链获得计算的安全性,对接分布式存储获得数据的可用性,以及对接社会化算力网络以获得网络加速、隐私计算、万物互联等能力。算力网络是指融合通用计算、存储、网络资源、异构算力(GPU 算力,TEE 算力,AI 算力,联邦学习算力)的智能化云网基础设施。依赖 5G、云计算、物联网、边缘计算等技术能力,面向社会吸纳算力与网络资源,将“云-边-端”多级异构的计算资源连接适配,基于区块链技术实现算力资源的记录、确权、调配和交易,从而实现泛在多方算力的统一编排和全局优化,解决云边端网协同和高效资源匹配的需求。

(三) 数字资产

■ 2.3.1 数字资产

广义的数字资产是指个人、企业拥有或控制的以电子数据形式存在的资产形式。数字资产不仅包括我们所熟悉的数字知识产权如专利、软著等，还包括新兴的加密货币等虚拟资产，也包括现实世界的实体资产通过数字化技术手段映射到数字空间的数字化资产，比如现实世界中的车产、房产、土地，通过区块链上链确权之后，就可以在数字空间进行交易流转。**狭义的数字资产专指登记在分布式账本上的计算机程序（通证）**，资产之间的交换实际上是账本上资产所属人的变更，通证不仅明确了资产在链上的所属账户，同时可以规定资产的使用规则。而目前业界所指的“原生数字资产”或“数字原生产”（Digital-Native Assets）主要是指在区块链上发行并流转的数字资产。这类数字资产自诞生之日起，就以纯数字化的形式存在于区块链之上。原生数字资产和基于原生数字资产的衍生数字资产都可以被视为是原生数字世界的资产类型。非原生数字资产主要包括“数字化资产”和“数据资产”两类。

数字化资产即非数字资产以数字化形式的呈现。传统金融体系中的股票、债券、衍生品等不是数字化后的资产，而是资产的数字化表达。数字化资产不光要求资产以数字形式呈现，还需要将资产所包含的信息、资产的交易模式设计以及如何适应权属关系的变化考虑在内。非原生数字资产的生成和构建步骤也可以看作是从资产数字化到数字资产化的过程，资产数字化是企业借助已有资产，对数据资源进行归纳汇集的过程。数据经过记录、筛选、转换等步骤，生成可以转化为资产的结构化信息资源；数字资产化（或数据资产化）则是将结构化数据与具体应用场景相结合，使数据转化为能够创造经济效益的资产的过程。如果说资产数字化侧重数据的积累汇集，那么数字资产化就是强调数据的价值挖掘。

■ 2.3.2 数据资产

数据资产是指由组织（政府机构、企业、事业单位等）合法拥有或控制的数据资源，以电子或其他方式记录，例如文本、图像、语音、视频、网页、数据库、传感信号等结构化或非结构化数据，可进行计量或交易，能直接或间接带来经济效益和社会效益。数据资产基于互联网产生的

交易数据、行为数据等，正逐步成为新的资产类别。

■ 2.3.4 数字资产交易市场

数字资产的交易模式主要分为两种：基于中心化平台的数字资产托管交易和基于区块链的数字资产交易。托管交易模式是指数字资产的拥有者将数字资产托管在交易平台，随后由购买方认购，托管交易模式也被称为第三方交易模式或中心化交易模式。中心化交易模式的优点是效率高，有准入机制，用户需要经过 KYC (Know Your Customer) 实名认证，但存在平台操纵市场等风险。基于区块链的数字资产交易又可分为两种：一种是利用智能合约实现资产的互换 (Swap) ，另外一种是通过订单簿 (Order Book) 实现资产的挂单交易。基于区块链的数字资产交易是一种分布式或多中心化交易模式，这种交易模式所有交易均在链上发生，保障了交易的透明性和安全性，但劣势是交易效率低，且存在监管困难、洗钱等合规风险。

海外加密资产交易市场包括中心化的交易所 (Centralized Exchange, CEX) 和分布式交易所 (Decentralized Exchange, DEX) 。中心化的交易所比如币安 (Binance) 、 Coinbase、OKEX、FTX 等等。2020 年随着分布式金融 (Decentralized Finance, DeFi) 的迅猛发展，分布式交易所也快速崛起，比如 Uniswap、Sushiswap、dYdX 等等。随着 Web3.0 的发展，分布式金融体现出的可组合性正在与 Web3.0 世界的其他应用场景深度结合，比如社交、游戏、组织协作等场景，不断丰富数字资产交易的内涵和外延。

与海外野蛮生长的加密资产交易市场相比，国内数字资产交易多集中于数据资产交易和数字藏品交易两个领域。在数据交易领域，全国多个地区包括贵阳、北京、上海等数据交易所积极探索区块链技术应用。2021 年 11 月，北京国际大数据交易所首创基于区块链的“数字交易合约”，把数据、算法、算力及综合服务应用作为可供交易的数字资产。2022 年 7 月，上海数据交易所首次将数字人民币支付方式融入到数据产品交易的清结算环节。在数字藏品交易领域，我国对数字藏品交易一直保持强监管态度。一方面，针对数字藏品的具体监管细则仍在研究制定中，同时国内文交所等官方机构积极参与，尝试打造合规化的数字文创交易平台。另一方面，我国数字藏品行业投机炒作和数字藏品金融化、证券化等倾向愈发严重。据零壹智库数据显示，目前国内上千家数藏平台有 30% 私下开设或通过“寄售”“转赠”“场外交易”等方式实现“二级市场”自由交易，投机炒作等乱象亟待监管制约和引导。

2.3.5 数据要素市场

Web3.0 价值互联网与我国数据要素市场的发展理念殊途同归。价值互联网和数据要素市场都着重讨论数据作为新时代的生产资料应该归谁所属，如何改善数字空间中数据要素的产权关系，数据要素如何安全自由流通，所产生的价值应如何合理分配。前者的基本对象是数字资产，后者的基本对象是数据资产。两者都尝试通过区块链技术对生产资料进行确权和流通，并形成有效市场，使市场在资源配置中起决定性作用。随着数字经济的纵深发展，数字资产交易将成为金融市场重要的组成部分。短期内，结合区块链技术可以实现金融资产、知识产权、数据等资产的链上确权与交易，在数字票据、跨境支付、数据交易、算力交易、能源交易等领域实现链上价值转移；长期看，面对蓬勃发展的原生数字资产，不仅需要结合新兴数字技术，开辟新型交易场所，同时要加紧制定配套的法律法规和交易规则，才能更好促进我国数字经济的繁荣和发展。

来源：可信区块链推进计划

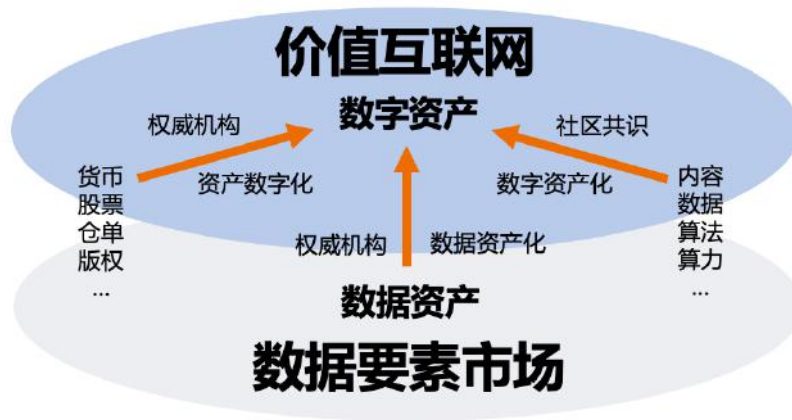


图 11：Web3.0 价值互联网与数据要素市场的关系

(四) 代表性链原生组件

■ 2.4.1 非同质化通证

NFT 是数字资产化的一种实现方式。非同质化通证 (Non-Fungible Token, NFT) 是区块链上管理特定数字资产转移逻辑的智能合约, 同时也是代表特定数字资产的权属凭证。NFT 能够标记特定的资产 (包括数字资产如在线艺术品、头像、域名、活动门票、游戏皮肤、装备、虚拟土地等, 实体资产如车产、房产、土地等), NFT 将该特定资产的相关权利内容、历史交易流转等信息记录在其智能合约的标识信息中, 并在对应的区块链上给该特定资产生成一个无法篡改的独特编码, 从而形成具有独特性并且可验证的权属凭证。

同质化通证 (Fungible Token, FT) 和非同质化通证本质都是基于区块链技术的数字资产管理手段。FT 标记的是同质化、可拆分的资产, 比如数字货币、数字积分等, 代表标准协议有 ERC-20、ERC223 等; NFT 标记的是非同质化、不可拆分、单位为一的数字资产, 代表标准协议有 ERC-721、ERC1155、ERC-998 等。不同形式的数据可以通过 NFT 在链上进行标记确权和资产化, 比如 Otherside、Sandbox 将元宇宙中的虚拟地产铸造为 NFT; Loot 将游戏道具信息铸造为 NFT; Mirror 允许作者将一篇文章铸造为 NFT; Lens Protocol 将用户的社交关系数据铸造为 NFT 等等。NFT 与可验证凭证 (Verifiable Credentials, VC) 具有一定相似性。NFT 和 VC 都是去中介化的数字证书, 两者都可以存储在数字钱包中, 都遵守某些标准协议。然而, NFT 用于表示主体拥有某些特定资产的所有权, 而 VC 用于证明主体拥有某些身份属性。

■ 2.4.1.1 数字藏品

近年来, Web3.0 概念大火主要是因为数字藏品领域的爆发式增长。数字藏品的文化属性和社交属性更贴近大众消费者, 它比其他 Web3.0 应用更容易受到消费者青睐。随着海外 NFT 市场一批头部品牌如加密朋克 (Cryptopunk)、无聊猿 (BAYC)、红豆 (Azuki) 等头像类数字藏品 (PFP) 收获强大的眼球效应, 吸引全球市场关注, NFT 市场也逐步从一个加密艺术市场走向游戏、社交、商业营销等领域。数字藏品通常都承载着特殊的文化价值符号精神象征意义或审美偏好, 相较于传统收藏品, 数字藏品更易通过网络进行传播展示, 收藏者通过区块链网络能够

展示数字身份下的数字藏品，满足了用户在数字世界彰显个人文化圈层认同感的表达欲望。

数字藏品是 NFT 的一种应用形式。目前，国内数字藏品基于联盟链进行铸造发行，是对数字艺术品进行标记的数字版权凭证，更多关注点是对数字内容创作者的版权保护，是对原有版权体系的数字化升级。同时国内严格限制二级市场交易，以尽可能削弱其金融属性并规避其炒作风险。而且数字藏品价格采用统一市场售价，定价权通常掌握在平台或者 IP 机构手中，导致国内数字藏品更像是一个数字消费品或者数字商品。而海外 NFT 基于公链进行铸造发行，低准入门槛意味着全球任何人都可以发行数字藏品并进行加工创作，并且公开透明的流通渠道能有效防止发行方增发、黑箱操作的行为。同时海外对二级市场交易容忍度高，NFT 价格会随市场行情和供需关系而波动，这使得海外 NFT 高度金融化，更像是一种新型的权益凭证，在不同领域会衍生出无数应用并反哺创作者，有益于文娱产业创新以及数字 IP 跨领域的综合利用，对原有版权体系具有颠覆性作用，但同时存在投机炒作、洗钱、非法金融活动、内容安全等风险隐患。

■ 2.4.1.2 CC0 协议

CC0 是免费知识共享 (Creative Commons Zero) 版权协议的简称，其对文创作品的作用类似于软件的开源。采用该协议意味着创作者宣布放弃创作的一切版权，将作品置于公共领域，成为人类共同的知识财产。任何人都可以使用该作品的版权进行商业行为，CC0 协议鼓励基于原创作品创造衍生作品，让后续使用者无需授权即可二次创作，这极大程度发挥了数字藏品的流通价值。当新的衍生品被创造和分享时，人们的注意力就会流向原作，进一步激发该 IP 系列的关注度并产生飞轮效应，每一个基于原创作品的额外衍生品都能增加原作的价值。

■ 2.4.1.3 版税

版税 (Royalty) 是指创作者在创作了一套 NFT 作品之后，可以设置一定比例的版税，后续 NFT 在每次交易机会中都会将部分利润金额返还给创作者，创作者能从后面的售卖中得到连续的版税盈利。比如 SuperRare 内置的艺术家佣金占有所有后续销售额的 10%。之后每一次的交易，这笔版税收费会从卖方的收益中自动扣除的，如果二级市场中这个 NFT 系列的流通性非常好，那么仅仅版税这笔收入就价值不菲。通过 NFT 或数字藏品中的版税机制，创作者们能获得可观的创作收益和创作价值。

2.4.1.4 数字藏品产业生态

目前国内的数字藏品生态主要包含四类角色：**基础设施层、平台层、衍生应用层、项目内容层**。其中，基础设施层为数字藏品的铸造、发行和交易提供区块链、智能合约和存储等技术支持，负责数字藏品价值的记录和结算，为整个数字藏品生态提供安全性和稳定性保障；平台层是数字藏品销售终端，也直接与购买数字藏品的用户进行沟通与交互，也是目前生态中国内数量最多的一层；应用层包括衍生应用层和项目内容层。衍生应用层是对铸造出的数字藏品项目的衍生应用，包装藏品内容并在平台上或者某些私域流量上进行发售或赠送，包括数字藏品二级市场、融资平台、社交平台等；项目内容层为数字藏品提供源头 IP 与内容，如艺术家、博物馆、版权所有者等，继而根据铸造协议铸造数字藏品并在一级市场发行，包括 IP 授权、项目创作、项目发行和发行平台。

来源：红洞科技

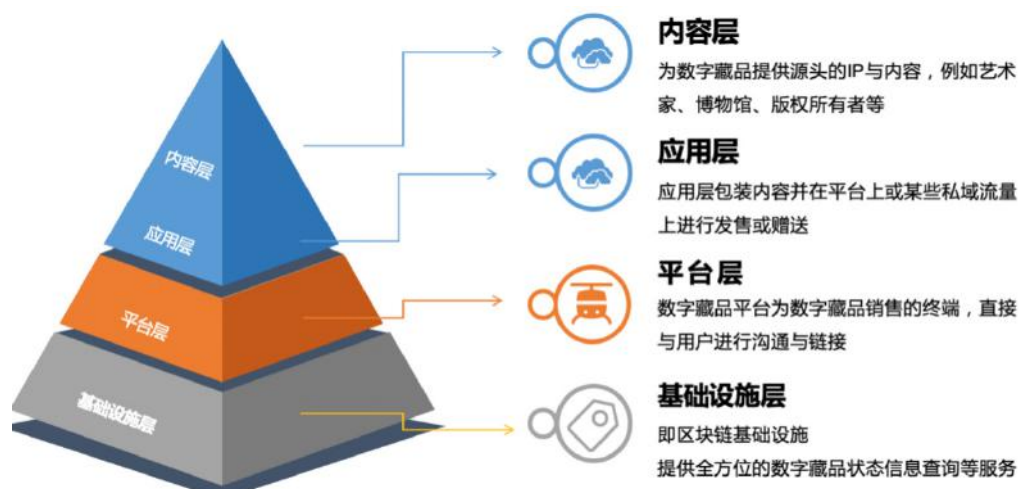


图 12：数字藏品产业生态分层架构

2.4.1.5 创作者经济与元宇宙

创作者经济是指独立的内容创作者（如博客作家、社交媒体网红、摄像师等）通过平台或社区等渠道方式发布自己的原创内容并获取收益的经济形式。在 Web2.0 时期，每个用户都拥有创建内容的机会，创作者、内容分发平台、MCN 机构、内容创作工具、数据分析产品共同构成了该时期创作者经济的基础生态，而创作者的内容都被存储在中心化平台当中，其内容传播和利益分发高度依赖平台。创作者向平台交出所有权来置换获利机会，而平台则利用这些所有权最大化自身的利益，暴露出收入分配不均、内容管理权缺失、恶性竞争等问题，这种由平台中心主导和平

台分配收益的模式并没有达到创作者经济真正的愿景。在 Web3.0 时期，NFT 为数字创作的确权、流通、价值发现提供了新途径新范式，通过将数字内容的所有权归还给用户，减少内容创作平台的抽佣分成比例，提高了内容创作者的地位，通过版税模式颠覆传统版权模式，构建全新利益分配机制，让创作者更容易从自己的数字劳动和创作中获益，激发了创作者内容生产的积极性，以更持续的创作收益、更开放的创作模式推动内容创作的体制革新，建立全新的创作者经济模式。

Web3.0 为元宇宙提供技术底座和经济基石，创作者经济是构建元宇宙产业链的关键要素。

目前，业界普遍认为，元宇宙描绘了一个虚实相融、身临其境的数字空间，人们可以在元宇宙内创建自己的虚拟分身、拥有自己的数字身份，在元宇宙内活动、社交、创作并获得收益。在前端层面，元宇宙主要依托虚拟现实技术打造沉浸式交互的虚拟社会形态。在后端层面，则依然遵从于 Web3.0 的基础网络架构和协议体系。未来，元宇宙将主要由普通人参与构建，用户既是应用服务的使用者，也是应用服务的建设者、维护者，能够在元宇宙中自定义数字内容和服务。

来源：可信区块链推进计划

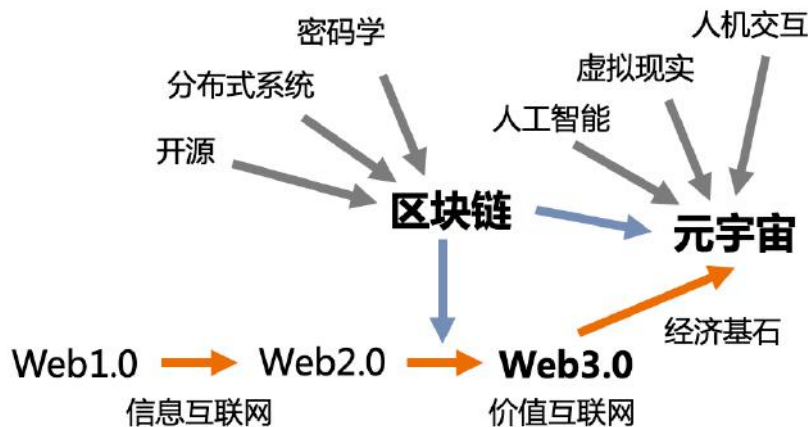


图 13: Web3.0 与元宇宙关键技术发展路径

2.4.2 分布式金融

分布式金融 (Decentralized Finance, DeFi) 是海外 Web3.0 的重要应用发展方向之一。2015 年基于以太坊开发的第一个金融方向的应用 MakerDAO 的诞生标志着 DeFi 的开端，之后分布式交易所 (Decentralized Exchange, DEX) 和分布式借贷等应用的产生，奠定了 DeFi 发展的基础。**链上稳定币、交易所与借贷，一并构成了 DeFi 的“三驾马车”**。其后随着区块链底层协议性能的提升、辅助工具的逐渐完善、数字资产市值的增长、链上用户的提升和各类机制创新，至今 DeFi 已经成为了一个具有千万级活跃用户、十亿级日交易量和百亿级参与资金量的庞大市场，是 Web3.0 中不可忽视的应用场景。DeFi 是一种金融范式的创新，具体体现在资产类型、交易匹配模式、市场公平机制、可组合性和组织治理方式上。DeFi 作为一种新型金融工具，能够撬动链上数字资产的流动性，促进链上活动的大幅度提升，为整个 Web3.0 创新和发展提供了源源不断活力的同时，也会为市场带来衍生风险和一定程度上的虚假繁荣。

来源：可信区块链推进计划

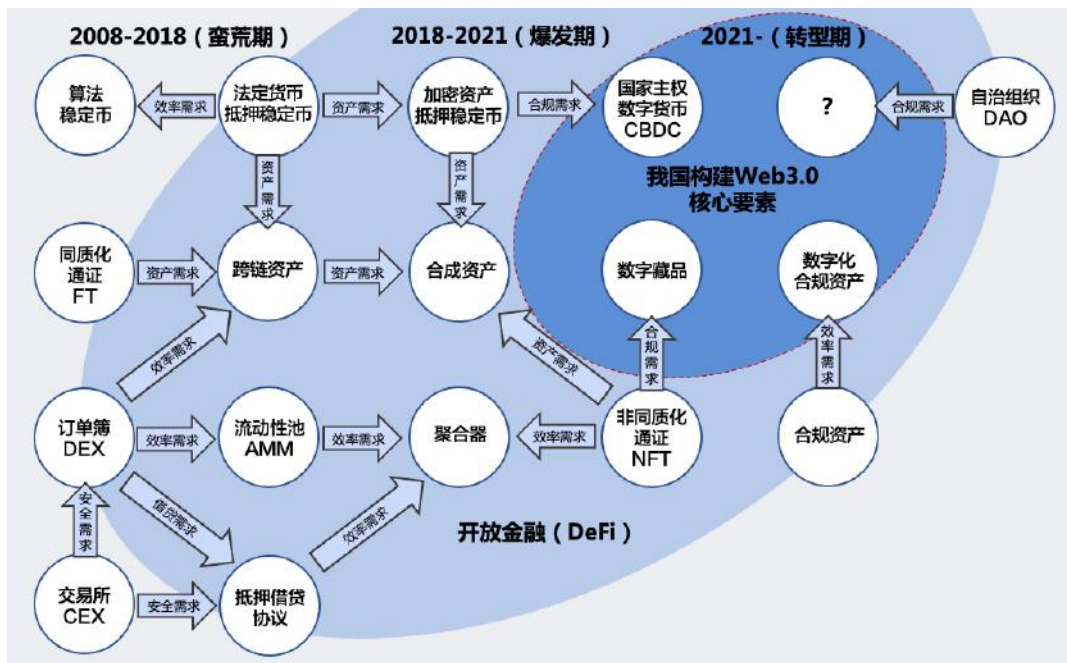


图 14: Web3.0 数字资产金融应用演进过程

■ 2.4.2.1 资产类型的创新

DeFi 经过 7 年的发展，已经发展成为了一个具有完备底层技术支持、中间层服务和各类细分赛道的新金融版图。从资产类型来看，链上数字资产从技术类型看可分为同质化通证（FT）和非同质化通证（NFT）。从产生方式看可分为链上原生资产（Native Token）和合约资产（如 ERC20 Token）。从资产类型可分为效用通证（Utility Token）和权益通证（Security Token）。从资产属性上看可分为稳定币（Stabelcoins）、治理通证（Governance Token）、合成资产（Synthetic Assets）等等。从技术栈的角度来讲，可以将 DeFi 的上下游相关技术分为：前端用户层（资产管理聚合器、钱包）、底层网络（公有链、侧链、二层网络）、核心组件层、流动性聚合层等等。其中核心组件层主要包括：稳定币（Stabelcoins）、分布式交易所（DEX）、借贷（Lending）、保险服务（Insurance）、资产管理服务（Asset Management）和衍生品（Derivatives）等等。由于 Web3.0 的技术特性，让 DeFi 既遵循参考传统金融的基本原理，又不完全沦为传统金融在区块链上的映射，DeFi 未来将具备服务更多资产和用户的能力。

法币稳定币是指锚定法币作为报价单位的加密资产，作为链上交易的基础，随着 DeFi 的发展其增速同样迅猛，目前稳定币总市值已超过 1600 美元。稳定币发行有诸多类型，目前占据主要份额的是由传统资产抵押发行模式的 USDC、USDT 等加密资产。此外超额抵押加密资产和算法稳定也是常见的稳定币机制。稳定币在 Web3.0 中充当了传统资产进加密市场的价值载体，未来随着各国央行数字货币的逐渐落地，稳定币市场会产生结构性变化。目前，业界普遍认为数字人民币将是我国发展 Web3.0 生态的重要支柱。由于链上数字社会中生产和消费中间缺乏直接兑换的媒介，目前国内链上难以形成原生的数字经济活动。没有价值兑换的媒介，数字社会就无法形成有效的经济活动，Web3.0 就无法成长起来。如何在合法合规的框架下，基于数字人民币探索数字资产应用，是我国构建 Web3.0 生态的关键路径。

分布式借贷是 DeFi 投资者重要的杠杆工具，交易者可将不愿出售的资产作为抵押在借贷平台获得其他资产的流动性。目前 DeFi 中的借贷普遍使用超额抵押模式，抵押资产在价格骤降时将面临清算风险，而由于抵押资产的价格波动性、预言机攻击等问题，参与借贷的交易者也面临极高风险。分布式金融衍生品是 DeFi 亟待发展的重要市场，是映射传统金融需求最强的领域，期货、期权、指数及保险等方向方兴未艾。同时，去中心化衍生品也出现了诸多原创的产品方向，如合成资产、质押资产流动化等等。

■ 2.4.2.2 交易匹配模式的创新

自动做市商模式 (Automated Market Maker, AMM) 是分布式交易所的关键技术创新之一，为解决传统交易流动性和公正性问题提供了一个全新视角的解决方案。在传统交易市场中，流通性和价格通常由做市商来提供。而在 AMM 中，任何人都可以作为流通性提供者 (Liquidity Provider, LP) 为交易市场提供流动性，同时商品交易价格由实现 AMM 模型的智能合约代码根据市场供需关系变化自动计算生成。从传统的对手方点对点 (peer-to-peer) 撮合，进化出了通过智能合约建立流动性池 (Liquidity Pool)。这种机制上的创新极大地适应了链上交易的特点，区别于传统的中心化订单撮合引擎的技术实现，效率极高成本极低地解决了长尾资产流动性不足的问题，极大地促进了链上资金整体流动性的效率。这也是 Uniswap 以极短时间和极低固定成本实现了纳斯达克交易所交易量的原因。在分布式交易所中体现为自动做市商机制，在借贷中体现为借贷资金池模式 (Collateral Deposit)。

Web3.0 的魅力很大程度来自于其开放性，不论从数据的角度还是金融的角度，开放网络为技术创新和金融创新都提供了施展空间。DeFi 的各类协议可以根据用户或开发者的需求叠加使用，这使得 DeFi 用户的资产利用效率由于杠杆的增加可以得到更大提升，同时为更多的产品和机制创新提供了多种可能性。目前 DeFi 各类协议的资金流都具有较强的勾稽关系，链上聚合器 (Yield Farming Aggregator) 这类 DeFi 项目就是基于可组合性兴起的赛道，因其最大程度地提升了资本效率制造了较高的收益率，吸引了大量用户和资金，目前也是行业中不可或缺的重要组件。

■ 2.4.2.3 市场公平机制的创新

服务提供者不基于牌照申请等准入方式，而是基于开源代码和社区共识，这是非常显著区别于传统金融的市场管理方式。Web3.0 的基础是信息透明与开源文化，关键项目信息很大程度上可以实现被动披露，为用户和投资者参与提供了足够充分的事实评价基础。而一个 DeFi 项目选择开展某项金融业务或提供某类金融服务并不需要获取牌照或资质审批，而是通过自身的技术与机制壁垒，及从公开市场获得用户的能力。同样，由于缺少监管强制力，市场也会出现野蛮增长和无序竞争的状况，用户的权益难以获得有效保障，这对用户安全使用及鉴别产品都提出了较高要求。

虽然目前 DeFi 已经进入成熟阶段，但要成为 Web3.0 生态更为坚实的金融基础，仍需要在监管合规、风险控制、机制创新和产品完备性等各方向从传统金融汲取经验，并在底层性能、

实用工具和链上安全性等方面持续提升。同时，越来越多的国家正在积极推出国家主权数字货币（Central Bank Digital Currency, CBDC），CBDC 将为全球金融系统带来大量创新机会。Web3.0 如果走向大众化就必然遵循合规需求，而 CBDC 将充当重要作用，如何让 Web3.0 生态更好地接轨 CBDC 的体系，已成为目前各国的战略重点。

■ 2.4.3 分布式数字身份

分布式数字身份是由许多身份属性，比如用户的资产、凭证、浏览记录、交易记录、行为记录等链上链下数据所组成，用户可以通过自我掌控的私钥进行数字签名来证明这些数字资产的所有权。目前，分布式数字身份与数据资产治理逐渐形成两套标准路径：W3C DID 和以太坊 NFT。一方面，狭义的 DID 是指由万维网联盟 W3C 推进的分布式数字身份标识（Decentralized Identifier, DID）体系，是数字身份的一种表现形式。这种标识符不仅可以用于人，也可以用于万事万物，包括一辆车、一台机器，甚至是一种算法。另一方面，NFT 也可作为数字身份的链上表达形式，同时 NFT 也让数字身份变成了一种“数字资产”。目前，海外公链生态以域名系统作为主流数字身份落地应用。例如，以太坊生态的 ENS、Polkadot 生态的 PNS、Nervous Network 生态的 DAS 等。这些域名系统通过提供全局唯一的、可读性强、可记忆的域名，来方便用户相互认知以及应用交互，并且为聚合多地址到同一数字身份下给出了可行路径。ENS 域名同样也是一种分布式身份标识符，只不过 ENS 的标识符是域名“xxx.eth”，W3C DID 的标识符是“did:method:xxxxxx”。W3C DID 不一定必须基于区块链，而 ENS 是用链上智能合约作为 DID 解析器的一种实现方式。同时 ENS 也是一种 NFT，这就意味着 ENS 可以在诸如 Opensea 的 NFT 交易市场上进行转售。

目前海外 Web3.0 生态高度金融化，链上通证更多表达的是可转让的金融化资产，钱包地址和钱包地址之间的关系并不能代表真实社会中的关系和身份，这会削弱链上活动的多样性和可拓展性。在 Web3.0 世界引入 Web2.0 身份是一种实现路径。加密资产交易平台对用户进行实名认证（KYC）；BrightID 通过 Zoom 会议进行身份验证；Instagram、Twitter 等社交平台支持 NFT 展示功能，允许用户将 NFT 设置为头像，将链上账户与 Web2.0 身份进行绑定，这些举措都加速了 Web3.0 身份体系与现实世界身份体系的融合。2022 年 5 月，以太坊创始人 Vitalik 提出了灵魂绑定通证（Soulbound Token, SBT）的概念，是一种不可转让的代表个人信誉、证

书和关系的身份通行证，希望能弥补目前公链生态的应用缺口，比如声誉系统、产权证明及拆分、抵御假身份攻击、账户恢复、筛选人群等场景。由于链上原生身份信誉系统的缺失而无法在区块链上进一步拓展应用，比如“传统”金融生态系统依赖于积累充分的数据和集中的信用评分来衡量借款人的信誉并支持多种形式的无抵押贷款，SBT 则希望通过用户在链上积累的行为数据和社交关系形成的用户链上数字身份来进一步拓展商业应用。W3C DID 的可验证凭证 (Verifiable Credentials, VC) 和 SBT 分别是构建身份凭证的两种实现思路，同样的底层技术逻辑两套技术标准。W3C DID 面向数据模型设计，链上 SBT 面向数据资产设计；W3C DID 不需要区块链，而 SBT 是基于区块链的智能合约通行证。

一个完善的 Web3.0 数字身份应用应至少具备聚合多链信息、自定义展示内容、数据写入接口、子域名管理、信源信道管理等多项功能。

■ 2.4.3.1 聚合多链信息

由于各区块链生态之间数据不互通，形成了多链生态下的一个个“区块链孤岛”。若是打通了链与链之间的数据，能够让用户以一个数字身份绑定多个公链生态的多个账户，在进行私钥签名证明其账户所有权的前提下，将其在多链上所拥有的数据统一聚合在一起。通过数字身份来进行用户在多链中的资产及行为等链上数据的确权，从而打通多链之间的数据，引爆区块链大数据分析的时代。

■ 2.4.3.2 自定义展示内容

数字身份聚合了多链信息与资源，但是作为用户的展示窗口，有必要提供给用户自主选择哪些信息展示，哪些信息隐藏。这也可以当作将数字身份本身作为信道来进行管理，防止一些隐私信息的泄漏。与中心化框架不同，用户可以将所需信息呈现给任何实体 (网站、应用程序等)。

■ 2.4.3.3 数据写入接口

数据资产可以通过读取链上信息在数字身份上展示，但数字身份不应止步于此。所谓身份的本意是指出生、地位，各种行为才造就了独特的身份。因此，数字身份应该有规范化的数据接口，以链接各种数据分析 DApp 的结果或是硬件采集的数据。比如用户的交易频次、社区贡献行为、

参与投票行为、DApp 访问行为等等。也应该兼容各监管机构所提供的 KYC 证明，以方便合规的审查。这种多方数据将造就了一个个形形色色的数字人，是 Web3.0 及元宇宙的核心。这与现实世界不同，现实世界以人为本体来构建身份，身份会创造数据；在 Web3.0 中，身份不再以人为本体，而是数据组成了身份。

■ 2.4.3.4 子身份的可拓展性

无论是个人用户还是组织机构，都有模块拓展的需求。对于个人而言，将自己不同的行为及技能组合在一起，会形成不同的角色，而在不同场合下展现自己不同的身份，好比社会上的”斜杠青年”；对于自治组织、企业和组织机构而言，需要界定不同产品、部门、职位等。这都要求数字身份可以进行扩展，能够将不同的子身份从属于一个数字身份下，满足不同场合的需求。

■ 2.4.3.5 信源信道管理

数字身份在 Web3.0 与 Web2.0 最大的区别，就是用户个人拥有对身份及数据的所有权。

以互联网用户的角度来看，在社交网络上发表的照片和文章，是依赖于平台的稳定运行，并且将用户的信息存入了这个平台的中心化数据库内，如果有一天这个平台不再运行，我的记录、数据就有可能消失。因此在 Web3.0 中，用户可通过数字身份来对自己所发的信息（信源）进行统一管理，这些信息存在于链上。某一个社交平台只是用户所选择的展示渠道（信道），某一渠道的关闭并不会导致我的信息丢失。实现了信源为我所有，信道为我所用。同一信息我可以选择多个信道去显示，但一旦修改信源，所有的信道都会显示修改后的信息。

■ 2.4.4 分布式自治组织

分布式自治组织（Decentralized Autonomous Organization, DAO）是一种建立在区块链上，通过智能合约规则进行决策与行动的新型社会组织形式。DAO 允许分散在世界各地的“工作者”在区块链上成立“利益共同体”并在低信任模式下充分参与决策，其主要特点是组织的协作规则由智能合约事前约束，任务分配、薪资发放、组织治理等协作流程公开透明，并由区块链技术保障组织协作规则的分布式自主运行。DAO 之于数字原生经济就像股份公司之于传统经济，但 DAO 和股份公司在组织架构上差别明显。DAO 打破了传统组织与市场之间的界限，进一

步推动了数字组织形式的创新。股份公司由层级分明和自上而下的股东、管理层、员工组成，公司治理决策、经营收益都遵循多数下层服从少数上层、按组织身份分得收益原则，是全球市场经济最主要组织形式。而 DAO 组织由社区管理者、开发者、创作者和财政管理者等角色以分布式的方式组成，通过区块链和数字资产把他们连接起来，重塑了生产者与消费者之间的“支配 - 依附”关系，消费者随时可以成为生产者，参与到组织的治理过程中。

当前阶段，DAO 会以一种数字化的方式去重现和验证过往人类各种各样的组织形态，在区块链生态的支持下未来有着旺盛的生命力。DAO 组织源于其扁平化管理和高效透明的决策、执行和激励机制，可以最大发挥成员和组织的积极性，快速推进场景中的价值实现。区块链为组织协作提供了多元参与的平台，开放的组织形态加快了组织创新和资源配置，生产者、参与者、所有者、消费者的身份边界消失，激励机制充分调动参与者的资源和积极性，参与者既能够参与构建项目获取报酬，也可以获得组织发展带来的经济利益。

由于 DAO 目前仍处在不成熟阶段，以下缺点更需要被我们重视。目前 DAO 组织的运行规则缺乏法律支撑，有违规或者发生争议时司法介入的难度较大，特别是在智能合约存在漏洞时 DAO 将发生严重的危机。因为公信力原因，有号召力的 DAO 组织对区块链生态较为依赖，当生态发生问题时自然会波及到 DAO 组织的根本；由于组织协作方式过于分布式，随着组织的壮大、人员和项目的逐渐增多，出现协作效率低和激励机制缺乏合理性等问题。在治理层面，DAO 组织通常作为管理组织调节链上应用的发展方向和经济系统，DAO 组织参与者以拥有数字资产的权重参与决策，但经济权重的治理方式将财富作为一种治理权利，资本可以通过“滚雪球式”的手段不断增加自己的权重，实现了对数字社会公共资源的垄断，最终服务于集体利益的公共治理将成为资本获利的手段。

(五) 代表性链外中间件

■ 2.5.1 数字钱包

数字钱包是 Web3.0 世界的入口，而数字身份是面向 Web3.0 应用服务及用户展示自身的出口。对于用户而言，数字钱包是私有的、内隐的，而数字身份是外放的、具象的。数字钱包存放了用户所有的数字资产，一般情况下，用户不希望把所有数字资产都展示给外人看，而数字身份是个人愿意展示给外人看的信息，当然，数字身份应用也可以结合隐私增强技术，使不想公开展示的信息“可用不可见”。数字钱包承载了用户的私钥。在与 Web3.0 应用交互时，私钥用于证明你拥有区块链上某地址（与对应公钥相关）所记录的资产，代表了用户对数字身份和数字资产拥有绝对的数字控制权。数字钱包是协助用户管理各类数字资产的工具，主要满足用户的数字资产使用和存储功能，是用户进入 Web3.0 的入口，公链主流钱包包括 Metamask、TokenPocket、Gnosis Safe 等。

■ 2.5.2 预言机

Web3.0 是运行在链上独立的数字空间，链外世界的的数据无法可信传递到区块链上。但在某些智能合约的应用场景中，又需要使用外部世界的的数据，例如某些智能合约需要获取外部资产的价格作为运行参数。在这些场景中，就需要用到预言机（Oracle）。预言机是一种单向的数字代理，可以帮助链上智能合约查找和验证链外数据，并将数据清理并提交给链上的智能合约，以便智能合约应用程序可以消费这些信息。预言机不仅提供了在链上传输数据的交付机制，而且还可以作为验证机制，以确保数据的完整性和真实性。预言机可以分成中心化预言机和分布式预言机两种实现模式。

■ 2.5.2.1 中心化预言机

中心化预言机是指由权威机构负责提供数据的预言机。这些数据源通常是一些链下世界可靠的机构，自身拥有良好信用和声誉，数据使用者只需要全权信任机构本身。同时，通过零知识证明、可信执行环境等真实性证明机制来证明自己运行在可信的执行环境中，提供的数据是数

据源在某个时间点真实的、未被篡改的数据。

■ 2.5.2.2 分布式预言机

分布式预言机是指多节点组成分布式节点网络，一起合作来提供数据。例如 MakerDAO 的 v2 版本的预言机，其节点就包括了 dYdX、0x 等机构。同时，参与提供服务的节点在提供数据时通常被要求质押一部分数字资产，一旦系统发现节点有作恶行为，质押的资产就会被没收。例如，Chainlink 是多中心的预言机网络，支持数据聚合模式。当请求链外数据时，预言机网络会从多个节点获取数据源数据，最后进行加权的平均值运算，上传到链上来保证这个数据是安全可靠的。同时，节点会在智能合约中质押资产，如果出现数据造假，节点会受到惩罚。

■ 2.5.3 跨链

当前的区块链应用和底层技术平台呈现出百花齐放的状态，但每条链大多仍是一个封闭独立的生态系统。在业务形式日益复杂的商业应用场景下，链与链之间缺乏统一的互联互通机制，这极大限制了区块链上数字资产价值的流动性，跨链需求由此而来。跨链技术本质上是一种将链上的数据、或信息安全可信地转移到另外一条链并在链上产生预期效果的一种技术。早期跨链技术以 Ripple、BTC Relay、Atomic Swap 为代表实现资产交换，而后跨链技术以 Polkadot 和 Cosmos 为代表实现更为通用的信息交换。Composable Finance 提出了跨链发展的四个阶段。第一阶段是实现基本的链间通信和资产转移；第二阶段是用户能够以统一入口参与使用不同链的应用；第三阶段是用户能够在多链生态开展更复杂的金融应用；第四阶段是单个应用将不同功能部署在多条链上，每个组件都在最合适的链上运行。

跨链依据其交换内容的不同可以大体分为数字资产交换和信息交换。在数字资产交换方面，当前资产交换主要依靠中心化的交易所来完成，由于中心化的交换方式要信赖中间商，既不安全、规则也不透明，业界对于中心化的交易方式不够信任，引发了跨链桥和去中心化交易所的创新如 Multichain、Uniswap、Curve、SushiSwap 等。其中，流动性置换是跨链桥的主要资产跨链方式。跨链桥在目标链上部署源链的智能合约，将目标链改造为源链的侧链，实现跨链双方的信息传递。项目方会在不同链上建立流动性资金池，一方面用户可以透过资金池直接兑换在另一条链上的原生产。另一方面流动性提供方也可以透过提供流动性资金，来获得部分跨链转帐的手续费作为

收入。根据 Dune Analytics 数据统计，2022 年 3 月，以太坊跨链桥的总锁定价值 (TVL) 达到最高峰约 250 亿美元，意味目前海外 Web3.0 已经形成了多链资产跨链互通的生态系统。

信息交换涉及链与链之间的数据同步和相应的跨链调用，实现更为复杂，目前各个区块链应用之间互通壁垒极高，无法有效地进行跨链信息共享。另一方面，区块链技术在单链架构下本身存在着性能差、容量不足等问题。单链受限于去中心化、可扩展性和安全性的权衡，难以支撑高交易吞吐量低延迟的商业场景应用。此外，随着区块链运行时间的增长，其存储容量也将逐渐增长，且这种数据增长的速度甚至会超过单链存储介质的容量上限。通过跨链技术实现多链协作的多层多链体系架构是解决区块链性能瓶颈的可取之道。跨链技术方案通常要解决的以下几个关键技术问题：跨链机制、互操作性、最终一致性和通用性。

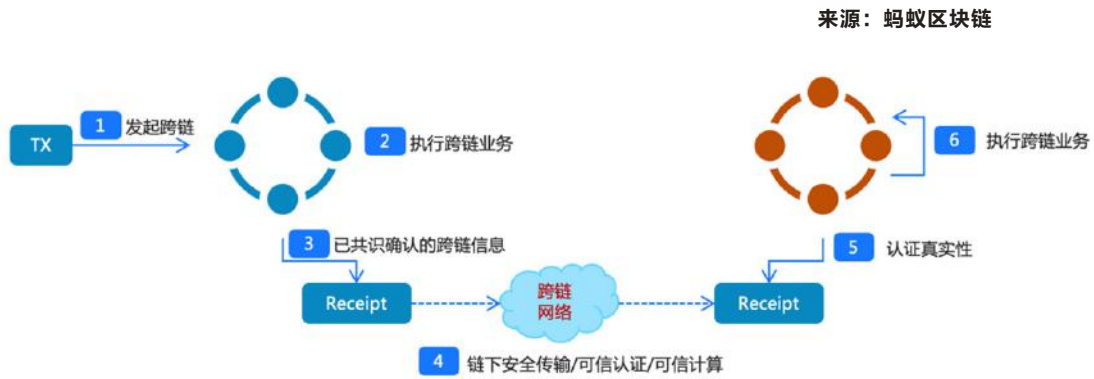


图 15：基于可信计算的通用跨链交互模型

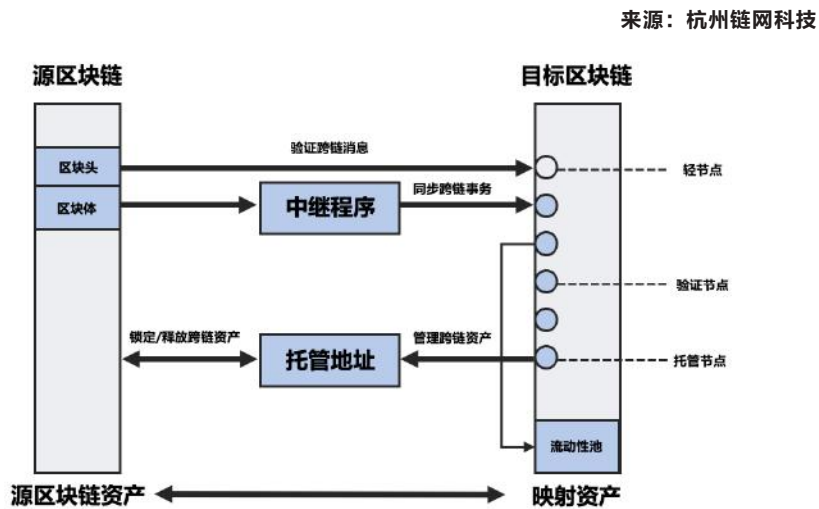


图 16：基于跨链桥的数字资产双向跨链方法

■ 2.5.3.1 跨链机制

跨链机制是指一条区块链上经过共识达成确定性的信息（包含信息、资产等写入账本的信息）被另外一条区块链读取并验证其完整性的机制，它解决信息在区块链之间安全可信传输的核心问题。两条区块链之间通常也需要引入第三方系统以实现跨链交互流程，好比区块链的安全性有共识机制保障，而共识机制需要引入安全假设，跨链机制通常也需要引入一定的安全假设，不同级别的安全假设也形成不同跨链机制信任模型。目前的跨链机制实现按信任模型可以分为半信任（semi-trusted）模型和无信任（trustless）模型两类实现。半信任模型指通过引入可信第三方来执行跨链信息验证，区块链信任可信第三方的验证结果。该可信第三方通常也成为公证人，可以由单个公认人组成，一些方案为了提高安全性，会由多个公证人组成公证人群体。无信任模型有两种主要实现，一种是无需引入可信第三方的侧链机制，一种是引入去中心化或去信任的第三方。

■ 2.5.3.2 互操作性

互操作性是指跨链系统为应用或者智能合约提供的跨链互操作功能，从跨链互操作的对象来分类，可以分为链间的资产交换和链间的信息交换两种，从通用性角度分类，会分为专用互操作功能和通用互操作功能。链间的资产交换功能指允许资产跨链从一条区块链流动到另外一条区块链上，且保障两条区块链之间资产守恒。链间的信息交换功能允许区块链上的功能模块（包括智能合约）进行信息交换，比如智能合约之间的消息传递，智能合约之间的跨链调用，基于信息交换，智能合约可以灵活自定义跨链逻辑，它是一种通用的互操作功能。跨链系统的互操作性影响该跨链系统的使用场景，但通用的跨链互操作性具有高复杂度实现，会带来一定的性能问题和安全性问题。比如公链场景里，目前场景以跨链资产流通为主，主流且成熟的跨链系统以实现专用的跨链资产交换为主，保障较有的性能和高安全性，在联盟链场景里，通常以场景适用性为主要考量点，会开发通用的互操作性平台满足自定义的跨链需求。

■ 2.5.3.3 最终一致性

最终一致性是指在链间资产交换（或者链间信息交换）时，实现互操作的多条区块链之间资产（或者状态）在指定时间窗口内能达到最终一致性，即要么大家都执行成功，要么都能回滚到互操作发起之前的状态。举个例子，从事务的角度理解，两条区块链分别执行先后两个子事务，

第一条区块链的第一个子事务已执行完成，第二条区块链需要按事务定义执行第二个子事务，不存在方法可以阻塞第二条区块链子事务的执行，或者使第二条区块链执行非事务定义的子事务，如果存在这种方法则表示不满足最终一致性。

链间资产交换是指资产在第一条区块链销毁（或冻结）后，第二条区块链最终能发行对应数量资产，不存在错误的状态如第二条区块链无法发行对应资产，而第一条区块链的资产永远冻结。通用跨链事务，指多个链上执行自定义的多个动作，形成一个分布式事务，该事务可以达成最终一致性，也可以回滚到最初状态。

最终一致性影响跨链的跨链业务安全进而限制跨链的使用场景，在最终一致性方面有安全隐患的跨链实现，可能会导致双花等问题使得跨链参与方利益得不到保障。一般的跨链方案里都需要围绕其最终一致性可能存在的问题设计额外的机制尽可能减少其发生的情况，比如跨链资产交换里，引入惩罚机制使跨链流动性提供方没有动力作恶而尽全力完成跨链交易，通用跨链事务里尽可能使用智能合约实现事务管理器，而不是依赖中心化的链下跨链事务管理器。

■ 2.5.3.4 通用性

跨链技术方案的通用性一般包括两个方面：互操作的通用性和异构链支持的通用性。互操作的通用性指不仅仅只支持跨链资产交换的单一场景，还可以扩展更复杂的跨链互操作类型，比如跨链信息交换的功能之上可以实现跨链智能合约通讯，进而可以自定义各种跨链事务，异构链支持的通用性指跨链方案能够适用于多种不同的区块链协议，实现异构链的互通。实现互操作的通用性的方法一般有两种思路，第一种是支持通用跨链事务，第二种是设计通用跨链通讯协议。

通用性会影响跨链方案的使用场景，但为了提高通用性，往往会跨链系统实现具有较高复杂度，越通用的方案导致跨链协议的复杂度、对异构链的适配的复杂度都很高。公链目前阶段主要应用还是以资产交互为主，故对互操作的通用性尚未那么高，联盟链广泛应用于多种不同的行业，不同行业的业务流程均有较高的差异性，且商业方面会存在多种异构链的存在，联盟链的场景里对两方面的通用性都有较高的需求。

■ 2.5.4 隐私计算

隐私计算 (Privacy-Preserving Computation) 一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系, 可用于在保证数据提供方不泄露原始数据的前提下, 对数据进行分析计算, 有效提取数据要素价值为目标的一类信息技术, 保障数据在产生、存储、计算、应用、销毁等数据全生命周期的各个环节中“可用不可见”。隐私计算技术非常契合 Web3.0 保护企业和个人数据的隐私安全、构建数据要素市场的社会需求, 可以在多主体间进行充分的数据共享与利用, 实现数据价值的转化和释放, 解决 Web2.0 存在的“数据垄断”、“隐私保护缺失”、“算法作恶”等问题。

■ 2.5.4.1 安全多方计算

多方安全计算是一种在参与方互不信任且对等的前提下, 以多方数据为输入完成计算目标, 保证除计算结果及其可推导出的信息之外不泄漏各方的隐私数据的协议。

■ 2.5.4.2 联邦学习

联邦学习是一种分布式机器学习范式, 包括两个或多个参与方, 这些参与方通过安全的算法协议进行联合机器学习, 可以在各方原始数据不出本地、不传输原始数据的情况下联合多方数据源建模和提供联合模型推理服务。

■ 2.5.4.3 可信执行环境

基于可信执行环境的安全计算是数据计算平台上由软硬件方法构建的一个安全区域, 可保证在安全区域内部加载的代码和数据的机密性和完整性方面得到保护。

■ 2.5.4.4 区块链与隐私计算

隐私保护一直是 Web3.0 的重要方向之一, 而隐私计算是保障 Web3.0 场景下用户隐私的关键技术之一。为降低链上计算开销, Web3.0 的构建与维护需要链上链下协同进行, 隐私计算技术保障该模式下“链上数据加密存储, 链下数据隐私合规”。链上链下共同构成 Web3.0 的基础网络。目前, 基于可信执行环境的隐私计算技术是构建链上链下协同计算能力

较为通用的技术方案。通过在 TEE 等可信执行环境中支持在智能合约处理敏感数据的能力，达到保护数据隐私的同时保证合约执行过程的可靠性（包括合约逻辑、数据的完整性）。

通过在区块链中引入用于隐私保护的密码学算法，如同态加密、环签名、零知识证明等隐私增强技术，可用于解决链上数据隐私保护问题。比较常见的方案是在账户模型上进行拓展，附加一层隐私交易方案，以此来保护账户和交易信息的隐私。比如对用户账户金额数值进行加法同态加密，除了拥有私钥的可信第三方机构外，所有节点都能验证交易但却无法得知具体数值，这将极大保护用户的账户隐私。实现链上隐私，即隐藏交易双方的身份，目前有 3 种常见方案，以 Monero 和 Zcash 等方案为主的匿名支付网络、以 Tornado Cash 为主的混币器通过集中汇款来打乱交易双方的链上联系、以及以 ZK-EVM、Aleo、Aztec、StarkNet、Polygon Nightfall 为主的零知识证明方案将可互操作的隐私集成到以太坊的扩容基础设施中。

■ 2.5.4.5 可验证计算

可验证计算技术是将计算任务外包给计算方，计算方需要在完成计算逻辑的同时，提供关于计算结果的正确性证明。零知识证明（Zero Knowledge Proof, ZKP）、Pedersen 承诺等技术是较为常见的可验证计算技术。目前 ZK 领域仍处于起步阶段，行业内主要解决方案包括 Starkware（dYdX、Immutable 采用）、zkSync、ZK Rollup 和 Polygon。可验证计算可以以二层网络的形式大幅降低链上的计算开销。例如 ZK Rollup 将计算任务、计算相关的全局状态全部置于链下维护。链下的计算方收到一批计算任务后，在链下完成计算并更新计算任务相关的状态。链下的计算方随后将一批计算任务打包成一笔上链交易，该交易内包含对每笔计算任务的精简描述，以及链下全局状态的状态根。计算方还需要生成一个证明以向链上的节点证明计算结果的正确性。

在隐私计算和可验证计算技术的帮助下，Web3.0 时代数据会以密文或摘要凭证的形态在区块链上流通。密文数据通常是由明文数据经过同态加密、秘密共享、承诺机制等技术加密后得出，具备一定程度的密态可计算、可排序特性，进一步支持了对密文数据的密态搜索或隐私推荐应用。而融合了差分隐私、机器学习技术的联邦学习技术，在同态加密等密码学技术的辅助下，可以支持“原始数据不出域”且算法模型不暴露，在保护原始数据、算法模型数据的前提下，对链上大数据进行处理分析。

2.5.5 服务治理

在服务治理层面，为了提升区块链的易用性，助力企业、独立开发者更加便捷地开发区块链应用，**联盟链和公有链分别衍生出以区块链即服务（Blockchain-as-a-Service, BaaS）为主和以软件即服务（Software-as-a-Service, SaaS）为主两种服务治理形态**。目前，海外公链生态 SaaS 服务包括以 Infura、Alchemy、Pocket Network 等为代表的第三方节点托管服务和以 Dune Analytics、Chainalysis、The Graph、Ceramic Network、CyberConnect 等为代表数据分析与数据治理服务。例如，第三方节点托管服务 Alchemy 主要是帮助开发者托管公有链节点，提供全面的开发人员工具和 API 服务套件，允许开发者安全地创建、测试和监控他们的分布式应用程序（Decentralized Application, DApp）；链上数据搜索服务 The Graph 帮助用户构建称为子图（Subgraph）的图谱结构数据，通过对区块链上的数据进行清理加工，将关联数据同步到图数据库中，为用户提供更快、更方便的链上关联数据和图数据查询服务。同时，用户可以将图谱数据铸造成 NFT 进行售卖；链上社交图谱服务 CyberConnect 利用 Ceramic Network 存储社交关系数据，将区块链作为“数据中台”允许不同社交应用访问链上用户身份信息、凭证、行为、社交图谱等数据，用户可以带着自己的身份信息、社交信息去使用不同的社交应用。

来源：可信区块链推进计划

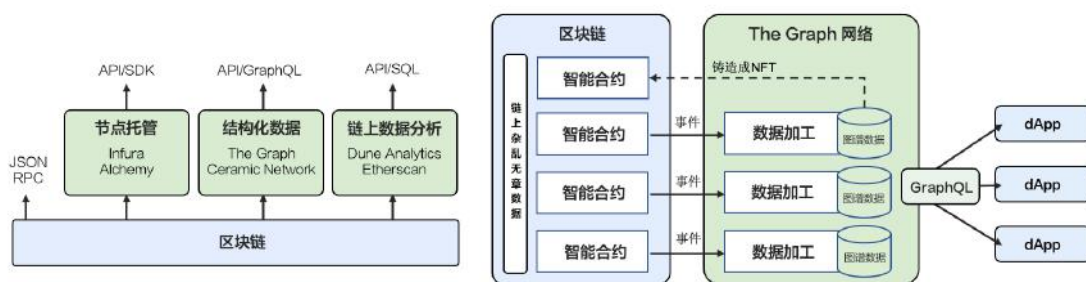


图 17：基于区块链的 SaaS 服务治理

公链生态 SaaS 服务与传统 SaaS 服务的主要区别在于两点。一方面，公链 SaaS 服务普遍引入数字资产作为服务治理工具，允许数字资产持有者参与应用服务的重大决策与项目治理，用户可以基于拥有数字资产的权重，对应用服务的产品迭代、业务规则、未来发展方向等提案进行投票。另一方面，SaaS 服务被分布式网络化，任何人都可以下载运行服务的源代码成为网络

节点，作为网络的一部分参与到分布式 SaaS 服务的运营中，作为劳动者、构建者、创造者为网络中的消费者提供服务。

■ 2.5.6 链上数据分析

与 Web2.0 时代的互联网相似，以区块链为底层的 Web3.0 时代，数字化空间的易用性和安全性仍然需要依赖对大量数据的处理与分析，其中就包括了通过链上数据判断安全事件主体的身份及行为。以目前区块链链上数据分析的实践经验来看，对链上地址进行标签化处理是比较普遍的做法。区块链地址标签分析在 Web 3.0 安全方面所能起到的作用也十分显著，比如对安全事件所涉及的恶意地址进行资金流向分析，又或者针对某些特定地址资产的异常流动进行预警。

目前，在数字资产交易领域，国内外的区块链数据分析已经比较成熟，特别是在数字资产安全事件发生后联合执法机构的资金追溯以及反洗钱等领域，区块链数据分析发挥了比较大的作用，在 Web3.0 时代，相关的数据分析经验也可以顺畅迁移。具体来说，区块链地址就如同银行卡号一样，是交易过程中最为重要的信息之一。而与传统银行卡号不同的是，任何一个用户都可以随意生成“无数”个地址，只要他持有私钥就可以随意构造并发起一次区块链交易。而这一过程虽然可以通过公开的区块链数据获取到，但也仅仅只能看到地址之间的交易，无法进一步获知更多与交易主体相关的信息。

区块链地址的标签化处理就是为了在一定程度上通过数据体现出的规律和模式，尝试解决类似交易主体身份无法明确等问题。通过对数据和内容上链前及上链后的处理分析，对链上公开数据进行标签化处理，能够构建基于数字资产的用户身份画像。简单来说，地址标签就是某些地址所具备的属性。如果给一个人打标签的话，可以说这个人高矮胖瘦、爱看书、爱旅游、脾气好等，链上地址也具有类似的属性，比如地址的格式、留存的资产、交易记录、交易时段等，就是地址的属性标签。通过地址标签，可以在某种程度上降低区块链的匿名性，提升对交易特征的识别度，尤其在“中心化”交易所逐渐实现 KYC 实名认证，链上地址与 Web2.0 社交应用的实名身份逐渐绑定的今天。区块链地址标签实际上是一个地址的各类属性，所以在分类上并没有一个统一的标准。比如，通过对 Silk Road 暗网中已添加标签地址的链上交易行为进行追踪，最终可以看到有部分资金流入了某些“中心化”数字资产交易所的地址。而数字资产交易所因其业务特性，可以在一定程度上完成对涉安全事件交易的定位和流向控制，可以理解为用户为了得到中心化平台

服务提供的“便利”，必须提供一些个人信息来完成在平台的整个注册和认证过程。

■ 2.5.7 安全审计

区块链安全主要包括三个维度，即应用服务的安全性、系统设计的安全性（包括智能合约和共识机制等）和基础组建的安全性（包括网络通信、数据安全和密码学）。区块链安全包括项目中所有代码的安全，如前端代码安全、智能合约安全等，任何层面的漏洞都可能导致区块链上的用户资产被盗。尽管重大安全事件在系统的各个层级都有出现，但超过 90% 的安全事件集中在智能合约和业务领域。智能合约本质上是一个运行在区块链系统上的计算机程序，其独特的开放性、透明性则需要更高的程序安全性。据区块链安全审计公司 CeriK 统计，在 2022 年上半年，海外 Web3.0 项目因黑客攻击和漏洞利用损失了超过 20 亿美元，而智能合约方面的漏洞种类最多。目前已有许多针对智能合约安全漏洞的验证工具，其验证方式主要可以分为静态分析、符号化执行、模糊测试等几类。而形式化验证 (Formal Verification) 是测试系统安全的常见方法，常见的是指用数学办法去证明系统无编程错误，为构建正确、可靠的系统提供了系统化手段。国内不少区块链安全公司提供的专业化安全服务，主要集中在钱包安全审计业务、智能合约安全审计业务、安全评测服务以及威胁情报服务等方面。

Web3.0 对互联网内容安全与治理提出了新的挑战。建立在区块链基础之上的 Web3.0 去中心化结构，针对内容违规等行为监管缺乏抓手，网络治理成本显著提高，如何把政府职能纳入 Web3.0 网络将会是一个全新课题。随着数字藏品的快速发展，越来越多社交文娱类应用开始引入区块链技术来记录和分发数字内容，为了预防用户在这些平台上发布或传播非法内容，网络经营者需要采用技术手段对用户发布的视频、音频、图片文字等内容进行合法性过滤和审核，确保信息内容安全。例如，在用户提交区块链交易上链之前，通过交易解析规则对接收到的区块链交易进行解析，并将解析得到的待检测数据发送至内容安全服务器，由内容安全服务器基于内容安全全匹配规则对接收待检测数据进行内容安全检查，待内容检查完毕后才能提交交易上链。

(一) 技术体系逐步成型，产业生态初具规模

尽管 Web3.0 发展仍在探索中，但 Web3.0 的基本技术体系和发展方向已初现雏形。据 Gartner 2022 年 7 月年发布的技术成熟度曲线分析报告显示，目前 Web 3.0 技术已经历了第一波创新高峰期，正在从“创新启动阶段”迈向“创新泡沫阶段”，技术体系逐步成型，市场热度较高，创业投资活跃，后续还将经历技术弱点暴露的“创新低谷阶段”、技术迭代完善的“创新爬升阶段”和日渐广泛应用的“生产成熟阶段”。其中，非同质化通证 (NFT)、分布式身份 (DID)、分布式金融 (DeFi)、分布式交易所 (DEX) 等 Web 3.0 核心组件技术正经历“创新低谷阶段”，还需 2-5 年进行技术更新迭代走向成熟。零知识证明 (ZKP)、分布式自治组织 (DAO)、可监管分布式金融 (CeDeFi)、可监管分布式交易所 (CeDEX) 正经历“创新启动阶段”，未来有望迎来更多创新。

来源：Gartner，可信区块链推进计划整理

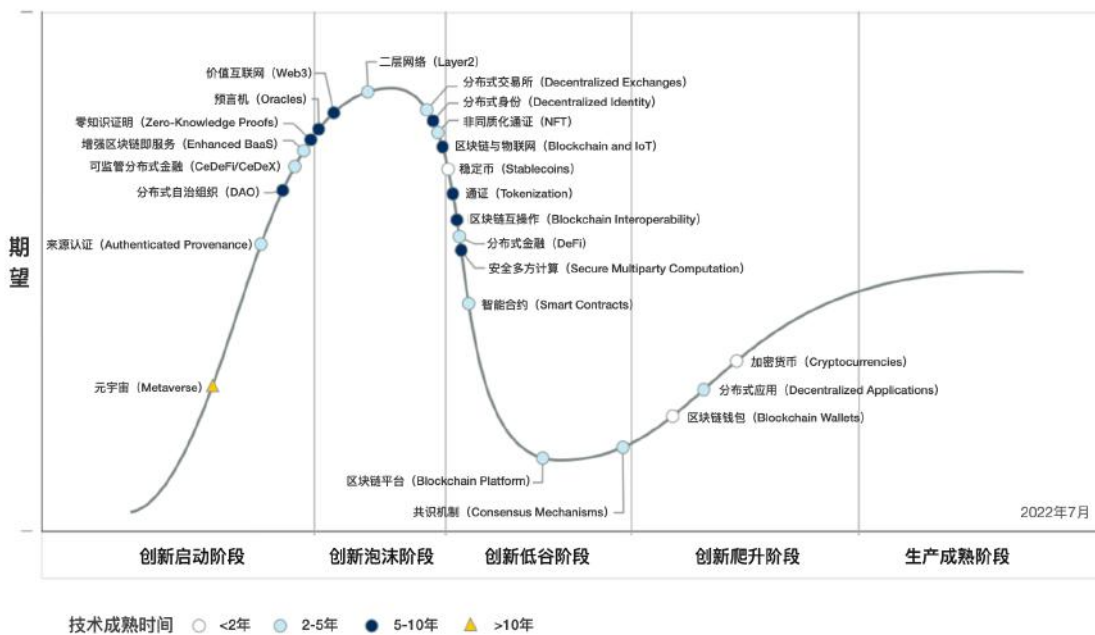


图 18: 2022 年 Web3.0 技术成熟度曲线

Web3.0 是区块链产业的一次品牌升级。随着海外区块链产业规模不断扩大，加密资产商业应用不断扩展，吸引全球资本、人才和用户争相涌入，从而催生大量技术和应用在其生态中野蛮生长，区块链及加密资产产业已成长为一个实际使用、逐渐普及的 Web3.0 商业生态。据中国信通院统计，2022 年上半年全球 Web3.0 业务营收规模约达 200 亿美元，我国联盟链业务营收规模约达 20 亿人民币。

来源：FM Research，可信区块链推进计划整理

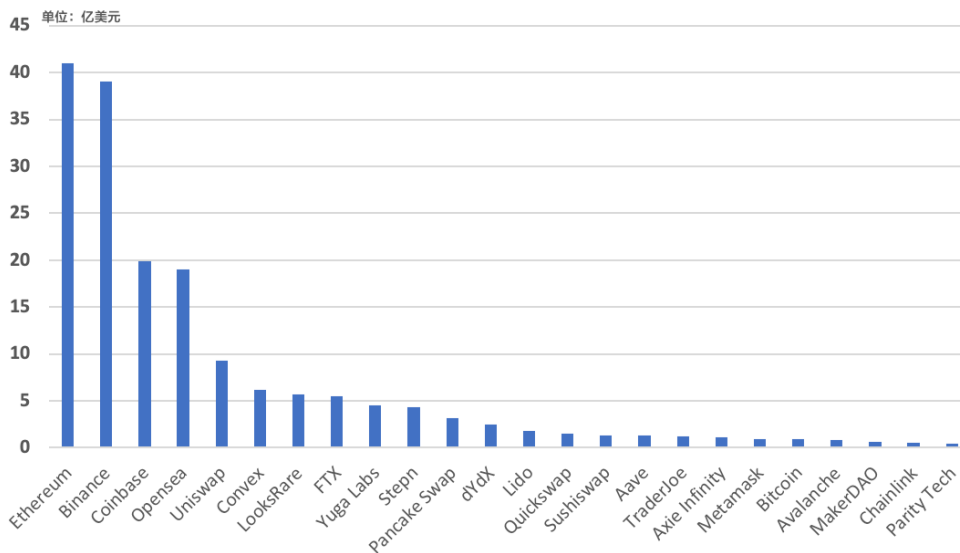


图 19: 2022 年上半年全球 Web3.0 项目营收规模测算

来源：FM Research，可信区块链推进计划整理

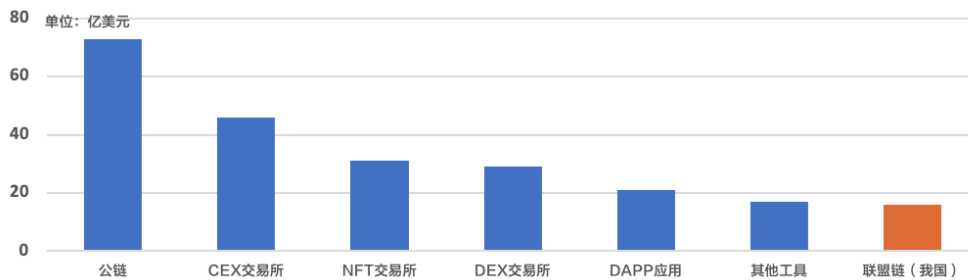


图 20: 2022 年上半年全球 Web3.0 业务营收规模测算

海外形成以以太坊为首的“一超多强”多链生态。据中国信通院统计，截至 2022 年 8 月 Github 上的 Web3.0 相关开源项目的月活开发者达 1.8 万人。在基础设施层，以太坊拥有最庞大的开发者社区和用户群体。以太坊生态实际月活用户达 3000 万，月活开源项目约达 4000 个，全职开发者约达 1200 人。以太坊生态月活开发者人数约达 4100 人、随后依次是 Polkadot (约 1400 人)、Cosmos (约 990 人)、Solana (约 860 人)、币安智能链 (约 340 人)。在组件层与应用层，以太坊拥有最发达的 DApp 生态系统。截至 2022 年 8 月，海外 Web3.0 生态稳定运行 DApp 约达 3.1 万个，吸引全球约达 9000 位月活开发者推动组件层和应用层技术演进，其中约达 4300 位月活开发者主要负责研发分布式金融相关组件。月活用户超过 10 人的 Web3.0 组件层相关项目达 1100 个，月活用户超过 100 人的 Web3.0 组件层相关项目达 450 个。其中，数字资产钱包 MetaMask 月活用户峰值达 3000 万人、分布式金融(DeFi)月活峰值用户达 400 万，分布式交易平台 Uniswap 月活用户峰值达 300 万人，区块链游戏 Axie infinity 月活用户峰值达 300 万人、NFT 交易平台 Opensea 月活用户峰值达 87 万人、区块链运动类 NFT 项目 StepN 月活用户峰值达 60 万人、分布式数字身份 ENS 月活用户峰值达 55 万人。

来源：Electric Capital、DappRadar，可信区块链推进计划整理

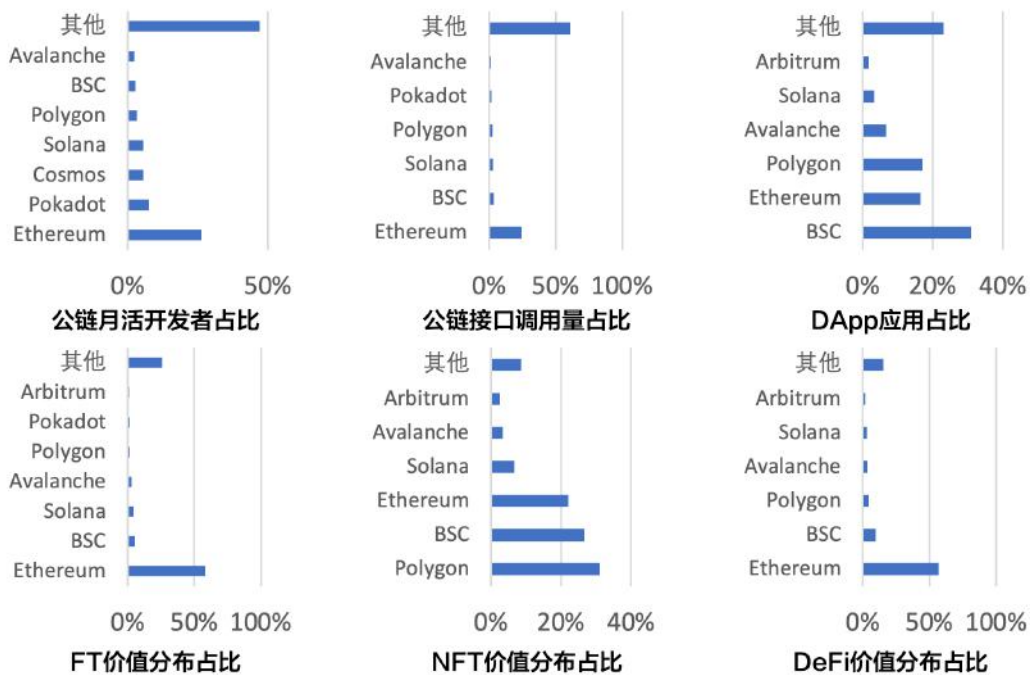


图 21：2022 年海外 Web3.0 生态产业现状

(二) 国外创业投资活跃，国内聚焦数藏领域

海外 Web3.0 创业投资额度增长迅速。据中国信通院统计，截至 2022 年 6 月，全球相关投融资总金额约达 1600 亿美元，投资机构主要分布在北美和欧洲，北美地区以约 733 亿美元投资额处于全球领先地位，欧洲地区以约 275 亿美元位列第二。同时，大量传统资本也在离开传统互联网涌入 Web3.0 领域，其中不乏有红杉资本、老虎环球基金、软银等传统投资基金，也包括谷歌、脸书、微软、三星等大型科技企业。

来源：公开网络数据，可信区块链推进计划整理

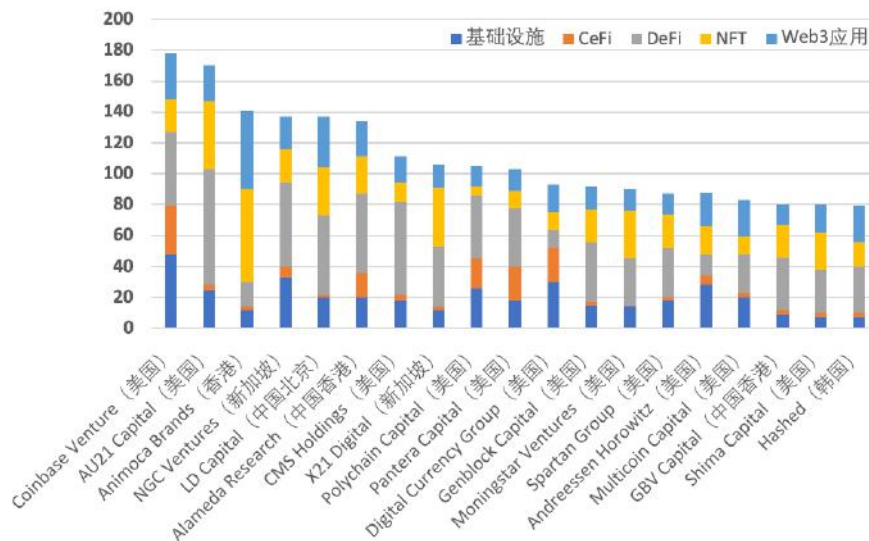


图 22: 全球 Web3.0 投资机构投资项目数量规模测算

来源：公开网络数据，可信区块链推进计划整理

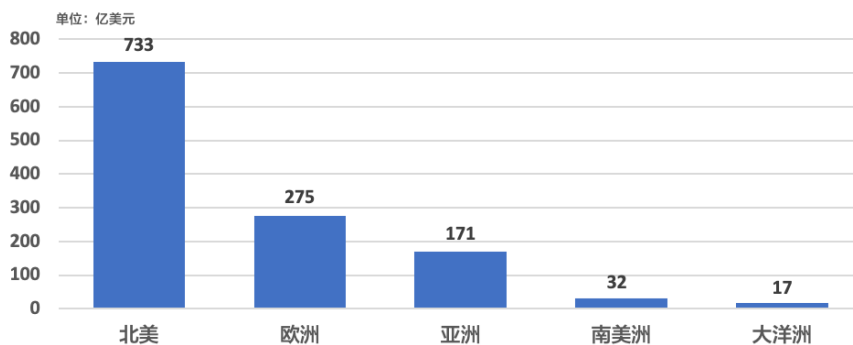


图 23: 2021 全球各地区 Web3.0 投资额度规模测算

国内企业积极布局 Web3.0 重点技术研发与数字藏品应用。目前，国内核心技术储备不亚于海外公链，腾讯、平安、蚂蚁、华为等科技企业更多聚焦区块链、隐私计算、数字身份等 Web 3.0 关键底层技术研发，业务方面则以服务实体经济为主，同时聚焦于数字藏品领域。据算力智库数据显示，2021 年国内共计发售数字藏品数量约 456 万份，总发行价值约为 1.5 亿元。2022 年上半年，国内共计发售数字藏品数量约 1536 万份，总发行价值约为 6.53 亿元。自 2022 年 5 月，国内数字藏品业务增长趋势逐渐放缓，各大数字藏品平台逐渐出现滞销现象，数字藏品发展进入“冷静期”。

来源：算力智库，可信区块链推进计划整理

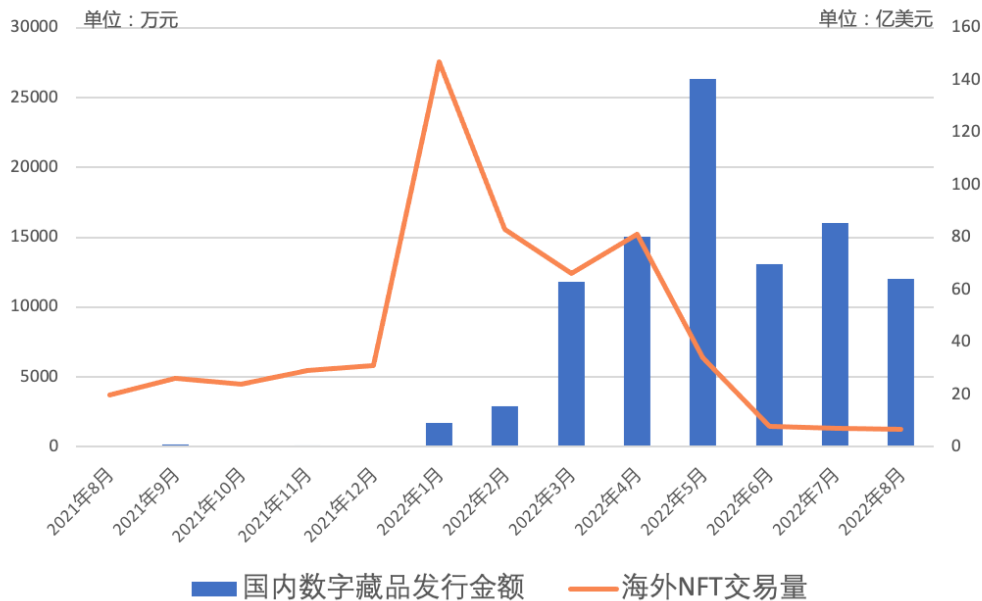


图 24：2022 年全球 NFT 交易与我国数字藏品发行规模测算

(三) 各国推动政策实施，监管举措逐渐升级

各国政府高度关注 Web 3.0 发展，陆续推动发展政策制定和监管制度完善工作。Web 3.0 的去中心化互联网形态给各行各业带来了重大变革，同时衍生出新的组织和产业形态也给监管也带来了重大挑战。例如，区块链技术支持下的匿名性社区，会给网络监管带来新的挑战；去中心化金融产品所蕴含的金融风险，也会考验金融管理部门的监管和防范能力。目前各国监管政策主要关注加密生态系统中的三大风险，一是洗钱和恐怖主义融资风险，二是消费者权益保护面临的风险，三是金融稳定方面带来的潜在风险。

美日政府已开始对 Web 3.0 进行战略布局。2022 年 3 月，美国总统拜登签署行政令，希望通过制定防范风险和引导负责任创新的政策，确保美国在全球数字资产生态中继续发挥领导作用。随后美国加快获得 Web3.0 生态控制权。2022 年 8 月，加密货币混币器 Tornado Cash 被美国财政部的下属机构海外资产控制办公室 (OFAC) 列入制裁名单，随后 Coinbase、Circle、Infura、Uniswap、dYdX、AAVE 等一系列 Web3.0 服务相继对相关链上账户拒绝提供服务，同时 OFAC 计划对以太坊节点服务商开展监管审查，意图主导海外 Web3.0 生态。同月，美国众议院监督和改革委员会经济和消费者政策小组致函美国各大加密资产交易所，要求提供自 2009 年以来与加密资产欺诈有关的所有文件。2022 年 5 月，日本首相岸田文雄表示，要从政治角度坚决推动 Web 3.0 以求引领日本经济增长，其目标是吸引海外资本并培育该领域的科技公司。2022 年 6 月，日本政府批准了《2022 年经济财政运营和改革的基本方针》，意图利用其在加密资产交易所和文娱领域积累的产业优势支持 Web3.0 发展，弥补日本在 Web2.0 时代的战略颓势。

欧、韩、新加坡等国政府对 Web 3.0 持开放发展态度。2022 年 3 月，欧盟议会通过《加密资产监管市场提案》，为加密资产的有序发行和交易提供监管制度基础。法国总统马克龙接受采访时表示希望欧洲在 Web3.0 发展中扮演“主角”。韩国总统尹锡悦在竞选时承诺将通过税收优惠和法律支持，积极促进 NFT 等数字资产交易市场发展。新加坡副总理公开发言表示要以开放的态度对待 Web 3.0，同时在政府积极推动下，新加坡成为全球 Web 3.0 企业创新创业的聚集地。2021 年，Coinbase、FTX、A16z 等欧美头部区块链公司相继在新加坡设立研发中心或总部，吸引全球互联网从业者落户新加坡。

（四）应用模式仍需探索，风险挑战不容忽视

Web3.0 发展仍存在不确定性，相关风险不容忽视。

一是业界认知不一致。虽然 Web 3.0 已经赢得了不少拥护者，但当前业界对 Web 3.0 认识还远未统一，各方对其发展前景也存在较大争议。在有些人眼里 Web 3.0 是技术体系、是建设者与用户共创的商业模式，在有些人眼里是制度、观念、是自由迭代创新的土壤，在有些人眼里则是金融游戏，是资本主义在数字空间的终极形态。2021 年 12 月，马斯克（Elon Musk）就发表推文称“现阶段 Web 3.0 并不真实存在，更像是市场营销术语”，推特前首席执行官 Jack Dorsey 也抨击说“Web 3.0 只是风投机构赚钱的概念性工具”。

二是应用模式尚不成熟。虽然 Web 3.0 代表了一种理想主义的未來网络愿景，已经得到业界大众的充分认可，但现有技术体系构建的 Web 3.0 仍存在信任洼地，其中的数字身份、数字资产、自治组织等关键应用目前均处于发展初期，且相关商业模式探索也处于早期实验阶段，未来技术演进路径还不清晰，是否能够破解当前技术瓶颈，找到真正有价值的应用场景，还存在较大不确定性。比如，目前大部分数字藏品只是把数字内容标识上链，其图片文件仍是存储在中心化服务器或分布式存储中，能否真正保障应用层、链上标识与存储环境三者的一致性，保障用户资产的持续性、安全性和可用性仍有待考验。

三是金融风险值得警惕。虽然 Web3.0 的数字资产具有补充数字经济活力的潜力，但同时也会对金融稳定造成扰动。数字资产的可编程性容易衍生融资、保险、借贷等金融服务，成为不法分子掠夺牟利的工具。一方面，Web3.0 与加密资产深度绑定，市场炒作、盲目投资等乱象频生，部分风投机构、加密资产参与者、技术创新者等市场主体，积极炒作 Web 3.0 及相关概念吸引投资，存在将 NFT 或数字藏品进行同质化变种并开展金融炒作的倾向，意图利用市场热度误导公众热炒。另一方面，Web3.0 的开放生态环境使得应用系统之间彼此深度依赖，其金融开放性、全民性、传染性容易引起连锁反应，衍生出金融危机。例如，2022 年区块链游戏 Axie Infinity 跨链桥遭受黑客攻击、稳定币 Luna 脱锚导致韩国 20 万人蒙受损失、三箭资本破产清算等事件持续发酵，都昭示着海外 Web3.0 生态的金融风险隐患不容忽视。

总结与展望

Web3.0 是一种新的数字经济发展模式，有望深刻影响下一代互联网形态，其技术价值和商业价值存在广阔的想象空间，我们既需要正确认识新技术产业发展规律，高度关注创新发展动向，准确把握发展机遇，抢占发展先机，同时又不可一味照搬国外发展模式，应结合国情采取包容审慎的态度，坚持发展和安全统筹兼顾，多措并举有效防范化解新技术新应用带来的风险挑战，积极稳妥探索具有中国特色的 Web3.0 之路。

（一）将 Web 3.0 纳入下一代互联网进行统筹战略布局

一是强化前沿布局，加强技术跟踪研究。组织政产学研专家共同推进下一代互联网前瞻性研究工作，加快制定我国 Web3.0 发展框架，强化新技术新应用发展管理政策储备，夯实我国 Web 3.0 技术产业发展基础。密切跟踪国外 Web 3.0 技术应用动向及在我国落地实践情况，研究分析 Web 3.0 在数字经济发展、互联网产业重构中的关键价值和风险隐患。二是完善顶层设计，规范行业发展环境。积极引导社会公众，客观理性对待 Web3.0 当前发展热潮，避免盲目夸大 Web3.0 对于传统行业的颠覆作用，警惕过分炒作、金融风险，同时密切关注由 Web3.0 带来的监管和网络安全新问题。三是加强多方治理规则和数字产权制度研究。探索多方参与的 Web 3.0 治理规则，加快推进国内联盟链互联互通，提升区块链网络的治理水平。建立符合中国国情的数字产权制度，合理界定数字产权关系，促进数据开放共享和重复利用，发挥 Web3.0 的真正价值。

（二）多方协同推动 Web 3.0 关键技术创新

一是统筹建设基于区块链的下一代网络基础设施，支撑 Web 3.0 技术创新发展和应用探索实践。针对区块链、非同质化通证、数字钱包、数字身份等 Web 3.0 关键技术和核心组件，依托国家项目加速技术自主创新。积极探索数字资产交易的“监管沙盒”试点模型，强化事前事中监管。二是鼓励企业积极探索数字藏品推动数字文化产业发展。通过国家产业和开源基金扶持开源生态，研究开源项目的合规融资框架，针对线上零工市场和自治组织建立明确的规则要求。鼓励建设区块链相关国家重点实验室、工程技术中心等科技创新平台，打造产学研用创新联合体，促进关键

技术联合攻关与基础平台开放共建，辐射带动产业发展。三是适度支持国内外技术交流，打通生态壁垒，加快培育相关产业、技术和人才，同步发展监管能力和治理体系。加强与 ITU、ISO 等国际标准组织的联系合作，积极参与国际标准制定，继续强化数字身份、互操作、行业应用等优势领域的标准规范，同时开拓数字资产、联盟治理等标准研制，抢占 Web 3.0 标准制定主导权。

附录：应用案例

数字身份

案例名称：基于腾讯云 TDID 的学分银行

案例简述：腾讯云分布式身份服务 TDID(TencentCloud Decentralized Identity)，以区块链为底层，以“分布式身份标识符 + 可验证的数据凭证”的方式构建可信身份模型，为跨系统、跨机构的可信数字身份和数据交换服务提供基础设施。基于 TDID 与多所院校推出学分银行，实现不同教育阶段、不同教育培训机构对用户身份的开放互认，帮助用户全生命周期、跨机构积累终身学习历程中的各类教育凭证，实现教育数据的自主管理和可信开放授权。

案例名称：蚂蚁链授权宝

案例简述：蚂蚁链数字徽章，是通过提供个性化的体验服务，帮助活动组织者更好地与观众进行互动。它是一种通过绑定用户身份体系 DID 进行分发加密徽章的机制，用于记录和纪念特定事件的发生，用户可以自行控制自己的数字徽章进行互动。蚂蚁链数字徽章不仅具有独特的设计，背后还包含了各种权益属性，用户可以通过参与各种行为（绿色出行、出席活动等）获得数字徽章。

案例名称：中移数字身份基础设施

案例简述：中国移动结合自身的业务特点，利用已有的超级 SIM 卡、CMCA 等能力，并采用基于 TEE 的密钥托管技术、基于代理重加密的身份凭证保存技术，正在推进面向 Web3.0 的登录与身份认证一体的产品的落地。在 Web3.0 时代，让普通用户把身份、数据、数字等资产安全装进口袋。

开放联盟链

案例名称：HyperRedox 如道链

案例简述：如道链（HyperRedox）作为一条更加合规、开放、多元化的开放联盟链，一定程度上对数字藏品在联盟链上的应用突破传统联盟链技术提出了治理上的更高需求，除了满足趣链科技、TBI 牵头发布的《联盟链运营治理框架》中的可监管性、稳定性、高效性、中立性、保障性、公正性以外，还需要满足合规开放性、收益分配机制可持续性、可竞争性、多中心性等特性。

案例名称：中移 OPB

案例简述：2022 年初，中国移动信息技术中心区块链团队自主研发的中移链加入 BSN，以开放联盟链的形式面向存在区块链业务需求的各行业客户提供接入服务。得益于中移链多年内部的耕耘，中移链开放联盟链（中移 OPB），将坚持以客户体验为中心，提供开发、业务、能力和支撑方面的优质服务，打造 BSN 上的中国移动自主研发开放联盟链品牌。

案例名称：众享链网

案例简述：众享链网由各行业头部企业联合共建发起，是国内首个分布式共治的产业级联盟链体系，坚持“融合·创新”，以发展新一代网络——融合互联网为自身定位，致力于构建“低成本、高效率、多兼容”的数字基础设施，打造“多链互联共生”的区块链生态圈。众享链网超级节点目前已涵盖物联网、大数据、云计算、人工智能、金融科技、便捷支付、司法存证、工业互联网、数字藏品等众多行业领域，未来将继续加大技术融合研发力度，筑建全链条创新技术体系，全力实现区块链与大数据、人工智能、物联网等高新技术领域的创新融合发展。

数字藏品

案例名称：基于至信链的小红书数字藏品平台 R-SPACE

案例简述：至信链是腾讯云主导发起建设的合规区块链平台（联盟链）。基于至信链元商品协议推出的小红书数字藏品平台 R-SPACE，将创作者的原创数字化作品打造成链上数字藏品，每个作品都有链上唯一标识，实现作品的确权，保护创作者权益。在 R-SPACE 内销售数字藏品，

为创作者提供作品变现渠道。用户购买数字藏品后可以在小红书个人主页展示，使用 AR 功能与数字藏品合拍发布笔记，还能把数字藏品转移至 QQ 等平台进行展示。

案例名称：StarCat 星际猫数字藏品

案例简述：StarCat 星际猫是国内首个具有元宇宙 AI 交互功能版权数字藏品。对标 BAYC 无聊猿，旨在打造有深度商业场景和强大社区生态的中国原创元宇宙超人气 IP。StarCat 星际猫已与十余家科技和文旅头部企业达成深度合作，将为数字藏品创造更多应用场景，共建商业生态。StarCat 星际猫将在原有商业生态上拓展，联合前沿科技研发、头部媒体传播、核心企业赋能、创作者网络共创，与全球先锋企业家、艺术家、科技精英和 Web3.0 意见领袖共建元宇宙生态。

案例名称：基于“星火·链网”的数字藏品服务平台——灵境藏品

案例简述：灵境藏品是基于国家区块链新型基础设施“星火·链网”构建的数字藏品服务平台，通过深入传统艺术、潮流文创、工业设计、元宇宙等多个领域发掘艺术瑰宝，以数字藏品为载体，链接知名潮流 IP、艺术创作者、艺术机构以及收藏爱好者，提供优质全面的数字藏品服务。灵境藏品在中国信通院的指导下，由纸贵科技提供技术支持，通过“星火·链网”提供的区块链底座和标准协议，为每个数字藏品构建独一无二、无法篡改、不可复制的电子凭证，为数字藏品的发行、购买、收藏和使用等全流程保驾护航。

案例名称：蚂蚁链“鲸探”数字藏品

案例简述：鲸探数字藏品是使用蚂蚁链的区块链技术进行唯一标识的经数字化的特定作品、艺术品和商品，包括但不限于数字画作、图片、音乐、视频、3D 模型等各种形式。鲸探是一款基于蚂蚁链技术，集数字藏品购买、收藏、观赏以及分享为一体的应用。鲸探平台目前数字藏品总发行量已超过 800 万，藏品平均售罄时间在 10 秒内。蚂蚁链作为国内外领先的区块链技术服务提供方，是很多头部数字藏品 IP 方进行数字化艺术探索的首选。

案例名称：灵境生态 - 元宇宙生态圈

案例简述：灵境生态致力于创建基于灵境链网及其相关底层设施的免许可、可组合的创新生态。

灵境链网是由上海开源技术协会元宇宙专委会发起管理，由上海金融信息行业协会作为支持机构，由分布科技提供技术实施的联盟链网络。灵境生态旨在帮助中国的区块链开发者打造一个生态开放、开发便捷、流量互通的东方元宇宙。

隐私计算

案例名称：Sacre 隐私计算融合服务平台

案例简述：隐私计算技术在维护用户数据主权的同时，充分发挥数据的应用价值，是 Web3 发展的重要技术前提。Sacre 是支持企业级应用的隐私计算融合服务平台，集成了隐私协同计算、密文托管、隐私证明、密文计算、密钥管理等服务，用于解决数据要素流转中的数据安全和隐私保护问题。平台采用可插拔式的密码学组件，并为用户提供了一系列规范的底层接口，同时满足物联网、浏览器、移动端、云等多种模式，适用于工业、金融、生物医药等丰富的应用场景。

案例名称：可审计机密计算服务

案例简述：隐私保护能力是 Web3.0 数据开放共建的重要技术前提。火山引擎数据安全中心利用机密计算技术提供高性能、高安全、高可用的隐私计算能力，可审计机密计算服务结合机密计算和区块链技术，将联合查询任务导入到数据沙箱中安全执行，保障相关数据隐私合规。同时将 SQL 语句等执行逻辑脱敏上链，供数据方对计算内容进行查证审计。

组织协作

案例名称：基于区块链的“共筑文明”大理市城市数字治理公众聚能平台

案例简述：“共筑文明”大理市数字治理公众聚能平台，将区块链技术应用创新与大理市城市治理的实际相结合，充分发挥区块链技术在可信存证、共识激励、多方协同等方面的优势，鼓励社会民众积极参与城市公共事务，并对个人诚信行为进行记录，助力弘扬诚信传统美德，增强社会成员诚信意识。该案例同时也获评了国家级奖项“2022 中国产业区块链十大杰出案例”。

案例名称：分布式认知工业互联网

案例简述：在工业 4.0 大背景下，分布式认知工业互联网为工业制造业的数字化转型提供了 Web3 解决方案。平台在工业互联网的基础上，集成了区块链、知识图谱、隐私计算等先进技术，在数据隐私和数据确权的前提下，打通数据壁垒，提供安全可靠公平的多方协作方式，并在全生命周期实现智能化生产。平台通过分层解耦、开放架构和经济机制，重构相关方生产关系，构建分布式商业模式和具备网络规模效应的协作生态。已应用在汽车、钢铁、石化、双碳等领域。

数据分析

案例名称：链上天眼

案例简述：近年来，越来越多的犯罪分子利用加密资产开展犯罪活动。为解决执法部门在执法过程中的众多疑难，欧科云链推出了链上天眼系列产品。链上天眼以区块链链上数据作为基础、以大数据治理作为技术支撑，综合运用机器学习、数据建模、相似度算法、特征工程等关键技术，解析并整合了上百亿条链上地址、交易记录，并将传统经济类案件中的技战术方法，运用到加密资产相关案件中，结合多种到决策分析方法和侦查逻辑，协助监管单位与执法机关进行加密资产的智能化追踪、一站式分析和取证研判，真正做到让数据说话、让数据作证，有效帮助办案人员快速的对被调查案件、地址、资金流向、关系脉络以及交易行为等特点进行快速了解和掌握。

致谢

单位（排名不分先后）：

中国信息通信研究院
北京红洞科技有限公司
杭州趣链科技有限公司
北京众享比特科技有限公司
上海万向区块链股份公司
北京欧科云链网络科技有限公司
北京火山引擎科技有限公司
中国移动信息技术中心
华为技术有限公司
南方科技大学
恒生电子股份有限公司
杭州融都科技股份有限公司
腾讯云计算(北京)有限责任公司
腾讯科技（深圳）有限公司
西安纸贵互联网科技有限公司
蚂蚁区块链科技（上海）有限公司
上海分布信息科技有限公司
中电数字场景科技研究院
无锡井通网络科技有限公司
咪咕文化科技有限公司
山大地纬软件股份有限公司
北京远古遗珍博物馆
广州广电运通金融电子股份有限公司
中兴通讯股份有限公司

个人（排名不分先后）：

吴因俭 魏凯 王蕴韬 张奕卉 庞伟伟 刘婷婷 刘宾 张立峰
邵兵 李克鹏 周子涵 王乐庆 张懿方 蔡庆普 韩鹏 许娅伦
王浩溟 武杨 徐思彦 李伟 张帅 张贝龙 李彭智 徐静
郜云杉 陈昌 侯伟 陈志乐 严挺 张雅琪 胡峰 邱鸿霖
张晓蒙 童骏 杜宇 郝玉琨 侯东圣 笕鸿飞 王子博 张仕根
许乾 蒋照生 孙宇林 张尧 季洪涵 冯庆玲 朱江 聂二保
朱宽 王晓涛 黄晏清 张沛 潘晓丰 李琳 桂祖宏 孙维佳
朱成康 魏茂华 闵新平 孔兰菊 仪莉 叶力瑛 王桂静 张一博
卫晓欣 杨鹏晖 马利 吴骞 黄峥 郭勇 郭海生

可信区块链推进计划
Trusted Blockchain Initiatives

网址: www.trustedblockchain.cn

邮箱: wuyinqian@caict.ac.cn