软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(9):3615−3647 [doi: 10.13328/j.cnki.jos.007611] [CSTR: 32375.14.jos.007611]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

Web 3.0 前沿技术研究综述*

王 斌[1,2], 伍羽放[1,2], 高 阳[1,2], 刘天健[1,2], 翁 渊[1,2], 李 超[1,2], 张大伟[1,2], 徐光侠[3], 许光全[4], 祝咏升[5], 沈 蒙[6], 祝烈煌[6], 王 伟[1,2]

[1](北京交通大学 计算机科学与技术学院, 北京 100044)

[2](智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044)

[3](广州大学 网络空间安全学院, 广东 广州 510006)

[4](天津大学 智能与计算学部, 天津 300072)

[5](中国铁道科学研究院集团有限公司, 北京 100081)

[6](北京理工大学 网络空间安全学院, 北京 100081)

通信作者: 王伟, E-mail: wangwei1@bjtu.edu.cn

摘　要: Web 3.0 是以区块链为技术底座的新一代互联网框架, 能够助力数据资产化, 形成可流通的数字资产, 促进数字经济发展. 然而, Web 3.0 在用户生态构建与数字资产流通两方面仍然存在挑战: (1) Web 3.0 用户信任机制多样导致用户数字身份管理难; (2) Web 3.0 数字资产侵权成本低、鉴权粒度粗导致数字资产高效流通难; (3) Web 3.0 开放自治且参与实体多元导致用户生态治理难; (4) Web 3.0 数据公开透明且攻击面多样导致隐私保护与安全监管平衡难. 围绕这 4 个挑战, 提出面向数据资产化的 Web 3.0 技术架构, 针对数据资产化在身份管理、资产流通、生态治理与安全监管这 4 个方面的需求, 结合技术自身特点, 对国内外相关的 Web 3.0 技术研究工作进行归纳、分类、分析与总结. 具体包括: (1) 分布式数字身份管理机制, 包含数字身份创建、标识鉴别与隐私保护等技术; (2) Web 3.0 数字资产流通机制, 包含数字资产确权、鉴权与流通等技术; (3) Web 3.0 生态治理机制, 包含用户声誉评价与权益激励等技术; (4) Web 3.0 数字资产安全防护与监管技术, 包含主动监管、链上数据监测与应用前端安全分析等技术. 最后, 展望 Web 3.0 技术的未来研究方向.

关键词: Web 3.0; 分布式数字身份; Web 3.0 数字资产流通; Web 3.0 用户生态治理; Web 3.0 安全监管

中图法分类号: TP311

中文引用格式: 王斌, 伍羽放, 高阳, 刘天健, 翁渊, 李超, 张大伟, 徐光侠, 许光全, 祝咏升, 沈蒙, 祝烈煌, 王伟. Web 3.0 前沿技术研究综述. 软件学报, 2026, 37(9): 3615–3647. http://www.jos.org.cn/1000-9825/7611.htm

英文引用格式: Wang B, Wu YF, Gao Y, Liu TJ, Weng Y, Li C, Zhang DW, Xu GX, Xu GQ, Zhu YS, Shen M, Zhu LH, Wang W. Survey on Cutting-edge Technologies of Web 3.0. Ruan Jian Xue Bao/Journal of Software, 2026, 37(9): 3615–3647 (in Chinese). http://www.jos.org.cn/1000-9825/7611.htm

Survey on Cutting-edge Technologies of Web 3.0

WANG Bin[1,2], WU Yu-Fang[1,2], GAO Yang[1,2], LIU Tian-Jian[1,2], WENG Yuan[1,2], LI Chao[1,2], ZHANG Da-Wei[1,2], XU Guang-Xia[3], XU Guang-Quan[4], ZHU Yong-Sheng[5], SHEN Meng[6], ZHU Lie-Huang[6], WANG Wei[1,2]

[1](School of Computer Science & Technology, Beijing Jiaotong University, Beijing 100044, China)

[2](Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing 100044, China)

[3](Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China)

[4](College of Intelligence and Computing, Tianjin University, Tianjin 300072, China)

* 基金项目: 国家重点研发计划 (2023YFB2703800); 国家自然科学基金联合基金重点支持项目 (U21A20463, U22B2027, U23A20304); 北京市自然科学基金面上专项 (M23019)
收稿时间: 2024-06-03; 修改时间: 2025-08-13; 采用时间: 2025-12-09; jos 在线出版时间: 2026-04-01
CNKI 网络首发时间: 2026-04-02

[5](China Academy of Railway Sciences Corporation Limited, Beijing 100081, China)
[6](School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

Abstract: Web 3.0 is a new-generation Internet framework based on blockchain technology, which facilitates data assetization and enables the formation of tradable digital assets, thus promoting the development of the digital economy. However, Web 3.0 still faces several challenges in user ecosystem construction and digital asset circulation: (1) The diversity of user trust mechanisms in Web 3.0 poses challenges to digital identity management. (2) The low cost of digital asset infringement and coarse-grained authentication in Web 3.0 hinder the efficient circulation of digital assets. (3) The open and autonomous nature of Web 3.0, together with the diversity of participating entities, leads to difficulties in user ecosystem governance. (4) The openness and transparency of data, along with diverse attack surfaces in Web 3.0, make it difficult to balance privacy protection and security regulation. To address these four challenges, a Web 3.0 technology architecture oriented toward data assetization is proposed. Focusing on the requirements of data assetization in identity management, asset circulation, ecosystem governance, and security regulation, and in combination with the technical characteristics of Web 3.0, relevant Web 3.0 research work at home and abroad is summarized, classified, analyzed, and reviewed. Specifically, this study includes (1) distributed digital identity management mechanisms, including technologies such as digital identity creation, identifier authentication, and privacy protection; (2) Web 3.0 digital asset circulation mechanisms, including technologies such as digital asset ownership confirmation, authentication, and circulation; (3) Web 3.0 ecosystem governance mechanisms, including technologies such as user reputation evaluation and incentive mechanisms; (4) Web 3.0 digital asset security protection and regulation technologies, including proactive regulation, on-chain data monitoring, and application front-end security analysis. Finally, future research directions of Web 3.0 technologies are discussed.

Key words: Web 3.0; distributed digital identity; circulation of Web 3.0 digital assets; Web 3.0 user ecosystem governance; Web 3.0 security and regulation

1 引 言

互联网发展至今已有超过 50 年的历史, 从最初的 Web 1.0——只读互联网, 演变成了当前的 Web 2.0——读写互联网. Web 1.0 时代的矛盾主要体现在用户体验与技术之间, 由于技术与场景的局限, 用户只能被动地浏览网页数据, 无法实现交互. Web 2.0 时代下的用户实现了数据内容交互, 形成了社交、智慧出行、网购等在线便捷服务, 极大地改变了人们的生活方式. 谷歌、微软、亚马逊等公司抓住了 Web 1.0 时代的机遇, 推动技术与服务升级, 成功在 Web 2.0 时代站稳脚跟并发展成为互联网巨头. 如今, 随着互联网中用户生成的内容日益增多, 用户与平台间的矛盾逐渐凸显.

一方面, Web 2.0 中用户创造的内容由中心化平台加工存储, 用户对数据的所有权难以得到有效保障. 例如, 用户在购物平台上所产生的活动数据通常会被平台擅自使用, 用户无法主动销毁这部分数据, 更无法获得自身数据所产生的经济效益. 另一方面, 在 Web 2.0 时代, 人们可以随意地复制并转发其他用户的创作内容, 削弱了数字内容的稀缺性, 极大降低了原创用户的积极性. 尽管我国的个人信息保护法明确禁止大规模的个人数据非法滥用、传播等行为, 但仍难以避免针对单个用户数据或少量用户数据的非法行为.

随着区块链、元宇宙与生成式人工智能 (artificial intelligence generated content, AIGC) 等技术的发展, 以用户为中心的新一代互联网框架——Web 3.0 正在加速崛起. Web 3.0 将用户所创作的数字内容视作数字资产, 用户拥有数字资产的所有权与控制权, 能够灵活自由地对数字资产进行管理与交易, 平台需获得用户许可后方可对数据进行加工使用, 从根本上化解用户与平台间的矛盾. Web 1.0、Web 2.0、Web 3.0 的区别如表 1 所示.

表 1 互联网不同发展阶段的区别

互联网发展阶段	架构	特点	内容创作	内容控制	身份管理	收益分配
Web 1.0	中心化	阅读式互联网	平台	平台	平台	平台
Web 2.0	中心化	可读可写互联网	用户	平台	平台	平台
Web 3.0	去中心化	价值互联网	用户	用户	用户	用户

数据价值化包含数据资源化、数据资产化、数据资本化这 3 个环节. 而 Web 3.0 的愿景是实现个人数据资产化, 这包含在我国数据要素市场的发展目标中. 国家重点研发计划“区块链”重点专项 2023 年度项目申报指南中共

包含 9 项指南任务, 其中 3 项为 Web 3.0 领域, 系“区块链”专项中首次出现 Web 3.0 指南任务, 涵盖了基础理论与共性关键技术, 旨在为基于区块链的数据要素市场关键技术与示范应用提供理论与技术支撑. 当前, 我国已开展数据要素流通试点, 但数据要素市场化配置的权属界定、估值定价、市场规则、流通技术等关键性难题仍有待破解. 随着 Web 3.0 的发展, 用户体验形式与商业形式将产生较大变革, 这些难题有望得以解决.

本文第 2 节将介绍 Web 3.0 的技术架构, 分别包括基础设施、身份管理、资产流通、生态治理与安全监管. 第 3 节将详细描述身份管理, 重点介绍去中心化数字身份 (decentralized identity, DID). 第 4 节将介绍资产流通, 包含数字资产确权、鉴权与流通等方面. 第 5 节将从用户声誉与用户激励这两方面介绍生态治理. 第 6 节将介绍安全监管, 从隐私保护与监管、合约安全等方面进行深入分析. 第 7 节对 Web 3.0 前沿技术的未来研究进行展望.

本文从数据资产化的角度对 Web 3.0 前沿技术进行了归纳、分类、分析与总结, 具有如下贡献.

(1) 提出面向数据资产化的 Web 3.0 技术架构. 围绕数据在全生命周期中的确权、使用与监管需求, 划分为基础设施、身份管理、资产流通、生态治理与安全监管这 5 个核心模块. 基础设施为上层功能提供可扩展、可信赖的技术底座; 身份管理聚焦于用户主权身份的确立与管理机制; 资产流通涉及数据确权、鉴权与流通等关键环节; 生态治理强调用户协作与平台共治的声誉、激励与治理机制; 安全监管则保障整个数据资产体系在隐私保护、合规执行与安全方面的可控性.

(2) 围绕当前 Web 3.0 技术在用户生态构建与数字资产流通两方面面临的核心挑战, 对身份管理、资产流通、生态治理与安全监管这 4 个方面的关键技术进行详细的分析与总结. 身份管理方面, 重点关注如何构建具备可信性、可验证性与用户主权保障的 DID 系统; 资产流通方面, 分析了数据确权、鉴权与流通等关键环节面临的互操作性不足与安全性挑战; 生态治理方面, 探讨了去中心化治理机制如何激励用户参与与维护生态稳定; 安全监管方面, 则聚焦于如何实现敏感数据的隐私保护与违规行为的可审计性追溯机制.

(3) 前瞻性地展望 Web 3.0 关键技术的发展趋势与研究方向. 身份管理方面, 构建支持身份可验证性、隐私可控性与跨域信任迁移的可信分布式数字身份管理机制, 融合零知识证明、多方安全计算等隐私增强技术; 资产流通方面, 设计支持多模态数据统一确权、跨平台流通与资产组合的通用资产流通机制, 以实现多场景下的可信价值转移; 生态治理方面, 发展面向共建共治的生态治理机制, 重点解决异构角色间协作治理与声誉激励机制设计问题; 安全监管方面, 建立覆盖资产确权、交易、存储到变现等环节的全生命周期安全防护与合规监管体系, 应对跨链资产滥用等 Web 3.0 特有安全挑战.

2 Web 3.0 技术架构

Web 3.0 技术架构涵盖了多个关键层次, 当前大部分工作是从技术垂直角度进行架构分层. Guan 等人[1]引入了区块链基金会所提出的 5 层技术架构. 该架构的第 1 层为交互协议平台与网络套件, 第 2 层为数据分发与交互层, 第 3 层则是作为前一层的功能扩展层, 实现加密消息传递等功能, 第 4 层是程序开发语言层, 包含 Solidity、Rust 与 Vyper 等主流语言, 第 5 层是交互层, Web 3.0 中的各种应用都属于这一层, 例如 OpenSea[2]、MetaMask[3]与 Uniswap[4]等. Jacksi 等人[5]提出了一个 4 层的 Web 3.0 技术架构, 分别为统一资源标识层、超文本传输协议层、文件传输协议层与 IP 安全层. Swati 等人[6]提出了一个由区块链网络层、区块链架构层与应用层所组成的基于区块链的 3 层技术架构. Petcu 等人[7]所提出的技术架构是由网络层、区块链交互层、中间设施层与应用层所组成的. Wan 等人[8]从 Web 3.0 应用开发的角度提出了 5 层 Web 3.0 技术架构, 包括数据库服务层、应用服务层、区块链服务层、网络服务层与前端后端交互层. Shen 等人[9]根据人工智能技术在 Web 3.0 中所发挥的不同作用, 将 Web 3.0 划分为基础设施层、接口层、管理层与应用层. 其中基础设施层面向数据管理, 接口层将真实世界的物理资产映射为数字资产, 管理层实现 Web 3.0 生态管理, 应用层则包含了 Web 3.0 中的各类应用.

数据要素价值化赋予了 Web 3.0 新型技术需求与应用场景, 但随着数据要素流通市场的不断扩大, Web 3.0 在数据采集、汇聚、确权与流通等关键环节仍然面临挑战. 具体而言, 数据要素的采集需要面对数据来源的多样性; 数据传输和汇聚则需要考虑网络通信的稳定性和数据的整合效率; 而数据的确权和运营则需要建立有效的数字资

产确认和流通机制; 在数字资产的流通过程中, 用户治理和监管成为至关重要的环节, 需要建立有效的参与机制和监管制度, 以保障数字资产流通的公平性和合规性. 已有技术架构大都是从区块链技术角度进行划分, 未能完全展现 Web 3.0 在数据资产化中的特点.

因此, 本文从数据资产化的角度划分 Web 3.0 技术架构, 包含基础设施、身份管理、资产流通、生态治理、安全监管这 5 个方面, 如图 1 所示.

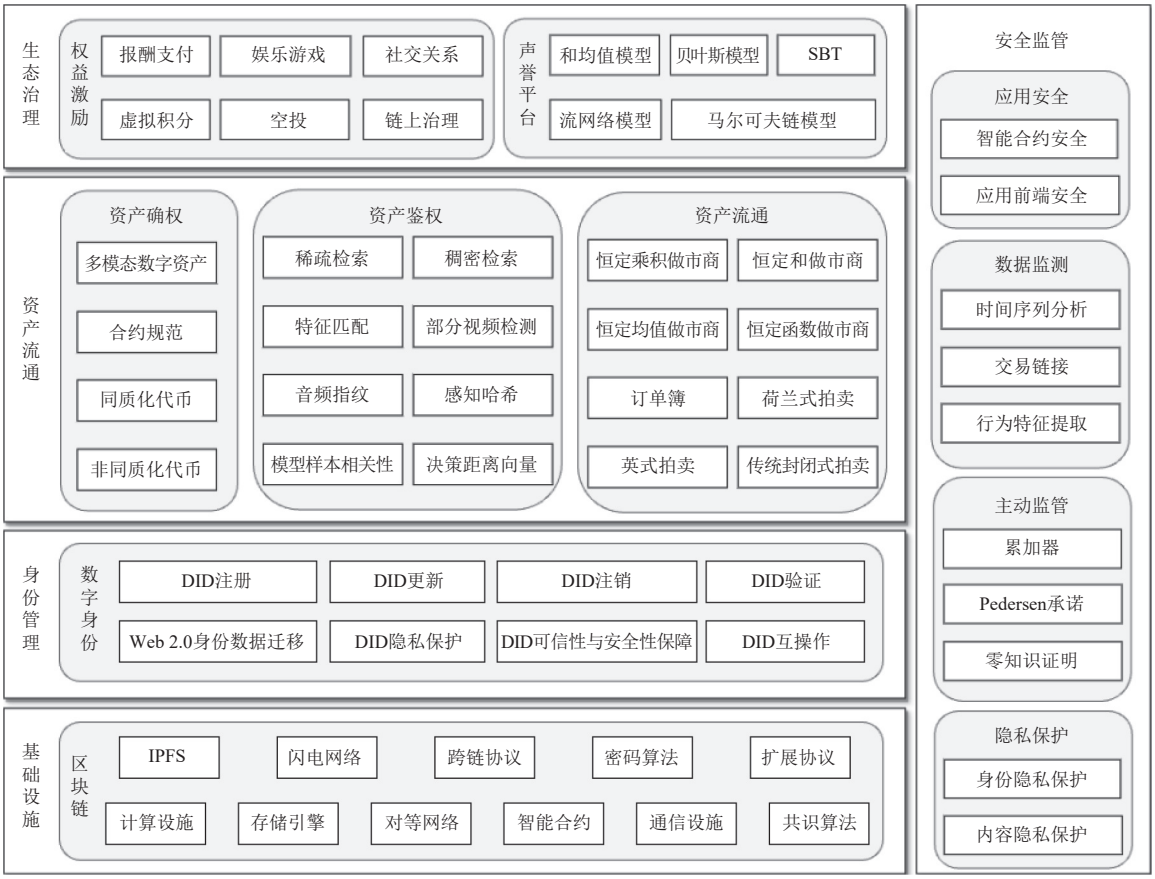

图 1 面向数据资产化的 Web 3.0 技术架构

(1) 基础设施. 负责数字资产流通过程中的计算、存储、传输, 包含计算、存储与通信等方面的设施和区块链的一些核心底层技术, 如共识协议、智能合约、跨链协议与扩展协议等. 由于已有相关综述均对区块链的基础设施进行了详细论述, 因此本综述不再进行赘述, 将聚焦与数据要素流通紧密相关的技术.

(2) 身份管理. 主要为用户提供数字身份标识与管理服务, 包括去中心化标识符的创建、注册、管理、验证与撤销等, 实现去中心化标识符互操作性, 提供安全保障与隐私保护功能. 利用去中心化标识符实现可验证的去中心化数字身份, 为现实世界中的物理资产 (如个人、组织、事物、数据等) 分配一个确定的数字身份, 通过可验证凭证防止欺诈攻击, 实现个人与企业对数据的所有权和控制权, 在无需将用户个人信息提供给第三方中心化网站或应用程序的情况下, 证明用户的在线身份, 满足数字资产流通过程中用户身份自主管理的需求.

(3) 资产流通. 提供数字资产流通交易过程中的数字资产确权、鉴权与流通交易等核心服务, 实现可靠公平的数据确权鉴权与可信高效的数字资产供需匹配. 在数字资产确权方面, 通过 NFT 技术将多模态数据 (例如文字、图片、音频、视频与神经网络模型等) 映射为数字资产, 并通过数据指纹与深度学习技术提取数据 DNA. 由于用户在确权阶段可能存在侵权行为, 因此需要利用深度学习等技术构建内容匹配技术, 实现多模态数字资产的可靠

鉴权, 为数字资产流通交易提供基础. 而在数字资产流通方面, 首先从任务需求的重要程度、数据自身的价值与市场经济等方面对数据进行估值定价, 针对不同的经济场景, 运用不同的定价机制; 然后利用自动做市商、拍卖与订单簿等技术实现多模态数字资产的供需匹配; 最后通过价格反馈机制, 结合用户市场行为偏好调查建立高效的市场调查分析机制, 进一步指导用户数据估值与定价, 稳定数字资产流通量, 促进数字资产供需匹配, 提高数字资产流通交易效率.

(4) 生态治理. 刻画用户在数字资产流通过程中行为 (具体指独立钱包或者去中心化标识符) 的声誉, 进一步的, 可以是一个去中心化标识符捆绑多链上的多个钱包和多种社会性网络服务 (social networking service, SNS) 账号, 建立用户声誉画像并从 Web 3.0 生态层面激励用户进行数字资产流通交易, 主要包含用户声誉评价与用户权益激励两个方面. 用户声誉评价方面, 首先将用户链上链下的声誉数据进行关联与聚合, 然后利用马尔可夫链模型与贝叶斯模型等技术实现用户声誉的计算与更新, 最后实现声誉数据的高效安全存储. 用户权益激励方面, 利用深度学习与博弈论等技术对用户贡献进行分析, 通过公平理论与多元规划等技术实现 Web 3.0 用户共享的权益激励, 保障用户的权益与 Web 3.0 数字资产流通生态的安全性和可持续性, 促进生态稳定发展与平稳运行.

(5) 安全监管. 分别针对 Web 3.0 基础设施、身份管理、资产流通与生态治理这 4 个方面的隐私保护与安全监管需求, 构建 Web 3.0 数字资产全生命周期安全防护与监管技术. 基础设施方面, 通过漏洞检测技术对钱包与智能合约进行安全性分析. 身份管理方面, 利用环签名、群签名等技术实现监管友好的用户身份隐私保护. 资产流通方面, 首先, 在确权阶段, 对多模态数字资产的内容进行审计, 防止包含敏感内容或恶意内容的数字资产流通; 其次, 针对不同的用户隐私保护需求, 采用分级加密保护技术, 设计多样化的数字资产隐私保护方法; 最后, 在数字资产流通阶段, 通过身份验证实现数字资产的可信交付与可靠追溯. 生态治理方面, 对用户链上身份与行为进行分析, 并且针对恶意用户的攻击行为进行检测, 例如女巫攻击、交易欺诈、洗钱等, 为用户声誉评价与用户权益激励提供安全支撑. 由于已有相关综述对身份隐私保护与监管、智能合约漏洞检测方面进行了详细论述, 因此本综述不再进行赘述, 将重点归纳、分类、分析与总结资产流通与生态治理方面的相关技术.

3 身份管理

在如今的互联网中, 用户身份信息均由所在平台管理, 用户对于自己的账户与身份没有操作与管理的权限, 无法对身份信息进行更新、删除与撤销等. 而在数据资产化框架中, 数字身份是确权的核心载体, 决定了资产归属与使用权的合法性.

身份管理层旨在解决上述问题, 设计可迁移、可扩展、可切换的分布式数字身份, 在此基础上建立安全高效的可验证身份凭证管理与隐私保护机制, 满足用户自主身份管理 (self-sovereign identity, SSI) 需求, 而其中最核心且备受关注的技术当属 DID. DID 不仅是用户在 Web 3.0 环境中安全参与交易与交互的前提, 也是跨平台资产流通与治理决策的信任基石. 本节将从 DID 相关概念、工业界与学术界中基于 DID 的身份管理方案进行介绍, 并总结分析现有工作在隐私性、扩展性等方面存在的问题.

3.1 去中心化身份

随着用户对于互联网身份自主管理需求的愈发强烈, Cameron[10]于 2005 年提出了自主身份管理的概念. 与传统的中心化数字身份和联盟化数字身份不同, SSI 强调以用户为中心构建互联网数字身份, 在不依赖于中心化平台的条件下实现对身份信息的管理, 将身份信息的控制权交还给用户, 互联网用户身份的演化过程如图 2 所示.

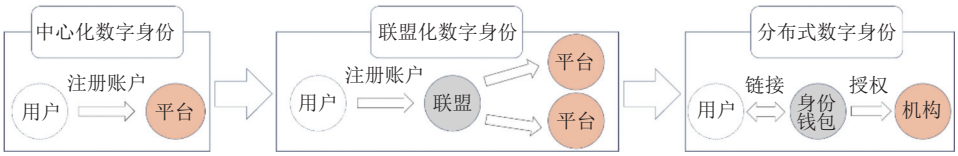

图 2 互联网用户身份的演化过程

DID 即为实现 SSI 的一种技术手段, 满足用户身份自主管理的需求. DID 允许个人、组织或设备拥有自主控制的、可验证的数字身份, 与中心化身份管理方式相比, 其区别如表 2 所示. DID 是一种新的身份标识, 无需中央注册机构就能够实现全球唯一, 并且完全由参与者本人掌控.

表 2　中心化身份管理与 DID 的对比

类别	属性	个人	平台	开发者
中心化身份管理	身份管理	身份信息在用户不知情的情况下被平台收集、存储与分享	收集的用户数据中心化存储在平台上, 存在单点故障的问题	需依赖第三方平台所提供的API用于用户身份验证, 认证过程存在隐私泄露风险
	数据操作	身份信息管理的权限属于平台, 用户无法自主对其进行操作	平台拥有用户身份信息的读写权利, 难以实现隐私保护下的用户身份信息验证	登录流程效率低下, 用户体验不佳
	密钥丢失与恢复	可通过手机验证等多种验证方式恢复账户访问权, 用户的密钥永久性损失风险低	平台掌握账户恢复的最高权限, 但也会成为被攻击者利用的环节	可直接依赖平台提供的成熟账户体系和恢复机制, 无需自行设计复杂的恢复逻辑
DID	身份管理	数据与 DID 完全掌握在用户手上	随时都能够验证用户凭证的真实性与完整性, 无需频繁向中心机构发送请求	无需密码和低效的验证过程
	数据操作	防止自身在平台与应用上的行为数据被非法利用	降低了签发防欺诈证书的成本	在保护用户隐私的前提下向用户请求数据
	数据安全	用于数据的完整管理权与控制权	更好地保护用户数据隐私与安全	—
	密钥丢失与恢复	私钥是唯一凭证, 一旦丢失, 身份和关联资产将面临永久性的损失, 恢复难度极高	无法干预或帮助用户恢复身份, 不承担因用户密钥管理不善造成的损失	—

然而, DID 将身份控制权完全交予用户的模式是一把双刃剑. 其在赋予用户数据主权的同时, 也表示用户需要承担全部的安全责任. 在传统的中心化体系中, 用户可通过“忘记密码”功能从服务提供商恢复账户, 但在 DID 体系下, 私钥是用户身份的唯一凭证. 一旦私钥因设备损坏、遗忘或被盗而永久丢失, 其数字身份以及所关联的全部数字资产将面临无法挽回的永久性损失. 这种严苛的风险为普通用户带来了较高的使用和安全风险, 是 DID 技术走向大规模应用前必须解决的核心挑战.

万维网联盟 (world wide Web consortium, W3C) 所推行的 DID 标准中包含了 DID 与可验证凭证 (verifiable claim, VC) 两个核心组件. 利用 DID 可以实现为某个实体构造一个唯一的、去中心化的标识符. 其体系架构如图 3 所示, 包含 DID 主体、DID 控制者、DID、DID 文档、DID URL 与可验证的数据注册表等基础组件.

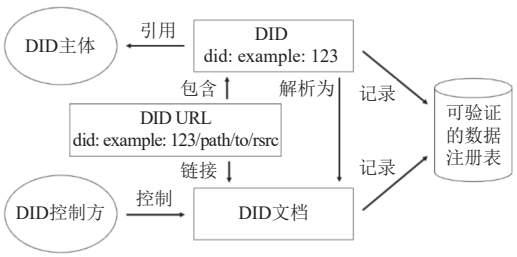

图 3　DID 体系结构

由于 DID 与 DID 文档内不包含用户的个人身份信息, 因此, 无法仅通过 DID 来验证用户身份信息的真实性, 必须依靠 VC 实现身份验证. VC 与 DID 相关联, 能够通过数字签名等技术为所关联的 DID 提供信任背书, 证明其真实性. VC 由凭证元数据、声明与证明这 3 部分所组成. 凭证元数据包含与凭证相关的一些附加信息, 如凭证的唯一标识符、颁发日期、凭证类型等, 实现凭证的管理. 声明包含了主体声明的所有个人信息的属性名与属性值. 证明则用于验证凭证的真实性与完整性, 包含了由凭证发行方的私钥所生成的数字签名与

密码学证明.

3.2 基于 DID 的身份管理方案

目前, 代表性的身份自主管理方案有 ShoCard[11]、WeIdentity[12]、Microsoft DID[13]、uPort[14]和 Sovrin[15]等. 接下来将分别对这些方案进行介绍, 并且比较它们的优缺点, 如表 3 所示.

表 3 身份自主管理方案对比

类别	方案	优点	缺点	隐私性	应用链
工业界	ShoCard[11]	SSI 作为核心架构, 兼容以太坊环境	分布式共享网络验证, 用户验证效率不高	采用数字签名方案, 用户数据内容未加密	公链
	WeIdentity[12]	通过第三方管理身份, 管理效率高	基于联盟链构造, 难以兼容公开环境	构造组群交易概念, 隐私数据可用户控制	联盟链
	Microsoft DID[13]	基于多条公链构造, 兼容公开环境	采用零知识证明, 用户证明效率低	用户数据加密, 隐私性优异	公链
	uPort[14]	基于以太坊构造, 适用于大部分 DApp	依赖于以太坊平台	身份属性加密, 但部分元数据公开	公链
	Sovrin[15]	用户身份信息自主可控	联邦网络环境验证身份, 用户管理效率一般	中心机构发放证书, 存储于分布式网络, 隐私数据由用户控制	公链
学术界	去中心化公钥基础设施[16]	解决PKI系统依赖可信第三方的安全性问题, 提供身份绑定服务	无隐私保护, 用户身份信息与证书公钥直接绑定容易泄露	无隐私保护	公链
	基于区块链的隐私感知PKI[17]	用户能够自主管理身份	用户自主管理身份信息粒度较粗	隐藏用户身份与公钥关联性	—
	基于许可区块链的隐私感知PKI[18]	实现了用户身份的隐私保护	应用面较窄	实现用户身份隐私保护	联盟链
	基于区块链的物联网PKI解决方案[19]	实现物联网设备之间无可信第三方的身份认证	仅适用于物联网设备	未实现用户身份隐私保护	—
	Coconut[20]	可抵御部分恶意证书颁发机构攻击	不支持对属性进行复杂的零知识证明	身份隐私保护, 且可以选择属性披露	—
	基于BBS+签名的匿名凭据颁发方案[21]	使用BBS+签名提高协议效率	凭证验证过程中需要辅助数据	利用数字签名技术对身份隐私保护	—
	zk-creds[22]	可对多个匿名凭证自由组合	需要可信凭证签发结构	身份隐私保护, 且匿名凭证可组合	—
	CanDID[23]	方案对用户友好	需要可信凭证签发结构	身份隐私保护, 利用唯一标识符以实现身份凭证的抗仿冒性	—
	Town crier[24]	可在传统和新兴身份验证体系之间建立桥梁	方案不够完整	对身份隐私具有一定的保护, 但身份的真实性需要进一步研究	—
	ZEBRA[25]	验证开销较低	证明生成开销较高	身份隐私保护	—

ShoCard[11]采用 SSI 作为核心架构, 旨在实现身份验证、授权审核证明交换和个人证书证明交换等功能. Sovrin[15]旨在解决 ShoCard 的身份信息发放以及效率层面的问题. 该项目的目标是为了实现任何人都可以颁发包含数字签名的证书, 其他人可以验证这些证书[26]. 为了提升分布式身份的实用性与隐私特征, WeBank 于 2019 年推出联盟区块链身份解决方案 WeIdentity[12], 旨在实现实体身份识别和可信数据交换. WeIdentity 通过联盟链的方式在隐私性与可用性方面增强了分布式数字身份的能力, 但由于其联盟链的特性难以广泛适用于公链环境. 因此, 2019 年, 微软发布了 DID 实施方案, 包括 Sidetree、身份叠加网络 (identity overlay network, ION) 和 DID 这 3 个部分[13], 该方案基于公链环境, 通过密码学技术重新构造网络协议, 实现分布式身份的高效管理. 为了充分发挥 DID 的特性, 其构造了基于以太坊的分布式数字身份管理服务——uPort[14]. 其允许用户在以太坊上进行身份验证、无密码登录、数字签名以及与其他应用程序交互. 然而, 由于 uPort 身份依赖于以太坊区块链, 它并不提供传统管理系统中的证书服务, 因此需要与各个发证机构 (Issuer) 合作, 帮助用户获取更多的 VC[27].

学术界主要聚焦面向区块链的身份管理与基于 DID 的去中心化匿名凭证认证服务方面的研究. Fromknecht

等人[16]提出一种基于区块链的去中心化公钥基础设施 (public key infrastructure, PKI) 数字证书管理系统, 提供密钥查询和身份绑定服务, 解决当前 PKI 系统中需要可信第三方机构导致的安全性问题. 由于用户的身份信息直接与证书公钥绑定, 没有进行隐私保护处理, 存在用户身份信息易泄露问题. Axon 等人[17]构建了一个具有隐私保护功能的 PKI 系统, 隐藏用户身份与公钥之间的关联性, 提供不可链接的短期密钥更新, 同时由用户自主决定是否公开身份信息和之前的公钥信息. Wang 等人[18]利用区块链的不可篡改和分布式特点, 构造一种基于联盟链的匿名数字证书发布方案, 实现了用户身份的隐私保护. Singla 等人[19]利用区块链技术构建替代传统 PKI 的身份管理方案, 实现物联网设备之间无可信第三方的身份认证.

近年来, 许多工作研究了特定场景需求下的匿名凭证及其验证, 将声明预设为已证明的属性, 实现在不侵犯用户隐私权的情况下证明所对应的凭证, 但只有很少一部分面向分布式身份. W3C 所提出的可验证凭证标准为去中心化匿名凭证提供了一个标准接口, 其中包含了基于 CL (Camenisch-Lysyanskaya) 签名与 BBS+签名的匿名凭证[28]. 然而, 并非所有分散匿名凭证解决方案都遵循 W3C 可验证凭证规范. 为了提高匿名凭证签发和验证过程中的安全性、效率与可扩展性, 相关学者研究如何进一步增强去中心化匿名凭证系统的可用性.

通常情况下, 凭证通过单个签发人签发, 签发人对承诺值进行群体签名. Sonnino 等人[20]提出了一种支持分布式阈值发行、公共和私人属性、重随机化及不可链接的选择性属性披露凭证方案, 在证书颁发机构的子集是恶意的或离线的情况下, 也能确保协议安全可用. Doerner 等人[21]基于 BBS+签名提出了一种带有门槛发行的匿名凭证方案, 提高了协议的效率. 但是, 这并没有减轻凭证验证过程中对辅助数据的需求. Rosenberg 等人[22]提出了一种使用通用零知识证明的协议, 使得凭证颁发者无需持有签名密钥, 并且能够将已有身份证件转换为匿名凭证, 支持对多个匿名凭证的自由组合. Maram 等人[23]提出了一种通过用户友好的方式颁发证书, 安全、私密地利用现有的、未经修改的网络服务提供商数据的身份凭证管理平台, 并结合唯一标识符以实现身份凭证的抗仿冒性.

当前的匿名凭证验证过程是假设存在可信的签发者, 但从传统数据中签发证书需要证明数据的来源. 因此, 增强去中心化身份管理系统与传统 Web 架构间的兼容性至关重要. 然而, 当前用户需要向授权机构获取许可后才能访问传统 Web 中的数据并对其来源进行证明. 为了解决这一问题, 研究者们提出了利用安全传输层协议 (transport layer security, TLS) 将传统 Web 凭证移植到去中心化架构中[24]. Zhang 等人[29]提出一个允许利用用户凭证来访问受控数据的数据馈送系统. 将 TLS 技术与去中心化匿名凭证相结合, 不仅可以保护数据的隐私, 还能够在传统和新兴身份验证体系之间建立桥梁. 然而, 在实际应用中仍然可能面临一些挑战, 例如, 如何确保数据的完整性和安全性、准确验证签发者的真实身份等问题, 都亟待进一步深入研究和探讨.

匿名凭证的链上验证一直是去中心化身份管理领域备受关注的研究热点, 研究者们不断探索如何降低链上验证成本. 零知识证明 (zero-knowledge proof, ZKP) 被认为是特殊用途匿名凭证的有前景替代品[30,31], 为匿名凭证的构建提供了新的可能性. Rathee 等人[25]通过将简洁非交互式知识论证 (succinct non-interactive argument of knowledge, SNARK) 与两层递归结构相结合, 成功降低了验证的开销.

综上, 无论是工业界还是学术界, 现有的 DID 方案在去中心化验证、隐私保护和可扩展性等方面均取得了显著进展. 然而, 这些方案大多聚焦于身份创建与验证等理想流程, 而对于“私钥丢失”这一问题普遍缺乏安全的应对机制. 为解决这一问题, 社区提出了“社交恢复 (social recovery)”[32]等前沿方案, 即允许用户预设一组可信的身份以协助恢复身份. 尽管该类方案提升了账户的可用性, 但其设计本身也引发了新的争议: 它通过引入对少数身份的信任, 在一定程度上重新将中心化风险带入去中心化体系, 与 DID 的初衷相悖. 此外, 所引入的身份合谋、被社会工程学攻击或自身密钥管理不善等问题, 都可能导致用户身份被恶意接管, 带来安全隐患. 因此, 如何在坚持去中心化原则与提供安全易用的恢复机制之间取得平衡, 是当前所有 DID 方案面临的共同瓶颈, 也是未来研究亟待突破的方向.

综上所述, Web 3.0 开放自治场景下分布式数字身份是实现用户数据自主管理的核心组件. 可信分布式数字身份管理机制通过统一的身份验证标准、增强的隐私保护能力以及跨平台的兼容性, 为数据确权提供了坚实基础. 不仅确保了用户对自身数据和资产的控制权, 还为资产的跨平台流通和生态治理提供了可信身份保障, 从而奠定了数据资产化进程中“确权”环节的制度与技术支撑. 然而, 在不同信任模型下, 现有研究工作仍存在多元实体的数

字身份可信创建与标识鉴别困难, 分布式交易场景下数字身份隐私过度泄露、访问控制策略僵化等问题. 此外, 现有的分布式数字身份管理技术缺乏 Web 兼容且可靠的标准与规范. 随着技术的不断进步和标准的逐步完善, 基于 DID 的身份管理方案有望在未来得到更广泛的应用.

4 资产流通

数字资产是指以电子形式存在且具有经济价值的资产, 如数字货币、游戏物品和电子礼品卡等. 这些资产的价值源自其实用性或稀缺性, 通常作为权益、身份或资产证明的载体. 在去中心化金融 (decentralized finance, DeFi) 中, 任何个体都可以创建独立的数字钱包、持有并交易数字资产, 用户能够在不依赖于中央金融机构的情况下实现融资、借贷、保险、交易等活动.

而随着 Web 3.0 的兴起, 数字资产的范畴已不再局限于传统形式, 而是扩展到了更多元的模态, 包括文本、图片、音频、视频以及神经网络模型. 此类新型数字资产可借助区块链和智能合约技术, 实现唯一性和所有权的加密保护和公开验证, 进而增加它们作为资产的价值和可交易性. 然而, 当前数字资产的确权、鉴权和流通方面还存在许多挑战和不足. 多模态数字资产 (如代币、非同质化代币、链上权益证明等) 的跨应用流通面临价值评估、鉴权确权与交易效率等多重挑战. 例如, 如何在去中心化的条件下实现资产所有权的可验证、可追溯、可审计, 以及如何高效而安全地进行资产鉴权和交易等, 解决这些问题将对推动 Web 3.0 环境下数字资产的健康发展起到关键作用. 本节将从 Web 3.0 的角度对数字资产确权、鉴权及流通这 3 方面进行详细讨论.

4.1 Web 3.0 数字资产确权

4.1.1 非同质化代币

非同质化代币 (non-fungible token, NFT) 是具有唯一标识符的数字代币, 能够与特定的链上地址相关联, 表示一个独特且不可代替的资产, 用于图像、音频、视频或其他艺术藏品的所有权证明. NFT 通常包含特定的属性或信息, 如元数据、签名信息或版权信息等, 并且其所有权和交易历史都是公开透明的, 为数字资产的价值和真实性提供了可验证的技术手段, 具有不可篡改性、可验证性、交易透明性、互操作性与持久性等特点. NFT 交易体系和交互组件如图 4 所示.

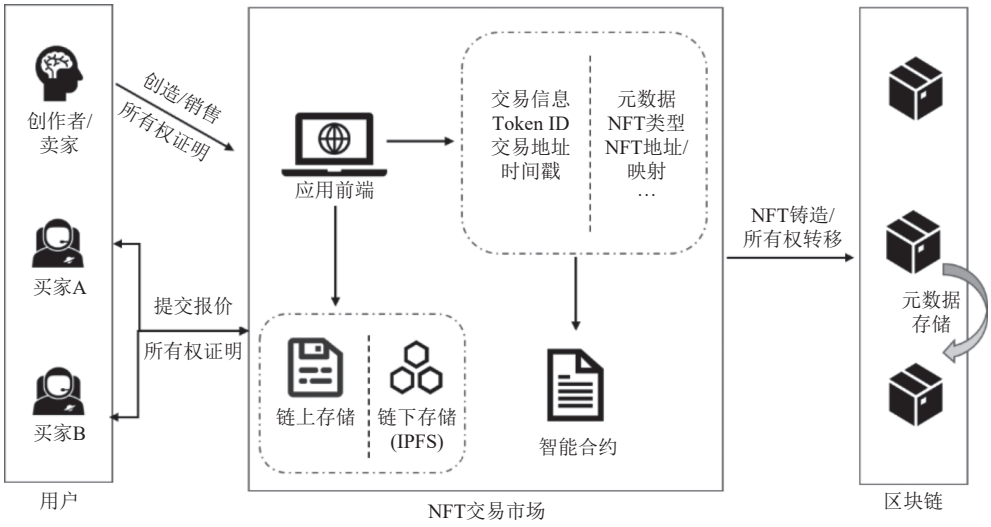

图 4 NFT 生态系统

用户: 用户是 NFT 生态中的核心参与者, 具体可分为创作者、买家和卖家. 创作者创建数字内容并生成唯一的数字标识符, 后续便可由卖家在平台或交易市场进行出售, 而买家则可以通过报价拍卖的形式购买相应 NFT,

其中卖家的身份为原始创作者或上一任买家.

NFT 交易市场: NFT 交易市场是 NFT 创建、存储、交易的数字化交易平台, 为用户提供一个透明、可靠的交易环境, 通常由面向用户的应用前端和与区块链交互的交易合约所构成. 智能合约可按照其功能分为代币合约以及 NFT 交易合约, 其中代币合约负责 NFT 的创建、转移及销毁, NFT 交易合约可处理平台中用户买卖的交易行为. 用户在平台内通过应用前端发起交易后, 由智能合约负责具体交易逻辑.

4.1.2 代币合约规范

代币在区块链和加密货币领域是一个代表资产或特定用途的数字单位, 不同的标准定义了智能合约及其发行代币所具有的不同功能.

ERC-721[33]是以太坊上的一种 NFT 标准, 为 NFT 提供了一个标准化的方式来追踪所有权、授权和转移, 从而允许开发者在应用或平台间实现 NFT 的交互. ERC-721 为 NFT 提供了互操作性, 并具有可扩展性, 为数字资产的交易和确权提供了标准化的框架. ERC-20[34]是当前以太坊上使用最广泛的 FT 标准, 通过定义一组通用接口, 使得每个代币与另一个代币具有完全相同的类型和价值属性. ERC-1155 是一种多代币标准, 扩展了同质化代币和非同质化代币的表现形式. 前述两个标准只允许实现单一类型的代币, 例如, ERC-721 可将一组 NFT 部署在具有相同配置的独立合约中, 而 ERC-1155[35]定义每个代币标识符都可以独立表示一种可配置代币类型, 允许在一个合约中创建和管理多种代币类型, 减少存储和交易成本. 此外, ERC-1155 提供了批量交易模式, 当进行大量的小额交易时, 可显著提高运行效率.

除上述标准以外, 还有 ERC-998[36]、ERC-3525[37]、ERC-2981[38]等标准, 它们在特定场景下都提供了有价值的功能和特性. ERC-998 是一种可组合的非同质化代币标准, 使得 NFT 可以“拥有”其他代币. ERC-3525 定义了半同质化代币 (semi-fungible token, SFT), 以解决代币分割问题, 从而满足部分 Web 3.0 金融场景的需求. ERC-2981 则是一个 NFT 版税标准.

在当前 Web 3.0 的数字资产确权领域, 不同的 ERC 标准为具体应用场景提供了不断演进的解决方案. 例如, 标准的 ERC-721 虽然保障了 NFT 的唯一性, 但在用户批量“铸造 (mint)”时, 其交易成本会随着 NFT 数量线性增长, 产生高昂的 Gas 费. 为解决此局限性, 业界在实践中推出了优化的 ERC-721A 标准, 并被 BAYC (Bored Ape Yacht Club)[39]等知名项目采用. 其核心技术优势在于, 通过优化数据存储方式, 使得在单次交易中铸造多个 NFT 的 Gas 成本几乎与铸造单个 NFT 相当, 极大地降低了用户的参与门槛, 提升了大型项目发行的效率.

另一方面, ERC-1155 标准则在游戏和元宇宙等场景中展现了巨大优势. 以知名元宇宙游戏 The Sandbox[40]为例, 其生态内存在土地、虚拟形象、装备等成百上千种资产. 若为每一种资产都部署独立的 ERC-721 合约, 将导致合约管理极为繁琐且交互成本高昂. 通过采用 ERC-1155, The Sandbox 可在一个智能合约内同时管理所有同质化 (如游戏金币) 与非同质化 (如特定装备) 的资产, 显著提升了其复杂经济系统的运行效率和可扩展性. 这些案例表明, Web 3.0 的资产确权方案正根据实际应用痛点不断演进. 尽管如此, 这些标准仍普遍面临交易成本高昂、合约日益复杂等问题.

4.2 数字资产鉴权

近年来, NFT 市场价值的爆炸式增长, 诈骗者也随之增加, 不断通过复制他人作品, 并重新创作为 NFT 流入市场进行交易, 从而获利, 扰乱市场秩序. 为此, 如何构建有效的 Web 3.0 数字资产鉴权机制成为当前亟待解决的问题.

NFT 具有两种鉴权方式, 一种是通过 NFT 身份验证来验证 NFT 有效性与合法性, 例如, 通过区块链的应用前端检查交易信息、钱包信息及 NFT 数据, 以此来确定 NFT 的所有权和来源; 或者验证 NFT 的数字证书, 包括 NFT 的标识符、创作者签名等, 然而并不是所有的 NFT 都拥有数字证书. 另一种是通过内容匹配的方式进行鉴权, 以此来确认当前所交易内容不是从先前的 NFT 中复制或伪造的. 接下来将重点介绍基于内容匹配的鉴权方法, 根据模态的不同, 其内容匹配方式也不一样, 包含文本、图像、音频、视频与模型这 5 种模态, 主要技术特点如表 4 所示.

表 4 多模态鉴权技术对比

模态	方案	主要技术	主要难点	技术特点	当前问题	计算开销	应用场景
文本[41]	TF-IDF[42–44]、PLM[45–47]	自然语言处理、文本相似度算法	语义理解、词汇匹配	侧重语义分析与文本结构	语境理解、特定条件下的文本检索能力	TF-IDF: 低 PLM: 高	TF-IDF: 链上文本内容初步关键词过滤 PLM: AIGC文本内容的原创性检测、去中心化社交平台内容查重
图像	CBIR[48]、图像哈希[49,50]、基于深度学习的图像匹配[51,52]	传统相似度计算算法、深度学习	图像识别、特征提取与匹配	侧重图像的直接视觉表征与模式识别	传统方法场景限制多、深度学习方法资源消耗大	传统方法: 低 深度学习: 高	传统方法: 用于NFT交易平台对图像的快速筛查 深度学习: 用于更精确的侵权检测、NFT内容推荐与系列聚类
音频	Shazam[53]、音频指纹[54]、感知哈希[55]、基于深度学习的音频匹配[56,57]	频谱分析、深度学习	音频指纹提取、噪声处理	侧重音频波形和频率特性	噪声干扰、语言与口音的多样性	音频指纹/哈希: 低 深度学习: 高	指纹/哈希: 音乐NFT的版权识别 深度学习: AIGC生成音乐的原创性分析、音乐NFT的风格分类与推荐
视频	NDVR[58]、TCA[59]、SPD[60]	视频内容识别、深度学习	视频内容匹配、视频段定位	结合视觉与音频处理技术	视频匹配精度、数据集较少	高	视频NFT的盗用检测、去中心化视频平台的内容溯源与侵权识别
模型	ModelDiff[61]、基于样本相关的模型检测[62]、感知哈希[63]	深度学习、神经网络分析	模型性能评估	侧重算法性能与模型输出	模型相似度评价标准	基于样本: 高 感知哈希: 中	AI模型NFT的所有权验证、去中心化模型市场中的模型窃取检测

4.2.1 文 本

文本内容匹配是指通过分析文本数据中的模式、词汇和语义, 将输入文本与相关的信息资源 (如文档或网页等) 相匹配的过程[41]. 在早期的工作中, 研究者将文档和输入文本表示为稀疏的术语向量, 为了构造稀疏向量表示, 设计了多种术语加权方法, 如词频-逆文档频率 (term frequency-inverse document frequency, TF-IDF)[42–44], 可根据稀疏查询与文本向量间的词汇相似度来估计相关度. 随着自然语言处理技术等的发展, 相关学者基于 Transformer[64] 及其变体提出了预训练语言模型 (pretrained language model, PLM)[45–47].

总体而言, 文本检索的关键在于如何学习文本表示并对相关匹配进行建模. 尽管现阶段稠密检索在几个标准数据集上具有不错的性能表现, 但在零样本检索等特定条件下的能力受限. 此外, 虽然稠密检索在语义匹配方面展现出强大的能力, 但相比之下, 在处理词汇匹配任务时, 其表现不如稀疏检索模型, 因此如何将稠密检索模型与稀疏检索模型合理结合, 取长补短, 是未来需要解决的问题.

4.2.2 图 像

与文本内容匹配专注于抽象的概念理解不同, 图像匹配主要关注结构、色彩、纹理和形状等视觉要素的相似度, 侧重于图像的直接视觉表征和特征.

余弦相似度是一种常用的计算向量之间相似度的方法, 将图像转换为特征向量并通过计算向量间夹角的余弦值, 从而得到图像相似度[48]. 哈希算法[49]同样被广泛应用于图像相似度计算, 通过将图像转换为固定长度的哈希值, 实现图像的相似度比较和检索[50], 具体可分为平均哈希算法 (average hash, aHash)、感知哈希算法 (perceptual hash, pHash) 与差异哈希算法 (difference hash, dHash). 直方图算法通过统计图像中不同颜色的像素数量计算图像之间的相似度. 近年来, 深度学习在图像匹配领域的应用越来越广泛[51,52].

这些技术在 Web 3.0 最核心的应用场景——NFT 市场中, 用于解决版权问题. 例如, 当用户在 OpenSea 等主流平台上传并铸造 NFT 时, 平台后台通常采用 pHash 算法, 计算图像指纹并与海量现有 NFT 数据库进行比对, 从而实现自动化的侵权检测.

然而, 这种试图用中心化的方法解决去中心化问题的模式, 在实践中也存在局限性. 首先, Web 3.0 无需许可的特性允许任何人创造和发行资产, 平台难以像 Web 2.0 一样进行有效审核. 其次, pHash 等算法在对抗性环境下鲁

棒性有限. 侵权者无需高深技术, 仅需对原创作品进行镜像翻转、增加微小噪点、裁剪或添加边框等简单操作, 就能生成一个不同的哈希值, 从而绕过检测机制. 这导致平台陷入两难困境: 若放宽检测阈值, 则会误判大量风格相似的原创作品; 若收紧阈值, 则会出现大量经过微小修改的抄袭品充斥市场, 严重损害用户权益. 这也体现了现有鉴权技术在 Web 3.0 开放环境下的应用瓶颈. 综上所述, 图像匹配方面的研究工作已经取得了较大的进展, 不同的相似度计算方法展现出各自的优势, 基于机器学习的图像匹配方法具有更好的泛化能力, 且能够理解图片间的语义差距, 而感知哈希则可用于审计, 相较于 AI 分类器, 也具有更强的针对性, 然而感知哈希无法应对简单的几何变换, 通过将原始图像进行旋转、翻转等操作后将会产生截然不同的哈希值, 能够轻易绕过检测算法. 基于机器学习的图像匹配方法更加倾向于使用深度神经网络, 而大规模的图像数据用于监督训练是一项困难且耗时的任务, 因此是否能够在无监督模式下进行性能评估是未来可能的研究方向.

4.2.3 音　频

音频作为一种能够存储和交易数字资产, 由于包含节奏、旋律、和声等独特的内在特征, 前述用于文本与图片等的鉴权方法无法适用于音频模态.

音频指纹作为音频信号的压缩特征, 能够区分不同内容的音频, 因此也可用于音频版权检测领域. 例如, 通过提取音频信号的频谱峰值[53]、将 SIFT 迁移到音频频谱图像[54]、感知哈希[55]等方法分析音频的内在特性, 如节奏、旋律、和声等, 确定不同音频间的相似性. 随着深度学习技术的发展, 越来越多的研究者开始利用神经网络进行音频侵权检测[56,57].

当前音频匹配在众多领域内展现了其潜在的重要性和实用价值, 如侵权检测、听歌识曲、音频定位等. 然而现有工作缺乏对噪声音频的有限评估, 攻击者可通过引入真实世界的噪声来欺骗检测器. 此外, 现有工作对于人声匹配讨论较少, 对除英语以外的具有不同发音特点的其他语言少有研究, 而不同口音对于音频匹配的影响也值得进一步深入研究.

4.2.4 视　频

针对视频模态, 同样可依靠视频指纹和哈希值比对技术来判断视频是否相同或相似, 在此节就不再详细讨论. 接下来将详细介绍部分视频检测技术.

Kordopatis-Zilos 等人[58]提出了一种基于深度度量学习的高效视频级近似视频检索 (near-duplicate video retrieval, NDVR) 方案. 此外, Kordopatis-Zilos 等人[65]还提出了一种视频相似性识别架构, 考虑视频间的细粒度时空关系. Shao 等人[59]通过自注意力机制将帧级特征之间的时间信息融合到视频检索中, 捕捉了视频间的细粒度时空关联. Jiang 等人[60]提出的 SPD 将时间对齐问题视作在帧对帧相似度矩阵上的对象检测任务, 有效地实现了段级别的复制内容检测.

然而, 当前的研究中仍然存在着一些瓶颈问题, 例如, 视频相似段定位不清晰、视频相似度评价指标缺乏段粒度的精确性和敏感性、目前缺少大规模公开视频数据集用以训练, 因此, 如何解决这些问题将成为未来的主要研究方向.

4.2.5 模　型

随着深度学习广泛应用于各类任务, 并且由于从零开始构建一个准确高效的大模型需要极高的成本, 用户可将其视作数字资产进行交易, 因此逐渐出现窃取用户模型的行为, 模型鉴权变成亟待解决的问题.

Li 等人[61]提出了一种基于测试的深度学习模型相似度比较方法, 将模型的行为模式表示为决策距离向量, 对比模型在同一组测试输入上的行为模式, 从而评估模型间的相似度. Guan 等人[62]提出了一种基于样本相关性的模型窃取检测方法, 选择错误分类的样本作为模型输入, 计算模型输出之间的平均相关性. Chen 等人[63]将感知哈希引入到模型相似度检测中, 将 CNN 的权重转换为固定长度的二进制哈希值, 通过比较目标模型与原模型之间的哈希值得到模型相似度.

可见, 模型窃取攻击引起了研究者对模型所有权的关注, 当前的研究工作已经取得了在模型知识产权方面的一些进展, 未来可将研究重点放在如何在保证模型效用的前提下添加有效的模型水印、如何使得当前相似度计算方法面对多样化和复杂的攻击场景, 以及设计多维度模型相似度评价标准上.

4.2.6 总 结

综上所述, 数字资产鉴权是 Web 3.0 的重要组成部分, 安全高效的鉴权方法能够保障创作者和持有者的合法权益. 然而, 当前主流的鉴权技术在实际应用中仍面临严峻挑战. 正如前文在图像鉴权部分所分析的, 即便如 OpenSea 等 NFT 市场采用了感知哈希等内容匹配技术来解决版权问题, 其效果也相当有限. 侵权者仅需对作品进行简单的镜像翻转或微小裁剪, 即可绕过检测, 这暴露了现有技术在 Web 3.0 开放环境下的普遍脆弱性. 当前数字资产鉴权领域在技术层面仍然存在着如下几个重要问题有待解决.

(1) 当前 Web 3.0 数字资产的内容相似性匹配机制仅针对单一模态, 缺乏处理多模态数据的能力, 这限制了其在应对高度复杂、多样化的数字版权验证需求方面的效能.

(2) NFT 同一系列中的内容由于风格和设计元素高度一致, 导致其相似度普遍较高, 使得利用传统的相似度计算方法难以有效区分同一系列内的合法作品和侵权复制品, 这将严重威胁到 NFT 创作者的版权和收益. 因此, 需要更精细化的分析工具来识别和区分这些作品的差异.

(3) 攻击者针对链下存储的 NFT, 通过复制 URI 或 Json 元数据中的 URL, 并重新铸造 NFT 存储在区块链上, 以此实现侵权攻击. 此攻击行为可以有效绕过数字资产内容匹配算法, 并利用区块链的不可篡改性来永久保存这些未授权的副本, 这不仅导致版权和知识产权的严重侵犯, 而且还可能导致数字资产市场价值的严重波动.

(4) 当前 Web 3.0 在交易后不为买方提供任何保护措施, 缺乏交易完整性的有效保证机制, 无法实现可信交付. 攻击者可通过撤销或修改指向链下存储 NFT 的链接, 轻易删除或替换现有的数字资产.

4.3 数字资产流通

数字资产的价值不仅体现在数字化特性上, 还包含相应的市场流通机制与使用方式. 去中心化交易所 (decentralized exchanges, DEX) 在流通过程中扮演了关键的角色, 允许用户在无中介机构的情况下完成交易, 通过智能合约执行买卖订单, 确保交易的透明度和安全性.

4.3.1 自动做市商

自动做市商 (automated market maker, AMM) 是一种基于区块链的 DEX 机制, 与传统订单簿不同, 其通过一个预设的价格策略来计算买卖价格, 并利用智能合约创建流动性池来自动执行交易, AMM 的基本结构和流程如图 5 所示.

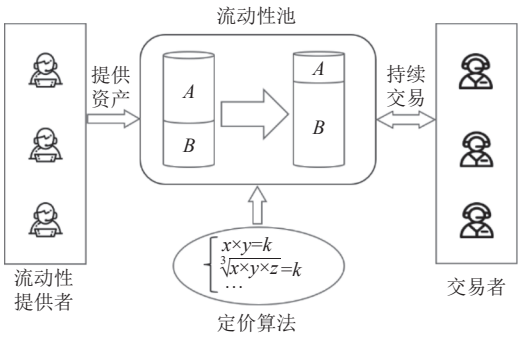

图 5 AMM 基本结构与流程

流动性池 (liquidity pool): 是用户锁定资产以提供市场流动性的智能合约, 允许资产之间的交换, 为交易者提供了买入和卖出资产的场所.

流动性提供者 (liquidity provider, LP): 将自有资产按比例存入流动性池中为交易提供流动性, 并以一部分交易费用作为回报.

交易用户 (trader): 通过指定输入和输出资产以及资产数量向流动性池提交交易订单, 智能合约根据守恒函数自动计算汇率和交易费用, 并执行相应的交易订单. 值得一提的是, 交易用户中存在部分套利者, 当 AMM 中的价格与外部市场存在差异时, 他们会进行交易以获利.

价格算法: 用于确定池中资产的相对价值, 实现动态定价.

AMM 具有以下几种常见模型[66].

● 恒定乘积做市商 (constant product market maker, CPMM): CPMM 是基于函数 $x\times y=k$, x 和 y 分别代表流动池中两种资产的数量, 其乘积为一常数 k, 当资产 x 的供给增加时, y 的供给数量则减少, 反之亦然. 然而, 当价格变动越大时, x 或 y 则会接近无穷大.

● 恒定和做市商 (constant sum market maker, CSMM): CSMM 是基于函数 $x+y=k$, 其是零滑点交易的理想选择, 但不能提供无限流动性, 若资产参考价格比不是 1:1, 则可能耗尽其中一种资产, 摧毁流动性.

● 恒定均值做市商 (constant mean market maker, CMMM): CMMM 可以创建具有两种以上资产的 AMM, 在标准的 50:50 分布之外加权, 每个资产的加权几何平均值保持不变. 例如, 对于 3 种等权资产组合来说其函数为 $\sqrt[3]{x\times y\times z}=k$.

● 恒定函数做市商 (constant function market maker, CFMM): CFMM 结合了多种功能和参数, 以实现特定行为, 如减少交易者的价格滑点, 从而创造更好的流动性.

在以上 AMM 模型中, 当前普及性较高的是 CPMM 做市模式. 与传统做市模式相比, AMM 的自动化模式简化了做市操作, 在去中心化的背景下其被操控风险较小, 可便捷地提供流动性, 且任何用户可以以任何资金量进行参与, 而流动性挖矿奖励也可激励用户提供流动性, 形成闭环.

DEX 的快速发展不仅源于其交易机制的创新, 也依赖其激励机制的演进. 除了交易手续费这一基础激励, 为解决 DEX 启动初期的冷启动问题, 流动性挖矿 (liquidity mining) 机制被引入, 其核心在于, LP 不仅能分得交易手续费, 还能额外获得 DEX 协议发行的治理代币. 这一模式有效激发用户参与的热情, 成功为众多 DEX 在短时间内吸引数十亿美元的流动性, 并实现了协议治理权的去中心化分配. 然而, 这种高强度的代币补贴也导致大量追逐短期收益的雇佣兵资本 (mercenary capital), 可能导致代币抛压过大和经济模型的不可持续性, 如何设计更稳定的激励机制, 是当前 DEX 的重要议题.

4.3.2 订单簿

订单簿 (Order Book) 是一种在数字资产流通中常见的交易机制, 提供实时动态的市场快照, 按照价格排序记录了市场上所有未成交的买入和卖出订单. Order Book 为用户提供一种直观的方式来查看当前市场的供求状况, 不仅显示了当前的市场价格, 也反映了用户对于特定资产的价格预期, 其示意图如图 6 所示.

Bid

Price (USDT)	Amount	Sum
49.72	0.200	4.570
49.55	0.751	4.371
…	…	…
46.63	2.315	4.319

Ask

Price (USDT)	Amount	Sum
50.05	0.303	0.246
51.31	0.796	0.086
…	…	…
51.63	0.226	2.580

Market trades

Time	Price (USDT)	Amount
20:43:19	46.63	0.133
20:43:15	47.00	0.909
20:43:14	46.85	0.008
20:43:05	45.69	0.792
20:42:58	48.01	0.284
20:42:48	49.64	0.300
20:42:13	48.53	0.442
20:42:01	49.21	0.391
…	…	…
20:40:32	50.01	0.050

图 6 Order Book 示意图

Order Book 主要由买单 (Bid) 和卖单 (Ask) 两部分组成. Bid 代表交易者购买特定资产的意愿, 包括买家愿意购买的价格和数量. Bid 中通常表明了对不同价格的资产的需求, 交易者可通过分析 Bid, 来确定当前市场需求并分析购入资产的时机. Ask 则代表交易者出售其数字资产的意愿, 交易者同样可通过分析 Ask 来确定卖出资产时机.

交易订单可按类型分为限价单和市价单. 限价单允许交易者指定他们愿意买入或卖出资产的具体价格, 在限价单中交易者可以控制交易价格, 若市场价格没有达到指定的限价, 订单不会被执行. 市价单则是以当前市场上可得到的最佳价格立即执行的订单, 市价单通常会在订单发布时立即执行, 但无法保证成交价格, 尤其在市场波动性

大的时候. 当一个新的 Bid 或 Ask 被提交到 Order Book 时, 交易系统会立即检查是否有相符的订单可以匹配, 若找到匹配订单, 交易会被立即执行.

Order Book 的透明性和实时性使得交易者能够清晰地查看市场供求状况. 然而, 在区块链上通过 Order Book 模式交易数字资产也存在着一些问题, 首先, 由于这种模式下每个操作都需要与链上交互, 大量的交易订单会产生极大延迟, 可能导致处理时间较长或交易拥堵. 此外, 在如以太坊的区块链上进行交易, 需要额外支付 Gas, 导致频繁更新交易或订单的成本较高.

订单簿与前述的 AMM 共同构成了当前数字资产交易的两种主流范式. 两者之间的区别在于, 是针对不同应用场景和技术约束下的平衡, 其并存的深层原因在于两者在流动性模式、资本效率和风险模型上存在本质区别.

首先, 在流动性供给上, 订单簿依赖专业做市商提供流动性, 成本高昂且难以覆盖海量的长尾资产. 而 AMM 通过“无需许可”的模式, 极大地降低了做市门槛, 允许任何用户为新兴的长尾资产池注入流动性, 这正是 DeFi 生态普遍采用 AMM 以激活海量多样化资产的根本原因. 其次, 在资本效率与风险上, 订单簿将资本高度集中于当前市价, 能以极高的资本效率处理大宗交易并维持低交易滑点, 但其在中心化交易所 (CEX) 中的主要风险是用户需承担平台方的对手方风险. 相反, 传统 AMM 的资本效率低下, 易产生高滑点, 且流动性提供者 (LP) 需承担价格波动带来的无常损失这一特有风险. 因此, 两者的选择实质上是一种权衡: 订单簿追求交易效率, 而 AMM 则优先保证了流动性的去中心化和可及性.

4.3.3 拍卖机制

随着 Web 3.0 中 NFT 及其他数字资产的兴起, 其价值往往受到创作者声誉、艺术价值、稀缺性以及社区需求等多种因素的影响, 意味着价格难以通过传统定价机制来确定, 因此拍卖机制成为 Web 3.0 中的一种理想解决方案. 2018 年 Andy Warhol 的艺术品在世界上首次被代币化, 并在以太坊上成功拍卖[67].

拍卖机制可按照拍品数量分为单品拍卖和多品拍卖. 其中单品拍卖专注于某单一资产的出售, 主要包括英式拍卖、荷兰式拍卖等[68–70], 而多品拍卖则涉及同时对多个资产进行拍卖, 可分为组合拍卖和多物品拍卖. 当前拍卖机制被各类 NFT 交易平台广泛使用, 不同的拍卖机制对比如表 5 所示.

表 5 拍卖机制对比

拍卖类别	拍卖模式	定义	特点	缺点	场景	复杂性	参与者体验	时间效率	费用	监管要求
单品拍卖	英式拍卖	价格逐渐升高、价高者胜	透明、竞争性出价	时间长	艺术品、房地产、加密货币	中等	高互动	中	低	中
	荷兰式拍卖	价格逐渐降低、快速决策先接受价格者胜	急售、加密货币发行	价格不一定最大化	农产品、鲜花、加密货币	低	简单直接	高	低	低
	传统封闭式拍卖	密封出价、价高者胜	出价保密、一次性出价	竞标者风险	国债、频谱、加密货币	低	保密性高	中	低	高
	高价密封拍卖	密封出价、价高者胜、并支付第2高的出价	鼓励真实出价、高效且公平	算法复杂	高价值资产、加密货币	高	复杂但公平	低	高	高
多品拍卖	组合拍卖	参与者对不同物品组合出价	高效率、评估和出价策略复杂	算法复杂, 计算量大	频谱、运输、加密货币	高	复杂但灵活	中	高	高
	多物品拍卖	同时拍卖多个或可互换的物品	适合分配大量相似商品	复杂性高, 成本高	公共资源、广告位、加密货币	高	复杂但灵活	中	高	高

在单品拍卖中, 英式拍卖和荷兰式拍卖是当前 Web 3.0 中最常见的拍卖模式, 主要适用于各类实体物品以及 NFT 和各类数字资产. 英式拍卖从较低的起拍价开始, 买家相互竞价, 直到在规定时间内没有更高的出价. 英式拍卖的竞价过程是公开透明的, 过程简单, 但时间较长, 费用较高, 需要一定的公平性监管. 荷兰式拍卖起始价格高, 价格逐渐下降, 直到买家愿意接受该价格. 荷兰式拍卖促使买家迅速决策, 时间效率高, 复杂性较低, 监管要求较松. 除 NFT 市场外, 其也适用于急售数字商品、加密货币发行以及各类实体物品, 由于买家和社区之间缺乏足够的信息, 荷兰式拍卖可能会导致不适当的出价. 传统封闭式拍卖也称为盲拍, 所有买家秘密地提交一次出价, 在截

止时间过后, 出价最高者即可获胜. 每位参与者只能提交一次出价, 所以需要独立评估资产价值. 此模式可以有效限制竞争对手故意抬价, 同时避免引起其他富有买家的不必要的关注. 高价密封 (Vickrey) 拍卖与传统封闭式拍卖类似, 但采用不同的支付机制. Vickrey 拍卖中, 当所有买家向拍卖师秘密提交竞价后, 出价最高者获胜, 但只需支付第 2 高的出价, 鼓励买家诚实出价[71]. 与其他拍卖形式相比, Vickrey 拍卖简化了出价策略, 监管要求相对严格, 最优策略即为出价等于个人对资产的真实估值. 由于降低了竞价风险, Vickrey 拍卖通常被认为是更有效率和公平的拍卖机制.

在多品拍卖中, 组合拍卖允许买家对一组数字资产的各种组合出价, 可以更有效地匹配需求和资产组合. 买家需要评估不同组合的价值, 并决定对哪些组合出价. 与传统拍卖相比, 组合拍卖涉及多个相关物品, 竞价复杂, 费用和监管要求高, 但提供灵活的资源配置. 然而组合拍卖在机制设计方面存在一些挑战, 如在多种组合下如何确定赢家. 而多物品拍卖是指拍卖品是多个相同或相似的物品, 这种拍卖方式允许买家针对所需的物品数量提出报价, 既可以固定价格拍卖, 也可以根据所需求数量确定最终价格, 买家体验较为直观灵活. 买家的需求量可能因价格变动而有所调整, 这种拍卖形式旨在根据价格变化和市场需求, 高效分配大量的相同或类似商品.

总体而言, 本节所探讨的跨应用、多模态数字资产流通机制, 不仅实现了以 NFT 为代表的原生资产在不同平台和应用间的安全、透明、高效交换, 还通过可信鉴权降低了交易风险. 该机制为数据资产化中的“流通”环节提供了关键技术支撑, 使数字资产能够在保持价值真实性和权属明确的前提下, 实现大规模流转.

在此基础上, 目前 Web 3.0 资产流通的边界正被迅速拓宽, 其前沿发展尤其体现在与真实世界资产 (real-world asset, RWA) 和稳定币这两大创新模式上, 进一步推动着数字经济生态的高效运转.

RWA 通过将房地产、美国国债等传统金融资产代币化, 搭建了链接 TradFi 与 DeFi 的桥梁, 为 Web 3.0 引入了海量的链下价值和更可持续的收益来源. 例如, MakerDAO 已开始接受 RWA 作为抵押品, 而 Ondo Finance 等项目则将美国国债搬上链, 极大地扩展了数字资产的类别与应用场景.

与此同时, 稳定币 (如 USDC、USDT) 则为这些日益丰富的链上资产提供了可靠的计价单位和交易媒介. 它们通过法币抵押或加密资产超额抵押等不同运作机理维持价格稳定, 构成了整个 DeFi 生态的“血液”, 是实现资产高效流转不可或缺的金融基础设施. 虽然算法稳定币 (如 Terra/UST) 的失败暴露了其内在风险, 但也推动了业界对更稳健的去中心化货币模式的探索.

综上, 从原生数字资产的流通, 到 RWA 的价值引入, 再到稳定币的底层支撑, 一个更多元、更稳健的 Web 3.0 数字经济生态正在形成.

5 生态治理

生态治理是数据资产化可持续发展的保障环节, 涉及数据使用规则制定、价值分配以及参与方行为规范. Web 3.0 生态治理层是指刻画用户在数据要素流通和社会治理中的行为画像, 建立 Web 3.0 用户的良性自演化声誉评价方法, 通过设计合理的用户权益激励机制来激励用户参与和维护数字资产安全高效地流通, 探索出 Web 3.0 中用户共建共治共享生态的良性演化规律, 进而实现用户共建共治的生态治理机制.

5.1 Web 3.0 声誉机制

各界对于声誉的定义一直存在着分歧, 牛津英语词典中将声誉定义为公众对某人或某物的总体评价, Mayhew 等人[72]则将声誉定义为个体或组织历史行为的表现, 而经济学研究者借助博弈论研究声誉. 声誉是随着个体的历史行为而积累产生的, 可以有效地反映实体在社会中的信用度.

通常, 声誉机制具有以下几种属性: 1) 活性: 用户的恶意行为始终会损害用户声誉, 即不存在声誉最低值; 2) 可见性: 声誉得分的可见性分全局和局部可见, 全局可见时所有节点均可查看实体的声誉, 而局部可见时节点子集可用的声誉评分可能与系统中其他地方的不同; 3) 持久性: 实体计算出声誉分, 并可将其永久存储以供节点访问, 仅当有新的反馈可用时才强制重新计算分数; 或声誉分数是暂时的, 但每次节点希望了解分数时都会重新计算.

Eigen Trust 是经典的 P2P 网络场景下的声誉评价算法, 通过加权迭代过程, 利用节点之间的局部信任值传递

和汇总, 最终得到每个节点的全局信任值; Peer Trust 更侧重于局部的信任的简历, 不依赖全部的信任计算, 具有较高的计算效率. 也可以使用深度学习和机器学习, 聚合链上交易数据和的链下数据, 计算更为全面, 多维的声誉值. 常见各类声誉评价算法对比如表 6 所示. 总的来说, 不同声誉算法在性能与适用性上差异显著. 如 Eigen Trust 与 Peer Trust 更适合去中心化网络的全局与局部信任计算, Page Rank 则依赖中心化架构但在排名稳定性上表现优异; 协同过滤虽在个性化推荐中效果突出, 但抗攻击性较弱; Assess Trust 与 COBRA 则在抗攻击与隐私保护方面表现突出, 尤其是 COBRA 结合神经网络可处理复杂特征, 但计算开销较大.

表 6　常见各类声誉评价算法对比

声誉算法	算法类型	数据来源	评价对象	计算方式	抗攻击性	计算复杂度	可扩展性	隐私保护能力	适用场景
Eigen Trust	去中心化	交易历史行为	P2P网络节点	加权迭代	抗女巫攻击	中	高	弱	P2P网络
Peer Trust			去中心化网络节点		抗女巫攻击	高	高	弱	大规模分布式系统
Page Rank	中心化	网页数据、链接结构	网页排名	加权迭代	抗垃圾链接攻击、抗女巫攻击	高	高	弱	Web 2.0网页
协同过滤		交易历史、评分反馈、用户属性	用户信誉	机器学习	无	中	中	弱	电商系统
Assess Trust		主观评分反馈	社交网络用户画像	递归分解	抗女巫攻击、抗垃圾攻击、抗信任注入攻击	中	中	弱	在线社交网络
COBRA		历史行为、评分反馈	代理系统、物联网设备	神经网络	抗隐私泄露分析	高	高	强	社交网络、物联网服务等

Web 3.0 中的声誉是指独立钱包或者 DID 的声誉, 进一步的, 可以是一个 DID 捆绑多链上的多个钱包和多种 SNS 账号. 当前阶段的发展目标是用户拥有数据所有权, 声誉凭证可以在网络上的各应用之间互通信息或价值. 当前平台上的声誉代币通常有两个用途: 1) 提供一种信号形式, 识别和奖励为平台贡献价值的用户, 从而提升公众声誉; 2) 提供一种补偿形式, 使贡献者能够将其创造的一些价值转化为可兑换可流通的金钱. 在目前的 Web 3.0 世界中, 用户链上活动数据将真实的映射出此用户的特征, 进而对应出该用户的链上声誉, 良好的声誉评价方法可以激励用户并约束用户的恶意行为. 链上声誉体系将在快速识别 Web 3.0 身份 DID 的信用以及特征中起到重要作用.

2022 年 5 月, Weyl 等人[73]首次提出了灵魂绑定通证 (soulbound token, SBT). 它具有可编程的、不可转让但可撤销与找回, 同时附带可验证信息的特点, 利用基于 SBT 的信用相关历史记录可以支持声誉的评价. 当前 Web 3.0 中链上用户的行为还没有具体且普适性的量化方式, SBT 的出现有助于建立链上用户声誉体系. Project Galaxy[74]是一个链上画像通用底层协议, 通过子图索引和钱包快照获取链上信息, 集成链下数据源获取链下信息从而建立用户交互数据库, 再以发放凭证的方式为每个地址打上标签, 从而实现明确、细分的用户画像标识.

在记录链上用户行为之后, 便需要通过参考用户行为为用户进行评分, 对用户信用形成量化的、长效的评价机制, 进而生成用户的链上声誉. Spectral[75]是一个开放的、可编程、可组合的链上声誉评分系统, 允许用户根据其链上交互活动获得链上信用评分, 推出了一个多资产信用风险预言机 (MACRO), 分析近 8 年的以太坊交易以及以太坊、Polygon 和 Avalanche 链上的去中心化金融事件构建信用评分模型, 对用户的借贷信誉进行评分. ARCx[76]是以太坊和 Polygon 上的一个去中心化流动性市场, 它通过使用 DeFi 信用评分在 DeFi 中提供去中心化借贷服务. ARCx 通过衡量和奖励高价值的借贷行为来提高 DeFi 借贷市场的效率. 它使用 DeFi 信用评分来持续分析链上行为并评估 DeFi 中每个钱包地址的信用风险. 表 7 汇总了 Web 3.0 生态中具有代表性的声誉机制项目, 涵盖了链上凭证聚合、去中心化社交协议、零知识隐私声誉、链上信用评分等不同技术路径. 这些机制在数据来源、信任构建方式、隐私保护能力以及适用场景方面存在显著差异. 例如, Gitcoin Passport 通过跨平台凭证聚合构建可组合的信任护照, 而 Sismo 则利用零知识证明实现了选择性披露的隐私声誉系统.

链上声誉由去中心化身份与去中心化社交的不断发展催生, 有助于构建 Web 3.0 丰富的身份内容与社交图谱. 但是目前的链上声誉项目较单一, 大多数项目还是主要停留在 DeFi 等去中心化金融上, 暂未形成基本的架构, 尚

未有一个较为全面可量化的 Web 3.0 声誉评价方法, 目前只是依据市场特定需求而建立; 同时针对用户的数据存储问题, 如何将大量的链上数据安全存储, 以及如何高效、安全地存储声誉相关数据并将链下数据充分利用, 为链上声誉构建提供依据. 这些问题在 Web 3.0 中仍未有效解决.

表 7　Web 3.0 声誉机制典型应用对比

机制名称	技术类型	主要功能	优点	缺点	典型应用场景
Gitcoin Passport	链上凭证聚合	收集用户链上/链下贡献凭证, 生成信任护照	跨平台可组合、透明	依赖外部数据源, 隐私风险	去中心化资助、DAO 参与
Lens Protocol	去中心化社交协议	将社交关系和内容绑定到链上 NFT	内容可迁移、抗审查	冷启动难、初始声誉导入不足	Web 3.0社交网络、内容创作
Sismo	零知识隐私声誉	选择性披露链上/链下声誉指标	隐私保护、可验证	生成与验证 ZK 证明成本高	隐私友好型 DAO、任务平台
Spectral	链上信用评分	基于链上交互生成信用分数和风险预言机	去中心化、可编程	场景主要集中在 DeFi	DeFi 借贷、信用市场
ARCx	DeFi 信用评分	基于交易行为计算借贷信誉	激励优质借贷、提高市场效率	对非金融行为覆盖不足	DeFi 借贷、资产管理

5.2　Web 3.0 激励机制

激励机制的研究不仅要探索合适的激励方式, 收益分配, 更重要的是通过不同激励方式解决各方参与者在最大化各自效用的同时, 实现集体利益最大化. Web 3.0 激励机制旨在鼓励用户参与生态建设与治理, 当前大部分项目方以代币作为主要的激励手段, 通过发行代币激励用户参与到项目中[77].

空投是 Web 3.0 中的一种典型营销方式, 通常是某个新的项目发布时, 项目方通过发行代币等来奖励参与该项目的用户, 从而达到吸引和激励用户的效果. Web 3.0 中许多著名项目, 如 Uniswap 和 Ethereum Name Service 平台都曾发起过空投奖励, 这两个平台的用户分别获得了数万美元的代币. 群智协同激励机制可以鼓励用户共同解决复杂问题, 比如众筹和众包项目, 这些机制可实现群体智慧的最大化. 其优点包括提高用户参与度和满意度, 但其可能的缺点为因激励设计不当而产生的参与质量不稳定问题. 分布式系统激励机制被用于鼓励分布式网络中的节点提供资源, 例如在点对点网络中分享文件存储空间或带宽. 这类机制有效地促进了资源共享和网络鲁棒性, 但可能需要不断地激励开销, 并且设计复杂的策略可能会减缓系统性能. 区块链激励机制在确保网络安全、促进链上活动和验证交易等方面发挥着核心作用.

这些机制通常在加密货币挖矿、DeFi 协议和 NFT 市场中见到, 它们提供了一个安全, 可预测和透明的激励框架. 尽管如此, 它们也受到了能耗高 (尤其是在工作量证明 (proof of work) 系统中) 和潜在的中心化风险 (比如财富集中) 的批评. 群智协同激励机制、分布式系统激励机制与区块链激励机制的优缺点如表 8 所示.

表 8　激励机制对比

类型	目的	方式	场景	关键技术	优点	缺点	IR	IC	IT	IF	SW	IA	IP	IS	SC	CC	BC
群智协同激励	贡献评分奖励	评分系统	众包平台	声誉系统	激励活跃参与	操纵评分可能性	√	×	√	×	√	×	×	√	√	中	√
	边际贡献激励	基于贡献的奖励	开源项目	权重分配算法	奖励实际贡献	测量困难	√	√	√	×	√	×	×	√	√	中	√
	动态声誉系统	声誉积分	协作研究	声誉评级算法	体现历史表现	建立难、易受主观影响	√	√	×	×	√	√	×	√	√	中	√
	等级制激励	级别升级系统	竞赛	级别划分算法	等级体现能力	激励单一化	√	×	√	√	√	×	×	√	√	中	√
	多阶段奖励	阶段性奖励发放	大型项目	任务管理系统	鼓励长期投入	需要细分管理	√	√	√	√	√	×	×	√	√	中	√
分布式系统激励	时效性奖励	反应速度奖励	实时数据处理	时间监控系统	提升效率	可能影响质量	√	√	√	×	√	√	×	√	√	中	√
	隐私保护奖励	隐私级别奖励	知识共享	隐私增强技术	保护参与者隐私	成本增加	√	√	√	√	√	×	√	√	√	高	√

表 8 激励机制对比 (续)

类型	目的	方式	场景	关键技术	优点	缺点	IR	IC	IT	IF	SW	IA	IP	IS	SC	CC	BC
分布式系统激励	合作稳定性奖励	长期合作奖励	数据联盟	合作关系管理系统	寻找长期伙伴	过度依赖特定参与者	√	√	√	√	√	√	×	√	√	中	√
区块链激励	工作量证明(PoW)奖励	密码难题解决奖励	加密货币挖矿	散列算法	安全性高	能源消耗大	√	×	√	×	√	×	×	√	×	高	×
	权益证明(PoS)奖励	持币时间奖励	加密货币交易	质押算法	能源消耗低	富者越富	√	√	√	√	√	√	×	√	√	中	√
	交易费用奖励	验证费用分配	分布式账本	交易验证算法	交易快速	费用波动	√	√	√	√	√	×	×	√	√	中	√
	代币空投	社区激励发放	项目营销	社区参与分析算法	社区拓展	效果可能短暂	√	√	√	×	√	×	×	√	√	低	√
	质押奖励	资金锁定奖励	网络治理	治理协议	提高网络安全	资金流动性受限	√	√	√	√	√	√	×	√	√	中	√

注: IR: individual rationality; IC: incentive compatibility; IT: incentive truthfulness; IF: incentive fairness; SW: social welfare maximization; IA: incentive automation; IP: incentive privacy; IS: incentive sustainability; SC: incentive scalability; CC: computational complexity; BC: backward compatibility

在 Web 3.0 中, 这些机制相辅相成, 提供了促进创新、资源共享和网络维护的经济动力. 群智协同促进了去中心化决策; 分布式系统激励保障了服务的去中心化运行; 而区块链激励通过加密激励机制提供了网络参与和安全的动力. 在这三者之间, 分布式系统和区块链的激励机制通常更为复杂和耗能, 而群智协同机制倾向于更容易启动和运行, 但可能面临质量控制的挑战. 区块链激励提供了高度可预测和安全的网络环境, 但它们的能耗和潜在的不平等问题仍然是重大挑战. 相对而言, 分布式系统的激励通常设计得较为简单和降低能耗, 但需要持续的激励才能保持住系统的参与度. 表 9 展示了 Web 3.0 中多种典型激励机制的技术类型、运行逻辑与应用场景, 涵盖流动性激励、一次性空投、存储挖矿、任务激励平台以及质押安全机制等模式. 这些机制在启动网络效应、维持用户活跃度和保障系统安全等方面发挥着重要作用. 例如, Uniswap V3 的流动性激励将奖励直接与交易行为绑定, 有效提升了资金利用率; 而 Filecoin 通过存储挖矿实现了可持续的资源供给. 但不同模式也面临特定挑战, 如 ENS 空投激励难以保持长期活力, RabbitHole 任务激励易被低质量参与稀释效果.

表 9 Web 3.0 激励机制典型应用对比

机制名称	技术类型	主要功能	优点	缺点	典型应用场景
Uniswap V3	流动性激励	交易手续费、代币分发	激励与行为绑定	收益受市场波动影响	去中心化交易所
ENS Airdrop	一次性代币空投	奖励早期注册用户, 启动治理	激励早期参与	长期激励不足	去中心化域名系统
Filecoin	存储挖矿	提供存储空间获得奖励	可持续市场机制	初期质押成本高	分布式存储网络
RabbitHole	任务激励平台	完成链上任务获得 NFT/代币	灵活可扩展	易被刷任务	Web 3.0教育、用户引导
Aave Safety Module	质押激励	质押代币提供安全保障	提高安全性、流动性奖励	质押资金流动性受限	DeFi 借贷安全机制

目前 Web 3.0 中激励形式还主要局限于加密货币、代币等激励形式, 以代币为核心的激励方式在用户积极参与的网络环境中可能难以克服“冷启动”等问题, 因此, 需要研究更多元化且适合 Web 3.0 下的激励形式, 如基于声誉的激励机制, 配合 Web 2.0 中社交关系激励、虚拟积分激励等多元激励形式, 同时设计更为公平, 全面的激励方法, 进而保证用户更全面, 安全地参与社区治理中.

5.3 Web 3.0 社区治理

目前 Web 3.0 社区治理模式主要分为链下治理和链上治理. 链下治理主要由社区核心开发者控制, 节点通过安装软件来发出决定信号, 全节点用户拥有全部责任, 其灵活性较高, 但需要更高的社会协调成本, 且缺乏合理的激励机制, 限制了新开发者的加入. 而链上治理通过链上提案投票机制的形式实现, 将决策权交给利益相关者, 利

用所持有的治理代币进行投票.

目前链上投票方式分为社区自主投票与引入第三方去中心化投票系统进行投票两种. 主流 Web 3.0 社区采用第 2 种方案. Snapshot[78]是一个去中心化投票系统, 为用户提供高效、低成本、去中心化的投票工具, 被众多平台所采用. 2022 年, 依靠 Snapshot 进行社区投票治理的项目有 5 700 多个, 而截至 2023 年 10 月已经暴增至 27 000 个. 表 10 综合比较了流动民主、二次方投票、全息共识、信念投票、怒退机制、加权投票与声誉投票以及知识可提取投票这 7 种社会治理机制的关键特征和技术应用. 这些机制被设计来优化决策过程、增强参与激励、和提高治理的透明度与安全性, 从而在不同应用场景中实现有效的社区或组织治理. 尽管每种机制都具备其独特的优势和局限性, 但通过智能合约的运用、参与者的质押和激励以及对投票权重和提案要求的精确设计, 这些治理机制共同促进了群体决策的效率和公平性.

表 10　Web 3.0 治理机制对比

机制名称	应用场景	参与条件	投票权重计算	提案要求	决策流程	激励措施	执行方式	安全性	可扩展性
流动民主	社区治理	任何人	持币量	社区批准	动态投票	加入激励	智能合约	抗串谋	高
二次方投票	公共物品资助	持币者	平方根计算	最小门槛	透明算法	对小额投票者更有利		防止资金操纵	中
全息共识	大规模决策	提案者质押	预测市场动态	预测市场成功	预测市场	奖励正确预测者		抗滥用	中
信念投票	预测市场	持币者	抵押代币	清晰定义的提案	实时动态	抵押回报		抗串谋投票	中
怒退机制	资金管理	身份验证	贡献度	社区法规同意	社区共识	退出选择	人工执行	资金安全	高
加权投票与声誉投票	组织决策	具有声誉分数	声誉分数	规定门槛	成员讨论	声誉积分		抗刷声誉攻击	中
知识可提取投票	专家决策	专业知识认证	知识证明	严格标准	专家审议	知识贡献奖励		知识验证	低

DAO (decentralized autonomous organization, 去中心化自治组织) 是 Web 3.0 社区治理的重要组织形态, 通常以智能合约为基础, 将资金管理、提案提交、投票与执行规则固化为链上逻辑, 从而减少人为干预, 显著提升治理过程的透明度与可验证性. 其核心特征包括开放参与、基于代币或声誉的投票权分配、自治资金池管理以及规则的自动化执行. 典型案例包括 MakerDAO, 由持有 MKR 代币的成员共同治理稳定币 DAI 的货币政策与风险参数; Uniswap DAO, 负责协议升级与资金使用决策; 以及 BanklessDAO, 通过任务驱动的方式组织社区贡献, 并基于治理代币进行奖励分配. 表 11 从决策主体、执行方式、透明度、参与门槛、投票权分配、激励机制以及优缺点等多个维度对比了传统链下治理、一般链上治理与 DAO. 可以看出, DAO 在透明性、可验证性和自动化执行方面具有显著优势, 同时其多元化的投票权分配与激励机制也为去中心化生态提供了灵活性.

表 11　DAO 与其他治理模式对比

对比维度	传统链下治理	一般链上治理 (非 DAO)	DAO
决策主体	核心团队、基金会	代币持有者或指定节点	所有符合条件的代币持有者、声誉持有者或多签成员
执行方式	人工执行决策	智能合约触发部分执行, 人工介入较多	智能合约全自动执行, 规则链上固化
透明度	低 (依赖公告与文档)	中 (投票记录可链上查询)	高 (提案、投票、资金流均链上可验证)
参与门槛	高 (需核心团队或股东身份)	中 (需持有一定代币)	灵活 (代币、声誉、任务完成度等均可作为门槛)
投票权分配	按职位/股份	按持币量为主	可多元化: 持币量、声誉值、任务贡献等
激励机制	较弱或无直接激励	代币奖励、手续费分红	代币激励+声誉积分+任务奖励等组合
优点	决策集中、响应速度快	投票上链、透明性提升	完全透明、可验证、参与广泛、自动化执行
缺点	易受中心化影响、缺乏透明度	代币集中化风险、参与率低	鲸鱼投票风险、规则僵化、投票冷漠问题
典型案例	ICANN (互联网名称与数字地址分配机构)	Tezos 链上治理	MakerDAO、Uniswap DAO、BanklessDAO

随着 Web 3.0 的发展, 攻击者也将目光瞄准了链上投票系统. Li 等人[79]针对当前主流 DPoS 区块链平台的恶意接管事件进行分析, 并证明 DPoS 区块链对接管的抵抗力取决于其底层基于代币的投票治理系统的理论设计和实际使用. 当选民积极合作抵制潜在收购时, 当前 DPoS 区块链的积极抵制远低于理论上限, 然而在实践中, 选民的偏好可能会有很大不同. 作者还对 EOSIO、Steem 和 TRON 平台所收到的被动接管阻力进行了大规模实证研究, 确定了在多个 DPoS 平台中投票选民偏好的多样性, 并描述了这种多样性对接管抵制的影响.

综上所述, Web 3.0 开放自治场景下的生态治理主要涉及用户声誉评价、用户激励与社区治理这 3 个方面的技术. 面向 Web 3.0 的生态治理机制通过可信的声誉评价体系和多样化的权益激励手段, 建立了促进良性行为、抑制恶意行为的制度基础. 这不仅增强了用户参与度与信任度, 还为数据资产化中“治理”环节提供了稳定、公平且可扩展的运行环境, 确保了数据资产在全生命周期内的健康运转与价值实现. 然而, 现有研究工作仍存在海量数据存储鉴别难, 多方用户激励难平衡, 用户声誉评价授权难确定等问题. 此外, 现有的治理制度存在易受到恶意接管等问题. 因此, 针对上述需求, 设计海量多维可信的链上链下声誉数据存储与聚合方法, 实现自演化可验证的用户声誉评价方法及稳定公平多样的用户权益激励方法, 将是下一步的主要研究方向.

6 安全监管

安全防护与监管是数据资产化全生命周期的底线保障, 贯穿确权、流通与治理的各个阶段. Web 3.0 中的数字资产面临跨平台流通下的隐私保护、交易溯源以及复杂攻击行为识别等挑战, 需要兼顾合规性与用户隐私.

然而, Web 3.0 自诞生起就伴随着大量的安全事件, 造成了巨大的损失, 表 12 列出了近几年一些 Web 3.0 安全事件[80,81]. 合约安全方面目前已有相关研究综述, 本节不再进行探讨. 从表 12 可以看出, Web 3.0 的安全风险涵盖监管缺失、合约漏洞、系统安全缺陷以及密钥管理失误等多个层面. 其中, 监管缺失导致的欺诈类事件 (如 Rug Pull、虚假交易所) 往往规模大、跨境难追; 合约与系统漏洞则更多依赖技术手段进行防御, 如形式化验证与算法升级; 而密钥泄露事件凸显了私钥保护与密钥托管机制的重要性. 这些案例反映出当前 Web 3.0 安全监管需在技术防护与制度监管之间建立多层次协同体系. 本节将从隐私保护技术、主动监管、链上数据监测和前端安全方面介绍当前的研究进展, 并分析现有工作存在的不足.

表 12　Web 3.0 安全事件

安全事件	案例	分类	影响范围	防御/应对措施
非法集资	2022 年“Big Daddy Ape Club”项目的“Rug Pull”失信行为	缺乏监管	数千投资者、数百万美元损失	引入多签托管、第三方审计、KYC 验证
虚假交易所	2017 年曝光的“BitKRX”交易所	缺乏监管	数万用户、数千万美元资金	交易所牌照审核、品牌认证、资金托管
智能合约漏洞利用	2023 年 Vyper 重入锁失效漏洞	合约安全	多个 DeFi 协议、数千万美元损失	代码审计、编译器升级、形式化验证
系统漏洞利用	2014 年门罗币“哈希碰撞”攻击	系统安全	网络整体、数百万美元潜在影响	升级算法、哈希难度调整
为洗钱、诈骗等非法活动提供支持	2023 年 Stake.com 私钥泄漏后续的洗钱活动	缺乏监管	跨链平台、数千万美元非法转移	私钥硬件隔离、链上监测与冻结机制
钱包私钥泄露	2023 年 Stake.com 私钥泄漏	钱包安全	单一钱包、数千万美元资产丢失	硬件钱包、多重签名、密钥分片

6.1 隐私保护技术

与传统的中心化隐私保护方案相比, 基于 Web 3.0 的数字资产交易系统的隐私保护方案需要在确保参与节点能够通过某种共识协议验证交易的正确性的同时, 参与节点不能得知交易的信息.

从隐私攻击的角度来看, 攻击方可以通过某一公开记录的发起者与接收对象标识 (地址或公钥), 进而追踪交易链条, 获得交易规则和地址之间的关系, 最终根据网络外部信息推断出用户的真实身份. 一般来说, 流通过程中

的隐私保护可以分为身份隐私保护与内容隐私保护[82]. 身份隐私是指用户身份信息与地址、地址与地址之间的关联关系; 内容隐私是指去中心化平台所存储的记录与记录背后的知识, 例如交易金额.

身份隐私方面, 比特币采用了分层确定性 (hierarchical deterministic, HD) 钱包, HD 钱包也是目前常用的确定性钱包算法, 其中 BIP 32[83]协议是比特币的一种具有身份隐私保护功能的公私钥生成算法, 利用多个一次性地址对应一个用户实体的方式增加了推断用户实体的难度, 但恶意敌手仍能构建交易链条以推断部分用户信息. 同时 Buterin[84]指出, 通过父公钥和子私钥, 可以破解同级的兄弟私钥和父私钥, 这可能会在一些共同管理的比特币钱包中产生安全隐患. 并且 BIP 32 仅为一种身份隐私保护算法, 没有对内容隐私即交易金额进行保护. Coinjoins[85]是 2013 年在比特币论坛上提出的一种交易身份隐私保护思想, 其核心是将多条交易合并, 并打乱发送与接收方地址间的关系, 这一思想促成了后续一系列方案的设计, 并且其本身也作为一种方案落地应用.

门罗币 (Monero)[86]主要利用环签名[87]、一次性密钥和数值承诺等技术, 构建基于一次性地址的交易接收方身份隐藏机制和基于环签名的交易发送方身份隐藏机制. 如图 7 所示. 隐藏接收方身份信息的一次性地址机制能够使每笔交易产生一个新的接收方地址, 身份混淆的空间为 $1/N$, 此外门罗币允许用户维护单个主钱包地址, 并生成任意数量的不可链接子地址. 每个事务只需扫描一次, 即可确定其是否对应用户的任何子地址, 并且支持同时对多个交易对象进行输出.

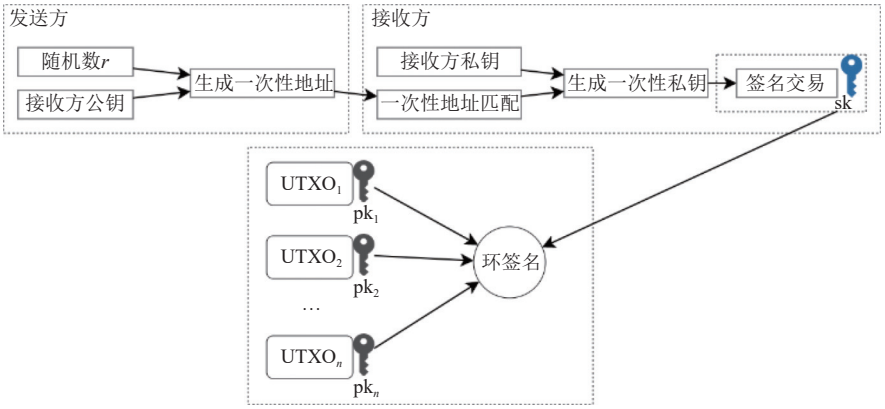

图 7 门罗币的身份隐私保护方案

门罗币的交易发送方身份隐藏机制使用了环签名算法, 将交易的发送方签名密钥隐藏在多个签名密钥中. 门罗币还通过 Pedersen 承诺对身份隐私与内容隐私进行保护. 但是由于其环签名的技术仅能保证发送方的地址在环签名成员中的混淆, 同时环签名成员的数量受到计算效率与存储空间的限制, 所以其对于用户身份隐私的保护能力是有限的.

零币 (ZCash)[88]是基于 Zerocash[89]协议发行的加密货币, 主要使用零知识简洁非交互式知识论证 (zk-SNARK)[90]技术保护了交易的身份与内容隐私, 能够在不泄露证据中的任何知识的前提下证明语言的正确性.

截至目前, 零币的协议已经更新了 3 个版本, 分别为 Sprout、Sapling 和 Orchard (其中 Zerocash 协议对应 Sprout 版本), 对算法与性能进行了优化, 例如, 在 Sprout 版本中, zk-SNARK 需要通过 6 个参与者运行多方安全计算协议 (multi-party computation, MPC) 生成结构参考串 (structured reference string, SRS); 在 Sapling 版本中, 参与者的数量被提升至 90 人; 而在 Orchard 协议[91]中, 设计了新的证明系统从而取消了生成 SRS 的需要.

Web 3.0 中已存在一些应用提供混币服务, 例如之前提及的 Coinjoins、Wasabi Wallet[92]等. 这些应用通常将交易发送方的加密货币与大量其他加密货币混合, 然后以较小单位将加密货币发送到交易接收者的地址, 同时收取 1%–3% 的服务费[93]. 这些混币服务大多为在现有的去中心化交易机制之上附加新的隐私保护解决方案, 旨在为现有的非隐私保护的区块链与用户提供隐私.

6.2 监管技术

数字资产由于取证、追溯困难的特性, 使其为部分洗钱、诈骗、赌博、恐怖主义等非法交易活动提供了温床. 而门罗币、零币等隐私保护加密货币更加增加了追踪取证的难度. 近年来, 如何监管破坏市场交易的行为, 对交易中钱款流动的交易链条进行追溯以此对用户进行追责已越来越受到关注. 当前主流的方法有主动监管技术和链上数据监测, 主动监管指在用户隐私保护方案的设计阶段, 设计由验证方或验证方与审计方两方合作为审计方留下的陷门, 在交易结束后审计方通过该陷门打开交易获得交易链条; 链上数据监测使用大数据的手段, 对交易信息进行分析, 推断交易链条、对网络的态势进行分析、对隐私保护方案进行安全性评估等, 同时这种对隐私保护脆弱性的分析方式也可作为恶意交易的识别与溯源方式, 维护交易市场的秩序. 表 13 对比了主动监管与链上数据监测的优缺点与应用场景.

表 13 Web 3.0 监管技术分类

类型	方案	应用场景	特点	不足
主动监管	PGC[94]	可监管的 Web 3.0 支付系统	交易隐私保护、可审计、轻量级密码学方案	实现难度大、不完全匿名
	PRCash[95]	可监管的数字资产交易平台	交易隐私保护、快速支付	依靠第三方监管机构、不完全匿名、不可审计
	Azeroth[96]	可监管的数字货币	可审计、灵活部署	计算效率低、地址明文传输
	FabZK[97]		交易隐私保护、可审计	吞吐量较低、实现难度大
	ACT[98]		可审计、交易金额隐私保护	计算效率较低
链上数据监测	启发式算法、时序追踪等[99–104]	用户身份隐私推断	交易图构建后进行账户数据分析与聚类	准确度较低、需要利用人工先验知识设定规则
	Goldphish、CoinSeer、ActCluster等[105–116]	用户恶意行为检测	借鉴异常检测的思想、交易图构建后进行交易数据分析	需要进行大量的数据处理、难以准确刻画恶意行为模式

6.2.1 主动监管

与隐私保护技术类似, 主动监管主要关注于交易的身份与内容两个部分. 2016 年 Garman 等人[117]对 Zerocash 的监管进行了讨论, 但没有进行具体方案的设计, 该论文主要的思想是通过 zk-SNARK 保证用户遵守交易策略, 这些策略允许交易者可验证地证明遵守公共交易的共识规则, 例如纳税、存款限额和可验证的硬币追踪, 同时保护每个交易的隐私.

为了对交易内容进行有效的监管, Chen 等人[94]设计了一种基于 Pedersen 承诺的公钥加密算法 Twist ElGamal, 并根据该算法设计了一种可审计的去中心化保密支付系统的方案. Twist ElGamal 继承了 Pedersen 承诺的同态性, 能够直接通过运算验证交易的平衡性, 同时可以使用 bulletproof 对数值进行范围证明以确保用户在转账时具备偿付能力. PRCash[95]使用 Pedersen 承诺和 ElGamal 加密算法分别对交易身份和交易内容进行了监管. 在该方案中, 定义了一个中央机构, 该中央机构能够对应实体的地址与实体的真实身份, 当用户的交易数额超过某一数额时, 用户必须向该中央机构披露自己的所有隐私.

FabZK[97]使用表格结构记录交易数值与身份, 节点发出交易时, 该交易发送方和接收方分别生成一个 Pedersen 承诺, 同时所有网络的参与节点都会给出一个承诺值为 0 的承诺, 同时在该承诺之上, 利用 Pedersen 承诺的同态性构造审计信息. 该方案的交易存储量与网络的参与用户数量成正比, 只适用于联盟链少量机构间的交易场景. Traceable Monero[118]在门罗币的基础上引入了监管机制, 对用户的身份隐私进行监管, 其基本思想同样为在交易策略中增加为监管方设计的陷门, 并通过 zk-SNARK 保证用户遵守交易策略. 在该方案中监管方能够恢复门罗币一次性地址所对应的长期公钥, 对交易进行追踪. ACT[98]使用了另一种监管思路, 该方案在交易记录在链上后, 如果交易存在疑点, 或者需要对交易进行审计, 由监管方对所有参与的成员发出挑战, 成员对于自己记录在链上的数据进行进一步的证明, 以满足监管方给出的条件.

Web 3.0 的主动监管方案目前尚处于起步阶段, 大多数都停留在理论阶段. 其中尚有需要解决的关键问题.

(1) 在隐私保护算法所带来的较大的计算与存储开销上, 又增加了监管所附带的计算与存储的开销, 使得方案的实际应用难以落地.

(2) 在 Web 3.0 的用户自治思想下, 难以界定监管的能力范围, 如何在用户自治的 Web 3.0 架构下引入监管以维护安全性、合法性, 需要更为深入的研究.

6.2.2 链上数据监测

用户身份隐私推断方面, 2013 年, Meiklejohn 等人[99]对比特币的可追溯性进行了分析, 他们通过分析并区分比特币的使用方式从而推断用户习惯. 例如, 购买商品、彩票交易、找零、混币等交易的交易特征如交易图结构、交易涉及的地址都是不同的, 该论文通过分析这些不同交易行为的特征, 对用户的习惯进行聚类, 从而降低了比特币的匿名程度. Kumar 等人[100]研究了在被动对手存在的情况下, 门罗币的期望的匿名集和有效匿名集的大小, 分析了零混合、输出合并与时间序列分析这 3 种攻击手段对交易匿名程度的影响. 这一工作在门罗币社区内引起了广泛的讨论, 门罗币对此引入了一系列协议的变更, 包括引入强制最小环尺寸. 与该论文同时期开展的相似内容的研究工作还有文献 [101], 该工作进一步对变更的门罗币进行了隐私性评估[102], 结果表明, 门罗币目前基本上不受已知被动攻击向量的影响, 也不受适用于其他加密货币的既定跟踪和追踪方法的影响. Zhang 等人[103]考察了莱特币的用户隐私泄露情况, 模拟了一种交易链接攻击的方式, 并提出通过调整价格、汇率、时间的不确定范围, 可大幅度降低大小为 1 的匿名集的比例. Wang 等人[104]以匿名混币平台 Tornado.Cash 和 Typhoon.Network 为例, 分析了零知识证明混合器的隐私保护能力.

用户恶意交易行为检测方面, 可分为异常交易行为的识别和异常交易用户的主动溯源两个部分. 沈蒙等人[119]对数字货币交易匿名性保护与对抗进行了深入剖析, 将其归纳为不可标识性、不可链接性和不可追踪性这 3 个方面. 因此, 相关工作旨在对抗这 3 个方面的特性.

为了检测用户利用区块链数字货币进行洗钱、诈骗、从事庞氏骗局等恶意行为, 现有研究工作大都利用链上交易数据构建交易图, 通过图聚类与图机器学习方法识别异常交易. Dey[105]针对联盟链面临的网络威胁, 提出了一种使用智能软件代理来监测区块链网络中利益相关者活动的方法, 并通过此方法检测合谋行为. Pham 等人[106]在比特币交易数据集的基础上构建用户网络图和交易网络图, 从中提取不同的关系特征, 通过密度和密度定律、K-means 聚类算法计算局部离群因子来识别用户或交易的异常情况. Chen 等人[107]采用图分析方法描述了以太坊上的 3 个主要活动, 即资金转移、智能合约创建和智能合约调用. 沈蒙等人[108]提出了一种基于动机分析的加密货币异常交易行为辨识方法, 通过设计异常交易行为的判定规则, 提炼出异常交易模式图, 并利用图匹配技术实现了比特币异常交易行为的辨识算法.

识别恶意交易后, 需要进一步对交易进行溯源, 对参与交易的节点采取相关措施. Koshy 等人[109]通过对比特币特殊交易的传播规律进行深入分析, 发现特殊交易模式可用于追溯始发节点. Gervais 等人[110]通过对比特币节点对网络中其他节点行为的综合评估, 采用一种比特币黑名单机制, 将可能对网络运行造成危害的节点列入黑名单, 并拒绝与其连接, 以维护网络安全. Biryukov 等人[111]提出一种基于邻居节点的交易溯源机制, 明确指出将邻居节点作为判断依据可有效提高溯源的准确性. Spagnuolo 等人[112]通过对比特币网络信息的详细导出和可视化, 实现对用户身份和资金流动的跟踪.

在链上数据监测的研究中, 除了针对用户隐私泄露与链上追踪的分析外, Web 3.0 还存在大量源于经济安全与机制设计缺陷的重大威胁, 这类攻击并非依赖破坏底层密码算法, 而是通过利用协议在价格获取、资金流动、投票治理等方面的激励机制漏洞, 从经济博弈层面直接操纵系统以获取不正当收益. 如表 14 所示, 攻击者可能操纵去中心化应用的价格预言机, 通过大额交易在低流动性池中制造价格波动, 从而影响借贷、清算等操作; 利用闪电贷的零抵押、即时还款特性, 在单个区块内完成价格操纵、参数更改等复杂攻击链; 通过监控交易池实施抢先交易和最大可提取价值 (maximal extractable value, MEV) 策略, 攫取额外利润; 在基于代币投票的治理体系中, 使用闪电贷瞬时获得大量治理代币从而控制提案投票结果; 或是针对跨链桥与流动性池的经济性设计缺陷, 制造流动性失衡和跨链套利空间. 这些威胁在 DeFi 协议、去中心化交易所和跨链基础设施中频繁出现, 其隐蔽性和策略性使得传统网络安全防护方法难以奏效. 针对这一问题, McLaughlin 等人[113]将 DeFi 中的行为构建成有向有权图,

实现了以太坊中大规模套利交易行为分析. Li 等人[114]通过交易发出的事件提取高层次语义信息, 从而实现了对捆绑交易中的套利行为模式识别. Das 等人[115]对 NFT 生态系统的市场动态和安全问题进行了深入研究, 发现了区块链外部的实体干预 NFT 市场的行为模式, 并量化了用户利用匿名机制所进行的恶意交易行为. Cernera 等人[116]通过分析当前 BSC 链和以太坊链上的代币与流动性池的活跃程度与活跃时间, 提出了相应的行为量化分析方法, 从而发现项目方可能存在的恶意欺诈行为.

表 14 Web 3.0 经济安全威胁分类与案例表

威胁类型	案例	攻击原理	主要影响	防御/应对措施
预言机操纵	2020年bZx平台攻击事件	操纵低流动性价格源导致借贷清算异常	协议资金被恶意清算, 资产损失数百万美元	使用多源预言机、价格延迟机制、去中心化数据聚合
闪电贷攻击	2021 年Alpha Homora与Cream Finance平台攻击事件	借入巨额资产瞬时完成价格操纵或逻辑漏洞利用	协议资金池被抽空或参数被篡改	限制关键操作的即时执行、引入多区块验证
MEV与抢先交易	Uniswap、SushiSwap 高频交易机器人	监控交易池并插入交易以获取额外利润	用户滑点增加、交易成本上升	引入私有交易通道、批量拍卖机制
治理攻击	2022 年Beanstalk DAO攻击事件	闪电贷获取投票权并强行通过提案	协议金库资金被转移	设置治理延迟、限制单账户投票权增长速率
跨链桥经济性漏洞	2022 年Wormhole攻击事件	跨链资产铸造与锁定机制缺陷	跨链资产供应失衡、被盗资产无法追回	增强跨链验证机制、双向资金证明、经济性压力测试

综上所述, 用户行为被动监管层面的研究工作已经取得了一些进展, 尤其是基于图的交易网络建模方法对异常交易行为识别提供了便利, 但还存在如下问题亟待解决.

(1) 恶意交易行为复杂多变、行为难以预测, 目前针对正常交易行为的精确刻画还缺乏深入研究. 恶意交易呈现出越来越智能、越来越隐蔽、越来越复杂等特点, 深入研究异常交易行为特征及内在规律变得越来越困难.

(2) 目前在未知异常交易攻击行为检测方面的研究工作较少, 并且绝大多数方法都只是静态的、从单个维度上针对交易数据进行行为分析与建模, 随着各类混币及隐私保护平台的普及, 如何从海量多维数据中实现异常交易用户主动溯源将是未来的主要挑战.

6.3 前端安全分析

Yan 等人[120]分别从前端代码与智能合约角度对当前区块链中第三方 SDK 的中心化现象进行了分析, 定义了去匿名化风险、私钥泄漏、合约中心化调用等中心化安全风险. Wang 等人[121]对当前 NFT 与链下资产链接的脆弱性、可访问性与重复性这 3 个角度进行评估, 发现存在部分 NFT 失去了与链下资产的链接, 且存在中心化存储的风险. Zou 等人[122]分析了当前 Web 3.0 社交平台中在个人经济的客观条件与社交选择的主观条件影响下的用户社交行为, 发现代币持有量多的用户更为活跃, 而代币持有量少的用户则更容易遭受到安全威胁. Qin 等人[123]提出了一种算法对通用交易机器人进行了具体分析, 并量化分析了区块链中的可提取价值, 验证了这一活动对安全性所造成的不良影响. Li 等人[124]通过将链上数据与链下网页证书信息、网页信息相结合, 实现了对当前 Web 3.0 中的诈骗网站的大规模分析. Torres 等人[125]对当前部分 DApp 的前端界面泄漏用户地址的程度进行了分析. He 等人[126]针对当前 Web 3.0 钓鱼网站检测方法未关联链上数据导致检测深度不足的问题, 提出了一种结合网站证书、网站关键词与链上数据的新型钓鱼网站检测方法.

综上所述, Web 3.0 数字资产全生命周期安全防护与监管技术通过隐私保护、溯源分析与智能识别手段, 实现了在不损害用户数据主权的前提下对资产流转过程的有效监管, 确保了确权、流通与治理环节的安全可控性, 为数据资产化提供了全流程、闭环式的安全与合规保障.

7 总结与展望

Web 3.0 能够助力数据资产化, 促进数字经济发展. 针对 Web 3.0 在用户生态构建与数字资产流通两方面的挑战, 本文提出了面向数据资产化的 Web 3.0 技术架构, 并从身份管理、资产流通、生态治理与安全监管这 4 个方

面对当前的 Web 3.0 前沿技术进行了归纳、分类、分析与总结. 下面将从这 4 个方面展望未来研究方向.

● 可信分布式数字身份管理机制

(1) 在不同信任模型下, 多元实体的数字身份可信创建和标识鉴别依然存在困难. 不同实体之间的关系复杂, 不同领域间的需求各异, 难以确立统一的身份验证标准.

(2) 现有技术未能有效解决用户在交易过程中的身份隐私保护问题, 并且在分布式交易场景下, 访问控制策略的僵化限制了用户对于身份数据的灵活管理.

(3) 现有的分布式数字身份管理技术缺乏 Web 兼容的标准与规范. Web 3.0 应用和服务需要一个统一的分布式数字身份管理架构, 然而目前的技术尚未解决这一问题, 导致分布式数字身份管理碎片化, 不同应用间难以达成一致.

因此, 如何利用环签名、零知识证明、多消息签名等技术实现高效的、端到端的分布式数字身份可验证凭证管理与隐私保护机制, 构建统一的数字身份管理架构是需要进一步研究的方向. 未来可通过零知识证明 (ZKP) 实现“最小化披露”身份验证, 使用户在不暴露敏感信息的前提下完成跨平台身份认证; 结合安全多方计算 (MPC) 实现身份数据的协同验证与分布式存储, 防止单点泄露; 利用去中心化数字身份 (DID) 与可验证凭证 (VC) 构建符合 W3C 标准的统一身份框架, 实现身份凭证在不同应用间的互操作性与可撤销性. 此外, 可引入基于区块链的“身份信誉链”, 将身份行为轨迹与声誉积分绑定, 用于增强跨应用信任传递能力.

● 跨应用的多模态数字资产流通机制

(1) 当前 Web 3.0 资产流通机制缺乏稳定高效的经济运行模型, 存在数字资产价值波动大、用户收益分配失衡、底层经济运行模式抵御风险能力低等问题.

(2) 现有 Web 3.0 数字资产的鉴权机制仅针对单一模态, 缺乏跨模态隐式关系推理与鉴权的能力, 无法应对高度复杂、多样化的数字版权验证需求.

(3) 现有数字资产估值与流通机制无法有效满足市场需求, 不同类型的资产之间存在着巨大的估值差异, 增加了交易的风险, 导致买卖双方难以在较小的价格波动量下完成大批量交易.

因此, 如何构建 Web 3.0 多模态用户数字资产的透明可信鉴权确权和稳定高效流通机制是需要进一步探索研究的方向. 未来可构建基于链上链下混合预言机的多模态资产定价与鉴权框架, 利用机器学习和知识图谱对跨模态隐式关系进行推理, 提高鉴权的精细度与抗欺诈性; 通过引入同态加密与零知识证明, 在不暴露资产内容的前提下完成真实性与所有权验证; 结合跨链通信协议 (IBC、LayerZero 等) 与多签托管, 实现资产在不同链与应用间的低延迟、安全流通; 并通过链上 AMM 动态调整流动性池权重, 提升大额交易时的价格稳定性与抗操纵能力.

● 面向 Web 3.0 共建共治的生态治理机制

(1) 现有用户声誉评价方法冷启动难, 对用户高质量声誉数据的鉴别能力有限, 难以有效区分用户声誉数据的真实性, 导致用户声誉评价结果的可信度低.

(2) 现有用户权益激励机制相对单一, 主要以通证激励为主, 缺乏创新性和多样性, 无法针对不同用户群体和行为实现个性化激励, 对于部分用户的吸引力不足.

(3) 现有 Web 3.0 用户生态治理机制缺乏有效的监督和调节机制, 无法对治理机制进行评估和动态调整, 难以保障治理的可靠性和可持续性.

因此, 如何利用预言机实现海量、多维、可信的链上链下声誉数据聚合, 并通过博弈论等方法建立稳定公平多样的用户权益激励机制是需要进一步探索研究的方向. 未来可利用跨域预言机聚合链上链下多源声誉数据, 通过图神经网络分析用户贡献度与可信度, 解决冷启动与数据真实性问题; 在激励层面引入声誉驱动的复合激励模型, 将通证激励与链上任务、治理参与度、内容贡献度等指标动态挂钩; 结合博弈论与机制设计优化投票权分配, 防止“鲸鱼”垄断; 引入链上 DAO 治理分析工具, 对提案执行效果与治理公平性进行持续监测与自动调节.

● Web 3.0 数字资产全生命周期安全防护与监管技术

(1) Web 3.0 数字资产价值可信流转需要同时兼顾隐私保护与安全监管, 在跨应用、跨平台的数据流转场景下, 现有的隐私保护算法无法适用于 Web 3.0 数字资产的多模态特性且制约了监管的有效性.

(2) 现有的溯源方法仅支持特定场景, 在面对 Web 3.0 数字资产的多样化使用场景时, 如期货、股权、债券等, 无法满足数据资产流转的全生命周期监管需求, 并且随着各类混币及隐私保护平台的普及, 如何从海量多维数据中实现交易溯源, 将是未来的主要挑战.

(3) 现有交易监管机制通常采用基于规则或模式匹配的方式进行交易行为识别, 然而随着 Web 3.0 应用的多样化, 恶意交易呈现出越来越智能、越来越隐蔽、越来越复杂等特点, 导致交易行为识别粒度粗, 监管效率低, 难以适配开放复杂场景下海量多源 Web 3.0 数字资产的交易监管需求.

因此, 如何利用同态加密、安全多方计算与人工智能等相关技术建立隐私与监管平衡的数字资产安全防护体系是需要进一步探索研究的方向. 未来可利用 MPC 与同态加密, 在保持数据加密状态下实现交易数据分析与风险评估; 结合零知识证明向监管机构提供可验证合规证明, 而不暴露完整交易细节; 基于 AI 的链上行为建模可识别更隐蔽的恶意交易模式; 在经济安全层面, 可引入机制仿真与压力测试框架, 提前发现预言机操纵、闪电贷攻击、治理操纵等高风险策略, 并通过自动化的智能合约补丁与参数动态调整机制, 实现交易、结算、清算全链路的主动防护.

Web 3.0 作为新一代互联网框架, 不仅是技术层面的革新, 更是对互联网商业模式和价值分配模式的重塑. 以数据主权为理念, 围绕身份管理、资产流通、生态治理与安全监管这 4 个方面, Web 3.0 正在逐步构建一个全新的数据资产化框架, 用户可以更加自主地管理和掌控自己的数据, 实现将数据价值归还给用户. 相信随着国家重点研发计划“区块链”重点专项在 Web 3.0 领域的持续深入投入与布局, 推动 Web 3.0 技术的高质量发展, 未来将会形成更为完善的新型数据框架、流通机制与经济体系, 赋能数据要素确权与流通, 促进数字经济与实体经济的融合发展.

References

[1] Guan C, Ding D, Guo JC. Web3.0: A review and research agenda. In: Proc. of the 2022 RIVF Int’l Conf. on Computing and Communication Technologies (RIVF). Ho Chi Minh City: IEEE, 2022. 653–658. [doi: 10.1109/RIVF55975.2022.10013794]

[2] Kapoor A, Guhathakurta D, Mathur M, Yadav R, Gupta M, Kumaraguru P. TweetBoost: Influence of social media on NFT valuation. In: Companion Proc. of the 2022 Web Conf. Lyon: ACM, 2022. 621–629. [doi: 10.1145/3487553.3524642]

[3] Pavuluri G, Kovvali RSK, Bandaru PK, Devarapalli BP. Block-Voter: A full-stack Ethereum-based electronic voting DApp. In: Proc. of the 2025 Int’l Conf. on Intelligent Computing and Control Systems (ICICCS). Erode: IEEE, 2025. 350–356. [doi: 10.1109/ICICCS65191.2025.10984491]

[4] Uniswap. Uniswap Interface. 2020. https://uniswap.org/

[5] Jacksi K, Abass SM. Development history of the world wide Web. Int’l Journal of Scientific & Technology Research, 2019, 8(9): 75–79.

[6] Swati J, Nitin P, Saurabh P, Parikshit D, Gitesh P, Rahul S. Blockchain based trusted secure philanthropy platform: Crypto-gocharity. In: Proc. of the 6th Int’l Conf. on Computing, Communication, Control and Automation (ICCUBEA). Pune: IEEE, 2022. 1–8. [doi: 10.1109/ICCUBEA54992.2022.10011026]

[7] Petcu A, Pahontu B, Frunzete M, Stoichescu DA. A secure and decentralized authentication mechanism based on Web 3.0 and Ethereum blockchain technology. Applied Sciences, 2023, 13(4): 2231. [doi: 10.3390/app13042231]

[8] Wan SC, Lin H, Gan WS, Chen JH, Yu PS. Web3: The next Internet revolution. IEEE Internet of Things Journal, 2024, 11(21): 34811–34825. [doi: 10.1109/JIOT.2024.3432116]

[9] Shen M, Tan ZH, Niyato D, Liu YZ, Kang JW, Xiong ZH, Zhu LH, Wang W, Shen X. Artificial intelligence for Web 3.0: A comprehensive survey. ACM Computing Surveys, 2024, 56: 247. [doi: 10.1145/3657284]

[10] Cameron K. The laws of identity. 2005. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[11] Dunphy P, Petitcolas FAP. A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 2018, 16(4): 20–29. [doi: 10.1109/MSP.2018.3111247]

[12] Li HZ, Li CX, Li HX, Bai XQ, Shi X. Anoverview on practice of FISCO BCOS technology and application. Information and Communications Technology and Policy, 2020, 46(1): 52–60 (in Chinese with English abstract). [doi: 10.3969/j.issn.1008-9217.2020.01.011]

[13] Stokkink Q, Pouwelse J. Deployment of a blockchain-based self-sovereign identity. In: Proc. of the 2018 IEEE Int’l Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing

(CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018. 1336–1342. [doi: 10.1109/Cybermatics_2018.2018.00230]

[14] Naik N, Jenkins P. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In: Proc. of the 2020 IEEE Int'l Symp. on Systems Engineering (ISSE). Vienna: IEEE, 2020. 1–7. [doi: 10.1109/ISSE49799.2020.9272223]

[15] Tobin A, Reed D. The inevitable rise of self-sovereign identity. White Paper, The Sovrin Foundation, 2016.

[16] Fromknecht C, Velicanu D, Yakoubov S. A decentralized public key infrastructure with identity retention. 2014. https://eprint.iacr.org/2014/803.pdf

[17] Axon L, Goldsmith M. PB-PKI: A privacy-aware blockchain-based PKI. In: Proc. of the 14th Int'l Joint Conf. on e-Business and Telecommunications. Madrid: SciTePress, 2016. 311–318. [doi: 10.5220/0006419203110318]

[18] Wang R, He J, Liu C, Li Q, Tsai WT, Deng EY. A privacy-aware PKI system based on permissioned blockchains. In: Proc. of the 9th IEEE Int'l Conf. on Software Engineering and Service Science (ICSESS). Beijing: IEEE, 2018. 928–931. [doi: 10.1109/ICSESS.2018.8663738]

[19] Singla A, Bertino E. Blockchain-based PKI solutions for IoT. In: Proc. of the 4th IEEE Int'l Conf. on Collaboration and Internet Computing (CIC). Philadelphia: IEEE, 2018. 9–15. [doi: 10.1109/CIC.2018.00-45]

[20] Sonnino A, Al-Bassam M, Bano S, Meiklejohn S, Danezis G. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. In: Proc. of the 2019 Network and Distributed Systems Security (NDSS) Symp. San Diego: Internet Society, 2018. [doi: 10.14722/ndss.2019.23272]

[21] Doerner J, Kondi Y, Lee E, Shelat A, Tyner L. Threshold BBS+ signatures for distributed anonymous credential issuance. In: Proc. of the 2023 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2023. 773–789. [doi: 10.1109/SP46215.2023.10179470]

[22] Rosenberg M, White J, Garman C, Miers I. zk-creds: Flexible anonymous credentials from zkSNARKs and existing identity infrastructure. In: Proc. of the 2023 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2023. 790–808. [doi: 10.1109/SP46215.2023.10179430]

[23] Maram D, Malvai H, Zhang F, Jean-Louis N, Frolov A, Kell T, Lobban T, Moy C, Juels A, Miller A. CanDID: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. In: Proc. of the 2021 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2021. 1348–1366. [doi: 10.1109/SP40001.2021.00038]

[24] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town crier: An authenticated data feed for smart contracts. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 270–282. [doi: 10.1145/2976749.2978326]

[25] Rathee D, Policharla GV, Xie T, Cottone R, Song D. ZEBRA: Anonymous credentials with practical on-chain verification and applications to KYC in DeFi. 2022. https://iacr.steepath.eu/2022/1286-ZEBRAAnonymousCredentialswithPracticalOnchainVerificationandApplicationstoKYCinDeFi.pdf

[26] Reed D, Law J, Hardman D. The technical foundations of Sovrin. 2016. https://sovrin.org/wp-content/uploads/2017/04/The-Technical-Foundations-of-Sovrin.pdf

[27] Lundkvist C, Heck R, Torstensson J, Mitton Z, Sena M. uPort: A platform for self-sovereign identity. 2017. https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

[28] World Wide Web Consortium. Verifiable credentials data model 1.0: Expressing verifiable information on the Web. 2019. https://www.w3.org/TR/vc-data-model/#core-data-model

[29] Zhang F, Maram D, Malvai H, Goldfeder S, Juels A. DECO: Liberating Web data using decentralized oracles for TLS. In: Proc. of the 2020 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2020. 1919–1938. [doi: 10.1145/3372297.3417239]

[30] Chase M, Ghosh E, Setty S, Buchner D. Zero-knowledge credentials with deferred revocation checks. 2020. https://github.com/decentralized-identity/snark-credentials/blob/master/whitepaper.pdf

[31] Saramago RQ, Meling H, Jehl LN. A privacy-preserving and transparent certification system for digital credentials. In: Proc. of the 26th Int'l Conf. on Principles of Distributed Systems (OPODIS 2022). Brussels: LIPICS, 2023. 9: 1–9: 24. [doi: 10.4230/LIPIcs.OPODIS.2022.9]

[32] Buterin V. Why we need wide adoption of social recovery wallets. 2021. https://vitalik.eth.limo/general/2021/01/11/recovery.html

[33] Entriken W, Shirley D, Evans J, Sachs N. ERC-721: Non-fungible token standard. 2018. https://eips.ethereum.org/EIPS/eip-721

[34] Vogelsteller F, Buterin V. ERC-20: Token standard. 2015. https://eips.ethereum.org/EIPS/eip-20

[35] Radomski W, Cooke A, Castonguay P, Therien J, Binet E, Sandford R. ERC-1155: Multi token standard. 2018. https://eips.ethereum.org/EIPS/eip-1155

[36] Lockyer M, Mudge N, Schalm J, Echeverry S, Zhou ZV. ERC-998: Composable non-fungible token. 2018. https://eips.ethereum.org/EIPS/eip-998

[37] Wang W, Meng M, Cai Y, Chow R, Wu ZX, Du A. ERC-3525: Semi-fungible token. 2020. https://eips.ethereum.org/EIPS/eip-3525

[38] Burks Z, Morgan J, Malone B, Seibel J. ERC-2981: NFT royalty standard. 2020. https://eips.ethereum.org/EIPS/eip-2981

[39] Bored Ape Yacht Club. Bored Ape Yacht Club—Welcome to the BAYC Clubhouse. 2021. https://boredapeyachtclub.com/

[40] The Sandbox. 2018. https://www.sandbox.game/

[41] Zhao WX, Liu J, Ren RY, Wen JR. Dense text retrieval based on pretrained language models: A survey. ACM Trans. on Information Systems, 2024, 42(4): 89. [doi: 10.1145/3637870]

[42] Salton G, Buckley C. Term-weighting approaches in automatic text retrieval. Information Processing & Management, 1988, 24(5): 513–523. [doi: 10.1016/0306-4573(88)90021-0]

[43] Aizawa A. An information-theoretic perspective of TF-IDF measures. Information Processing & Management, 2003, 39(1): 45–65. [doi: 10.1016/S0306-4573(02)00021-3]

[44] Robertson S. Understanding inverse document frequency: On theoretical arguments for IDF. Journal of Documentation, 2004, 60(5): 503–520. [doi: 10.1108/00220410410560582]

[45] Devlin J, Chang MW, Lee K, Toutanova K. BERT: Pre-training of deep bidirectional Transformers for language understanding. In: Proc. of the 2019 Conf. of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Vol. 1 (Long and Short Papers). Minneapolis: Association for Computational Linguistics, 2021. 4171–4186. [doi: 10.18653/v1/N19-1423]

[46] Liu Z, Lin W, Shi Y, Zhao J. A robustly optimized BERT pre-training approach with post-training. In: Proc. of the 20th Chinese National Conf. on Computational Linguistics. Huhhot: Chinese Information Processing Society of China, 2021. 1218–1227.

[47] Brown TB, Mann B, Ryder N, *et al*. Language models are few-shot learners. In: Proc. of the 34th Int'l Conf. on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2020. 1877–1901.

[48] Kaur S, Aggarwal D. Image content based retrieval system using cosine similarity for skin disease images. Advances in Computer Science: An Int'l Journal, 2013, 2(4): 89–95.

[49] Du L, Ho ATS, Cong RM. Perceptual hashing for image authentication: A survey. Signal Processing: Image Communication, 2020, 81: 115713. [doi: 10.1016/j.image.2019.115713]

[50] Ou Y, Rhee KH. A survey on image hashing for image authentication. IEICE Trans. on Information and Systems, 2010, E93. D(5): 1020–1030. [doi: 10.1587/transinf.E93.D.1020]

[51] Zhang R, Isola P, Efros AA, Shechtman E, Wang O. The unreasonable effectiveness of deep features as a perceptual metric. In: Proc. of the 2018 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Salt Lake City: IEEE, 2018. 586–595. [doi: 10.1109/CVPR.2018.00068]

[52] Bai YS, Ding H, Bian S, Chen T, Sun YZ, Wang W. SimGNN: A neural network approach to fast graph similarity computation. In: Proc. of the 12th ACM Int'l Conf. on Web Search and Data Mining. Melbourne: ACM, 2019. 384–392. [doi: 10.1145/3289600.3290967]

[53] Wang ALC. An industrial-strength audio search algorithm. In: Proc. of the 4th Int'l Conf. on Music Information Retrieval. Baltimore: Library of Congress and Johns Hopkins University, 2003. 7–13.

[54] Zhu BL, Li W, Wang ZR, Xue XY. A novel audio fingerprinting method robust to time scale modification and pitch shifting. In: Proc. of the 18th ACM Int'l Conf. on Multimedia. Firenze: ACM, 2010. 987–990. [doi: 10.1145/1873951.1874130]

[55] Ansori MRR, Allwinnaldo, Alief RN, Igboanusi IS, Lee JM, Kim DS. HADES: Hash-based audio copy detection system for copyright protection in decentralized music sharing. IEEE Trans. on Network and Service Management, 2023, 20(3): 2845–2853. [doi: 10.1109/TNSM.2023.3241610]

[56] Lee J, Bryan NJ, Salamon J, Jin ZY, Nam J. Disentangled multidimensional metric learning for music similarity. In: Proc. of the 2020 IEEE Int'l Conf. on Acoustics, Speech and Signal Processing (ICASSP). Barcelona: IEEE, 2020. 6–10. [doi: 10.1109/ICASSP40776.2020.9053442]

[57] Li ZL, Song PF. Audio similarity detection algorithm based on siamese LSTM network. In: Proc. of the 6th Int'l Conf. on Intelligent Computing and Signal Processing (ICSP). Xi'an: IEEE, 2021. 182–186. [doi: 10.1109/ICSP51882.2021.9408942]

[58] Kordopatis-Zilos G, Papadopoulos S, Patras I, Kompatsiaris Y. Near-duplicate video retrieval with deep metric learning. In: Proc. of the 2017 IEEE Int'l Conf. on Computer Vision Workshops. Venice: IEEE, 2017. 347–356. [doi: 10.1109/ICCVW.2017.49]

[59] Shao J, Wen X, Zhao BC, Xue XY. Temporal context aggregation for video retrieval with contrastive learning. In: Proc. of the 2021 IEEE Winter Conf. on Applications of Computer Vision. Waikoloa: IEEE, 2021. 3267–3277. [doi: 10.1109/WACV48630.2021.00331]

[60] Jiang C, Huang KM, He SF, Yang XD, Zhang W, Zhang XB, Cheng Y, Yang L, Wang Q, Xu FR, Pan T, Chu W. Learning segment similarity and alignment in large-scale content based video retrieval. In: Proc. of the 29th ACM Int'l Conf. on Multimedia. ACM, 2021.

1618–1626. [doi: 10.1145/3474085.3475301]

[61] Li YC, Zhang ZQ, Liu BY, Yang ZY, Liu YX. ModelDiff: Testing-based DNN similarity comparison for model reuse detection. In: Proc. of the 30th ACM SIGSOFT Int'l Symp. on Software Testing and Analysis. ACM, 2021. 139–151. [doi: 10.1145/3460319.3464816]

[62] Guan JY, Liang J, He R. Are you stealing my model? Sample correlation for fingerprinting deep neural networks. In: Proc. of the 36th Int'l Conf. on Neural Information Processing Systems. New Orleans: Curran Associates Inc., 2022. 36571–36584.

[63] Chen HZ, Zhou H, Zhang J, Chen DD, Zhang WM, Chen KJ, Hua G, Yu NH. Perceptual hashing of deep convolutional neural networks for model copy detection. ACM Trans. on Multimedia Computing, Communications, and Applications, 2023, 19(3): 123. [doi: 10.1145/3572777]

[64] Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, Kaiser Ł, Polosukhin I. Attention is all you need. In: Proc. of the 31st Int'l Conf. on Neural Information Processing Systems. Long Beach: Curran Associates Inc., 2017. 6000–6010.

[65] Kordopatis-Zilos G, Papadopoulos S, Patras I, Kompatsiaris Y. ViSiL: Fine-grained spatio-temporal video similarity learning. In: Proc. of the 2019 IEEE/CVF Int'l Conf. on Computer Vision. Seoul: IEEE, 2019. 6350–6359. [doi: 10.1109/ICCV.2019.00645]

[66] Port A, Tiruviluamala N. Mixing constant sum and constant product market makers. arXiv:2203.12123, 2022.

[67] Shi ZS, De Laat C, Grosso P, Zhao ZM. Integration of blockchain and auction models: A survey, some applications, and challenges. IEEE Communications Surveys & Tutorials, 2023, 25(1): 497–537. [doi: 10.1109/COMST.2022.3222403]

[68] Arditi A, Garimidi P, Hirsch D, Milionis I. An initial framework for NFT auction mechanism design: Impossibility results and solutions. 2021. https://timroughgarden.github.io/fob21/reports/r2.pdf

[69] Kulkarni K, Ferreira MVX, Chitra T. Credibility and incentives in gradual Dutch auctions. 2023. https://cdn.prod.website-files.com/648bdc0d4b8ce322f27da0af/66d88f6fcd1770433049409d_Research%2019.pdf

[70] Fazli MA, Owfi A, Taesiri MR. Under the skin of foundation NFT auctions. arXiv:2109.12321, 2021.

[71] Klemperer P. Auction theory: A guide to the literature. Journal of Economic Surveys, 1999, 13(3): 227–286. [doi: 10.1111/1467-6419.00083]

[72] Mayhew BW, Schatzberg JW, Sevcik GR. The effect of accounting uncertainty and auditor reputation on auditor objectivity. AUDITING: A Journal of Practice & Theory, 2001, 20(2): 49–70. [doi: 10.2308/aud.2001.20.2.49]

[73] Weyl EG, Ohlhaver P, Buterin V. Decentralized society: Finding Web3's soul. 2022. https://www.microsoft.com/en-us/research/publication/decentralized-society-finding-web3s-soul/

[74] OP Research. On-chain profiling projects and scenario analysis, exploring the value of Web3 user behavior. 2022 (in Chinese). https://foresightnews.pro/article/detail/12658

[75] Spectral. Introducing Challenge #1: Decentralized credit scoring in Web3. 2023. https://blog.spectral.finance/challenge-1-credit-scoring-web3/

[76] ARCx Labs. Not your average Web3 analytics. https://www.arcxanalytics.com/

[77] Republic. Cultos-Republic. 2022. https://republic.com/cultos

[78] Snapshot. https://snapshot.org/#/

[79] Li C, Palanisamy B, Xu RH, Duan L, Liu JQ, Wang W. How hard is takeover in DPoS blockchains? Understanding the security of coin-based voting governance. In: Proc. of the 2023 ACM SIGSAC Conf. on Computer and Communications Security. Copenhagen: ACM, 2023. 150–164. [doi: 10.1145/3576915.3623171]

[80] Qian P, Liu ZG, He QM, Huang BT, Tian DZ, Wang X. Smart contract vulnerability detection technique: A survey. Ruan Jian Xue Bao/Journal of Software, 2022, 33(8): 3059–3085 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6375.htm [doi: 10.13328/j.cnki.jos.006375]

[81] Dong WL, Liu Z, Liu K, Li L, Ge CP, Huang ZQ. Survey on vulnerability detection technology of smart contracts. Ruan Jian Xue Bao/Journal of Software, 2024, 35(1): 38–62. (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6810.htm [doi: 10.13328/j.cnki.jos.006810]

[82] Zhu LH, Gao F, Shen M, Li YD, Zheng BK, Mao HL, Wu Z. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170–2186 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2017.20170471]

[83] Wuille P. BIP 0032: Hierarchical deterministic wallets. 2012. https://en.bitcoin.it/wiki/BIP_0032

[84] Buterin V. Bitcoin multisig wallet: The future of bitcoin. 2014. https://bitcoinmagazine.com/technical/multisig-future-bitcoin-1394686504

[85] Coinjoins.org. Coinjoins—Learn about collaborative bitcoin transactions. https://www.coinjoins.org/

[86] Monero. Monero research lab (MRL). 2018. https://www.getmonero.org/resources/research-lab/

[87] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: Proc. of the 7th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Gold Coast: Springer, 2001. 552–565. [doi: 10.1007/3-540-45682-1_32]

[88] Zcash. Zcash protocol specification, version 2025.6.3-84-gf58f5c [Overwinter+Sapling+Blossom+Heartwood+Canopy]. 2025. https://zips.z.cash/protocol/canopy.pdf

[89] Ben Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from bitcoin. In: Proc. of the 2014 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2014. 459–474. [doi: 10.1109/SP.2014.36]

[90] Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum J, ed. Advances in Cryptology—CRYPTO 1991. Berlin, Heidelberg: Springer, 1992. 129–140. [doi: 10.1007/3-540-46766-1_9]

[91] Lai YT. ZIP 224: Orchard shielded protocol. 2021. https://zips.z.cash/zip-0224

[92] Wasabi Wallet. Wasabi Wallet—The privacy focused bitcoin wallet. 2018. https://wasabiwallet.io/

[93] World Crypto Index. Coin mixers | What are coin mixers and how do they work? 2018. https://www.worldcryptoindex.com/what-is-a-coin-mixer/

[94] Chen Y, Ma XC, Tang C, Au MH. PGC: Decentralized confidential payment system with auditability. In: Proc. of the 25th European Symp. on Research in Computer Security. Guildford: Springer, 2020. 591–610. [doi: 10.1007/978-3-030-58951-6_29]

[95] Wüst K, Kostiainen K, Čapkun V, Čapkun S. PRCash: Fast, private and regulated transactions for digital currencies. In: Proc. of the 23rd Int'l Conf. on Financial Cryptography and Data Security. Frigate Bay: Springer, 2019. 158–178. [doi: 10.1007/978-3-030-32101-7_11]

[96] Jeong G, Lee N, Kim J, Oh H. Azeroth: Auditable zero-knowledge transactions in smart contracts. IEEE Access, 2023, 11: 56463–56480. [doi: 10.1109/ACCESS.2023.3279408]

[97] Kang H, Dai T, Jean-Louis N, Tao S, Gu XH. FabZK: Supporting privacy-preserving, auditable smart contracts in hyperledger fabric. In: Proc. of the 49th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN). Portland: IEEE, 2019. 543–555. [doi: 10.1109/DSN.2019.00061]

[98] Jiang YH, Li Y, Zhu Y. ACT: Auditable confidential transaction scheme. Journal of Computer Research and Development, 2020, 57(10): 2232–2240 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2020.20200400]

[99] Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S. A fistful of bitcoins: Characterizing payments among men with no names. In: Proc. of the 2013 Conf. on Internet Measurement Conf. Barcelona: ACM, 2013. 127–140. [doi: 10.1145/2504730.2504747]

[100] Kumar A, Fischer C, Tople S, Saxena P. A traceability analysis of Monero's blockchain. In: Proc. of the 22nd European Symp. on Research in Computer Security. Oslo: Springer, 2017. 153–173. [doi: 10.1007/978-3-319-66399-9_9]

[101] Möser M, Soska K, Heilman E, Lee K, Heffan H, Srivastava S, Hogan K, Hennessey J, Miller A, Narayanan A, Christin N. An empirical analysis of traceability in the Monero blockchain. Proc. on Privacy Enhancing Technologies, 2018, 2018(3): 143–163. [doi: 10.1515/popets-2018-0025]

[102] Hinteregger A, Haslhofer B. Short paper: An empirical analysis of Monero cross-chain traceability. In: Proc. of the 23rd Int'l Conf. on Financial Cryptography and Data Security. Frigate Bay: Springer, 2019. 150–157. [doi: 10.1007/978-3-030-32101-7_10]

[103] Zhang ZY, Yin JY, Liu YZ, Liu JW. Deanonymization of litecoin through transaction-linkage attacks. In: Proc. of the 11th Int'l Conf. on Information and Communication Systems. Irbid: IEEE, 2020. 59–65. [doi: 10.1109/ICICS49469.2020.239510]

[104] Wang ZP, Chaliasos S, Qin KH, Zhou LY, Gao LF, Berrang P, Livshits B, Gervais A. On how zero-knowledge proof blockchain mixers improve, and worsen user privacy. In: Proc. of the 2023 ACM Web Conf. Austin: ACM, 2023. 2022–2032. [doi: 10.1145/3543507.3583217]

[105] Dey S. Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work. In: Proc. of the 10th Computer Science and Electronic Engineering (CEEC). Colchester: IEEE, 2018. 7–10. [doi: 10.1109/CEEC.2018.8674185]

[106] Pham T, Lee S. Anomaly detection in the bitcoin system—A network perspective. arXiv:1611.03942, 2017.

[107] Chen T, Li ZH, Zhu YX, Chen JC, Luo XP, Lui JCS, Lin XD, Zhang XS. Understanding Ethereum via graph analysis. ACM Trans. on Internet Technology, 2020, 20(2): 18. [doi: 10.1145/3381036]

[108] Shen M, Sang AQ, Zhu LH, Sun RG, Zhang C. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency. Chinese Journal of Computers, 2021, 44(1): 193–208 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.00193]

[109] Koshy P, Koshy D, Mcdaniel P. An analysis of anonymity in bitcoin using P2P network traffic. In: Proc. of the 18th Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2014. 469–485. [doi: 10.1007/978-3-662-45472-5_30]

[110] Gervais A, Ritzdorf H, Karame GO, Capkun S. Tampering with the delivery of blocks and transactions in bitcoin. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. Denver: ACM, 2015. 692–705. [doi: 10.1145/2810103.2813655]

[111] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in bitcoin P2P network. In: Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security. Scottsdale: ACM, 2014. 15–29. [doi: 10.1145/2660267.2660379]

[112] Spagnuolo M, Maggi F, Zanero S. BitIodine: Extracting intelligence from the bitcoin network. In: Proc. of the 18th Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2014. 457–468. [doi: 10.1007/978-3-662-45472-5_29]

[113] McLaughlin R, Kruegel C, Vigna G. A large scale study of the Ethereum arbitrage ecosystem. In: Proc. of the 32nd USENIX Conf. on Security Symp. Anaheim: USENIX Association, 2023. 3295–3312.

[114] Li ZH, Li JF, He ZY, Luo XP, Wang T, Ni XZ, Yang WW, Chen X, Chen T. Demystifying DeFi MEV activities in flashbots bundle. In: Proc. of the 2023 ACM SIGSAC Conf. on Computer and Communications Security. Copenhagen: ACM, 2023. 165–179. [doi: 10.1145/3576915.3616590]

[115] Das D, Bose P, Ruaro N, Kruegel C, Vigna G. Understanding security issues in the NFT ecosystem. In: Proc. of the 2022 ACM SIGSAC Conf. on Computer and Communications Security. Los Angeles: ACM, 2022. 667–681. [doi: 10.1145/3548606.3559342]

[116] Cernera F, La Morgia M, Mei A, Sassi F. Token spammers, rug pulls, and sniper bots: An analysis of the ecosystem of tokens in Ethereum and in the binance smart chain (BNB). In: Proc. of the 32nd USENIX Security Symp. Anaheim: USENIX Association, 2023. 3349–3366.

[117] Garman C, Green M, Miers I. Accountable privacy for decentralized anonymous payments. In: Proc. of the 20th Int'l Conf. on Financial Cryptography and Data Security. Christ Church: Springer, 2017. 81–98. [doi: 10.1007/978-3-662-54970-4_5]

[118] Li YN, Yang GM, Susilo W, Yu Y, Au MH, Liu DX. Traceable Monero: Anonymous cryptocurrency with enhanced accountability. IEEE Trans. on Dependable and Secure Computing, 2021, 18(2): 679–691. [doi: 10.1109/TDSC.2019.2910058]

[119] Shen M, Che Z, Zhu LH, Xu K, Gao F, Yu CC, Wu Y. Anonymity in blockchain digital currency transactions: Protection and confrontation. Chinese Journal of Computers, 2023, 46(1): 125–146 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2023.00125]

[120] Yan KL, Zhang JL, Liu XY, Diao WR, Guo SQ. Bad apples: Understanding the centralized security risks in decentralized ecosystems. In: Proc. of the 2023 ACM Web Conf. Austin: ACM, 2023. 2274–2283. [doi: 10.1145/3543507.3583393]

[121] Wang ZW, Gao JS, Wei XT. Do NFTs' owners really possess their assets? A first look at the NFT-to-asset connection fragility. In: Proc. of the 2023 ACM Web Conf. Austin: ACM, 2023. 2099–2109. [doi: 10.1145/3543507.3583281]

[122] Zuo WR, Raman A, Mondragón RJ, Tyson G. Set in stone: Analysis of an immutable Web3 social media platform. In: Proc. of the 2023 ACM Web Conf. Austin: ACM, 2023. 1865–1874. [doi: 10.1145/3543507.3583510]

[123] Qin KH, Zhou LY, Gervais A. Quantifying blockchain extractable value: How dark is the forest? In: Proc. of the 2022 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2022. 198–214. [doi: 10.1109/SP46214.2022.9833734]

[124] Li XG, Yepuri A, Nikiforakis N. Double and nothing: Understanding and detecting cryptocurrency giveaway scams. In: Proc. of the 2023 Network and Distributed Systems Security (NDSS) Symp. San Diego: Internet Society, 2023. [doi: 10.14722/ndss.2023.24584]

[125] Torres CF, Willi F, Shinde S. Is your wallet snitching on you? An analysis on the privacy implications of Web3. In: Proc. of the 32nd USENIX Conf. on Security Symp. Anaheim: USENIX Association, 2023. 769–786.

[126] He BW, Chen Y, Chen Z, Hu XH, Hu YF, Wu L, Chang R, Wang HY, Zhou YJ. TxPhishScope: Towards detecting and understanding transaction-based phishing on Ethereum. In: Proc. of the 2023 ACM SIGSAC Conf. on Computer and Communications Security. Copenhagen: ACM, 2023. 120–134. [doi: 10.1145/3576915.3623210]

附中文参考文献

[12] 李辉忠, 李陈希, 李昊轩, 白兴强, 石翔. FISCO BCOS 技术应用实践. 信息通信技术与政策, 2020, 46(1): 52–60. [doi: 10.3969/j.issn.1008-9217.2020.01.011]

[74] OP Research. 链上画像项目与场景分析, 探索 Web3 用户行为价值. 2022. https://foresightnews.pro/article/detail/12658

[80] 钱鹏, 刘振广, 何钦铭, 黄步添, 田端正, 王勋. 智能合约安全漏洞检测技术研究综述. 软件学报, 2022, 33(8): 3059–3085. http://www.jos.org.cn/1000-9825/6375.htm [doi: 10.13328/j.cnki.jos.006375]

[81] 董伟良, 刘哲, 刘逵, 黎立, 葛春鹏, 黄志球. 智能合约漏洞检测技术综述. 软件学报, 2024, 35(1): 38–62. http://www.jos.org.cn/1000-9825/6810.htm [doi: 10.13328/j.cnki.jos.006810]

[82] 祝烈煌, 高峰, 沈蒙, 李艳东, 郑宝昆, 毛洪亮, 吴震. 区块链隐私保护研究综述. 计算机研究与发展, 2017, 54(10): 2170–2186. [doi: 10.7544/issn1000-1239.2017.20170471]

[98] 姜轶涵, 李勇, 朱岩. ACT: 可审计的机密交易方案. 计算机研究与发展, 2020, 57(10): 2232–2240. [doi: 10.7544/issn1000-1239.2020.20200400]

[108] 沈蒙, 桑安琪, 祝烈煌, 孙润庚, 张璨. 基于动机分析的区块链数字货币异常交易行为识别方法. 计算机学报, 2021, 44(1): 193–208. [doi: 10.11897/SP.J.1016.2021.00193]

[119] 沈蒙, 车征, 祝烈煌, 徐恪, 高峰, 余聪聪, 吴言. 区块链数字货币交易的匿名性: 保护与对抗. 计算机学报, 2023, 46(1): 125–146. [doi: 10.11897/SP.J.1016.2023.00125]

作者简介

王斌, 博士生, 主要研究领域为 Web 3.0, 区块链安全.

伍羽放, 博士生, 主要研究领域为 Web 3.0, 区块链安全.

高阳, 硕士生, 主要研究领域为 Web 3.0, 区块链安全.

刘天健, 硕士生, 主要研究领域为 Web 3.0, 区块链安全.

翁渊, 博士生, 主要研究领域为 Web 3.0, 区块链安全.

李超, 博士, 副教授, CCF 高级会员, 主要研究领域为 Web 3.0, 区块链安全.

张大伟, 博士, 副教授, 主要研究领域为 Web 3.0, 区块链隐私保护.

徐光侠, 博士, 教授, CCF 高级会员, 主要研究领域为 Web 3.0, 区块链理论技术.

许光全, 博士, 教授, CCF 杰出会员, 主要研究领域为 Web 3.0, 物联网安全.

祝咏升, 博士生, 副研究员, 主要研究领域为 Web 3.0, 铁路信息网络架构.

沈蒙, 博士, 教授, CCF 杰出会员, 主要研究领域为 Web 3.0, 区块链安全.

祝烈煌, 博士, 教授, CCF 杰出会员, 主要研究领域为 Web 3.0, 区块链安全, 网络与信息安全.

王伟, 博士, 教授, CCF 专业会员, 主要研究领域为 Web 3.0, 区块链安全, 隐私计算.