Web3.0 领域技术人员法律合规分析报告

北京市京顺律师事务所

Web3.0 法律合规团队

2025 年 5 月

前言

随着区块链、加密货币、去中心化应用（DApp）、智能合约等 web3.0 技术的快速发展，全球互联网正经历着从 Web2.0 向 Web3.0 的深刻变革。Web3.0 不仅推动了数字经济、数字资产和新型商业模式的诞生，也为技术人才带来了前所未有的职业机遇。越来越多的程序员希望投身 web3.0 行业，参与到区块链底层开发、智能合约编写、去中心化应用设计等前沿领域，获得更广阔的职业发展空间。

根据《"十四五"数字经济发展规划》及《区块链技术和应用发展白皮书（2023年）》等政策文件，国家鼓励区块链等新兴技术的创新应用，推动数字经济与实体经济深度融合。与此同时，监管部门对加密货币、虚拟资产等领域实施了严格的合规要求，强调防范金融风险和保护用户权益。

在此背景下，web3.0 行业的特殊性也带来了诸多法律与合规风险。程序员在转型过程中，既面临着技术创新和高薪发展的机遇，也需应对劳动合同、薪酬结算、税务申报、数据安全、项目合规等多方面的挑战。合规问题已成为影响职业选择和行业健康发展的重要因素。

为帮助程序员群体全面了解 web3.0 行业的法律环境、识别并有效防控相关风险，本所 web3.0 法律合规团队特出具本分析书，系统梳理 web3.0 程序员转型过程中可能遇到的主要风险、相关法律法规依据及风险控制建议，助力程序员群体安全、合规地迈向 web3.0 新领域。

第一篇 web3.0 行业定义与发展现状

一、 Web3.0 的定义与技术本质

“Web3”是“Web 3.0”的简称，是互联网发展的第三阶段，继承并超越了传统“Web 1.0（静态网页）”和“Web 2.0（用户生成内容与中心化平台）”模式。Web3.0 核心特征是**去中心化**(Decentralization)、**用户主权**(User Ownership)和**价值互联**（Value Internet）。

Web3.0 并不是某一项具体的技术，而是由一系列新兴技术构成的集合体，包括：

- **区块链技术**：用于数据的可信存储与不可篡改；
- **智能合约**：用于去中心化应用（DApps）的自动执行；
- **去中心化身份（DID）与零知识证明**：用于用户身份管理与隐私保护；
- **代币经济机制（Tokenomics）**：用于激励机制设计；
- **DAO（去中心化自治组织）**：实现社区共治的组织方式。

Web3.0 并非等同于“虚拟货币”或“炒币”，它本质上是一种以**信任机制重构数据与价值交换关系**的技术范式转变。从技术角度看，Web3.0 不是某一单一行业或业务，而是一系列新兴技术的融合应用，其技术本身具有中立性，广泛应用于金融、游戏、社交、供应链、版权、身份管理等多个领域。

二、 国内外 Web3.0 发展现状

2.1 海外发展趋势

自 2020 年以来，Web3.0 作为全球数字经济发展的重要方向之一，已在多个国家和地区形成初步产业体系。具体表现如下：

- **美国**：硅谷资本大量进入 Web3.0 初创公司，Coinbase、Ethereum 基金会、OpenSea、Solana Labs 等头部企业占据产业核心；
- **欧洲**：欧盟发布《加密资产市场法案》(MiCA)，提出统一监管路径，鼓

励合规创新；

- **新加坡、阿联酋**：推行包容性监管沙盒，吸引大量 Web3.0 项目和技术人才入驻；
- **以太坊、Polkadot、Cosmos 等公链生态**：推动 DApp 开发、跨链互操作、模块化区块链等技术演进。

自 2018 年以来，全球 Web3.0 技术和应用逐渐成熟，以下是主要趋势：

- **技术层**：以 Ethereum、Solana、Polkadot 等为代表的链上基础设施持续演进，智能合约语言（如 Solidity、Rust、Move）开发人才需求高速增长。
- **应用层**：DeFi、NFT、DAO、DID 等应用场景不断扩展，为开发者提供了大量编程、设计与运维岗位。
- **开发范式变化**：前端+合约+节点协同开发成为主流，远程、开源、Bounty（赏金）成为开发者新型就业方式。

📌 参考数据：据 Electric Capital 2024 年报告，全球 Web3.0 月活跃开发者超过 25 万人，90%以上为远程开发者，60%为非加密背景程序员转型而来。

2.2 国内的发展态度与路径

尽管中国大陆对**虚拟货币投机、ICO 融资等金融风险活动**实施严格监管，但对于**区块链技术**与 **Web3.0 创新能力建设**始终保持鼓励态度：

政策方面	技术层面
2021 年《“十四五”数字经济发展规划》明确提出：“推动区块链、隐私计算、分布式身份认证等前沿技术创新应用”	腾讯、蚂蚁、百度等大型科技公司布局“联盟链”“数字藏品平台”
2023 年中央网信办提出“有序推进	高校如清华、复旦、中科院等设立“区

Web3.0 等新一代互联网架构研究与试点”	块链研究院”推动人才培养
多地（如北京、上海、海南）设立“区块链创新试验区”，鼓励合法场景应用	工信部发布多项区块链技术评估标准，如 BSN（区块链服务网络）等国家级底层设施

中国大陆对区块链技术本身持支持态度，但对加密货币相关活动（如 ICO、交易、支付等）实行严格监管。主要法规包括：《关于防范代币发行融资风险的公告》（2017 年 9 月 4 日，七部委联合发布）；《关于进一步防范和处置虚拟货币交易炒作风险的通知》（2021 年 9 月 24 日，央行等十部委联合发布）；《中华人民共和国网络安全法》；《中华人民共和国数据安全法》；《中华人民共和国个人信息保护法》等法律法规。因此，中国大陆政府对 Web3.0 相关技术态度总体上保持**“支持底层创新，严控金融风险”**的原则：

领域	政策导向	文件依据
区块链基础技术	鼓励研发与融合创新	《十四五国家信息化规划》、《区块链白皮书（2022）》
区块链+政务、供应链等场景	鼓励产业落地试点	工信部、地方政府多个示范区建设
NFT（数字藏品）	控制炒作，鼓励合规数字版权	网信办、人民银行等通报
虚拟货币、ICO 等活动	明令禁止	2017 年七部委《代币融资风险公告》、2021 年《关于防范虚拟货币交易炒作风险的通知》

综上，技术本身受到政策支持，但以“代币融资、炒作、面向公众推广”为核心的行为高度敏感。因此，程序员学习技术、从事远程开发、参与开源项目是合法的，而涉及代币募资、投资推荐、KOL 推广等行为则存在合规风险。

第二篇 web3.0 技术人员风险分析及合规建议

一、项目合规

1.1 非法业务风险

根据中国的监管政策，中国自 2021 年起明确禁止加密货币交易、挖矿及相关业务。若公司业务涉及加密货币的交易与挖矿业务，即使公司注册在海外，若服务对象为中国大陆用户，仍可能被追究“非法吸收公众存款罪”“集资诈骗罪”法律责任；若公司业务被认定为 ICO、资金盘或洗钱，员工可能面临“非法经营罪”、“洗钱罪”或“帮助信息网络犯罪”的指控；若公司业务涉及传销活动，则员工可能涉嫌“组织、领导传销活动罪”（仅组织者、领导者获罪）；若公司业务涉及赌博等非法活动，其中员工可能涉及“开设赌场罪”等。

1.2 业务识别合规建议

根据上述场景，技术人员所选择的公司业务异常重要，因此在这一环节中识别业务的非法性异常重要，建议在选择 web3 相关工作或项目时，务必充分了解公司及其业务的合法性，尤其要避免参与任何涉及加密货币交易、挖矿、ICO、资金盘、洗钱、传销、赌博等被中国法律明令禁止的活动。即使公司注册在海外，只要服务对象涉及中国大陆用户，相关风险依然存在。遇到可疑业务时要及时拒绝参与，并主动向专业机构或法律顾问咨询，对公司业务充分背调，选择有牌照的大公司，以免给自己带来法律和职业上的严重后果。

二、隐私与数据安全

2.1 隐私与数据风险

Web3 技术人员面临多重隐私与数据安全风险：其一，链上数据公开性导致开发者的钱包地址、交易记录可能被追踪分析，暴露个人身份或资产信息；其二，智能合约漏洞（如重入攻击、权限缺陷）可能被黑客利用窃取用户敏感数据或资产；其三，去中心化存储（如 IPFS）若未加密或权限设置不当，易导致隐私文件非法访问；其四，远程协作工具（如未加密通信）可能泄露代码密钥或商业机密。此外，参与匿名协议开发（如混币器）可能因技术被用于洗钱而承担连带法律责

任。

2.2 数据安全合规建议

建议开发者尽可能使用去标识化身份参与开源社区（如使用技术账号而非实名）、通过硬件钱包或多签方案保障数字资产安全、避免在链上部署合约时绑定真实身份信息（如 ENS、邮箱、Github 名等）；同时，应接受数据最小化原则培训，减少在不受控平台发布个人数据。此外，可借助于 web3.0 领域专业平台，提供隐私风险评估、数据隔离部署工具、私钥管理训练等合规服务，从源头降低链上身份与个人现实身份之间的联动风险。

三、就业合规

3.1 劳动风险

许多 web3.0 企业注册在海外，采用远程办公、加密货币或外币结算。根据《中华人民共和国劳动合同法》》规定，中国劳动者与境外企业签订劳动合同，若工作地点在中国境内，仍可能适用中国劳动法相关规定。但实际维权难度较大，劳动争议处理、社会保险缴纳等存在不确定性。同时，海外公司通常不为中国员工缴纳社保、公积金，个人需自行承担相关风险。未依法缴纳社保，劳动者在医疗、工伤、失业等方面的权益无法保障。

3.2 劳动权益保护

对于选择与海外 web3 公司远程就业的程序员来说，务必提前了解劳动合同、薪酬结算、社保缴纳等方面的具体安排，切勿忽视自身权益保障。由于跨境劳动关系维权难度较大，建议在签约前寻求专业机构的法律咨询和合同审核服务，确保合同条款明确、合法，最大程度降低劳动争议和社保缺失带来的风险。专业机构不仅能帮助识别潜在合规问题，还能在遇到纠纷时为个人提供法律支持和维权指导，有效维护自身合法权益。

四、薪酬结算与税务风险

4.1 加密货币/外币结算

根据中国境内监管政策，如境内人员直接收取加密货币或外币，可能违反中

国外汇管理规定。加密货币在中国大陆被严格监管，相关交易和支付存在法律风险。如果通过非正规渠道收取外币或加密货币，可能被认定为非法金融活动。

另外，如果未依法申报境外收入，或对加密货币收入未如实申报，可能构成逃税，承担法律责任。加密货币收入应折算为人民币后申报，税务机关有权追溯未申报收入。

4.2 结算与税务合规建议

对于通过加密货币或外币结算薪酬的情况，建议务必通过正规渠道收款，并严格按照中国相关税务规定如实申报境外收入，避免因违规收款或逃税而承担法律风险。由于加密货币和外币结算涉及复杂的外汇和税务合规问题，建议在入职前或收款前，保留相关收入凭证，并主动寻求专业机构的指导。专业机构能够帮助个人梳理合规流程、规避政策风险，并在申报、汇兑等环节提供全程支持，确保薪酬结算合法合规，切实保障自身利益。

第三篇 整体合规建议与风险防控措施

针对以上分析的情形，为帮助 Web3 项目技术人员降低法律风险，提出以下合规建议:

1.尽职调查项目合规性

在参与任何 Web3 项目之前，务必对项目的商业模式和合规性进行充分了解。核实项目是否涉及面向中国境内公众募集资金、发行代币、承诺保本付息等行为;是否包含拉人头推广、多级分销;是否有博彩竞猜功能;以及资金流动是否涉及非法渠道。如果发现项目可能涉嫌非法金融活动(如未经许可公开集资等)，应提高警惕。特别指出，一些未经批准发行虚拟币并向社会宣传募资的行为已构成犯罪，程序员在加入此类项目前应充分认识风险。必要时，可要求项目方出具法律意见书或相关部门的许可文件。如果项目本身在法律上存疑，建议谨慎参与或直接拒绝。

2.坚守法律红线，不执行非法指令

程序员在开发过程中应坚持职业操守，对明显违法的开发要求坚决说“不”。例如，若被要求开发篡改交易数据以欺骗用户的功能、植入资金盘多层级返利机制、设置真钱兑换渠道用于赌博，或其他显失公允的需求，应当怀疑其合法性。的案例表明，技术人员按违法要求修改 K 线导致投资人受骗，最终被认定构成犯罪。因此，当上级或合作方的指令涉嫌违反法律时，开发人员有责任拒绝实施，并可提出质疑或建议合法替代方案。切勿为了报酬或服从心理而参与实现明显非法的功能模块。一旦留存了自己开发非法功能的证据，将来极难在司法中脱身。

3.限定自身角色，避免深度介入可疑业务

如果身处的项目领域合规风险较高(如涉及资金、交易的领域)，程序员应尽量限定自己的职责在纯技术范畴，避免介入资金管理、市场推广等敏感环节。技术人员参与业务运营越多，越容易被认定为共犯中的重要成员。在高风险项目中，保持相对独立的技术顾问或合同制开发身份，记录好自己的工作范围，有助于在事后证明自己并非犯罪策划者。例如，不经手用户资金账号、不参与制定投资收益方案等，可以作为自己作用有限的佐证。当然，这并非意味着可以明知违法还

继续做技术支持;而是在合法前提下，尽量不涉足非技术事务，以免被认定“角色转化”为项目组织者的一部分。

4.加强合规沟通与风控意识

在开发过程中，主动与公司法务合规团队沟通，了解项目是否采取了必要的风控措施。例如，询问项目方是否对用户进行了 KYC 身份认证和 AML(反洗钱)监控、平台是否设置了反传销和反赌的技术屏障等。指出，在技术开发阶段需要做好数据安全、用户隐私及技术安全合规，在宣传推广阶段必须遵守所在地法律。程序员应将这些要求融入开发工作:例如，实现交易监测和可疑行为报警功能，防止平台被用于洗钱或诈骗;限制用户转账频率和额度，防范资金盘跑路;禁止在产品中内置多级分销接口，避免被不法营销利用。通过技术手段预防违法场景发生，既是合规要求也是自我保护。一旦发现自己开发的系统被运营方滥用于非法目的，应及时提出警告和整改建议。

5.及时止损，远离非法业务

如果在工作过程中逐步发现所在项目出现违法苗头，应当果断采取行动。“及时止损”既是对投资者的告诫，也是对从业者的提醒。具体而言，当程序员觉察公司业务模式不对劲(例如突然要求删除数据销毁证据、或开展明显违反监管政策的活动)，应首先自我保护:记录相关情况并向上级书面报告表达疑虑。如果公司依然执意为之且无法纠正，技术人员应考虑立即退出该项目，以切断进一步的共犯关系。强调，一旦发现公司业务或自身工作内容有任何违法行为，要及时悬崖勒马。切勿因为已经投入精力或抱有一丝侥幸而“骑虎难下”。要明白，及早退出不仅能减少自己卷入违法行为的时间跨度，也是将来区分责任的重要因素(脱离犯罪集团越早，相对责任越小)。必要时，可以匿名向监管机关举报涉案业务以阻止犯罪扩大，并作为自己拒绝违法的证明。

6.保存证据，划清责任边界

在日常工作中，注意保存能够体现自己工作性质的记录。例如，保存劳动合同或外包合同,明确约定自己的职责仅为技术开发,不涉及经营决策;保留邮件、聊天记录，证明自己曾就可疑事项向主管提出疑问或反对意见;记录项目需求变

更通知，以证明某违法功能可能是在自己离职后才由他人加入等。这些资料在事后都有可能成为区分程序员是无辜参与还是共谋的关键证据。在刑事调查中，如果能提供书面证据显示程序员曾抗拒非法指令或不知情某些业务，将有利于争取从轻或不起诉处理。当然，保存证据不是为了对抗公司，而是作为自我保护的手段之一，应在不违法、不违背职业道德的前提下进行。

7. 研读政策法规，持续学习合规要求

Web3 领域技术更新快，监管政策也在快速演变。开发人员应当关注中国有关虚拟资产的新规和典型案例。持续学习可以使程序员在接到业务需求时，提高直觉判断力，一眼识破潜在法律风险。公司层面也应当对技术团队进行合规培训，让程序员了解非法集资、传销、赌博等行为的法律特征和边界，做到心中有数。

8. 寻求专业机构的意见

当遇到拿不准的情况，例如项目要求设计复杂的代币经济模型，涉及投资者权益和资金池管理，此时应建议该领域的专业机构人员或者专业律师。在当前环境下，“谋定而后动”胜过事后补救。如果经专业评估确认项目存在重大刑事风险，那么技术人员可据此慎重决策去留。正如业内所言，Web3 创新层出不穷，运营模式层层包装，传统开发者难以辨别法律风险时，一定要寻求专业意见。专业机构和人员的指导能够为程序员指出哪些做法是安全的、哪些红线绝不可碰，从而避免无意中触法。