



中國投資協會

TAHOTA  
泰和泰

2022

全球区块链产业

规范与治理

分析报告

中国投资协会新基建投资专业委员会

泰和泰（上海）律师事务所

# 2022

## 全球区块链产业规范与治理 分析报告

## 特别声明

本报告由中国投资协会新基建投资专业委员会与泰和泰（上海）律师事务所区块链法律实验室—BClaw 团队共同整理分析。本报告仅做区块链合规应用、规范发展借鉴，比较之用途，并非针对任何自然人或机构而出具，也不构成任何法域下的法律意见或投资建议。未经发布方书面授权，不得转载或使用该报告中的内容（含文字、图片等资料）。如您有意就相关话题进一步交流探讨，欢迎联系 BClaw 团队。



扫一扫上面的二维码图案，加我为朋友



报告撰写团队：王宜峰    刘 兴    王振华    韩颖梅  
张竹一    王彦恺    王心依    何美婕

## 前 言

区块链被认为是人类第五次计算革命。随着区块链由以比特币为代表的 1.0 时代向大规模商用化的 3.0 时代的发展，发展区块链技术产业已经上升为国家战略的重要环节。国务院在《“十四五”数字经济发展规划的通知》中“加快推动数字产业化”部分提出，增强关键技术创新能力，需要瞄准传感器……区块链、新材料等战略性前瞻性领域，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力。因此，可以预见，区块链必将为经济社会发展创造更多机遇，为社会治理带来更大变革。2021 年，区块链产业政策继续保持强劲态势，中央和地方密集发布相关文件，范围覆盖电子政务、乡村振兴、智能制造等多个领域。

区块链的商用也同样处于蓬勃发展期，大量国际企业不仅将区块链技术应用于供应链、内控等管理范畴，更是开始布局区块链的产业应用。在国内，包括“区块链+碳中和”、“区块链+金融监管”在内的多项应用，预示着区块链技术将继续赋能传统产业转型升级，推动新业态诞生与发展。

但也应注意到，在区块链 3.0 时代相关产业大面积铺开的同时，对区块链技术应用的合规与监管仍然是需要严肃面对的课题。区块链技术最显著的特征在于多中心化、高隐私性、高自治性与高可信度。以隐私性为例，区块链除通过密码学技术进行信息加密外，还针对特定成员或用户的联盟链具有网络准入与节点授权功能。区块链的高隐私性为个人信息与商业秘密保护提供了便利，但也成为金融犯罪的高风险地带，使得传统反洗钱手段面临技术代差。另外，区块链从业人员合规意识不足、反洗钱与反恐怖主义融资意识不强、忽视税收风险等问题若得不到重视也将阻碍区块链应用的合规发展。因此，合规与监管是区块链技术健康发展的关键。

作为中国律师行业早期从事区块链法律研究与服务的团队，BClaw 区块链法律实验室始终以合规与监管为核心对区块链持续实践，不断为区块链行业的规范发展建言献策。

通过撰写方团队持续数月整理，《2022 全球区块链产业规范与治理分析报告》终于出炉，该报告既分析总结了我国国内与区块链产业相关的立法、司法

和政策动态，也从全球视角出发，对世界各主要经济体的区块链合规监管规范进行了整理与解读，希望通过国际视角为我国区块链产业发展提供更多借鉴及更有益监管的维度，为区块链从业人员和区块链相关企业提供较为明确的合规指引，使我国在区块链技术广泛应用中不断保持国际领先优势，助力我国数字经济建设。

## 目 录

第一章 坚守：中国区块链强监管 重合规.....	1
一、当前区块链主要监管规范.....	1
二、国家层面区块链产业政策.....	10
三、部分省市区块链产业政策.....	12
四、典型意义区块链案例分析.....	17
五、区块链从业者易涉及的法律风险.....	24
第二章 远观：全球主要经济体区块链监管动态.....	29
一、亚洲地区.....	29
二、欧洲地区.....	34
三、北美洲地区.....	37
四、南美洲地区.....	40
五、大洋洲地区.....	42
第三章 解析：典型应用场景.....	45
一、2021 年全球区块链产业融资.....	45
二、具有影响力的跨国企业表现.....	45
三、NFT——赋能文化艺术.....	49
四、生成型电子文书平台——可信的“意思表示”.....	56
第四章 瞻望：合规与监管.....	68
一、央行数字货币——建设数字经济底座.....	68
二、司法存证——为公平正义.....	73
三、他领域——风华尽展.....	80

四、挑战——无处不在.....	83
第五章 致未来.....	90
参考文献.....	92





## 第一章 坚守

### 中国区块链强监管 重合规

#### 一、当前区块链主要监管规范

区块链作为数字经济的底层技术，我国一直予以重视并鼓励区块链在各个领域的大范围探索应用，但于此同时，技术创新作为双刃剑也必然伴随着风险。一些区块链从业人员法律意识欠缺、风险与合规意识淡薄、管理措施与技术保障能力低下等问题造成的合规风险时有发生。更有甚者将区块链技术概念用于违法犯罪，并因此引发了大量传销、集资诈骗等刑事案件。

近年来，我国针对互联网领域的立法动态活跃，网络安全、数据保护等专门性立法不断出台和逐步完善。为保障区块链产业的健康发展，区块链从业人员应当及时了解现行法律法规，提升合规意识。本节将按照法律规范层级对2021年新出台的相关法律法规进行梳理归纳，为区块链从业者提示合规与监管红线。

##### （一）法律

除《中华人民共和国民法典》、《中华人民共和国刑法》及此前通过的《网络安全法》、《电子商务法》、《电子签名法》外，2021年通过《个人信息保护法》、《数据安全法》与《科学技术进步法》对区块链有较大影响。

##### 1. 《中华人民共和国个人信息保护法》

该法于2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过，于2021年11月1日实施，是继《网络安全法》《电子商务法》《消费者权益保护法》与《刑法》针对个人信息保护内容进行专项修改，及《民法典》将个人信息保护作为一项重要民事权利规定后，针对个人信息的专门立法。

《个人信息保护法》增强了法规范的系统性、针对性和可操作性。区块链从业者需要关注：

（1）个人信息处理规则。处理个人信息应当采用正当方式，具有明确目的且限于实现处理目的的最小范围。该法确立了以“告知—同意”为核心的一系列个人信息处理规则。设专节对处理敏感个人信息作出更严格的限制，只有在

具有特定的目的和充分的必要性的情形下，方可处理敏感个人信息，并且应当取得个人的单独或书面同意。

(2) 个人信息跨境提供规则。首先，跨境提供个人信息的“告知-同意”规则在该法中被更严格要求：应当向个人告知境外接收方名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类等事项，并取得个人单独同意。其次，对于关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的处理者，若确需向境外提供个人信息的，规定应当通过国家网信部门组织的安全评估；其他需要跨境提供个人信息的，则规定了经专业机构认证等途径。

(3) 个人信息处理活动中处理者的义务。该法明确了个人信息处理者的合规管理和保障个人信息安全等义务，要求制定内部管理制度和操作规程，采取安全技术措施，并指定负责人对其个人信息处理活动进行监督；要求定期对其个人信息活动进行合规审计；对处理敏感个人信息、向境外提供个人信息等高风险处理活动，应事前进行风险评估；履行个人信息泄露通知和补救义务等。

## 2. 《中华人民共和国数据安全法》

该法于 2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过，于 2021 年 9 月 1 日实施。数据是数字经济的基础，该法将数据安全上升到总体国家安全观的高度，旨在建立健全与此相适应的数据安全治理体系和提高数据安全保障能力。

区块链运行的基础是数据；区块链的大规模商用本质是数据处理，包括数据的收集、存储、加工、传输、提供等行为。因此，区块链健康发展的关键是数据安全。该法第 3 条同时明确“数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。区块链从业者须关注：

(1) 数据安全保护义务。开展数据处理活动应当建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。应当加强风险监测，定期开展风险评估并向有关主管部门报送。数据交易中介服务机构提供服务需承担法定的数据审核义务，并需要依法留存审核、交易记录。

(2) 政务数据安全与开放。对于电子政务建设中的政务服务提供方，该法专章规定了政务数据安全内容。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

### 3. 《中华人民共和国科学技术进步法》

该法于 2021 年 12 月 24 日第十三届全国人民代表大会常务委员会第三十二次会议第二次修订，于 2022 年 1 月 1 日起施行。该法是科技领域的基本法，是国家推动科学技术进步、坚持新发展理念、坚持科技创新与自立自强的重要法律依据。

随着区块链技术在应用层的大范围推广，国家层面的区块链应用研究与成果转化、企业科技创新、税收优惠及保障措施方面的内容也在持续跟进。该法第 29 条明确，国家加强面向产业发展需求的共性技术平台和科学技术研究开发机构建设；第 43 条明确，包括但不限于科技型中小企业、投资初创科技型企业的创业投资企业是法定税收优惠主体；第 87 条要求，财政性科学技术资金的适用对象包括“重大共性关键技术应用和高新技术产业化示范”。

## (二) 行政法规

### 1. 《关键信息基础设施安全保护条例》

该条例于 2021 年 7 月 30 日公布，9 月 1 日起施行，是《网络安全法》的下位法，该条例专章要求强化关键信息基础设施运营者的主体责任。随着区块链技术在政务服务领域的普及，政务服务提供者、运营者需要基于该条例完善自身合规体系，加强网络安全监管。运营者需要建立健全网络安全保护制度与责任制：设置专门安全管理机构，并对负责人和关键岗位人员进行安全背景审查；承担风险评估义务，应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估；具有通报义务，在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，应及时向网信部门、公安部门报告。

同时，运营者的专门安全机构的具体职责在本法中也进行了相应规定。包括拟订关键信息基础设施安全保护计划，开展网络安全监测、检测和风险评估，制定本单位应急预案，定期开展应急演练，处置网络安全事件，建立健全

个人信息和数据安全保护制度等。

## 2. 《防范和处置非法集资条例》

该条例于 2021 年 1 月 26 日公布，5 月 1 日起施行，着力解决行政机关防范和处置非法集资的法律依据不足、手段不够等问题。

“非法集资”在现行刑法中对应非法吸收公众存款罪与集资诈骗罪，而在行政法规中则突出预防性，将“非法集资”行为一体化作为规制对象，坚持防范为主、打早打小、综合治理、稳妥处置的原则。

由于近年来政策对虚拟货币的打击维持高压态势，该条例是对《国务院关于进一步做好防范和处置非法集资工作的意见》（国发〔2015〕59 号）的进一步细化。主要包括：

（1）定义非法集资。条例第 2 条规定，非法集资是指未经国务院金融管理部门依法许可或者违反国家金融管理规定，以许诺还本付息或者给予其他投资回报等方式，向不特定对象吸收资金的行为。据此，即使是自然人间帮助他人投资虚拟货币的行为，也存在被认定为非法集资的风险，情节严重的可能涉嫌非法吸收公众存款罪。

（2）企业名称与经营范围的限制。条例第 9 条要求，除法律、行政法规和国家另有规定外，企业、个体工商户名称和经营范围中不得包含“金融”、“交易所”、“交易中心”、“理财”、“财富管理”、“股权众筹”等字样或者内容。若存在其他与集资有关的字样或内容的，条例要求包括市场监督管理部门在内的处置非法集资牵头单位“及时予以重点关注”。

（3）涉嫌非法集资的行为。条例第 19 条对常见的非法集资行为进行了不完全列举，包括但不限于：①设立互联网企业、投资及投资咨询类企业、各类交易场所或者平台、农民专业合作社、资金互助组织以及其他组织吸收资金；②以发行或者转让股权、债权，募集基金，销售保险产品，或者以从事各类资产管理、虚拟货币、融资租赁业务等名义吸收资金；③在销售商品、提供服务、投资项目等商业活动中，以承诺给付货币、股权、实物等回报的形式吸收资金；④违反法律、行政法规或者国家有关规定，通过大众传播媒介、即时通信工具或者其他方式公开传播吸收资金信息。

### （三）部门规章

2021年实施的涉区块链部门规章共4篇，其中国家发改委2篇，商务部、人社部、统计局各1篇。

发布部门	实施日期	规章名称	内容
国家发改委	2021.03.01	西部地区鼓励类产业目录（2020年本）	在重庆、新疆、青海将区块链作为新增鼓励类产业。
国家发改委、商务部	2021.01.27	鼓励外商投资产业目录（2020年版）	将“区块链技术研发与应用”列入鼓励外商投资产业目录。
人社部	2021.03.01	网络招聘服务管理规定	鼓励从事网络招聘服务的人力资源服务机构运用大数据、区块链等技术措施，保证其网络招聘服务平台的网络安全、稳定运行，防范网络违法犯罪活动，保障网络招聘服务安全，促进人力资源合理流动和优化配置。
国家统计局	2021.05.27	数字经济及其核心产业统计分类（2021）	将区块链技术列入互联网数据服务、新技术基础设施建设、数字化通用及专用设备制造、数字化运输设备制造、数字化电气机械器材和仪器仪表制造等产业。

表 1-1 2021 年涉区块链部门规章统计

值得注意的是，2021年国家发展改革委联合公安部、财政部、中国人民银行、网信办等多部门发布了《关于整治虚拟货币“挖矿”活动的通知》（发改运行〔2021〕1283号）（下称《通知》）。《通知》在效力层级上仅属于部门工作文件，但却对国内虚拟货币发展产生重要影响。《通知》明确通过各部门合力，加强虚拟货币“挖矿”活动上下游全产业链监管，严禁新增虚拟货币“挖矿”项目，加快存量项目有序退出，促进产业结构优化和助力碳达峰、碳中和目标如期实现。该政策文件的正式印发标志着有关方面将采取更大力度开展“挖矿”行为的整治工作。

继《通知》之后，浙江省发改委、内蒙古发改委、海南省发改委和贵州省发改委也相继出台本地有关虚拟货币“挖矿”用电实行差别电价的政策。

虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对推动经济社会高质量发展和节能减排带来不利影响。对“挖矿”的整治体现出国家政策层面正在积极引导区块链技术向对国民经济贡献度高、对科技进步

带动力强的领域应用，尽量降低区块链技术对经济社会发展的不良影响。

#### （四）司法解释与司法文件

##### 1. 《人民法院在线诉讼规则》

最高人民法院于 2021 年 6 月 17 日发布的《人民法院在线诉讼规则》（下称《规则》），规则第 16 至 19 条规定了区块链技术存储证据的相关规定。

《规则》第 16 条规定：“当事人作为证据提交的电子数据系通过区块链技术存储，并经技术核验一致的，人民法院可以认定该电子数据上链后未经篡改，但有相反证据足以推翻的除外。”该条首次明确了区块链存证的效力。

《规则》第 17 至 19 条则规定了在区块链技术平台保存的证据如何审查的问题。其中第 16 条提到“存证平台是否符合国家有关部门关于提供区块链存证服务的相关规定”，下一步，国家将会推进制定并出台区块链存证服务相关标准或规定。

##### 2. 《最高人民法院发布十起人民法院助推民营经济高质量发展典型民商事案例》

最高人民法院于 2021 年 9 月 3 日发布《最高人民法院发布十起人民法院助推民营经济高质量发展典型民商事案例》。案例 8 中，浙江省嘉兴市桐乡市人民法院创新运用“5G+AI+LBS+区块链”技术，实现动产“活查封”、“数智化”。法院通过在保管场地安装视频监控设备取代传统的封条查封，确保查封设备可正常使用，生产经营不中断运行。同时，5G 网络实现了图像、视频的回传和留存，法官在手机端即可查看动产状态。监测区域内使用移动通信基站 LBS 定位技术，当设备位置发生改变时，系统即时发出预警，避免保全财产被恶意转移。运用区块链技术，对区域内的机器设备数量、位置、外观进行图像固化并上传链接，将整个保全过程同步摄录并上传至“云上物证室”，确保保全数据可信任可追溯、保全行为规范可信。

运用“数智化”手段，将区块链技术应用于司法执行，在疫情防控常态化、经济下行压力增大的今天，最大程度体现了执行善意，减少了保全查封对公司正常经营的影响，同时确保了法院执行的严肃性，保障了生效裁判的执行力。

##### 3. 《最高人民法院关于人民法院知识产权审判工作情况的报告》

2021年10月21日公布的《最高人民法院关于人民法院知识产权审判工作情况的报告》中，在关于健全知识产权诉讼规则，破解知识产权司法保护难题层面，报告指出为努力破解知识产权纠纷中“举证难”问题，出台知识产权民事诉讼证据司法解释，审理区块链存证等案件，支持当事人通过区块链技术固定、保存、提交证据；建立“云上物证室”，运用3D扫描技术建立电子物证管理系统，便利当事人举证、质证。

在深化知识产权审判领域司法改革，推进知识产权审判体系和审判能力现代化层面，报告指出要充分运用智慧法院建设成果，加快建设适应知识产权审判的科技法庭，积极运用5G、AR、人工智能等现代科技，提升审判质效。建成全国法院统一的司法区块链平台，支持当事人在线进行数据存证和验证。

#### 4. 《最高人民法院关于印发〈2021年人民法院司法改革工作要点〉的通知》

最高人民法院在2021年3月16日发布《最高人民法院关于印发〈2021年人民法院司法改革工作要点〉的通知》，第8条指出，要全面加强智慧法院建设，完善司法大数据管理和应用机制。推进区块链中枢建设，着重推进智能合约在审判执行和社会治理中的应用落地场景，探索实现跨链应用。

#### 5. 《最高人民法院司法改革领导小组关于印发〈人民法院司法改革案例选编（十一）〉的通知》

2021年6月16日，最高人民法院发布《关于印发〈人民法院司法改革案例选编（十一）〉的通知》。在该选编第176号中，广东省广州市中级人民法院将区块链应用于授权委托验真，从源头确保授权委托真实可信。该技术可实现可视化智能存储全程留痕，平台对整个授权见证过程实行全程同步录音录像、实时业务日志记录，音视频文件通过后台服务器实时存储于法院内网服务管理平台，业务日志通过广州市司法区块链——“网通法链”实时上链。授权见证结束后，委托过程形成的音视频等数据经加密后，采用分布式存储与集中式存储相结合方式自动保存至中央大容量存储服务器。办案人员可随时登录后台服务器查看，并支持刻录成光盘入卷，为后期案件审判过程提供证据材料，也可为当事人提供业务溯源、文书校验、智能提取等便利服务。

改革案例第178号中，四川天府新区成都片区人民法院创新数据应用标准

模式，构建在线诉讼防火墙，确保数据应用安全。通过深度运用区块链技术，实现可信保护。深度转化应用最高法院“互联网审判可信操作”司法链应用试点成果，全面强化区块链技术应用，确保诉讼材料安全、可信。内外网办案平台与区块链平台对接，完善上链证据交互和采信规则。推动司法文书、电子签章及签名等业务流程电子数据实时记录存证，并提供校验服务。2020年以来，法院记录存证数据 1863 次。

#### 6. 《最高人民法院发布 11 起充分发挥检察职能推进网络空间治理典型案例》

最高人民法院 2021 年 1 月 25 日发布《最高人民法院发布 11 起充分发挥检察职能推进网络空间治理典型案例》，案例七“时某祥等 15 人组织、领导传销活动案”指出，该案例在依法严厉打击以金融创新为名实施的新型网络犯罪具有重要意义。近年来随着区块链技术、虚拟货币的持续升温，一些犯罪分子打着金融创新的旗号，假借国家对外政策，实施违法犯罪活动，迷惑性很强，危害性巨大。检察机关办理此类案件，要坚持“穿透式”审查理念，结合行为方式、资金流向、盈利模式等，分析研判是否符合国家法律规定，准确区分金融创新与违法犯罪。构成犯罪的，依法严厉打击。

#### （五）区块链相关技术标准

标准化是区块链技术发展的基石，区块链技术从小规模应用探索到大规模应用的实践过程中，标准制定尤为重要。通过国家标准、地方标准和行业标准的有机结合，进一步促进行业规范发展，有利于市场主体低成本进入区块链行业并形成良性循环。

目前我国的多项区块链国家标准正在起草或征求意见中，2021 年计划的具体标准如下：

名称	计划号	归口单位	状态
信息技术 区块链和分布式记账技术系统测试要求	20213310-T-469	全国区块链和分布式记账技术标准化技术委员会	正在起草
信息技术 区块链应用服务中间件 参考架构	20213307-T-469		
信息技术 区块链和分布式记账技术 术语	20210929-T-469		
信息技术 区块链和分布式记账技术 存证应用指南	20201612-T-469		



信息技术 区块链和分布式记账技术 智能合约实施规范	20201615-T-469		
信息安全技术 区块链技术安全框架	20210998-T-469	全国信息安全标准化技术委员会	正在征求意见
信息安全技术 区块链信息服务安全规范	20210991-T-469		

表 1-2 2021 年区块链国家标准统计

除国家标准外，各地也在积极探索制定区块链在各行业应用的地方标准。

2021 年新发布或实施的地方标准如下：

1. 《基于区块链的农畜产品追溯平台规范》（DB15/T 2478-2021），该标准由内蒙古市场监督管理局制定，于 2021 年 12 月 25 日发布，2022 年 1 月 25 日实施，规定了基于区块链的农畜产品追溯平台的总体要求、体系结构、性能标准、功能要求、追溯数据管理、安全保障和运维要求等内容，适用于基于区块链的农畜产品追溯存证平台建设。

2. 《财政电子票据区块链技术应用规范》（DB33/T 2382-2021），该标准由浙江省市场监督管理局制定，于 2021 年 9 月 30 日发布，2021 年 10 月 30 日实施，规定了基于区块链技术的财政电子票据的系统架构、总体要求、业务通用要求、技术要求、业务流程要求和数据要求，适用于基于区块链技术的财政电子票据系统的设计、开发、部署和应用，以及财政电子票据全生命周期管理。

3. 《金融行业区块链平台技术规范》（DB4403/T 127-2020），该标准由深圳市地方金融监督管理局归口上报，主管部门为深圳市市场监督管理局，于 2020 年 12 月 7 日发布，2021 年 1 月 1 日实施，适用于深圳市企业建设金融区块链和分布式账本系统、开展金融区块链和分布式账本服务，重点关注金融区块链服务的功能架构和技术规范，但并不适用于直接构建金融区块链服务的具体解决方案、技术实现与部署等。

4. 《基于区块链的电子商务价值行为认定规范》（DB50/T 1048-2020），该标准由重庆市大数据应用发展管理局归口上报，主管部门为重庆市市场监督管理局，于 2020 年 11 月 30 日发布，2021 年 3 月 1 日实施，规定了基于区块链的电子商务价值行为的术语和定义、分类、认定流程、认定方式，适用于运用区块链技术的电子商务主体。

5. 《基于区块链的电子商务价值行为数据存证规范》（DB50/T 1049-

2020), 该标准由重庆市大数据应用发展管理局归口上报, 主管部门为重庆市市场监督管理局, 于 2020 年 11 月 30 日发布, 2021 年 3 月 1 日实施, 规定了基于区块链技术的电子商务价值行为数据存证的技术要求、业务流程, 适用于基于区块链技术的电子商务价值行为数据存证。

另外, 2021 年还出台了一部通信行业标准——《基于区块链技术的去中心化物联网业务平台框架》(YD/T 3905-2021), 该标准由中国通信标准化协会归口上报, 主管部门为工业和信息化部, 于 2021 年 5 月 17 日发布, 2021 年 7 月 1 日实施, 规定了一种基于区块链技术的去中心化物联网业务平台, 定义了物联网区块链的概念、特征、技术要求, 以及物联网区块链的参考模型、能力要求、主要工作流程和应用用例, 适用于物联网区块链及其应用。

## 二、国家层面区块链产业政策

产业政策是产业发展的风向标。国家层面, 2021 年中共中央、国务院及各相关部门积极探索区块链产业发展方向。十三届全国人大四次会议通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》明确提出要“加快发展现代产业体系, 推动经济体系优化升级, 坚持把发展经济着力点放在实体经济上, 坚定不移建设制造强国、质量强国、网络强国、数字中国, 推进产业基础高级化、产业链现代化”。将数字化、网络化、现代化作为产业升级的重要抓手, 提振了以区块链技术为核心的商用市场的信心。

2021 年中央层面的区块链政策包括两项针对特定地区的产业扶持政策(成渝地区与浦东新区), 及多项全国性政策。

2021 年 1 月 31 日, 中共中央办公厅、国务院办公厅印发《建设高标准市场体系行动方案》, 要求要强化市场基础设施建设, 实施智能市场发展示范工程。“加大新型基础设施投资力度, 推动第五代移动通信、物联网、工业互联网等通信网络基础设施, 人工智能、云计算、区块链等新技术基础设施, 数据中心、智能计算中心等算力基础设施建设。”

3 月 24 日, 中共中央办公厅、国务院办公厅印发《关于进一步深化税收征管改革的意见》, 指出要全面推进税收征管数字化升级和智能化改造, 深化税收大数据共享应用, “探索区块链技术在社会保险费征收、房地产交易和不动产登

记等方面的应用，并持续拓展在促进涉税涉费信息共享等领域的应用。”

7月6日，中共中央办公厅、国务院办公厅印发《关于依法从严打击证券违法活动的意见》，指出要着力提升证券执法司法能力和专业化水平，“丰富证券执法手段，有效运用大数据、人工智能、区块链等技术，建立证券期货市场监测预警体系，构建以科技为支撑的现代化监管执法新模式，提高监管执法效能。”

7月15日，中共中央、国务院发布《中共中央 国务院关于支持浦东新区高水平改革开放打造社会主义现代化建设引领区的意见》，要求要增强全球资源配置能力，服务构建新发展格局，完善金融基础设施和制度。“构建贸易金融区块链标准体系，开展法定数字货币试点。”

8月2日，中共中央发布《中共中央关于加强新时代检察机关法律监督工作的意见》，“加强检察机关信息化、智能化建设，运用大数据、区块链等技术推进公安机关、检察机关、审判机关、司法行政机关等跨部门大数据协同办案，实现案件数据和办案信息网上流转，推进涉案财物规范管理和证据、案卷电子化共享。”

10月10日，中共中央、国务院印发《成渝地区双城经济圈建设规划纲要》，该《纲要》合计在四个部分提及区块链：1.大力发展数字经济：合力打造数字产业新高地，培育人工智能、区块链等创新应用，联手打造具有国际竞争力的电子信息产业集群。2.培育发展现代服务业：积极支持区域金融改革创新，在成都建设基于区块链技术的知识产权融资服务平台。3.高水平推进开放平台建设：推进中新（重庆）战略性互联互通示范项目，合规有序发展供应链金融和特色跨境金融服务平台，依托贸易金融区块链平台，探索形成贸易金融区块链标准体系。4.推动城乡要素高效配置：增强城乡建设资金保障，运用大数据、区块链等技术，提高涉农信贷风险管理水平。

12月1日，中共中央、国务院印发《国家标准化发展纲要》，提出要“加强关键技术领域标准研究。在两化融合、新一代信息技术、大数据、区块链、卫生健康、新能源、新材料等应用前景广阔的技术领域，同步部署技术研发、标准研制与产业推广，加快新技术产业化步伐。”“促进标准与国家质量基础设施融合发展，通过人工智能、大数据、区块链等新一代信息技术的综合应用，

完善质量治理，促进质量提升。”

不难发现，2021 年国家相关政策中，区块链的应用场景集中于金融、司法行政、基础设施建设、现代制造业、现代服务业等领域。同时，“区块链”一词与大数据、新能源、人工智能等并列出现，显示出国家对区块链技术重要性与普适性的进一步认可。

### 三、部分省市区块链产业政策

地方区块链产业政策与法规是国家区块链产业政策与法律规范细化落实的关键，是地方招商引资、营商环境优化的重要指标，对投资者、从业人员选择投资、从业地域有标志性意义。2021 年，各地密集布局区块链产业，合计实施地方性法规 54 部，地方规范性文件 325 部，地方工作文件 748 条。从专题分类来看，长江经济带发展、长三角一体化发展、黄河流域生态保护与高质量发展、粤港澳大湾区建设、自由贸易试验区内容较多。

从区块链专项政策的定位上来看，各省市多注重区块链产业园区的发展，积极培育和引进区块链企业。区块链产业园作为区块链企业发展和技术创新的重要载体之一，能够加快区块链产业协同发展，充分整合本地区科研、人才、产业资源，加速推进经济增长和产业化转型，提升地区区块链产业综合实力。

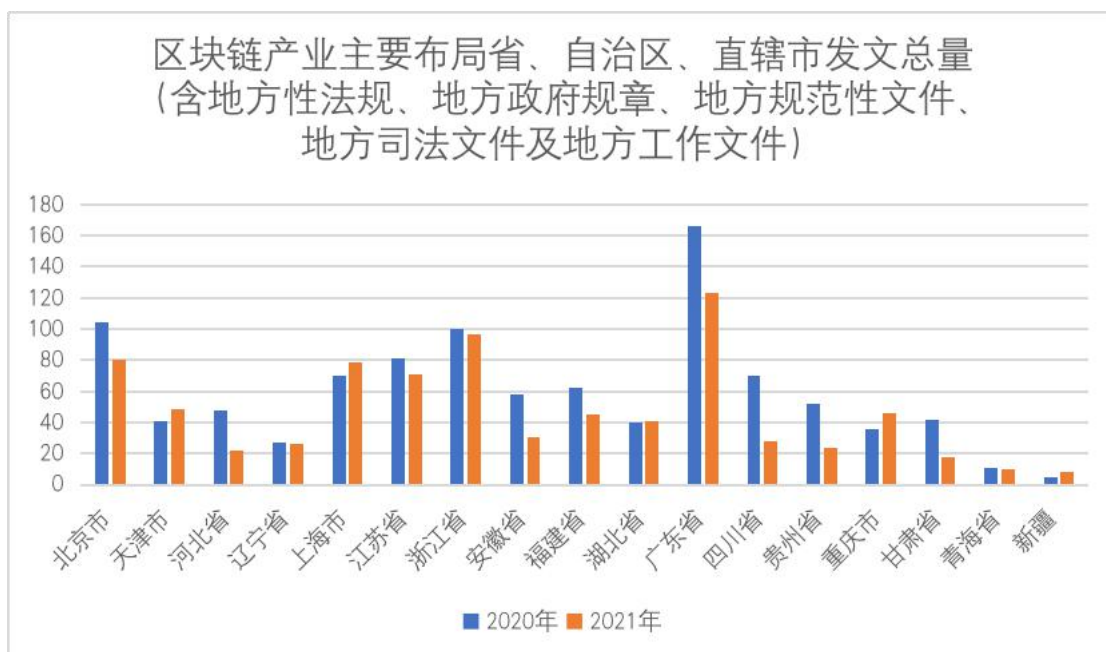


图 1-1 区块链产业主要布局省、自治区、直辖市发文总量

上表统计了区块链产业主要布局的省、自治区、直辖市在 2020 年与 2021

年的发文总量，统计对象包括地方性法规、地方政府规章、地方规范性文件、地方司法文件及地方工作文件。地方发文总量可以一定程度上反映出一地的区块链产业的活跃程度与开放程度，为区块链从业者提供参考。

统计显示，广东省在统计区间内发文数量遥遥领先，广州、深圳、珠海三地占比最高。该结果与广东省长期推进珠三角国家自主创新示范区建设，深化粤港澳大湾区创新发展合作，打造互联网产业集群息息相关。

长三角经济带中，沪苏浙皖四地发文数量相对平均，浙江省发文数量最高。而京津冀地区的区块链发展可能存在地区不均衡、一体化程度有待提高的情况。除北京外，天津、河北地区的区块链发文数量相对较低，仅约为北京的50%。

2021年10月，中共中央、国务院印发《成渝地区双城经济圈建设规划纲要》，通过培育发展成渝地区双城经济圈，引领中国西部地区发展，发挥沟通西南西北、连接国内国外的独特区位优势，推动长江经济带和丝绸之路经济带战略契合互动。《纲要》大篇幅提及区块链技术，未来区块链有望赋能西南地区经济发展，成为西南地区经济新的增长极。

需要指出的是，由于地方性法规、地方政府规章的立法成本显著高于一般工作文件，发文数量不能真实反映地方政策与地方立法工作的质量。以2021年实施的《上海市数据条例》与《深圳经济特区数据条例》为例，这两部条例都是基于《数据安全法》与《个人信息保护法》而制定，条例作为地方数据立法的试点，对各地区的数字经济规范化发展都有极强的指导意义。

地方	文件名	实施日期	内容
北京	北京市无障碍环境建设条例	2021.11.1	支持信息无障碍领域的技术研发与应用，推进人工智能、物联网、区块链等技术在信息无障碍领域的成果转化，支持新技术在导盲、声控、肢体控制、图文识别、语音识别、语音合成等方面的应用。
	北京市禁毒条例	2021.10.01	加强禁毒信息化建设和应用，建立毒品监测预警平台，依托互联网、大数据、人工智能、区块链等技术为禁毒工作提供服务和支撑，分析、研判各类涉毒信息，开展毒品监测评估和毒品问题预警通报。
	北京市中医药条例	2021.05.01	市药品监督管理部门应当会同中医药、农业农村等部门加强中药材质量监督管理，支持和引导药品生产企业、

			中药材经营者等应用大数据、区块链等新技术开展中药材流通追溯。
天津	天津国家自主创新示范区条例	2021.11.29	在示范区加快发展现代服务业，推动信息技术应用创新、人工智能、大数据、区块链、科技金融、海洋经济等细分产业发展。
	天津市乡村振兴促进条例	2021.11.01	市和区人民政府应当加强数字乡村建设，充分运用物联网、大数据、区块链、人工智能等现代信息技术，加快农业生产经营管理和公共服务数字化应用，推进乡村振兴数字化、网络化、智能化发展。
	天津市促进智能制造发展条例	2021.11.01	推动企业在制造环节深度应用数字孪生、人工智能、新一代移动通信技术、大数据、区块链等新技术，探索形成智能场景。
	天津市推进北方国际航运枢纽建设条例	2021.09.01	鼓励建设基于大数据、人工智能、云计算、区块链等现代信息技术的基础设施，推进装卸、运输、仓储等环节自动化、智能化改造升级和新一代自动化码头建设；支持建设基于区块链的跨境贸易大数据平台，拓展电子商务全供应链服务功能，建设跨境电子商务综合试验区。
上海	上海市档案条例	2021.12.01	鼓励和支持档案科学研究和技术创新，促进科技成果和区块链、大数据、人工智能等信息技术在档案收集、整理、保护、利用、信息化建设等方面的转化和应用，推动档案科技进步。
	上海市知识产权保护条例	2021.03.01	鼓励公证机构创新公证证明和公证服务方式，依托电子签名、数据加密、区块链等技术，提供原创作品保护、知识产权维权取证等公证服务。
江苏	江苏省地方金融条例	2021.07.01	完善现代金融基础设施建设，鼓励、支持云计算、大数据、人工智能、区块链、物联网等新兴科技在金融服务和金融监督管理领域的运用，推动金融科技发展和应用。
	中国（江苏）自由贸易试验区条例	2021.03.01	自贸试验区发展贸易新业态、新模式，推动互联网、物联网、大数据、人工智能、区块链与贸易有机融合，培育扩大保税展示交易、期货保税交割、融资租赁、汽车平行进口等新型贸易。
	江苏省优化营商环境条例	2021.01.01	县级以上地方人民政府及其有关部门应当推动区块链、人工智能、大数据、物联网等新一代信息技术在政务服务领域的应用。
浙江	浙江省人大常委会关于网络虚假信息治理的决定	2021.09.30	省、设区的市、县（市、区）人民政府应当采取措施，鼓励和支持网络虚假信息治理等领域人工智能、区块链等技术的研发和推广应用。

			重点推进新一代移动通信网、大数据中心、工业互联网、物联网、车联网、人工智能、区块链、卫星通信等新型数字基础设施建设，加快市政、交通、能源、电力、水利等传统基础设施的数字化改造。
	浙江省数字经济促进条例	2021.03.01	重点推动集成电路、高端软件、数字安防、网络通信、智能计算、新型显示、新型元器件及材料、网络安全等产业发展，促进云计算、大数据、物联网、人工智能等技术与各产业深度融合，培育区块链、量子信息、柔性电子、虚拟现实等产业发展。
			鼓励有关部门依托物联网、区块链等技术，在教育、医疗、交通、邮政、生态环境保护、药品监管、工程建设、公共安全等重点领域推行监管智能化应用。
	杭州城市大脑 <sup>①</sup> 赋能城市治理促进条例	2021.03.01	市人民政府应当推动大数据、云计算、区块链等新技术在中枢的融合应用，提高中枢的安全性、稳定性、扩展性。
安徽	安徽省大数据发展条例	2021.05.01	县级以上人民政府及其有关部门应当推动大数据在服务业广泛应用，支持云计算、移动互联网、物联网、人工智能、区块链等新一代信息技术产业发展，鼓励发展现代服务业。
	广东省市场监管条例	2021.12.01	各级政府及监管部门应当充分运用人工智能、互联网、大数据、区块链等技术手段，依托国家统一建立的在线监管系统，推行以远程监管、移动监管、预警防控为特征的非现场监管。
广东	广东省数字经济促进条例	2021.09.01	推动发展智慧医疗，推进人工智能、大数据、区块链和云计算在医学影像辅助诊断、临床辅助决策、智能化医学设备、公共卫生事件防控等领域的应用。 探索建立数字经济关键核心技术攻关新型体制机制，重点在新一代移动通信、人工智能、区块链、数字孪生、量子科技、类脑计算等前沿技术领域，加快推进基础理论、基础算法、装备材料等关键核心技术攻关和突破。
			统筹推进人工智能、区块链、云计算等新技术基础设施建设，支持建设底层技术平台、算法平台、开源平台等基础平台，建立领先的通用技术能力支撑体系。
	广州市科技创新条例	2021.07.01	市、区人民政府应当建立科技金融服务中心等服务机构或者平台，利用大数据、区块链、人工智能等科技手

① 根据《杭州城市大脑赋能城市治理促进条例》第三条，城市大脑是指由中枢、系统与平台、数字驾驶舱和应用场景等要素组成，以数据、算力、算法等为基础和支撑，运用大数据、云计算、区块链等新技术，推动全面、全程、全域实现城市治理体系和治理能力现代化的数字系统和现代城市基础设施。

			段，为科技企业提供线上化、智能化、批量化投融资对接等服务。
	广东省社会信用条例	2021.06.01	鼓励市场信用服务机构利用大数据、云计算、区块链、人工智能等现代技术开发具有自主知识产权的信用产品，拓展信用应用服务领域。
	广州市优化营商环境条例	2021.01.01	加强人才大数据建设，建立人才区块链支撑平台、人才大数据标准规范体系和安全管理平台，提升人才服务业的精准服务能力。
	珠海经济特区突发公共卫生事件应急条例	2021.12.01	市、区政府及卫生健康、市场监管等部门应当发挥大数据、云计算、区块链、人工智能、物联网等信息技术在监测预警、调查溯源、防控救治、资源调配、信息交流与情报合作等方面的支撑作用，提升智能化防控水平。
	深圳经济特区绿色金融条例	2021.03.01	鼓励金融机构和金融科技企业利用区块链、人工智能、大数据、云计算、物联网等金融科技手段支持绿色金融创新发展。 支持以区块链为基础的跨境绿色资产标准化、认证、仓储和交易平台建设，探索构建跨境合作机制。
			充分利用人工智能、大数据、区块链、移动互联网等现代信息技术，推进数据共享与融合，简化办事流程。
	深圳经济特区优化营商环境条例	2021.01.01	推行区块链发票和缴费凭证、增值税电子专用发票以及其他电子票据、凭证的广泛使用。 整合跨境贸易数据资源，综合利用大数据、区块链、移动互联网等现代信息技术，为市场主体、监管部门等提供跨境贸易综合服务。 推动利用区块链等现代信息技术，加强公益性融资服务平台建设，为市场主体提供线上化、智能化、批量化投融资对接服务。 推进人工智能、大数据、区块链、移动互联网等现代信息技术的智能监管方式应用，推行远程监管、移动监管、预警防控等非现场监管。
	四川省优化营商环境条例	2021.07.01	统一政务服务标准，创新政务服务方式，推动区块链、人工智能等新一代信息技术在政务服务领域的应用，不断提高政务服务质量。
四川	成都市美丽宜居公园城市建设条例	2021.10.01	坚持场景驱动、算法赋能、智能协同、多元共治理念，充分运用大数据、云计算、区块链、人工智能等前沿技术推动智慧城市建设，构建智能化城市运行指挥和服务体系，提升城市智慧治理能力。
	成都市科技创新中心建设条例	2021.10.01	鼓励围绕前沿医学、人工智能、区块链、量子通信、氢能等重点领域，推进前沿交叉研发平台建设，开展技术预测和基础前沿技术、关键核心技术攻关，发展前沿技术和未来产业。
	重庆市社会信用条例	2021.07.01	鼓励信用服务机构利用大数据、云计算、区块链、人工智能等技术开发具有自主知识产权的信用产品，满足社会需求。
重庆	重庆市优化营商环境条例	2021.07.01	市、区县（自治县）人民政府及其有关部门应当统一政务服务标准，创新政务服务方式，推动区块链、人工智能、大数据、物联网、云计算等信息技术在政务服务领域的应用。



表 1-3 2021 年涉区块链地方文件统计

## 四、典型意义区块链案例分析

2021 年，涉区块链案件较之前相比仍处于增长状态。民事案件中，呈现出技术性强、涉外因素普遍、损失认定困难、证据要求高等特点。刑事案件中，虚拟货币作为其核心的新兴技术产物，逐渐成为犯罪分子新的目标，以“炒币”为幌子的非法集资、诈骗、传销类犯罪时有发生；另一方面，虚拟货币难以管控易成为洗钱犯罪的工具。

本部分拟主要归纳整理 2021 年涉区块链典型纠纷案件，及在事实认定和法律适用方面存有争议，缺乏明确依据的案件，并拟在下一部分归纳总结区块链行业面临的主要法律风险。

### （一）民事案件

涉区块链民事案件主要涉及虚拟货币<sup>①</sup>的合同纠纷，可细分为委托合同纠纷、买卖合同纠纷、民间借贷纠纷等。近年来，虽然行政机关对虚拟货币持续保持高压态势，多部门发布了一系列规章专门规制虚拟货币，警示市场风险，如《中国人民银行关于防范代币发行融资风险的公告》、《中国人民银行、中央网信办、最高人民法院等关于进一步防范和处置虚拟货币交易炒作风险的通知》等，但一方面，涉虚拟货币合同纠纷仍然层出不穷，另一方面，对于非典型合同各法院在裁判思路上存在差异。

#### 1. 朱某某与方某某买卖合同纠纷<sup>②</sup>

2018 年 1 月，原告方某某与被告朱某某约定由方某某向朱某某购买 113019900 个 Tripio 币（等值 1500 个以太币，包括 1350 个非基石以太币和 150 个基石以太币，一个非基石以太币可折算 72916 个 Tripio 币；一个基石以太币可折算 97222 个 Tripio 币）。方某某履行给付义务后，朱某某尚欠 67811940 个 Tripio 币未履行。方某遂诉至法院。2020 年 8 月，经一审法院释明合同有效后，朱某某未经方某某同意单方履行了剩余的给付义务。

本案法律关系较简单，是常见的买卖合同一方瑕疵履行引起的民事纠纷。

<sup>①</sup> 本报告中提及的“虚拟货币”，是指非经货币当局发行，使用加密技术及分布式账户或类似技术、以数字化形式存在的货币。故，网络游戏、社交平台自行推出的游戏币、代金币等虽处于“虚拟货币”的语义射程内，但由于无关区块链技术，故不属于本报告讨论的对象，应予以排除。

<sup>②</sup> 北京市高级人民法院，(2020)京民终 747 号。

首先，二审法院明确了案涉虚拟货币不具有货币属性，但尊重虚拟货币具有的商品交易属性以及公民交易行为的自由。由于双方当事人之间买卖 Tripio 币的行为并非代币发行融资行为，故不违反我国法律法规和相关政策的效力性、强制性规定，买卖合同合法有效。其次，在合同有效基础上，法院尊重了虚拟货币市场的交易习惯，明确了案涉 Tripio 币在双方未明确约定时的“合理交付期间”应为即时交付。

## 2. 刘某某与盛某某委托合同纠纷<sup>①</sup>

2018 年 10 月，原告刘某某（甲方）与被告盛某某（乙方）签订《资产管理顾问协议》（以下简称“《协议》”），约定由乙方为甲方提供比特币增值管理服务，保持长期稳定盈利。《协议》约定，“2.3 止损权力：为了进行风险控制，防止甲方遭受大额损失，约定一个最大亏损机制，因乙方交易原因造成甲方账户投资本金亏损比例达到 15% 时，乙方告知甲方并解释原因，由甲方决定是否继续交易。当甲方账户投资本金亏损比例达到 20% 时，需要执行止损措施；如出现 20% 比例外的本金亏损，这部分亏损将由乙方承担，即如果在合作终止时，甲方账户中的本金亏损大于 20% 部分，需要由乙方向甲方补偿该部分损失。若出现黑客事件的意外状况（非乙方操作）如交易平台资金被盗等，甲方自行承担所有损失”。后原告认为被告未尽到止损义务等行为具有重大过错，应承担损失补偿责任，遂诉至法院。

一审法院对被告主张《协议》无效不予认可，因为被告主张《协议》内容违反《关于防范比特币风险的通知》、《关于防范代币发行融资风险的公告》、《关于防范比特币等所谓“虚拟货币”风险的提示》的规定不属于法律、行政法规的范畴，合同有效，但通过违法介入国际互联网进行交易比特币系违法行为，该行为不受法律保护，由此产生的相应损失亦属于风险自甘。

二审法院虽然维持原判，但在说理逻辑上存在一定区别。二审法院未从法律规范效力位阶的角度着手，但认为上述规章内容涉及金融安全等社会公共利益，应依法确认合同无效。盛某某为刘某某提供的数字货币量化交易服务，实质上是为了规避国内的金融监管而进行的比特币交易、流通和炒作，属于非法金融活动，由此产生的相应损失不受法律保护，不利后果应由其自行承担。

<sup>①</sup> 北京市第三中级人民法院，(2021)京 03 民终 14106 号。

### 3. 雷某某、李某某民间委托理财合同纠纷<sup>①</sup>

原告李某某、被告雷某某系朋友关系。案涉“U 宝币”为优联万家控股集团衡量发行的加密货币。原告经被告宣传签订《协议》，约定由被告为原告投资“U 宝币”，由原告享有所有权，回本后投资收益在原被告间“八二分成”。双方约定被告承担投资风险，若出现意外，则剩余本金由被告在三个月内向清偿。后“U 宝币”平台因涉嫌组织、领导传销活动罪被查处。被告在偿还部分本金后因案涉投资形成的责任分担问题与原告产生纠纷，诉至法院，并请求法院认定合同无效。

本案属于民间委托理财合同纠纷。法院认为由于原被告均明知投资款去向，且该投资行为明确为《中国人民银行法》、《禁止传销条例》等相关法律、行政法规所禁止，主要责任人员因犯罪被追究刑事责任，故案涉协议的相应约定应属无效。根据原被告双方的过错程度，判决被告承担 80% 赔偿责任，原告承担 20% 赔偿责任。

近年来，以区块链为幌子的虚拟货币为在短期内扩大影响、吸收资金，多采用传销模式发展层级，通过对被发展人员以其直接或者间接发展的人员数量或者业绩为依据计算和给付报酬。基于虚拟货币发行方利诱性的承诺，及对亲戚、朋友关系的信任，大量个体投资者在投资虚拟货币后血本无归。对于该类投资形成的合同，本案明确为民间委托理财合同，受托人负有投资风险提示义务、注意义务及委托过程中的一系列其他义务，同时委托人亦应承担投资损失的相应风险，故双方应当按照过错比例承担责任。

### 4. 新型实务案例——借用虚拟货币投资案件的认定和分析

实务中出现的涉及虚拟货币的新型案件类型之一即为借用虚拟货币进行投资后产生的纠纷。例如，甲乙丙三人约定合资用以太坊 ETH 参与一代币投资项目，其中乙向甲借用一定数额的 ETH 作为乙向该项目的出资份额，三方约定由甲代理乙丙实施投资行为。后甲乙间因返还 ETH 产生纠纷。

该案例是常见的民间共同投资虚拟货币的法律模型，部分民众因不了解虚拟货币操作流程、缺乏相关知识而选择与他人（通常是亲戚、朋友）共同投资，最后产生法律纠纷。该类案件往往涉及两层法律关系，第一层为甲乙间的

<sup>①</sup> 浙江省丽水市中级人民法院，(2021)浙 11 民终 1027 号。

借用关系，第二层为乙丙与甲之间的委托代理关系。在处理该类案件时，须准确把握纠纷发生于哪一段法律关系，并判断两种法律关系在效力上是否会产生相互影响。

对于第一层借用关系，甲可以基于返还原物请求权请求乙返还借用的 ETH。不论后续投资行为效力如何，甲乙间的借用事实存在，借用合同成立。首先，从 ETH 的法律性质出发，ETH 可以作为特殊商品持有和流转。《关于防范代币发行融资风险的报告》规定任何组织和个人不得非法从事代币发行融资活动以及代币融资平台不得买卖“虚拟货币”，但并未禁止虚拟货币的持有和合法流转。其次，由于 ETH 的交易流通是通过互联网交易平台进行的，兑价比率实时变化，难以确定市场现值，故考虑以返还原物请求法院支持。

对于第二层借用关系，需要考虑的是投资行为违法是否必然导致出借行为无效，目前理论与实务界存在两种观点：

第一种观点是，当事人非货币发行方，实际系利用虚拟货币进行投资以期获得盈利，而非代币发行融资行为，借用关系成立，但适用自甘风险。

第二种观点是，虽然甲乙间系借用关系，但双方从事的基本性业务是购买网络虚拟货币，该行为属于从事非法金融活动，扰乱了经济金融秩序，违反了公序良俗。ETH 系一种虚拟商品，存在价值不稳定性和非法性，所以存在损失无法确定和因非法债务不受法律保护而无法主张的情况。换言之，由于后续投资行为的非法性影响到了债权的效力，使得借用行为不受法律保护。

需要注意的是，第二种因数字货币本身的性质而直接对法律关系认定无效的观点在司法实务界存在争议，目前尚无相应法律效力层级的文件可作为认定合同无效的依据。

但退一步讲，依据《民法典》第一百五十七条，民事法律行为无效、被撤销或者确定不发生效力后，行为人因该行为取得的财产，应当予以返还；不能返还或者没有必要返还的，应当折价补偿。有过错的一方应当赔偿对方由此所受到的损失；各方都有过错的，应当各自承担相应的责任。从这一角度而言，即使因为 ETH 本身的性质争议而认定借用合同无效，行为人因该行为取得的财产，也应当予以返还。

## （二）行政案件

## 1. 胡某某传销行为案<sup>①</sup>

当事人胡某某在接触“PTY”火龙果项目后，为进一步在富阳推广该项目，于2020年9月29日下午在杭州某酒店组织了“杭州社区火龙果项目招商会”。新会员通过“PTY”火龙果项目老会员分享二维码下载“PTY火龙果”APP，进行充值500元后方可注册成功。“PTY”火龙果项目具体的奖励制度如下：（1）定存算力，即个人买了币以后，在不交易的情况下，通过币本身的增值，也包括矿机产生新币，达到增值的目的，从而实现营利，具体的营利值和营利率因目前系统未完全启用，无法确定，本块收益为固定收益，即静态收益；（2）推广算力，即通过推广给其他会员，从而提高自己的收益率，推广的人越多，算力就越高，例如平台承诺预期投资回报为3倍，那么初始投资1万元，预期收益就为3万元，假设预期为3个月，算力提高可以缩短预期收益时间，即不需要3个月；（3）全网算力，即“PTY”火龙果交易所每天总共通过挖矿产出2600个“PTY”币，这是通过全网所有人员产出“PTY”币的总和，另外还根据下线每天的购买币数来计算上线的提成。胡某某直接推荐徐某某成为“PTY”火龙果会员。目前因“PTY”火龙果项目系统尚在会员推广初始阶段，项目收益未实际产生，故当事人的非法经营额和违法所得无法计算。

本案中“IAC”平台的运营方式符合《禁止传销条例》第七条第（一）项、第（二）项“下列行为，属于传销行为：（一）组织者或者经营者通过发展人员，要求被发展人员发展其他人员加入，对发展的人员以其直接或者间接滚动发展的人员数量为依据计算和给付报酬（包括物质奖励和其他经济利益，下同），牟取非法利益的；（二）组织者或者经营者通过发展人员，要求被发展人员交纳费用或者以认购商品等方式变相交纳费用，取得加入或者发展其他人员加入的资格，牟取非法利益的；”的规定，属于传销平台。

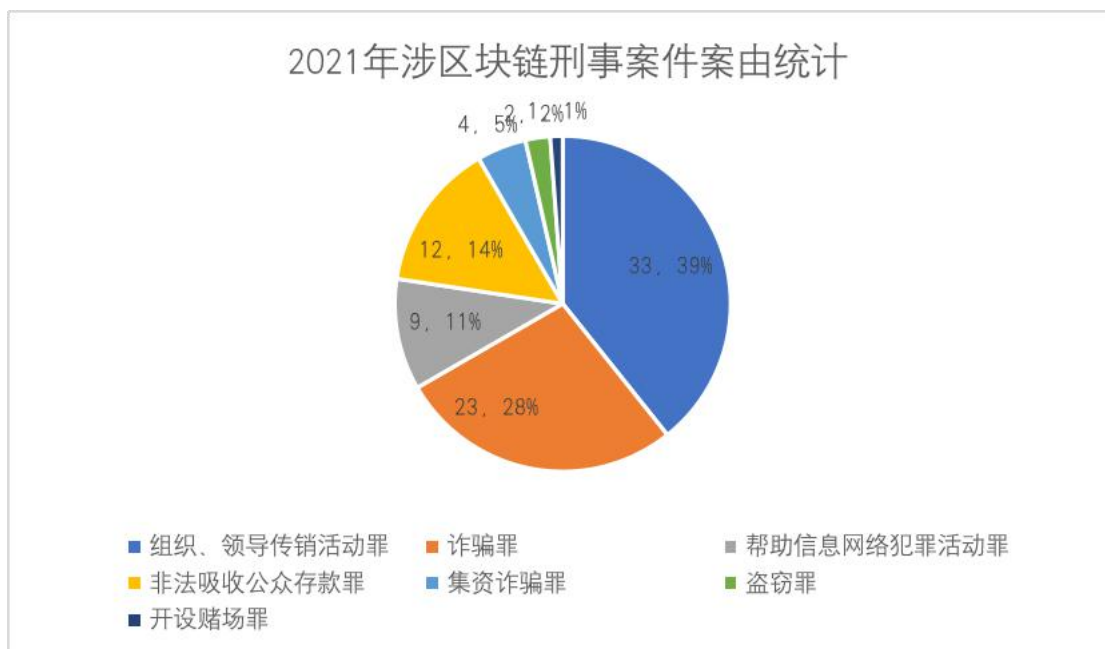
因当事人有介绍他人参与传销活动的事实，根据《禁止传销条例》第二十四款的规定，存在“介绍、诱骗、胁迫他人参加传销的，由工商行政管理部门责令停止违法行为，没收非法财物，没收违法所得，处10万元以上50万元以下的罚款”给予10万元的处罚。绝大多数情况下，当事人仅有参与传销的事实，可以处2000元以下的罚款。

<sup>①</sup> 杭州市富阳区市场监督管理局，（杭富）市监罚处字（2020）103号。

### （三）刑事案件

2021 年于“中国裁判文书网”中公开的涉区块链刑事案件，所涉罪名及数量、比例如下图所示。

图 1-2 2021 年涉区块链刑事案件案由统计



据统计，2021 年涉区块链刑事判决中，组织、领导传销活动罪数量最多，占比高达 43%，包括有较大社会影响的“艾尔发币案”、“恩必爱集团案”等。其次是诈骗罪，占比近三成。非法吸收公众存款罪与帮助信息网络犯罪活动罪位列第三、第四。

根据上海检察机关发布的《上海网络犯罪检察白皮书（2021）》，网络经济新业态伴生的犯罪增长显著，网络犯罪链条化、产业化态势明显，已经构建起完整的网络黑灰产业链，且不断拆分细化，出现各种新型的“关联产业”。虽然相较于传统刑事案件，涉区块链案件数量较少，但技术发展的伴生性极强，容易造成严重后果，且犯罪手法复杂、专业性强，为司法机关的证据固定、定罪量刑造成一定困难。

#### 1. 姜清波、贾彦峰组织、领导传销活动案<sup>①</sup>

“艾尔发币”（IPA coin）是由一韩国公司发行的虚拟货币，并在互联网上建立了会员管理平台管理并发展会员，形成金字塔式的网络化布局和上下线关系。2016 年，被告人姜清波将“艾尔发币”引入国内，并通过网络公开推广宣

<sup>①</sup> 湖南省怀化市中级人民法院，(2020)湘 12 刑终 343 号。

传“艾尔发币”具有基于比特币区块链点对点去中心化支付，开源代码，限量发行，唯一获得虚拟货币牌照，与支付宝对接，可以在国际交易平台自由交易、自由提现等特点，利用“艾尔发币”币值被人为制造不断上涨的假象及其会员制度、推广奖励制度及提现制度，引诱他人购买“艾尔发币”及继续发展下线成员。“艾尔发币”的具体制度包括：（1）会员制度：新会员须由老会员推荐，设置最低购买门槛，并按照购买金额对应会员级别，分配不同比例的“艾尔发币”；（2）推广奖励制度：设置直推奖、对碰奖、管理奖等，按照“艾尔发币”实时价格返币到会员账户；（3）提现制度：“艾尔发币”以美元计价，会员注册时以实时价格按照美元与人民币 1：7 的兑换比率购买，注册三个月可以以实时价格按照美元与人民币 1：6 的兑换比率提现，另扣除 3% 的手续费。案发时，平台实际收取传销资金 1136191000 元；该传销组织通过 9 个银行账户共收取涉案资金 1010702515.09 元，还通过支付宝、微信账号收取涉案资金并提现 97512817.41 元。

组织领导传销活动罪，是指以推销商品、提供服务或纯资本运作等经营活动为名，要求参加者以缴纳费用或者购买商品、服务等方式获得加入资格，并按照一定顺序组成层级，直接或者间接以发展人员的数量作为计酬或者返利依据，引诱、胁迫参加者继续发展他人参加，骗取财物，扰乱经济社会秩序的传销活动行为。由于我国对虚拟货币打击的高压态势，投资渠道受限，近年来参与投资国外发行的虚拟货币的模式多为通过代理人引入国内，在国内建立平台发展会员。该模式存在极大的刑事风险，即使不存在假借区块链名义对投资者进行诱导与欺骗的主观故意，一旦符合传销的特征，也有极大的可能受到行政甚至刑事处罚。

## 2. 罗业葑盗窃案<sup>①</sup>

被告人罗业葑于 2019 年 4 月 19 日至 26 日间，利用计算机网络漏洞，非法侵入被害单位上海谱唯网络科技有限公司的服务器，从该服务器中的数字货币钱包内窃取泰达币（USDT）1,890,792.538 枚，共计价值人民币 1,200 余万元。嗣后，被告人罗业葑将上述泰达币兑换成数字货币以太坊（ETH）及比特币（BTC），并将部分以太坊向他人出售，共计获利 91 万余元。

<sup>①</sup> 上海市静安区人民法院，(2020)沪 0106 刑初 551 号。

被告人对起诉指控认定构成盗窃罪有异议，认为泰达币属于计算机信息系统数据，不是刑法意义上的财物，获取泰达币的行为不符合盗窃罪的构成要件，应属于非法获取计算机信息系统数据罪。

法院认定，被告人犯罪行为的目的是通过公钥与私钥转移他人对虚拟货币的占有，并取得虚拟货币带来的财产性利益。虚拟货币虽然并无实体，但具有财产属性，可以认定为刑法所保护的财物。因此，仅认定其非法获取计算机信息系统数据不足以评价其犯罪行为，应当既构成非法获取计算机信息系统罪，亦构成盗窃罪。

对于犯罪数额的认定，法院认为，由于我国不认可任何虚拟货币交易价格信息发布平台对于虚拟货币的交易价格数据，故不应当认定涉案泰达币根据相关网站的历史价格计算价值 1200 余万元。考虑到罗业药将泰达币兑换以太坊后，又将以太坊兑换人民币，实际获利约 90 万元，故认定被告人犯盗窃罪数额为 90 万元。

## 五、区块链从业者易涉及的法律风险

### （一）民事风险

#### 1. 涉虚拟货币交易合同效力认定存在争议，发生纠纷或无法获得司法救济

合同效力问题是民事责任承担的基础。涉虚拟货币交易纠纷中，一方当事人（通常是违约方）往往会请求法院认定合同无效来规避法律责任。近年来，包括中国人民银行、中央网信办、最高人民法院等部门单独或联合发布了一系列部门规章，如《关于进一步防范和处置虚拟货币交易炒作风险的通知》、《关于整治虚拟货币“挖矿”活动的通知》等，对虚拟货币交易、投资等行为作出了强有力的行政手段规制。但是一方面，我国《民法典》第 143 条规定不违反法律、行政法规的强制性规定，不违背公序良俗的民事法律行为有效，目前涉虚拟货币相关法律法规存在效力位阶缺陷。另一方面，各类委托合同、买卖合同等层出不穷，效力认定及后续的赔偿额计算等问题上存在口径不统一。

在“江西建金置业有限公司、深圳玖星科技有限公司计算机软件开发合同纠纷”二审民事判决书<sup>①</sup>中，最高人民法院对涉虚拟货币合同效力问题作了详尽的论述，可供参考。

<sup>①</sup> 最高人民法院，(2021)最高法知民终 494 号。



原告建金公司不服一审判决，对被告玖星公司提起上诉，案涉合同标的为虚拟货币交易平台开发。建金公司诉请之一为请求法院认定案涉合同无效，由被告向原告返还不当得利。

最高人民法院认为：（1）关于合同无效的主张与审查。首先，对于民商事合同纠纷的处理应当秉持“鼓励交易”的原则。人民法院审理民商事合同纠纷案件应当尽可能尊重当事人基于意思自治达成的合意，在当事人未主张的情况下不能依职权变更或者撤销合同。其次，在尊重当事人意思自治的前提下，人民法院仍应依法审查合同是否存在违背公序良俗，违反法律、行政法规的强制性规定等无效情形，此种审查为依职权审查，不以当事人主张与否为转移。因此，即使合同当事人不主张合同无效，仅要求判令解除合同或追究对方的违约责任，人民法院仍可依职权认定合同无效，并向当事人释明合同无效的法律后果。（2）关于合同无效的审查依据。人民法院应慎重判断“强制性规定”的性质，特别是要在考量强制性规定所保护的法益类型、违法行为的法律后果以及交易安全保护等因素的基础上准确认定其性质。下列强制性规定，应当认定为“效力性强制性规定”：强制性规定涉及金融安全、市场秩序、国家宏观政策等公序良俗的；交易标的禁止买卖的；违反特许经营规定的；交易方式严重违法的；等等。

因此，由于案涉合同属于“开发行为”而非“经营使用行为”，不符合涉及金融安全、市场秩序与国家宏观政策的公序良俗，应认定为涉案合同有效。

## 2. 司法实践中赔偿损失请求获得支持困难

进一步，即使被认定为合同有效，在赔偿请求上也恐难以获得法院支持。由于我国仅承认虚拟货币的商品交易属性，且包括《关于进一步防范和处置虚拟货币交易炒作风险的通知》在内的部门规章已多次释明参与虚拟货币投资交易活动存在法律风险，故一旦案涉合同被判定存在投资性质，法院往往会适用“自甘风险”。就目前 2021 年公开判决的检索统计结果，仅有包括上文“朱某某与方某某买卖合同纠纷”在内的少数案件的当事人最终被判决支持了赔偿请求。

## 3. 涉虚拟货币案件存在涉外因素，须关注证据效力问题

虚拟货币交易平台位于境外，在交易平台中形成的包括交易记录在内的一

系列证据属于域外证据，应当适用《最高人民法院关于民事诉讼证据的若干规定》第 16 条关于域外证据的相关内容<sup>①</sup>，由所在国公证证明，或履行双边条约中有关规定。然而在发生纠纷时，一方面，域外证据公证程序较为繁琐；另一方面，当事人的证据意识不强，提交的证据缺乏域外证据合法性要件，导致法院对证据效力无法认定，最后无法采信。区块链从业者除应当培养证据意识与风险防范意识外，还应特别关注是否存在域外因素，防止域外因素在证据合法性认定上的干扰。

## （二）刑事风险

目前司法实践中出现的涉区块链刑事案件可分为两类：一是打着“区块链”的旗号，以区块链概念之名，行非法集资、传销、诈骗等犯罪行为之实。二是对区块链技术的滥用导致落入刑法规制的范围。

### 1. 存在实施侵害财产类犯罪的可能

需要注意的是，虽然虚拟货币交易行为在民法上可能因具有投资性质而被认定为合同无效，但在刑法语境下，虚拟货币具有的稀缺性、价值性和移转可能性等财产属性已得到司法实践的确认，属于刑法意义上的“财物”，可以构成财产类犯罪的对象。

区块链涉及的侵害财产类犯罪，主要包括盗窃罪、诈骗罪等。虚拟货币的占有人能够对自己持有的虚拟货币实施支付、转移等管理行为，虚拟货币的经济价值也可以以货币进行衡量。虽然 2021 年《关于进一步防范和处置虚拟货币交易炒作风险的通知》进一步明确了虚拟货币不具有与法定货币等同的法律地位，不应且不能作为货币在市场上流通使用，但需要明确此类部门规章是基于国家金融安全、市场秩序而人为作出的否定性评价，世界各国也存在允许虚拟货币流通并进行代币交易，故不可直接否认虚拟货币具有财产属性，其仍可能具备财产犯罪对象的财物的特征，可能可以纳入刑法所保护的法益范围之内。

### 2. 存在实施信息网络犯罪的可能

信息网络犯罪包括非法获取计算机信息系统数据罪、非法利用信息网络罪、帮助信息网络犯罪活动罪等。如果行为人通过虚拟货币交易平台为实施诈

<sup>①</sup> 《最高人民法院关于民事诉讼证据的若干规定》第十六条 当事人提供的公文书证系在中华人民共和国领域外形成的，该证据应当经所在国公证机关证明，或者履行中华人民共和国与该所在国订立的有关条约中规定的证明手续。

骗等违法犯罪活动发布信息的，即使不构成诈骗罪，也涉嫌构成非法利用信息网络罪。

如果行为人明知他人利用虚拟货币交易平台实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的，可能构成共同犯罪的同时构成帮助信息网络犯罪活动罪。例如在“仲某某非法获取计算机信息系统数据”一案<sup>①</sup>中，被告人仲某某通过软件远程控制其在比特大陆公司工位上的电脑，使用权限进入公司租用的阿里云服务器，在比特币钱包程序中插入代码转移了 100 个比特币至其在互联网的个人信息钱包中，造成比特大陆公司经济损失 3.6 万元。案发后仲某某退还公司 90 个比特币，另 10 个比特币无法找回。法院认为，被告人仲某某采用技术手段非法获取计算机信息系统数据，造成经济损失 1 万元以上，情节严重，其行为已构成非法获取计算机信息系统数据罪，应予惩处。

### 3. 存在实施经济类犯罪的可能

“经济类犯罪”是指破坏社会主义市场经济秩序罪这一类罪中的破坏金融管理秩序罪、金融诈骗罪、危害税收征管罪与扰乱市场秩序罪。其中又以非法吸收公众存款罪、集资诈骗罪、逃汇罪、洗钱罪、组织领导传销活动罪为刑事风险高发罪名。

(1) 非法吸收公众存款罪与集资诈骗罪。构成非法吸收公众存款罪需要符合非法性、公开性、利诱性与社会性四要件。在我国当前金融监管体系下，所有的 ICO 型代币与稳定币的发行与交易均符合“公开性”与“社会性”特征<sup>②</sup>，因此行为人以发行虚拟货币的方式筹集资金，若再符合“非法性”与“利益性”的特征，就存在构成非法吸收公众存款罪的风险。集资诈骗罪在非法吸收公众存款罪的基础上需要“以非法占有”为目的，如果行为人套取资金后有逃匿等行为，则可认定存在非法占有的目的。

(2) 洗钱罪。虽然 2021 年未检索到已公布的涉区块链洗钱罪相关判决，但以比特币为代表的虚拟货币一直是洗钱犯罪的理想工具。由于各个国家和地区对比特币等虚拟货币采取的监管政策存在差异，通过境外虚拟货币服务商、交易所，可实现虚拟货币与法定货币的自由兑换，虚拟货币被利用成为跨境清

<sup>①</sup> 北京市海淀区人民法院，(2018)京 0108 刑初 1410 号。

<sup>②</sup> 柯达：《论区块链数字货币的非法集资刑法规制》，载《东北大学学报（社会科学版）》2020 年第 6 期。

洗资金的新手段。2021年3月最高人民检察院与中国人民银行发布的6个惩治洗钱犯罪典型案例中，“陈某枝洗钱案”即为虚拟货币洗钱犯罪的典型案例。被告人陈某枝按照上游集资诈骗犯罪被告人陈某波指示，将陈某波用非法集资款购买的车辆以90余万元的低价出售，随后在陈某波组建的微信群中联系比特币“矿工”，将卖车钱款全部转账给“矿工”换取比特币密钥，并将密钥发送给陈某波，供其在境外兑换使用，当前陈某波仍未到案。

（3）虚拟货币自身基于区块链的特征及互联网无国界与现实社会国家间监管差异等因素使得虚拟货币容易逃避政府监管，引发逃汇、逃税、传销、毒品犯罪、走私犯罪、非法经营罪等。

## 第二章 远观

### 全球主要经济体区块链监管动态

#### 一、亚洲地区

##### (一) 日本

日本是世界第三大经济体，由于区块链技术的提出者中本聪被认为是日裔，所以日本政府和社会对区块链与虚拟货币的发展持开放态度。但由于出现过影响较大的涉区块链安全事件，故而近年来，日本在区块链与虚拟货币的开放程度有所收缩。

在日本，虚拟货币的法律地位由该货币的功能决定，主要包括以下三类：

1.加密货币和功能型代币（如比特币、以太坊），属于日本《交易服务法》下的加密资产。从事加密货币买卖、交换和居间业务，或为他人利益管理加密资产的经营主体，均需要注册为加密资产交易服务提供商。在《交易服务法》中，以下商业行为被定义为加密资产交易服务：

- (a) 出售或购买加密资产，或将一项加密资产交换为另一项加密资产；
- (b) 就第(a)项所列活动居间、或担任代理人；
- (c) 管理与(a)及(b)项所列活动有关的客户资金；
- (d) 管理客户的加密资产。

2.证券型代币，属于《金融商品交易法》下的“电子记录的可转让权利”；从事发行、购买、出售、交换、居间等业务的经营主体，必须进行第一类金融产品经营者注册。

3.稳定币，取决于是否可以与法定货币兑换，存在被认定为加密资产或资金汇款交易中的支付手段两种可能。

第一类加密货币与功能型代币的交易服务提供商受到了愈发严格的监管，包括但不限于：禁止受管理的加密资产与管理者个人加密资产混同；强制要求大于95%用户的加密资产以冷钱包存储，并且非以冷钱包存储的加密资产，必须与管理者个人的加密资产为相同类型和数量（因此被称为“保证性加密资产”）等。

同时应当注意，日本虚拟货币交易协会对首次代币发行发布了行业自律性

规范《销售新加密资产规则》。根据该规则，首次代币发行根据发行主体不同可分为交易所提供商自行发行并销售新代币和代币发行方委托交易所提供商销售新代币。该规则对代币发行提出以下要求：

- 1.应当维护通过首次代币发行筹集资金的目标企业的治理结构；
- 2.应履行代币的信息披露、发行者的资金用途等信息披露义务；
- 3.应独立管理财产；
- 4.应妥善处理筹集资金的账目和财务披露；
- 5.应保障新发行代币及其区块链、智能合约、钱包工具等安全；
- 6.对新发行的代币进行适当的估值。

对于第二类证券型代币，根据《金融商品交易法》原则上应当构成“集体投资计划性利益”。一般认为，在日本法中，若符合 1.投资者向企业投资现金或其他资产；2.该项出资投资于本企业；3.投资者有权从对企业的投资中获得利润或资产的股息三项构成要件，则应当被认定为“集体投资计划性利益”。

在反洗钱领域，根据日本《防止转移犯罪收益法》，加密资产交易服务提供者应当履行下列合规义务：1.为进行交易和业务的目的，核实客户和对客户的业务有实质性控制权的人的身份资料；2.编制核查记录和交易记录；3.将记录保存七年；4.向有关部门报告可疑交易等。

## （二）新加坡

新加坡的央行——新加坡金融管理局（The Monetary Authority of Singapore, MAS）目前尚未发行或支持任何零售加密货币，但新加坡金融管理局已经参与试点“Ubin 项目”，探索使用区块链和分布式账本技术进行支付和证券业务。<sup>①</sup>该项目作为试点项目已于 2020 年 7 月圆满结束，据了解，通过该项目开发的支付网络原型将有助于开发跨境支付基础设施和客户应用程序。

根据《2019 年支付服务法案》（Payment Services Act 2019, PSA），新加坡的加密货币存在受监管与不受监管的加密货币两种分类。由于加密货币类型各异，根据 PSA 的定义实际上并未完全覆盖所有的加密货币。此外，部分加密货币若属于新加坡《证券和期货法案》（Security and Futures Act, SFA）中定义的资本市场产品或证券的特征，则可能受到该法的监管。

<sup>①</sup> Project Ubin: Central Bank Digital Money using Distributed Ledger Technology, <https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.2022-2-17>.

### 1. 《2019年支付服务法案》(PSA)

根据 PSA 要求, 经营加密货币支付服务业务的人需要行政许可, 获得支付牌照。PSA 定义了七种支付业务, 即开立账户、电子货币发行业务、跨境转账业务、国内汇款业务、收购业务、数字支付令牌 (DPT) 业务和兑换业务。

同时 PSA 规定了两种类型的行政许可, 即标准支付机构牌照 (standard payment institution license) 和主要支付机构牌照 (major payment institution license):

对于从事开立账户、国内汇款业务、跨境转账业务、收购业务和数字令牌业务的主体, 若一自然年中在一个月内接受、处理或执行单个支付业务的总价值超过 300 万新元 (或等值外币) 或两个及以上支付业务超过 600 万新元 (或等值外币), 则需要获得主要支付机构牌照。

对于从事电子货币发行业务的主体, 若 (1) 在单个自然年内, 存储在该主体且向该主体确定为新加坡居民的用户开立的任何支付账户, 及在新加坡发行的所有电子货币单日内总价值的平均值超过 500 万新元 (或等值外币), 或 (2) 在单个自然年内, 单日内所有发行的指定电子货币超过 500 万新元 (或等值外币), 则需要获得主要支付机构牌照。

除上述情况外, 支付服务提供者只需要获得标准支付机构牌照即可。

除此之外, PSA 规定了申请人获得许可证的资格要求, 以及对被许可人的持续合规要求。对于标准支付机构牌照, PSA 要求最低资本不得少于 10 万新元; 对于主要支付机构牌照, 则要求不少于 25 万新元。申请人还被要求必须有至少一名新加坡公民或永久居民担任执行董事, 或至少一名新加坡公民或永久居民担任非执行董事, 以及至少一名持有新加坡就业证的执行董事。此外, 牌照申请人必须在新加坡设有永久营业地或注册办事处, 且须保存与申请人提供的支付服务有关的所有交易。

2021 年, PSA 迎来修订, 新加坡金融管理局被授权在必要时可以增设行政许可类别, 通过设置额外类别的牌照提供特定的付款服务, 以保障客户的资金。因此, 修订后即使是标准支付机构也可能面临与主要支付机构同等的监管措施。

### 2. 《证券和期货法案》(SFA)

根据 SFA，加密货币可能与传统类型的资本市场产品具有类似的特征，如证券、衍生品合约和以杠杆式外汇交易为目的的即期外汇合约等。因此，SFA 中关于上述金融产品的监管措施可同样适用于加密货币的交易，例如代理人须持有资本市场服务许可证；又如加密货币在 SFA 下的非公开发行，要求在 12 个月内向不超过 50 人发出要约，筹集的总金额不得超过 500 万新元（或等值外币）。

目前，新加坡尚未出台直接适用于挖矿活动的禁令或监管立法。但如果被挖掘的加密货币构成受监管的产品，则该加密货币及其挖矿行为可能落入 SFA 的监管范围。

根据新加坡《贪污、贩毒及其他重罪没收违法所得法案》[Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, CDSA]，交易服务提供方有义务向新加坡警方有关部门报告可疑交易，若怠于履行该义务则可能构成 CDSA 法案下的犯罪行为。

根据新加坡《反恐怖主义融资法案》[Terrorism (Suppression of Financing) Act, TSFA] 有关方应当向警方披露包括但不限于占有、保管或控制财产等信息的任何恐怖分子或组织。有关方还应确保涉加密货币服务的合规性，如遵守 TSFA 项下针对特定主体的金融制裁要求，遵守新加坡内政部、联合国安理会决议等要求。

### （三）韩国

韩国涉及虚拟资产和区块链的行政部门及其对应行政事权如下：

部门	行政事权
金融服务委员会（SFC）	管理、监督虚拟资产服务提供商包括但不限于反洗钱在内的事项
经济和金融部	虚拟资产征税、违反外汇交易法的监督检查
科学与通信部	培育区块链产业，防止虚拟资产服务提供商网络攻击
公平交易委员会	防范与处置虚拟资产服务提供商不正当竞争行为
个人信息保护委员会	防范虚拟资产交易中个人信息泄露及侵权
国家税务局	虚拟资产税收制度，强制征收高价值虚拟资产违法者
韩国海关	监管违反外汇交易法的行为

2021 年韩国涉虚拟资产相关法律法规更新主要为《报告和使用特定金融交



易信息法》（Reporting and Using Specified Financial Transaction Information Act, SFIA）修正案和一项针对个人的虚拟资产交易的税收法案。其中，SFIA 修正案主要修订了虚拟资产和虚拟资产服务提供方的概念，以及虚拟资产服务提供方的报告义务和反洗钱义务。

关于虚拟资产的概念，修订后的 SFIA 规定，虚拟资产是具有可电子交易或可转让的经济价值的电子代币（包括对虚拟资产所享有的任何权利），但不包括：

- 1.不能通过货币、商品或服务交换的代币或代币信息，且该代币或代币信息的使用和地点受到发行方的限制；
- 2.《游戏产业促进法》第 32 条第 1 款第 7 项下的通过游戏产品获得的有形及无形物品；
- 3.《电子金融交易法》第 2 条第 14 项下的电子预支付方式，和第 2 条第 5 项下的电子货币；
- 4.《证券电子登记法》第 2 条第 4 项下的经电子登记的股票；
- 5.《电子票据发行法》第 2 条第 2 项下的电子票据；
- 6.《商法》第 862 条下的电子提单；
- 7.《电子金融交易法》第 2 条第 16 项下的电子债券；
- 8.在手机等移动设备上储存和使用的商品券；
- 9.韩国金融情报院（KDI）根据交易的类型和特点，将符合 SFIA 第 1 条和第 2 条的其他项目排除在虚拟资产之外的类别（目前尚未公布）。

根据 SFIA，由于“证券代币”并未明确排除在虚拟资产的定义之外，故证券代币可能同时构成证券与虚拟资产，可能同时受到 SFIA 和金融投资服务和资本市场法的约束。

关于虚拟资产服务提供方的概念，修订后的 SFIA 规定，虚拟资产服务提供方是指从事下列任何一项业务的人：

- 1.出售和购买虚拟资产；
- 2.交换虚拟资产以换取另一虚拟资产；
- 3.根据客户的要求，转移虚拟资产以供交易、交换、存储或维护等虚拟资产；

4. 储存或管理虚拟资产；

5. 就第 1 或 2 项下的任何交易进行经纪、调解或作为代理人。

SFIA 要求虚拟资产服务提供者有义务向韩国金融情报院报告，若拒不报告或虚假陈述则主要负责人可能承担五年以下的监禁，并处或单处五千万韩元以下的罚款。

应当注意的是，韩国将发行虚拟资产排除在虚拟资产服务提供者的运营范围之外，反映了金融当局在事实上禁止 ICO 的立场。

在韩国，成为虚拟资产服务提供者首先需要获得信息安全管理系统（ISMS）证书。若该提供者拟提供法定货币与虚拟资产之间的兑换业务，则提供者必须在韩国国内银行开立实名账户。需要注意的是，SFIA 同时适用于服务对象为韩国公民的境外企业，因此境外企业在韩国提供兑换业务较为困难。

韩国 SFIA 同样规定了对于虚拟资产的反洗钱合规要求。如果客户在一次交易中将价值超过 100 万韩元的虚拟资产转移至另一虚拟资产服务提供者，则后者必须在交易时提供发送方与接收方的姓名与账户，以满足反洗钱合规要求。其他具体的反洗钱义务包括：

1. 分别管理客户的交易明细；

2. 分别管理客户存款与虚拟资产服务提供者的专有资产；

3. 对未完成验证程序的客户交易的限制；

4. 不得与未履行任何业务报告义务的虚拟资产服务提供者进行交易；

5. 不得在客户与其他虚拟资产服务提供者的客户之间进行虚拟资产的销售或交换。但是，如果其他服务提供者已履行反洗钱义务，并完成了许可和注册等手续，则可以代理此类交易。

6. 验证虚拟资产是否为转账记录无法识别的虚拟资产。

## 二、欧洲地区

### （一）欧盟

2021 年 2 月 19 日，欧洲央行公布了对加密资产监管草案（MiCA）的意见。MiCA 在欧洲议会的立法程序目前仍处于一读阶段，预计于 2022 年底生效。

MiCA 旨在明确加密货币的处理规范，并监管已不受现有欧盟法律监管的

加密资产及加密资产服务。由于欧洲各国对加密资产领域的法律规定缺乏一致性，企业难以在该领域开展业务，这也使得市场参与者缺乏公平竞争的机会。

MiCA 的通过将会对发行人、服务提供商和交易场所会产生较大影响。加密货币发行者须发布产品白皮书以遵守信息披露义务，并向有关金融监管部门提交相关资料。此外，MiCA 决定，加密资产托管人、交易场所运营商等加密服务提供商若希望在欧盟提供产品和服务，必须在欧盟成员国设立注册办事处，对于小型企业来说，该监管规定可能会造成某些不利影响，如公司可能面临高昂的成本，例如，为获得许可证、为符合报告要求或为设置安全 IT 基础设施所涉的成本。

欧盟对虚拟货币同样实施了反洗钱筛查。金融行动特别工作组（FATF）分别在 2015 年和 2019 年更新了虚拟资产和虚拟资产提供者基于风险的方法指南，其中包括修订第十五建议案，并对虚拟资产和虚拟资产提供者进行了定义。

实际上，欧盟的第五反洗钱指令（AMLD V）并未直接提及虚拟资产，仅提到了虚拟货币，这种狭义定义方式的合理性值得探讨。基于此，2020 年 9 月欧盟出台《加密资产市场法规》（MiCA），其中就将加密资产定义为“一种可以通过分布式账本技术（DLT）或类似技术，以电子方式转移和存储价值或权利的数字形式。”

欧盟各成员国间对加密资产的税收、披露义务等具体规范的参差，使得逃税、洗钱风险进一步增加。

2021 年 3 月 10 日，欧盟委员会启动一项调研，旨在加强行政合作，扩大涉电子货币和加密资产的信息交流。该项调研的结果将为行政合作指令（Directive on Administrative Cooperation, DAC）提供依据。DAC 预计会在通过后的 12 至 18 个月内实施，其覆盖范围将比欧盟目前的法规更广，并将为金融机构提供新的选择，以采取行动打击税务欺诈和避税活动。目前一些欧盟国家已实施或将要实施针对加密资产服务提供商的申报义务。同时调研结果也显示，各国不同的合规要求可能对加密资产和电子货币服务提供商造成额外的行政负担，从而抑制创新。<sup>①</sup>

<sup>①</sup> Reed Smith Guide to the Metaverse. <https://fingfx.thomsonreuters.com/gfx/legaldocs/bdwpkwnyopm/MetaverseWhitePaper2->

## （二）英国

英国是国际上对区块链技术和数字货币最为宽松的国家之一，自 2018 年以来始终在现有法规范体系内将监督作为主基调，并且为全球区块链初创企业提供了优惠的政策。

2018 年 10 月，英国财政部、英国央行和英国金融行为监管局（FCA）联合发布关于加密资产的报告，这被认为是英国在政府层面着手对区块链与数字货币进行监督管理的起点。在该报告中，加密数字货币被定义为“加密资产”的子集，而“加密资产”指“使用密码保护、分布式账本技术（DLT）并可以电子方式转移、存储或交易的价值或合同权利”。基于该定义，该报告进一步对加密资产做出三种学理性分类：交易型代币（Exchange Tokens）、证券型代币（Security Tokens）、功能型代币（Utility Tokens）。<sup>①</sup>2019 年 7 月，FCA 发布《加密资产指南》，将加密资产分为受监管的代币（Regulated Tokens）和不受监管的代币（Unregulated Tokens）。<sup>②</sup>上述分类标准对应关系如下：

不受监管的代币	交易型代币：去中心化的、用作交易手段的代币。
	功能型代币：向消费者提供当前或未来产品或服务的代币，消费者获得类似于预付费凭证的权利。
受监管的代币	证券型代币：提供类似于《2001 年金融服务和市场法令》（RAO）中特定投资项下权利义务的代币。
	电子货币代币（E-money Tokens）：是指满足 2011 年电子货币条例的代币。

尽管英国金融监管机构已对投资加密资产发出警告，但加密资产在英国并未受到严格管控，英国认可并保护加密资产的所有权。2019 年 11 月，英国司法工作组（UK Jurisdiction Taskforce, UKJT）发布报告《关于加密财产与智能合约的法律声明》，认为加密资产具备英国法下“财产”所要求的所有特性，能够被视为一种财产形式。<sup>③</sup>该报告虽然不具有法律效力，但是该观点已被英格兰和威尔士高等法院采纳并在司法实践中得到应用。<sup>④</sup>

除反洗钱制度的某些内容专门适用于加密资产相关业务外，英国尚未出台

[compressed.pdf 2022-2-21](#).

① Cryptoassets Taskforce: Final Report, p.11, [www.gov.uk/government/publications](http://www.gov.uk/government/publications). 2022-2-8.

② PS19/22 Policy Statement: Guidance on Cryptoassets, <https://www.fca.org.uk/publication/policy/ps19-22.pdf>. 2022-2-9.

③ UK Jurisdiction Taskforce, *Legal Statement on cryptoassets and smart contracts* (November 2019), p.21-22, [https://35z8e83m1h83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056\\_JO\\_Cryptocurrencies\\_Statement\\_FINAL\\_WEB\\_111119-1.pdf](https://35z8e83m1h83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf). 2022-2-8.

④ 如 AA v. Persons Unknown [2019] EWHC 3556 (Comm) (17 January 2020).

针对加密资产金融监管的专门性立法。目前英国规制加密货币所依据的一般性法律规范主要包括：2000年《金融服务和市场法案》（Financial Services and Markets Act 2000, FSMA）、2017年《支付服务条例》（Payment Services Regulations 2017, PSRs）、2011年《电子货币条例》（Electronic Money Regulations, EMRs）。因此，私主体在英国经营涉加密货币业务是否需经许可取决于经营活动是否属于FSMA定义的“受监管的活动”，或属于PSRs和EMRs规定属于需要授权的支付服务或电子货币活动。

虽然目前涉加密货币的投资和发行行为未落入英国法的监管范围，但2020年7月英国财政部拟提议拓宽监管范围，将不受监管的加密资产添加到受控投资列表中，并扩大受控活动列表，包括与此类加密资产的购买、出售、认购或承销相关的活动。<sup>①</sup>该提案暂未获通过，但也表明英国政府存在对加密资产加强监管的倾向。若该提案被采纳，则仅有经许可的主体有权实施不受监管的加密货币的发行、承销等行为。

涉加密货币反洗钱制度主要规定于2017年《洗钱、恐怖主义融资和资金转移条例》（Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, MLRs）。2020年1月，在MLRs的修订中，加密资产交易服务提供者与托管服务提供者被纳入监管对象。需要注意的是，基于MLRs修订中加密资产交易服务提供者的定义，其监管的范围可能涵盖在通常情况下不被认定为的市场参与主体，如加密资产经纪人与发行人。

### 三、北美洲地区

#### （一）美国

加密货币一直是联邦政府和州政府关注的焦点。联邦一级的关注点集中在美国证券交易委员会（SEC）、美国商品期货交易委员会（CFTC）、美国国税局（IRS）、金融犯罪执法网络（FinCEN）等。在州一级，许多州政府也提出或通过了有关加密货币和区块链技术的法案，立法活动活跃。

州一级的规制措施可大致分为两类。其一如怀俄明州，对加密货币持开放态度，并希望利用区块链技术投资刺激本州经济发展，改善公共服务。目前怀

<sup>①</sup> HM Treasury, *Cryptoasset Promotions – Consultation* (July 2020), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/902891/Cryptoasset\\_promotions\\_consultation.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902891/Cryptoasset_promotions_consultation.pdf) 2022-2-10.

俄明州已通过立法，允许设立以加密货币为业务的新型银行和储蓄机构。该类金融机构既可作为托管机构，也可作为受托机构，使企业能够安全合法地持有数字资产。该州被誉为美国对加密货币最友好的州。其二如爱荷华州、马里兰州和夏威夷等，对公众投资加密货币发出警告。值得注意的是，部分曾经对加密货币持保守态度的州在 2021 年有所放宽，如纽约州曾通过了高限制性的法律，如今已放松了比特币持牌的限制。

一般而言，只有在以下情况下，加密货币的销售才会在美国受到监管：1. 根据州或联邦法律构成证券的销售，2. 根据州法律被视为货币传输，或根据联邦法律使个人成为货币服务企业（MSB）的其他行为。CFTC 对涉及被视为大宗商品的加密资产的市场操纵行为具有管辖权，由于芝加哥期权交易所（CBOE）和芝加哥商品交易所（CME）均推出了与比特币价格相关的期货，目前看来 CFTC 有较大可能使用行政手段介入加密货币交易以维护市场秩序、防止操纵市场。

美国对某项商品是否属于证券采实质性判断——即“豪威测试”。SEC 已经明确其对加密货币交易的立场，即使在 ICO 中发行的代币属于功能型代币，但如果满足豪威测试，该代币仍将被视为受《证券法》监管的证券，发行人必须向 SEC 履行注册程序，或根据豁免注册要求提供该证券。

截至目前，SEC 已经对包括 Telegram 和 Kik（均为即时通讯软件）在内的主体采取法律手段。2019 年 10 月，SEC 对 Telegram 提起诉讼，称该公司通过发行 29 亿 GRAMS 币（该公司发行的本地加密货币）获得 17 亿美元融资。GRAMS 币允许即时通信业务的客户使用该加密货币作为 Telegram 应用生态系统内的商品和服务的结算依据。SEC 认为，Telegram 发行的 GRAMS 符合豪威测试的标准，应当属于证券，Telegram 作为发行方未履行注册义务。2020 年 3 月，纽约南区法院认同了 SEC 的观点，即对未来代币发行的协议（Simple Agreement for Future Tokens, SAFT），及依据 SAFT 协议的后续转售，不应被割裂的视为两个独立的阶段，而应当被视为一个整体，并发布一项初步禁令。最终，Telegram 放弃了发行 GRAMS 代币的计划，同意向投资者偿还 12 亿美元，并支付 1850 万美元的民事罚款。

2020 年 10 月，联邦法院终审判决 Kik 公司于 2017 年未经注册发行 Kin 币

的行为违反美国证券法。法院认定 Kik 公司发行 Kin 币的行为构成“投资性合同”，因此 Kin 币属于证券。最终 Kik 同意支付 500 万美元罚款。

SEC 在 Telegram 和 Kik 案中的立场可能会使代币发行方难以区分通过虚拟货币进行的融资活动和非投资性的功能型代币的发行。同时，鉴于发行风险，许多代币发行方已经选择将美国公民排除出投资者行列，选择限制销售给非美国国籍投资者。

根据《银行保密法案》，对 MSB 的监管属于 FinCEN 的职权范围。2013 年 3 月，FinCEN 曾发布一份指南，若某一实体符合“1.该实体从事虚拟货币交换业务，且 2.该实体拥有虚拟货币中心化存储的管理者，且该管理者行使虚拟货币发行权和赎回权”，则该实体可能被认定为 MSB。MSB 作为货币传输者必须对洗钱风险进行全面评估，并履行反洗钱义务。FinCEN 要求 MSB 制定并执行一套反洗钱与反恐怖主义融资方案，该方案必须：1.包含确保持续合规的书面政策、程序和内部控制；2.指定一名个人合规官，负责确保项目和 BSA 要求的日常合规；3.为适当的人员提供可疑交易识别方面的培训；4.提供独立审查以监测和维护。

其次，所有美国公民均被禁止与美国财政部外国资产控制办公室（Office of Foreign Assets Control, OFAC）特别指定国民和被封禁实体名单（Specially Designated Nationals and Blocked Entities List, SDN List）上的外国实体进行交易。从事虚拟资产服务的实体需要制定合规计划，以避免因不合规而受到 OFAC 的民事甚至刑事处罚。

## （二）加拿大

加拿大主要依靠其国内的证券法律体系对加密货币进行规制，虽然证券法律制度不属于加拿大联邦一级法律，但加拿大证券管理局（CSA）代表了各地区的证券监管机构，并建立了基本统一的证券规则。

“证券”的定义在加拿大立法中极为广泛，根据“投资性合同测试”（Investment Contract Test，类似于美国“豪威测试”），若符合以下四项要件，就应当被归入证券范畴，适用证券法律制度：1.存在金钱的投资；2.该投资期待利益的产生；3.该投资针对特定事业；4.利益的产生源自发行人或第三人的努力。

对于加密货币发行行为（Cryptocurrencies Offerings, CCOs），加拿大证券监管机构在实践中会进行个案分析，重点关注发行的实质和结构。若发行符合证券立法之目的，则即使未列入《证券法》列举的非独家证券类别清单仍须受证券法律制度的监管。CSA 认为，许多代币产品虽然在多数情况下以软件产品的形式进入市场，但仍应当视为证券。

2021 年 3 月，CSA 发布通知，提示加密货币发行人如何履行信息披露义务，主要包括：

1. 发行人的业务描述，包括其对第三方服务提供商的依赖；
2. 发行人业务面临的风险，特别是与加密资产相关的风险；
3. 发行人的业务发生的重大变化；
4. 发行人对加密货币会计和审计标准、政策和相关指导的遵守情况，特别是涉及加密货币会计、“挖矿”、估值等情况；
5. 发行人加密资产防盗或防损措施；
6. 披露发行人是否使用加密资产交易平台持有加密货币的声明。<sup>①</sup>

加拿大是第一个将加密货币纳入反洗钱监管的国家。《反洗钱和恐怖主义融资法案》（The Proceeds of Crime (Money Laundering) and Terrorist Financing Act, PCMLTFA）是规制加密资产洗钱犯罪与恐怖主义融资的主要法律规范，该法案使用了“虚拟货币”（Virtual Currencies）的定义，包括可用于支付目的的交易型代币和可用于投资目的的证券型代币。法案将处理虚拟货币交易的主体认定为现金服务提供者（Money Services Businesses, MSBs），符合现金服务提供者资格的交易商必须在加拿大金融交易与报告分析中心（FINTRAC）注册，并妥善执行经过独立评估的反洗钱合规方案。

## 四、南美洲地区

### （一）巴西

巴西经济部下辖四部门——联邦税务局（*Secretaria Especial da Receita Federal do Brasil*, RFB）、巴西央行（*Banco Central do Brasil*, BCB）、证券交易委员会（*Banco Central do Brasil*, BCB）和私人保险监督协会（*Superintendencia*

<sup>①</sup> CSA Staff Notice 51-363: Observations on Disclosure by Crypto Assets Reporting Issuers (11 March 2021), [https://www.osc.ca/sites/default/files/2021-03/csa\\_20210311\\_51-363\\_observations-disclosure-crypto-asset.pdf](https://www.osc.ca/sites/default/files/2021-03/csa_20210311_51-363_observations-disclosure-crypto-asset.pdf).2022-2-10.



*de Seguros Privados, SUSEP*) ——负责加密资产相关事务。

加密货币和其他的虚拟资产在巴西被归类为动产或商品。虽然目前为止加密资产在巴西不具有货币资格，也未受到专门性法律法规的规范，但巴西政府对加密资产的态度非常开放。巴西联邦政府和地方当局正在审查具有社会影响力和变革潜力的区块链技术应用场景，并努力发展基于该技术的生态系统，以利用区块链和加密资产作为公共和私营部门创新的渠道。2021年3月，第14129/21号法案正式启动了数字政府规划，旨在提高公共服务的效率，减少官僚主义，促进创新，实现政府机构的数字化转型。一直以来，巴西国家现代化特别秘书处 (*Secretaria Especial de Modernizagao do Estado, SEME*) 保持与公共部门合作以发展巴西区块链网络，并致力于研究如何利用技术提高公共部门的效率。

区块链技术给巴西法律体系带来了很大挑战。目前，数字资产监管框架主要由行政当局的条例组成，但尚未制定具体的法律来规范这一问题。2021年以来，巴西国会开始审议多项有关区块链和加密资产的法案，大多数法案旨在解决社会问题，减少欺诈和庞氏骗局，其他也引入了数字资产的遗嘱认证和继承规则。

目前，在下议院通过的第2060/19号法案对包括加密值、工具、资产、令牌等提出了更规范的定义。该法案同时引入了加密资产发行规则，并将其在“金字塔”或庞氏骗局和加密资产的非常规交易中的欺诈使用规定为犯罪行为。同时，上议院也正在审议包括涉加密资产的第3825/19号法案、第3949/19号法案、第4207/20号法案等在内的法案。上述法案除了对加密资产进行定义及分类并与现有法律体系保持一致性外，也规制涉加密资产的违法犯罪行为。例如，第4207/20号法案根据“加密资产的发行、调解、托管、分配、清算和管理”的规定，将不合规的交易归类为危害国家金融系统的犯罪（即“白领重罪”）。

巴西证券交易委员会 (*Comissao de Valores Mobiliarios, CVM*) 在虚拟资产交易方面采取了非常严格的审查措施，特别是为巴西公民提供服务但没有获得证券监管机构的许可的国外交易平台。

对于反洗钱与反恐怖主义融资，第9613/98号法案是巴西反洗钱法。该法

设立了金融活动管制委员会（*Consetho de Controle de Atividades Financeiras*, COAF），该联邦机构是金融情报的中心，负责藏匿资产和价值、洗钱和恐怖主义融资等可疑案件。COAF 的法律职责包括与特定行业的监管机构进行协调，以及对不受政府机构监管的行业拥有监管权与执法权。商事主体有义务就可能引发洗钱风险的事项向 COAF 报告所进行的交易，报告须包括内部合规措施、客户和交易的识别和记录、以及超过一定数额的交易的披露等。在 2021 年 3 月 COAF 的一项决议中，被纳入监管的实体必须根据交易量周期性运行内部风控测评。

RFB 第 1888 /19 号规则要求加密货币交易所有义务向 COAF 报告其交易情况，但除了当局强制要求披露的信息外，行业自律组织加快制定的规则也已被采用，以协助反洗钱、反恐怖主义融资活动。例如，交易所已经广泛接受了巴西加密经济协会（ABCripto）制定的行业规则，要求参与加密货币交易和经纪业务的公司在其平台上采取措施以避免可能具有非法活动或金融犯罪特征的交易。

## 五、大洋洲地区

### （一）澳大利亚

迄今为止，澳大利亚政府对加密货币的监管基本上采取了不干涉主义的方法，允许该领域在没有重大监管限制的情况下快速发展。澳大利亚技术和金融中心特别委员会（Select Committee on Australia on Technology and Financial Centre）在 2021 年 3 月发布的第三期文件中也再次强调了政府对加密货币的支持态度。虽然部分立法修正案对加密货币的使用作出规定，但此类修正案主要关注在涉及加密货币的交易活动中产生的法律关系，而非加密货币本身。

目前，澳大利亚法律并未将数字货币与法币挂钩，且“数字货币”不被视为“货币”。澳大利亚央行澳大利亚储备银行（The Reserve Bank of Australia, RBA）虽然已经主导或参与了许多加密资产相关的项目，但目前尚未表明有发行央行数字货币的意愿。

除支付领域外，澳大利亚社会对于包括加密货币在内的加密资产能被接受为一种投资门类有较高期待。2021 年 6 月，澳大利亚证券和投资委员会（Australia Securities and Investments Commission, ASIC）启动了一项咨询程

序，旨在调研公众对交易所交易产品和其他投资产品基础资产中加密货币资产的预期。

ASIC 在 2021 年重申了其对于法律义务和监管要求属于技术中立的观点，并且适用于提供监管服务的技术模式。目前澳大利亚国内尚未有立法将加密货币作为一个独立的法律领域进行规制，因此一般性法律规范适用于加密货币。例如，加密货币如作为 2001 年公司法规制的集体性投资产品（或该产品的一部分）将落入澳大利亚现行金融服务监管制度的范围内。又如，涉加密资产的借贷关系若属于 2009 年国家信贷消费者保护法中信贷活动的范围，则相关实体需要持有澳大利亚信贷许可证或豁免许可证。

2021 年 3 月，ASIC 对其发布的公共信息表《INFO2019 评估分布式账本技术》概述了在未来区块链技术普及后可能面临的监管难题及初步的解决方案。在该报告中，使用分布式账本技术经营市场基础设施或提供金融或消费信贷服务的企业，仍需遵守现行许可制度下的合规要求。一般认为，在提供受管制服务方面依赖技术的实体必须具备必要的组织能力和技术资源，并制定风险管理计划。

同时，ASIC 在其《INFO225 首次代币发行》中表明，若私主体从事与现有金融产品或证券具有类似特征的加密货币相关业务，则会触发相关监管义务。ASIC 表示，加密货币的法律地位取决于 ICO 的结构和附属于加密货币或代币的权利。根据具体情况，加密货币或代币可能构成集体投资工具、证券及证券衍生品等，或落入兜底的“金融产品”之类别。上述所有门类都受到澳大利亚金融服务监管制度的约束。在该报告中，ASIC 为涉加密资产利益相关方

在 INFO 225 中，ASIC 为加密资产利益相关方提供了更为详细的监管指示，以确定他们是否有法律和监管义务。加密资产利益相关方包括了加密资产发行人、加密资产中介、“矿工”、加密资产交易所和交易平台、加密资产支付服务提供商、钱托管服务提供商等。

ASIC 的合规建议在大体上与其他监管机构的立场保持一致，ASIC 同时建议希望进行 ICO 或其他代币销售的主体寻求包括法律合规服务在内的专业建议。这反映 ASIC 愿意将加密货币作为一种资产类别建立更大的投资者信心。然而，ASIC 强调企业需要遵守消费者保护相关法律，并已采取相关措施停止了

违反披露义务和未提供澳洲金融服务牌照（Australian Financial Services License, AFSL）的金融产品的代币发行。

自 2021 年 10 月 5 日起，澳大利亚金融产品的发行方和分销商必须遵守设计和分销义务（Design and Distribution Obligation, DDO），旨在确保一项特定金融产品符合潜在投资者类别。该义务可能会影响未来加密货币的结构和销售方式。

对于反洗钱与反恐怖主义融资方面的合规要求，自 2018 年起，数字货币交易提供商有义务向澳大利亚交易报告和分析中心（Australian Transaction Reports and Analysis Centre, AUSTRAC）注册，违反注册义务可能被处以 2 年以下的监禁或/和 111,000 澳元以下罚款。2021 年 6 月，AUSTRAC 推动金融行动特别工作组为反洗钱与反恐怖主义融资指标的指引发出警告，该指引为监管机构和负有报告义务的实体制定了实践，并为如何制定下一步与数字货币相关的反洗钱与反恐怖主义融资立法提供了参考。

## 第三章 解析

### 国际区块链合规应用

#### 一、2021 年全球区块链产业融资

2021 年，全球区块链产业融资情况依然火热，从投融资行业看，除仍然受到资本青睐的加密货币、区块链解决方案外，NFT、隐私计算、技术融合等也逐渐成为新的火热赛道。

从融资情况看，据不完全统计，2021 年，全球区块链产业共产生融资 1812 起，其中 1433 起公开披露具体融资数额，总计达 486.74 亿美元，平均单笔融资额达 3396.65 万美元。

从融资事件地区分布看，全球区块链产业融资分布不均衡。美国的区块链融资计 536 起，占全球总数的 42.54%，中国计 105 起，占 8.33%，英国计 99 起，新加坡计 96 起，加拿大计 51 起。<sup>①</sup>

#### 二、具有影响力的跨国企业表现

##### （一）三星电子

三星电子正在开发手机特殊化的自有区块链平台“Flatun”，并开发出了名为“Platoon”的自有区块链主网和在 Platoon 上运行的多种去中心化应用程序（DApp）。

在 Platoon 上开发的第一个应用程序是使用代币经济的 HR 服务“Mobileway Wallet”。通过 Mobileway Wallet 向三星内部其他部门请求业务协助时，可以通过发送三星代币进行，拥有三星代币越多的职员，在人事考核中越能得到好评。三星的构想是将跨部门协作的工作量定量化，并反映到人事评价中。

三星的 IT 部门——三星 SDS 以地方自治团体、医院、机场等为对象，构建了多数区块链项目。其中包括一站式医疗请求处理服务，患者可以在医院接收中心、自助服务厅或手机上提交请求。Nexledger 是三星 SDS 的企业定制型

<sup>①</sup> 陈丽珊：《2021 年全球区块链投融资报告》

[https://mp.weixin.qq.com/s?\\_\\_biz=MzA3NjE4NjQ4NA==&mid=2650583777&idx=1&sn=3120f1d0a72de55d56eb295c8078f020&chksm=876d04fab01a8dec28a7483673d00591b62145387211233f7e327c9ff8324a87ebf00ac4252&scene=21#wechat\\_redirect.2022-3-13](https://mp.weixin.qq.com/s?__biz=MzA3NjE4NjQ4NA==&mid=2650583777&idx=1&sn=3120f1d0a72de55d56eb295c8078f020&chksm=876d04fab01a8dec28a7483673d00591b62145387211233f7e327c9ff8324a87ebf00ac4252&scene=21#wechat_redirect.2022-3-13)

区块链平台，可以广泛使用作为第四次产业革命的核心技术而备受瞩目的区块链技术。另外，三星 SDS 开发了基于区块链技术的银行共同认证服务“BankSign”，用户在一家银行签字并获得该银行认证后，在其他银行只要通过简单的认证就可以方便地使用交易银行的移动银行服务。2019 年，三星提出打造 Nexledger Universal，将提供三星 SDS NCA（Nexledger Consensus Algorithm）、通用区块链技术 Hyperledger Fabric、Ethereum 等共同适用的标准 API（应用程序接口）。通过这一技术，顾客只要用三种中的一种技术开发用户认证、支付结算、原始证明等应用服务，就可以轻易适用于其他技术。

## （二）福特汽车

2019 年 1 月 19 日，福特汽车公司、华友钴业、IBM、LG 化学和 RCS Global 联合启动一项新项目，在 IBM 平台上使用区块链试点来进行规范的钴采购。福特公司希望跟踪钴供应链，以确保公司在生产锂离子电池时不会使用劣质钴，并且承诺在进一步提高全球矿物供应链透明度的同时，支持人们的合法权利以及环保事业。

钴是制作锂离子电池的重要原材料。现如今，市场对于钴的需求量日益增长。摩根士丹利此前曾预测，到 2026 年，市场对钴的需求预计会增加到现在的八倍。因此，如何透明化、环保化采钴成了业界需要解决的问题。

福特公司主导的该项区块链项目旨在演示如何以负责任的态度在供应链中生产、交易和加工各种原材料。平台会记录钴矿石从华友钴业位于刚果的工业化矿场开采出来，然后运至 LG 化学位于韩国的阴极厂和电池厂进行熔炼，最终进入福特汽车工厂的整个过程。

此项目的平台以 IBM Blockchain Platform 为基础构建，采用 Linux 基金会的 Hyperledger Fabric 技术。IBM 表示该平台的设计可以负荷其他行业，并将继续开放该平台在其他行业的应用，例如航空航天、汽车、电子和国防工业等领域。

## （三）沃尔玛

2022 年 1 月 18 日，沃尔玛向美国专利及商标局提交七份申请，显示沃尔玛正在准备入局元宇宙，并计划生产和销售虚拟商品。值得注意的是，提交给美国专利及商标局的文件也显示，沃尔玛计划创建自己的加密货币和 NFT。

在美国商标电子搜索系统上，一份由沃尔玛提交于 2021 年 12 月 30 日的申请表示，其将提供金融服务，即通过全球计算机网络为会员提供加密货币。

对于沃尔玛将发行 NFT，目前官方消息十分有限。有观点认为沃尔玛推出 NFT 很有可能是为了迎合新生代消费群体的喜好。也有观点认为，NFT 等虚拟资产有可能成为未来元宇宙的主要支付手段，而支付对于零售业至关重要。提早布局对于沃尔玛来说有利无害。

2021 年底，沃尔玛首席财务官在财报会议上表示，如果客户需要，沃尔玛愿意并允许消费者使用加密货币付款。而外界普遍认为，沃尔玛作为合规的零售机构，会以合规的方式来接受加密货币付款，当中最大的可能性是推出稳定币。稳定币兼具了传统货币价值相对稳定的特点以及加密货币的去中心化、透明度，因此相较于传统数字货币更加具有抗风险的能力。沃尔玛希望开发与美元挂钩的稳定币，一方面为沃尔玛提高了消费者品牌忠诚度，另一方面扩大了其业务范围。

目前，沃尔玛正与专门从事比特币 ATM 的加密钱包和支付公司 Coinme 合作，设立 200 个 Coinstar 售货亭销售比特币。如今沃尔玛允许客户在美国的数十家商店购买比特币，对于区块链行业有一定的影响。2021 年 10 月开始，客户可以在沃尔玛大型商店内的 Coinstar 机器上购买比特币。沃尔玛通讯总监 Molly Blakeman 接受 CoinDesk 采访表示，美国各地的沃尔玛商店内有 200 个 Coinstar 售货亭，它们是此次沃尔玛试水市场的一个步骤。

#### （四）Meta（前身为 Facebook）

2022 年 1 月 27 日，有报道称，Meta 正在出售旗下稳定币项目 Diem，美联储会员银行 Silvergate Capital 将以 2 亿美元收购 Diem 与其技术资产。

Libra（后更名为 Diem）是 Facebook 提出的一种基于区块链的许可支付系统。2019 年 5 月，Facebook 确认布局加密货币，2019 年 6 月 18 日，该项目正式宣布名为 Libra。该计划在 2020 年发布，但只发布了基本的实验代码。

Silvergate Capital 实际上在 2021 年就已经与日渐式微的 Diem 达成战略合作，计划推出与美元挂钩的加密稳定币。2021 年 5 月，Meta 公司宣布将 Diem 主要业务从瑞士转移至美国。与此同时，Meta 还宣布与 Silvergate Bank 达成战略合作，后者将成为 Diem 美元稳定币的独家发行方，并将管理 Diem 美元储

备。

2021 年 12 月，Diem 项目创始人 David Marcus 离开了 Meta。2022 年 2 月 3 日，Facebook 更名 Meta 后的首份财报惨遭滑铁卢，Meta 公司股价暴跌 26%，市值蒸发 2000 多亿美元。

Meta 最新的季度财报显示，旗下 Facebook 社群应用软件每日活跃用户首次连续下跌，还有备受人们关注的 Reality Labs 部门，亏损更是达到 100 亿美元。虽然在净利润与利润率上都有着不错的增长，但用户数的下跌则让投资者认为 Meta 公司已经进入增长放缓的阶段，从而创下该公司 18 年来最大的单日下跌。

但 Meta 公司的创始人扎克伯格坚信，互联网的下一代就是元宇宙。虽然市场对此持怀疑的态度，但扎克伯格仍然砸下大笔资金建设元宇宙。Meta 去年在元宇宙建设方面的支出总额超过 100 亿美元。扎克伯格表示，希望在未来花更多的钱继续建设元宇宙，但元宇宙的投入近期都不会看到回报。由于短期变现能力较差，外加市场信心不强，种种原因都让 Meta 公司股价遭到了抛售。

#### （五）马士基（Maersk）

2021 年 5 月 10 日，由 IBM 和马士基联合发起的 TradeLens 项目在中国启动。该项目旨在通过区块链实现集装箱航运业的文书数字化，目前已有超过 10 家成员加入该网络。值得注意的是，就在 TradeLens 在中国开展业务的两个月前，总部位于香港的竞争对手 GSBN 也获得了在亚洲地区开展业务的监管批准。

TradeLens 合作项目主要使用 IBM 的区块链技术，为全球贸易参与者提供一个安全共享信息和数字化合作的平台。除了跟踪和分享储存在区块链上的信息，还能够将海运提单等贸易文件数字化。TradeLens 在 2018 年进行了首次试点，截至目前，已经跟踪了超过 4200 万个集装箱货运，并数字化了超过 2000 万个文件。

截止 2021 年，TradeLens 目前接入了超过 300 家单位，包括世界排名前五的国际海运企业中的三家（马士基、地中海航运、法国达飞）。2021 年 TradeLens 在中国开展业务后，已有厦门港、浙江港及多家物流供应商接入该网络。



TradeLens 与 GSBN 对港口与海运市场的瓜分趋于白热化。法国达飞曾是 GSBN 的发起人之一，但最后加入了 TradeLens。赫伯罗特（Hapag-Lloyd）最初是 TradeLens 的参与人，如今却是 GSBN 的主要持股方之一。有分析指出，由于国际海运业的高度关联性，如果在海运市场同时存在两个互不兼容的区块链平台，可能导致整体运营有效性的下降，与区块链信息技术为海运业赋能增效的目标背道而驰。例如，一家航运公司接入 TradeLens 网络，但目的港使用 GSBN 网络，目前这两个平台之间是否存在兼容的可能还有待观察。新加坡港口运营方 PSA 同时接入了 TradeLens 与 GSBN，但全球各主要港口的运营方似乎并没有同时接入两家网络的意图。

### 三、NFT——赋能文化艺术

2021 年第一季度，NFT 异常火爆，尤其是在数字艺术和收藏品领域，通证化的艺术品成为区块链应用中最受欢迎的项目，仅 2021 年 2 月 NFT 数字通证的销售额就是整个 2020 年的两倍。2021 年 3 月 11 日，由 Mike Winkelmann（又名 Beeple）创建的 JPG 文件在网络拍卖中以 6900 万美元的价格售出，这是佳士得拍卖行的第一笔纯数字拍卖，即无实物复制的拍卖。2021 年 4 月 5 日《CCTV 央视财经》节目中报道了 NFT 的相关内容，并表示 NFT 是数字资产真实性和所有权的可靠证明。

NFT 在我国也被称作“数字藏品”。2022 年两会期间，全国政协委员、北京大学中文系教授、著名文化学者张颐武在全国政协十三届五次会议中建议大力推进“区块链+”在文物文博领域的深度运用。张颐武表示，推进国家文化大数据的建设，需要区块链等通用技术支持文博领域数据资源的互联互通。我国“区块链+文物文博”领域已经有良好的基础，政策规定比较完备，技术标准和规范体系已经相较于其他国家更完善，算法自主创新能力逐年增强。目前，区块链在文物文博领域创新实践已经形成行业规模，比如国内的数字藏品已经成为激活传统文化、让文物活起来的重要载体。

#### （一）NFT 的基本概念和特点

##### 1. 什么是 NFT

NFT 全称 Non-fungible Token，被译作非同质化代币，即不可替代的通证。

NFT 技术应用起源于 2017 年，但在此之前，数字通证和加密货币已在艺术界有所应用。2014 年，Monegraph 平台在美国启动，借助该平台，原始创作者可以在区块链中注册艺术品。作者若想证明其对作品享有所有权，只需将其图像上传到 Monegraph，并在通过身份验证后即可获得一个唯一的智能代码——一串类似于版权认证的数字。不难看出，早在区块链发展的早期，已有了最早的数字所有权和资产通证化的尝试。

目前，公众更为了解的是同质化代币即 Fungible Token，大部分数字货币例如比特币、以太币等都是同质化代币。相同价值的两个同质化代币可以进行互换，也可以分割成多个价值更小的同质化代币。而非同质化代币则不同，其价值唯一，不可分割，不可交换。NFT 使用区块链进行验证，在区块链上生成对唯一数字对象的所有权信息，其诞生和流转都具备透明可追溯的历史记录。这些信息和记录在区块链上对所有人都可见，但不可编辑。区块链技术保证了从当前所有者到原始创建者的追踪可能性。区块链技术和智能合约的应用使得艺术品的买卖合同和真品验证实现了程序上的统一和简化。通过区块链上数字资产所有权的通证化，使得数字资产得到确权和保护。

举个简单的例子，假设您在网络上创作了一个 GIF 格式的表情包图片，该图片被广泛传播于整个互联网上，那么您如何证明自己是该图片的真正的所有权人？这就要用到 NFT，您只需要将该图片在区块链上添加数字证书标记，通过全网的数据账簿广播更新，所有节点都会获悉并记录您是这一图片的著作权人。简而言之，NFT 就是对数字产品进行标记上载并将其所有权实现确认和流转的过程。

## 2. NFT 如何交易？

NFT 交易主要在基于区块链技术的应用平台上进行，因此要购买 NFT 通常需要使用数字货币。目前 NFT 交易主要使用比特币和以太币作为支付手段。但也有加密艺术市场允许使用普通银行卡支付，如 Bitski 平台允许 NFT 创作者通过银行账户出售其商品，收藏者可以使用普通的银行卡付款购买。

## 3. NFT 有什么特点？

(1) 唯一性：区块链上的每一个 NFT 都有自己的独特标识。每个 NFT 都是唯一的，在同一条公链上不能同时被出售两次，其所有权只能属于一个账

户。

(2) 确权性：每个数字证书都记录在区块链中，因此很容易验证其所有权。NFT 基于区块链技术，因此同样具有去中心化，不可篡改和密码学加密的特性。当一件数字作品被加上标记，其创作信息，上链时间、原始创作者的信息等都会被永久记录在链且不可修改。每一次流转也都会被记录在区块链中，保证了收藏者的所有权真实有效，任何时候都可以验证权属。

(3) 真实性：区块链系统本身被认为是真实可靠的，因为每个后续区块中的记录都包含来自前一个块的哈希值，即已处理的数据，这也是整个系统以链的形式出现的原因。试图伪造其中一块的记录则会破坏该链，因为该块中的数据不再与存储在下一个块中的哈希值匹配。因此 NFT “唯一正品”的真实性依靠技术本身得以实现和保证。

(4) 开放性：开放性表现在 NFT 对数字对象的存在形式、定价和地域都没有限制。任何一张卡片，一张图片，一段音乐，一段影像都可以被 NFT 化。而数字对象的具体价值由创造者自由确定。由于数字对象的流转主要基于互联网，其不受传统地域限制。因此，对于 NFT 交易流转本身而言，其简化权利管理，降低交易成本和时间，具有一定的开放性。

## (二) 法律纬度下 NFT 的本质与挑战

NFT 的本质是被记录在分布式信息储存的区块链网络上数据记录，其包含关于某一数字对象独立资产所有权的所有信息，并在区块链上实现流转和验证所有权。公众可以将 NFT 附加到任何数字产品，例如图像、视频、音频等。

NFT 的创新之处在于实现了数字作品所有权的确权和流转记录，使得资产所有权通证化，其具有区块链技术本身去中心化的特点，不依赖于任何中心化机构的服务即可得到验证。

### 1. 代码为合同背书——NFT 与智能合约

NFT 的真实性和唯一性是基于区块链技术本身的特性和智能合约的应用所保证的，数字艺术品交易平台可以编写该平台的智能合约条款并在区块链中严格执行该合约（类似于纸质合同），但智能合约的成立和执行不同于一般合同的概念。按照我国《民法典》第四百六十四条规定，合同是民事主体之间设立、变更、终止民事法律关系的协议。合同是当事人协商一致的产物或意思表示一

致的协议，包括以下要素：第一，合同的成立必须要有两个以上的当事人。第二，各方当事人须互相作出意思表示。第三，各方意思表示是一致的，也就是说当事人在平等、自愿基础上达成一致的协议。而 NFT 所提前预设的智能合约是由代码形式确定的合同，当运行条件被触发时，则开始自动执行。相较于靠法律背书的传统合约，智能合约则依赖代码背书保证执行。在 NFT 交易中，人的主观意思表示只表现在加入智能合约之前，一旦开始执行便失去了意思表示的可能，合约的执行将会导致必然的权利义务关系变化。从这一角度而言，选择进行 NFT 交易，即意味交易双方对相应平台所制定的智能合约的认同和接受。

## 2. 数字作品确权与保护——NFT 与物权

对于收藏者（买家）而言，NFT 数字证书使得其获得了对特定数字作品独一无二的所有权权属认证，收藏者成为该特定数字作品原件的所有者，而其原始创作者可以像有形艺术品的创作者一样保留该数字作品的著作权和复制权。就像收集有体实物绘画作品一样，任何人都可以购买《戴珍珠耳环的少女》的复制品，但是原件所有权只归属于特定的收藏者。

从权利主体和客体的辩证关系来看，NFT 作为一种数字通证，是信息时代产生的物的特殊形式，其与一般物权客体有着相通的属性。但是，NFT 所转移的所有权存在一定的瑕疵。所有权属于物权，应具有排他的性质。所有权人有权排除他人对于其行使权力的干涉，并且同一物上只能存在一个所有权，而不能并存两个以上的所有权。但是，在目前的 NFT 应用领域，尚不能保证任一数字作品的绝对排他性。作为数字作品的原创者，若将同一个作品上传到不同的公链上，数字作品的排他性便很难得到保证。

对于数字作品本身而言，NFT 的出现使得每一个网络域名，每一个网络图片或视频，甚至每一条网络上的留言都有了被保护的可能，数字作品的确权真正得以在技术的支持下实现。虽然 NFT 目前由于技术发展限制，持有人尚且不具备对 NFT 完全的排他性支配管理，但是物权保护依旧是最符合其权利内容的法律保护类型，其未来仍有被明确认定为网络虚拟财产的可能，进而获得更多法律保护空间。

## 3. 数字版权的新时代——NFT 与知识产权

NFT 的所有权转让不会导致数字作品的著作权的转让。创作者可以上传作品的多个版本，每个版本都有自己的 NFT。本质上而言，NFT 是原始作品的数字副本，并且原始创作者可以控制其作品的许可方式，可以在交易中自行决定数字作品转移所有权的同时是否转移著作权。

目前，关于 NFT 的知识产权内容主要由交易双方自行约定或数字作品交易平台的服务条款进行规范。从法律上来看，NFT 是数字作品本身数字通证的所有权，而不是基础产品的所有权，数字作品的著作权和部分财产权仍归作品的原始创作者所有。由于 NFT 是一个新兴领域，因此购买此类数字通证所获得的知识产权内容和种类尚待明确，同时相关权利被侵犯后如何认定权利人的损失或者侵权人获得的利益也是值得思考的问题。

除此之外，NFT 还革新了传统意义上的版税制度。版税又称版权使用费，是知识产权的原创者或版权持有人对其他使用其知识产权的人所收取的金钱利益。NFT 在创作之初，可由原作者设置版税标准，目前，国外加密艺术市场通行的标准是 10%，这意味着 NFT 数字作品在之后的二次和多次流转中，每一次交易其原作者都能得到交易额 10% 的版税或按初始约定结算的版税。具体版税约定都在数字作品买卖合同的要约发起之前通过智能合约的方式加以确定，无需再和任何中介机构商讨服务费用。版税已在智能合约中明确，并在执行智能合约后自动转到创作者的加密钱包。

#### 4. 没有绝对的安全——NFT 盗版与盗窃

NFT 为内容创作者提供了新兴的盈利方式，但是与此同时，出现了新的版权侵权形式。因此，目前尚不完全清楚 NFT 如何确切地适用于现有的知识产权保护。此外，还要考虑数字内容本身的风险，例如无法保证数字作品的质量不会降低、文件格式不会过时、网站或平台不会消失以及钱包密码不会失窃。

对于销售者是否是原始创作者，NFT 加密艺术平台无法保证交易标的的合法所有权，即任何人都有可能将他人的作品 NFT 化并出售。目前少数较为领先的数字艺术交易平台会对作者身份进行验证，尽可能避免盗版情况出现。

除了盗版，NFT 还面临着大部分数字平台都无法完全规避的黑客风险。前不久在交易平台 Nifty Gateway 上就出现了多起盗窃事件。黑客在掌握了账户密钥后在钱包持有人不知情的情况下盗走 NFT，并购买了新的 NFT 并再次进行转

移。但作为平台运营方，Nifty Gateway 仅提示，用户应该遵循安全预防措施，包括启用 2FA 安全密码验证方式并且永远不要重复使用密码。

因此，目前来看，NFT 还没有被任何监管机构所监管，交易平台管理难以统一，原创者和收藏者的权益都很难获得法律意义上的保护。随着 NFT 市场的不断发展以及与更多产业的不断结合，数字资产将如何适应现有的监管框架、NFT 发行者和购买者之间的交易行为会产生哪些权利义务关系、如何界定 NFT 的法律地位从而明确对其获利行为征税、如何规避 NFT 交易可能存在的洗钱风险，即何种主体来承担识别用户并向监管机构报告大型可疑交易的义务等都是接下来各国都不可避免所亟待解决的法律问题。

### （三）数字藏品——国内 NFT 探索与尝试

在国内 NFT 被称作“数字藏品”，两者本质的技术属性是一样的。但是在当前环境下，数字藏品主要发行于各联盟链支持的区块链平台之上。数字藏品在区块链技术支持下保证了 IP 数字版权唯一性及真实性，很大程度上解决了实体手办或藏品山寨泛滥却又难以追溯的问题，对 IP 开发与转化有独特的价值。相较于国外的 NFT，数字藏品弱化了二次交易的属性，主要强调持有者的收藏、欣赏、使用、无偿转让等行为。以此来明确对版权的保护，迎合监管的趋势。

#### 1. 数字藏品的底层技术

从底层技术方面来讲，数字藏品主要采用是联盟链技术。联盟链只针对特定某个群体的成员和有限的第三方，内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程，其他第三方可以通过该区块链开放的 API 进行限定查询。由于联盟链相较于公链具备一定的准入机制，可以使交易性更容易提高，该技术在协助监管、储存和能源消耗等方面都具有一定的优势。

#### 2. 数字藏品的衍生功能

从衍生功能方面来讲，目前，各大平台仍持谨慎态度，尚未对用户开放更多衍生功能。通常购买 NFT 作品之后，所有权就属于用户。用户可以对这个 NFT 进行商业活动诸如，可以印刷在衣服，或者任何一个环境。而购买数字藏品，几乎没有任何商业活动的使用权，没有版权就意味着滥用就会被追究法律

责任。因此，目前用户在购买数字藏品时应仔细阅读和遵守相应的平台规则与用户协议。

### 3. 数字藏品的内容制作

从内容制作方面来讲，主要参与者包括数字藏品发行平台以及内容发行方。内容发行方依托数字藏品业务将 IP 的收藏价值转化为收益，也进一步扩大 IP 的市场认知度和影响力。而就数字藏品发行平台而言，目前我国主要的数字藏品发行平台包括三种，第一种是以头部互联网公司运营为主的各大平台，其已在互联网领域拥有一定的技术优势、内容生态、平台流量。第二种是新生元宇宙公司，其以开发区块链应用为公司发展方向，构建各类区块链应用、游戏及社交内容等。第三种是其他平台，其并非自身开发区块链技术，缺乏持久的技术保障，各类基础设施均不完善、存在各类潜在风险的平台。

为方便读者更好地了解国内数字藏品领域的现状，我们对目前我国主要互联网公司旗下数字藏品平台简要梳理如下：

- 鲸探，支付宝旗下平台，所用底层技术为蚂蚁链；
- 幻核，腾讯旗下平台，所用的底层技术是腾讯的至信链；
- 灵稀数字藏品，京东旗下平台，所用底层技术为京东智臻链；
- 网易星球数字藏品平台，网易旗下平台，所用技术为网易区块链；
- 百度数字藏品平台，百度旗下平台，所用技术为百度超级链；
- 哔哩哔哩数字藏品，B 站旗下数字藏品尝试，所用技术为 B 站高能链；

2021 年 12 月 24 日，新华社发文宣布将发行 2021 年新闻摄影报道的数字藏品，官方媒体的 NFT 尝试也预示着 NFT 在境内与虚拟货币截然不同的发展道路。NFT 的火热更新着公众对区块链技术应用的认知，NFT 所代表的数字资产化和资产所有权通证化的概念也将会与更广泛的产业领域相结合，在更多的项目中得以运用。对于任何具备唯一性的物的流转或是特定的身份确认均可以进行 NFT 化登记和验证。

在我国，随着区块链技术的不断完善以及数字人民币的研发和应用，NFT 未来在资产上链、确权等场景具有广阔的探索前景。在知识产权领域，可以利用 NFT 明确所有权，进行版权登记，专利识别；在金融领域，可以用来实现更多数字资产的应用，促进数字市场诞生更多种类的金融衍生品来满足公众在数

字经济条件下的需求。而在监管层面，则可以探索建立监管沙盒机制，对 NFT 制定统一的技术标准，利用区块链技术交易透明、不可篡改的特点，通过智能合约对 NFT 的交易进行合规检查、原创认证等。同时，NFT 如果被利用作为代币，其仍然有被利用进行代币发行从而进行非法融资的隐患，NFT 参与者应对此保持警惕。

#### 四、生成型电子文书平台——可信的“意思表示”

传统的纸质文书签名或盖章（赴现场或快递）费时费力费钱，纸质文书的收发存在寻址难、时效差、费用高、送达难等问题，由此，普通的电子文书应运而生。但是电子邮件、微信难以认证收发双方身份、无法固化内容证据、无法实现司法送达，私有化部署的电子签名系统只能实现平台与其用户的单向签名，无法实现社会主体之间的双向签署和文书收发，更无法自证清白。

基于生成型电子文书平台则可以高效解决上述所有问题。自然人通过“姓名+公民有效身份证号+面部信息识别认证+录入设备指纹”完成注册确认；法人通过“账号绑定统一社会信用代码+法定代表人刷脸认证+绑定操作员/法定代表人设备指纹”完成主体确认；在签署时通过“帐户+手机号码+手机设备+私钥+PIN 码”完成签署人身份确认。以上环节表明产品具备识别功能，可以准确识别签署人。

	普通电子合同平台	生成型电子文书平台
功能模式	电子合同签署（不支持个体工商户及非企业机构）	基于数字社会体系的电子文书签发、送达、流转、验真；会议签署
合法性	不符合《电子签名法》，实人注册≠实人登录，实人登录≠实人操作；私钥托管在平台+手机验证码调用私钥，不能确保电子签名制作数据仅由签名人控制	符合《电子签名法》，分散式私钥绑定用户手机设备并由 PIN 码调用；基于区块链的新型电子文书平台无法参与 PIN 码验证过程、无法参与私钥签名值合成过程；确保签名制作数据仅由签名人控制
	不符合《网络安全法》，对身份证号码及手机号码等用户隐私数据，无脱敏处理机制	符合《网络安全法》，脱敏处理用户身份证号码等隐私数据
自证清白	不能，司法不采信	能，司法采信



验真方式	非即时验真（电子文件验签）， 不便捷	即时验真（扫码/输码原文比对，或移动端 点击“签章”）； 非即时验真（电子文件验签、HASH 校 验）
	私有化部署为主，SaaS 未推广 开	SaaS

表 3-1 普通电子合同平台与生成性电子文书平台对比

本节内容以“签达通”（注，原为“弹址”，下同）生成型电子文书平台为例对其平台生成的电子签名及形成的电子证据效力做简要法律分析和探讨。签达通电子文书移动签署与实人收发平台采用分散式密钥智能终端移动签名技术，具有即时性、去地域性和安全性的特点。签达通与工信部认可的第三方电子认证服务机构合作，为通过实人认证后的互联网自然人或机构申请数字证书，用户通过签达通完成实人认证并使用数字证书获得电子签名服务。其运作中主要包含以下几个法律确认环节：

1. 签发主体确认：签达通采取以下方式实现对从事民事法律行为不同主体的确认：自然人通过“姓名+公民有效身份证号+面部信息识别认证+绑定手机号及手机设备指纹”完成注册确认；机构通过“账号绑定统一社会信用代码+法定代表人刷脸认证+绑定操作员/法定代表人的手机设备指纹”或“打款”银行账号核验比对等方式完成主体确认；在签署时通过“帐户+手机号码+手机设备+私钥+PIN 码”完成签署人身份确认。以上环节表明产品具备高可靠的智能识别功能，可以准确识别签署人身份及其意愿。电子签名必须与签发主体之间通过字符及编码建立可靠的联系，才能实现电子文书（包括合同）的法律效果由签发主体承担的功能。

2. 签发行为确认：签达通电子文书（包括合同）签约行为确认采取先通过“操作人员/法定代表人验证码登录+设备指纹验证+手机 TEE/SE 信息核验”进行登录确认，再通过“设备指纹验证+签名时输入 PIN 码”对具体操作的签署行为进行确认。该确认环节表明产品具备表达意向功能，可以充分表达签发方的签署意向。在签发合约时，双方在签达通云平台上进行签署确认。

3. 签发后的存证确认：签达通平台生成的电子文书在签署后可通过即时验真（扫码/输码原文比对,或移动端点击“签章”）、非即时验真（电子文件验签、

HASH 校验) 两种方式进行核验。该确认环节表明产品具备高可靠的电子证据功能, 需要证明在签发后证明电子文书的真实存在。平台对签发全流程进行实时记录与留痕存证。

### (一) 生成型电子文书平台上电子签名服务的合规性

#### 1. 关于电子认证服务提供主体的资质

我国《电子签名法》第 16 条至 26 条对电子认证服务机构作出了详细规定, 要求电子签名需要第三方认证的, 由依法设立的电子认证服务提供者提供认证服务。工业和信息化部颁布的《电子认证服务管理办法》规定, “在中华人民共和国境内设立电子认证服务机构为电子签名提供电子认证服务。向社会公众提供服务的电子认证服务机构应当依法设立。”在我国, 电子认证服务提供者即 CA 机构, 此类机构有权制作国家认可的数字证书, 其负责签发证书、认证证书、管理已颁发证书的机关。通过验证、识别用户身份, 并对用户证书进行签名, 以确保证书持有者的身份和公钥的拥有权。签达通采用符合《电子认证服务管理办法》的中国金融认证中心(CFCA)的数字证书服务, 符合《电子签名法》的要求, 同时体现出该平台的第三方中立和专业的特点。

#### 2. 关于生成的电子签名性质

就电子签名本身而言, 我国《电子签名法》第 2 条, “电子签名”是指数据电文中以电子形式所含、所附, 用于识别签名人身份并表明签名人认可其中内容的数据。其中“数据电文”则指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。签达通所形成的电子签名属于上述范畴。

#### 3. 关于数据信息采集的合规情况

依照 2021 年 9 月 1 日即将施行的《数据安全法》第三十二条的规定, 任何组织、个人收集数据, 应当采取合法、正当的方式, 不得窃取或者以其他非法方式获取数据。签达通在收集用户个人数据和生理特征信息时, 均在用户知情且许可的情形下进行, 符合《数据安全法》对数据信息采集的总体要求。

签达通所采用电子签名在技术表现上依赖数字签名和生理特征签名从而保证民事法律主体在网络空间的身份识别。除了传统的身份信息手机号验证, 还辅以人脸识别、声音识别等生物信息核验, 具备更强的识别性。电子签名在记录阶段完成之后, 需要对形成的信息进行整体可信存储。签达通电子签名文书

利用有序的链式数据结构存储数据，利用加密算法更新数据，利用哈希值加密等密码学技术保障数据安全，使得存证信息具备更强的法律效力。就电子签名本身而言，签达通提供的电子签名服务符合我国《电子签名法》的规定。

## （二）生成型电子文书平台上生成签名的法律效力

根据《电子签名法》第 14 条，可靠的电子签名与手写签名或者盖章具有同等的法律效力。电子签名本质上是与数据电文相关联的电子数据，并依靠这些电子数据产生对签名人身份的确认作用，在我国只有被认定为“可靠的”电子签名时，该电子签名或盖章才能够产生与手写签名同等的法律效力。《电子签名法》对于可靠电子签名应具备的条件作出了规定，依据该法第 13 条的规定：

“（1）用于电子签名的制作数据，属于电子签名人专有；（2）电子签名的制作数据在进行签署时，仅由电子签名人控制；（3）签署后对电子签名的任何改动能够被发现；（4）签署后对数据电文内容和形式的任何改动能够被发现。当事人也可以选择使用符合其约定的可靠条件的电子签名”。从以上规定可知，能够产生法律效力的电子签名必须由签名人专有或控制，并包含于完整的数据电文当中，否则将无法识别签名人的身份，即无法起到认定缔约意思表示是缔约人所签发的归属作用。结合该法律要求和技术特点进行考量，签达通提供的电子签名服务符合《电子签名法》对电子签名可靠性的程度要求。因为其提供的法律服务符合以下三个条件：

第一，签名人即为签名行为发出者本人。签达通通过生物信息和数字信息的实人认证确保签名人即为本人，其对自己所做出的民事法律行为负责；

第二，电子签名具有不可伪造性，即除签名人以外的任何人都无法伪造该签名。签达通私钥绑定用户信息及其手机设备指纹等，无法被导出和复制到其他环境使用，并且分散式私钥部分绑定用户手机号、手机设备指纹及 TEE/SE 信息+PIN 码保护机制；

第三，围绕电子签名的真伪发生了争执，能够通过技术准确验证真伪。签达通每一次签收均会留有送达回证，利用密码学技术实现全程存证。区块链上存储的是用共识算法计算出的数据信息的哈希值，是数据摘要而非数据信息本身。哈希值具有唯一性与可识别性，一旦发生争议，可以将链下保存的电子数据计算出的哈希值与链上存储的哈希值做对比，以验证电子数据是否被篡改。

若哈希值一致，则证明电子数据没有被篡改，反之则被篡改。通过区块链技术本身的特性，可以实现该产品的实时验证防止篡改。

### （三）生成型电子文书平台上生成合同形式的法律效力

从合同形式合规角度而言，《民法典》第 469 条明确了电子合同是书面合同的一种形式：“当事人订立合同，可以采用书面形式、口头形式或者其他形式。书面形式是合同书、信件、电报、电传、传真等可以有形地表现所载内容的形式。以电子数据交换、电子邮件等方式能够有形地表现所载内容，并可以随时调取查用的数据电文，视为书面形式”。《电子签名法》第 3 条明确合同约定采用数据电文形式，不得仅因采用数据电文形式而否定其法律效力。因此，通过签达通平台生成的电子合同是法律认可的合同的书面形式。

从合同效力角度而言，当事人约定采用电子合同形式时，其法律效力不得因采用电子合同形式而被否定。电子合同的效力认定应当符合我国《民法典》、《电子签名法》、《电子商务法》等相关法律制度的基本原则和要件。

此外，关于电子合同的成立时间和地点法律亦有明确规定。《民法典》第 491 条，“当事人采用信件、数据电文等形式订立合同要求签订确认书的，签订确认书时合同成立”以及《民法典》第 492 条，“承诺生效的地点为合同成立的地点。采用数据电文形式订立合同的，收件人的主营业地为合同成立的地点；没有主营业地的，其住所地为合同成立的地点。当事人另有约定的，按照其约定。”根据以上规定，基于签达通电子文书收发平台缔约各方所订立的电子合同，除合同文本另有约定之外，合同自成立时生效，收件人的主营业地默认为合同成立的地点。

### （四）生成型电子文书平台上生成电子证据的证明效力

首先，电子证据是我国民事诉讼法规定的法定证据类型。我国《民事诉讼法》第 63 条规定，依据我国相关法律的规定，民事诉讼证据的类型包括当事人的陈述、书证、物证、视听资料、电子数据、证人证言等。《最高人民法院关于民事诉讼证据的若干规定》第 14 条对此进一步细化，明确电子数据包括下列信息、电子文件：

（一）网页、博客、微博客等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信

信息；

(三) 用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；

(四) 文档、图片、音频、视频、数字证书、计算机程序等电子文件；

(五) 其他以数字化形式存储、处理、传输的能够证明案件事实的信息。

基于区块链技术存证的电子数据，只是从存证方式上革新了电子证据的类型，并非一种新的证据种类。《最高人民法院关于互联网法院审理案件若干问题的规定》第 11 条第 2 款指出，“当事人提交的电子证据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。” 签达通所创建和使用的各类电子数据信息属于上述范畴，属于我国法律规定的法定证据类型。

其次，符合法律要求的电子证据才具有强有力的法律效力。证据要得到法院的支持，要满足证据的合法性、真实性以及与待证事实的关联性。而电子证据属于法定证据的一种，其证明力也需要满足以上特点。在司法实务中，法院对电子证据的采纳一向持谨慎态度，因为电子证据存在很高的篡改可能性。电子证据在生成、收集和存储等环节容易侵犯他人合法权益而导致不合法，进而被法院排除。

### 1. 真实性

电子证据的真实性是指证据本身形成过程是客观真实的，不是出具证据的一方有意伪造的，同时其中的内容是能客观反映待证事实的。排除人的主观因素的判断程度越高，证据的客观性也就越强。在考察证据特点时需要考虑电子证据载体的真实性、电子数据的真实性和电子证据内容的真实性。杭州互联网法院有关《民事诉讼电子数据证据司法审查细则（试行）》提到，应着重审核第三方数据服务提供商的电子数据来源的真实性、技术手段的安全性，审查电子数据形成的合法性以及形成、传输、接受、存储、提取的过程及方法的可靠性、电子数据的完整性、保持完整性方法的可靠性，审查电子数据与其他证据相互印证的程度，并由此认定证据的效力。电子证据的真实性着重要依靠技术本身来证明。

签达通平台所采用的区块链和哈希值存证技术可以基本实现对电子证据的自我验真。每一张文书的签署均被权威时间源加盖时间戳，过程不可逆，篡改会留痕，这一技术特征使其本身可对交易过程进行客观、准确地描述，从而实现自我验真。在以区块链为基础的电子文书平台运行中，入链保存的数据从元数据到所有的交易信息都可以被查验，基本保证电子数据的真实性。

而载体的真实性是电子证据真实性的一个重要审查方面，包括载体来源的真实性与载体在诉讼流转中的真实性。与现有电子证据存证平台相比，签达通生成的电子文书具有传统电子证据所不具备的优势。在传统电子证据收集模式下，传统电子证据的载体来源于提交该证据的当事人，并且由当事人将电子数据向区块链存证系统上传，载体来源依然是当事人，所以仍然无法确保此种情形下电子证据载体来源的客观性。如果有关人员在收集时有存在个人倾向性，选择性地收集，那么便会造成收集到的证据带有一定主观性，可能会影响到事实认定。但是在签达通系统中，数据是由系统自动收集，而且操作过程是经过当事人数字签名，确保收集证据行为和电子数据的真实性，并且平台的收集操作处于其他节点的监督下，不存在人为选择性收集。此外，区块链技术用于存证使得电子证据在诉讼流转方面发挥优势。通过签达通电子文书平台生成的电子文书，其数据在区块链上生成、存储，电子数据从生成到验证均在平台之上，由一系列加密技术与来保障电子数据的完整与安全。对于该电子数据形成的记录作为证据，法院可以通过验证当事人提交的数据包与平台的哈希值进行比对，比对一致即可验证提供的数据是否真实，由此降低了电子数据收集、保全与验证的难度与成本，提高司法证明效率。

因此，可以通过技术验证，签达通作为电子证据具有一定的客观真实性，并且能够更客观完整地呈现电子证据的数据样态。

## 2. 合法性

合法性是证据必备形式，只有在合法性的前提下，才会再去审查证据的真实性和关联性。证据合法性在民事诉讼法中的具体表现如下：证据如要作为定案的依据，要求它具有合法的来源和形式，即证据的收集的主体和过程都要合法。前文已作叙述，签达通平台具备法律规定的相应资质，而区块链技术实现了电子数据生成时的环境清洁，使用密码学保证传输和访问安全。除了主体合

规，签达通平台的证据在生成和存证过程也具备合规性，在登录和使用时，进行多种方式的实人身份认证，符合《网络安全法》的强制要求，有效确保了数据存证的签名主体问题。

此处提示，关于电子证据内容的合法性，应注意以下内容的电子文书不适用电子签名，包括：

- (1) 涉及婚姻、收养、继承等人身关系的；
- (2) 涉及停止供水、供热、供气等公用事业服务的；
- (3) 法律、行政法规规定的不适用电子文书的其他情形。

### 3. 关联性

考察电子证据的关联性包括电子数据的信息与待证事实之间的关联性，电子数据的信息载体同诉讼参与人之间的关联性。在司法实务中，法院在决定是否采纳电子存证时，需要了解该产品的技术层面是否可篡改、时间源的取得、是否可自我验证等。同时不可仅仅凭借的电子存证就认定待证事实，电子存证只是电子数据的真实记载，并不能完整证明电子数据在案件中关系，待证事实需要集合其他线索和证据综合认定。签达通电子文书平台属于利用区块链技术的生成性电子证据。相比于传统存证型电子证据，由于存在人为主观性，技术本身并不增强电子证据的关联性；而对于生成型电子证据，由于全程留痕，可靠性更强，也使得证据的关联性更确定。

电子数据的信息载体同诉讼参与人之间的关联性则侧重考量以下两方面：

(1) 身份关联。这实际上证明当事人就是虚拟平台中以某个特定身份行事之人。在第三方存证平台中电子数据是否具有关联性，不仅需要看电子数据的信息所反映出的内容是否证明了待证事实，而且还要确定产生电子数据的账号的现实操作人。签达通电子文书平台通过生物信息和数字信息的多重验证解决了主体认证的问题,通过实人认证的方式保证点击屏幕或操作客户端的主体即是从事相关民事法律行为的对应主体。

(2) 来源关联。电子数据是被储存在网络平台的服务器上，考察电子数据是否具备关联性，必须证明电子数据的来源存储介质是否与当事人具有联系。签达通电子文书平台可依照司法需要出具认证，提供在线合同的来源网址及保存时间，并且可以通过技术自身的特性保证该认证书是自动生成不可篡改，只

要该时间内当事人登录过来源网址，那么便可将该在线合同和当事人关联起来。因此，可以认为签达通电子文书平台使得电子证据的关联性得到加强。

《杭州互联网法院电子证据平台规范》要求提交至证据平台的电子数据应：（一）能够有效表现所载内容；（二）电子数据的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容。广州互联网法院《关于电子数据存储和使用的若干规定》要求传输至证据平台的电子数据应：（一）与原始数据具有唯一对应当性；（二）能够有效表现所载内容。根据证据法基本原理，越是原始的、接近来源的证据，其所表达的信息越准确，这也是原始证据与传来证据在证明力上被区别对待的法律理论基础。签达通电子文书平台属于生成型电子证据，其合同相关数据在区块链系统生成并存储，其后发生的所有行为均被记录在链上，由权威时间源确保时间可信问题，形成一个完整的交易周期，能够有效表现所载内容。从区块链系统所调取的该电子数据即是原始证据，是产生于虚拟空间的原始记录。该类证据具有自我验真属性，可被推定为真实，除非有优势证据可以反驳。因此，签达通电子文书的生成型电子证据基本符合目前我国互联网法院对电子证据的有关规范。

## （五）生成型电子文书平台运营和后续发展中应注意规避的风险

### 1. 防范算力不足等技术风险

电子数据的本质是二进制序列，是一组代码的组合，所以其存储的载体对电子数据的影响很大。一旦在保存过程中出现一些不良操作或物理损坏，都会对电子数据真实性造成明显影响。在区块链中，工作量证明由工作量证明函数、区块大小及难度值决定。随着签达通平台的推广，用户的增多，签署行为的增加，需要考虑算力和存储的问题。区块大小便是指需要存储数据的大小，在基于区块链的存证系统中如果所保存的电子数据过大，那么便会导致工作量证明计算难度极高，会极大消耗节点算法，存证的效率也会降低，就算存储上链，也会占据大量的存储空间。所以，应注意伴随该产品发展所产生的技术保障问题。

### 2. 注重数据隐私保护

签达通电子文书平台目前已取得公安部信息安全第三等级保护认证，对用



户隐私数据进行脱敏保护处理，具有有效的数据安全隐私保护机制。但依然要对数据隐私问题保持审慎的态度，应该把保护个人信息安全和隐私信息的处理准确性作为基础义务，避免侵犯隐私权的情形出现。根据《中华人民共和国网络安全法》第四十一条，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。参照全国信息安全标准化技术委员会组织制定的国家标准 GB/T 35273-2020《信息安全技术个人信息安全规范》产品在识别、处理、检测等合同全周期加强个人信息保护，在收集个人信息时应尤其注意以下几点：

(1) 收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；

(2) 收集个人敏感信息前，应征得个人信息主体的明示同意，并确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

(3) 收集个人生物识别信息<sup>①</sup>前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；

(4) 收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；

除此之外，平台在提取、固定、加密、存储电子数据环节都有可能侵犯到个人隐私。如果在第三方电子数据保全过程中，侵犯了当事人或第三人的隐私权，那么所保全的电子数据的合法性就会受到质疑。侵犯他人合法权益或违反法律禁止规定取得的证据，不能被法律承认。在区块链中，每个节点的信息查看权限不同，所以在用户使用签达通系统时，应当在首页明显位置提供信息查看选项，可由用户自行设置数据将被哪些节点查看，同时提示如果涉及个人隐私，务必谨慎设置和使用。

### 3. 妥善履行数据安全保护义务

2021 年 6 月 11 日，《中华人民共和国数据安全法》出台，同年 9 月 1 日生

<sup>①</sup>注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

效。随着《数据安全法》的实施以及即将颁布的《个人信息保护法》以及其他与数据安全相关的法律法规和标准的出台，签达通作为基于数据信息运营的企业，面临更高的合规要求。建议紧密关注数据合规立法动态、配套法规、标准，加强合规意识，完善合规工作布局。提请特别注意。根据《数据安全法》的规定，经营者的数据安全保护义务主要包括以下几点：

- (1) 经营者应建立健全全流程数据的安全管理制度；
- (2) 经营者应组织开展数据安全教育培训；
- (3) 采取相应的技术措施和其他必要措施，保障数据安全；
- (4) 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；
- (5) 发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告；
- (6) 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任；按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告；
- (7) 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

按照上述规定，签达通电子收发平台作为开展数据处理活动的经营者，应开展数据安全教育培训，建立数据风险评估制度，加强风险监测。必要时，建议聘请律师事务所或其他第三方机构，协助进行合规培训和数据风险检测，编制风险评估报告。

#### 4. 完善证据传送链条

最高人民法院于 2018 年 9 月发布了《最高人民法院关于互联网法院审理案件若干问题的规定》，第 11 条对区块链技术作为电子存证手段进行了法律确认。区块链技术因其自身特性而与司法需求相契合，被日益广泛地应用于确权与存证领域，也更加突显了电子证据的独立价值。第三方平台的电子数据如果要在法庭上作为证据使用，就必须把电子数据从存证平台移送到法庭。目前，该行为主要是通过申请法院直接登录存证平台来实现。而法院须对电子存证平台进行可靠性审查，一旦法院认为平台的技术手段不可信或不具备中立性，那

么所保存电子数据也将不被认可。基于区块链的存证系统因其技术的可靠性可以规避上述风险，电子数据一旦被存储进系统，存证平台、公证机构、司法鉴定机构、电子数据认证机构、法院便组成了一条完整的证据移送链条，每个节点在清洁的计算机环境下安全地交换数据。

所以，为了提高生平台上生成的电子文书作为电子证据的认可度，平台应与司法机构加强合作，特别是公证处、仲裁机构和互联网法院等，推广实行同步存证。一旦发生合同纠纷，平台可发挥优势，提供完整证据材料，并为用户在公证机构出具公证书，委托司法机构出具司法鉴定等。公证处可以实时见证完整行为发生过程，并获取电子数据进行固化，与此同时对电子合同缔约主体、电子意识表示进行验证，并最后出具公证处盖章的电子证据保全报告，实现高效存证。

## 第四章 瞻望

### 合规与监管

《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标建议》明确要求，“建设现代中央银行制度，完善货币供应调控机制，稳妥推进数字货币研发，健全市场化利率形成和传导机制”。2021年7月，《中国数字人民币的研发进展白皮书》提出，应根据国内试点与国际社会需要，在依法合规的要求下建立数字货币体系及监管合作机制。

放眼全球，2021年各国继续加速试水央行数字货币，逾五十多国央行在2020年末前就开始布局从事央行数字货币研发工作。一方面，Facebook发布的Libra稳定币的研发推进将对法币形成挤压甚至替代，威胁他国央行货币和汇率政策的主导权；另一方面，数字金融的发展能够打破数据孤岛，实现金融服务的降本增效，既可基于账户转移，也可基于价值转移，对传统现有账户体系形成有效补充，在经济下行压力增大的后疫情时代对降本增效具有重大意义。

#### 一、央行数字货币——建设数字经济底座

央行数字货币（Central Bank Digital Currency, CBDC）是一国中央银行发行和支持的电子化法定货币。由于加密货币的流行削弱了央行对货币流通的管控力，各国央行发行数字货币的意愿愈发强烈。2021年，共计占全球GDP超过90%的80余国正在探索试点央行数字货币。

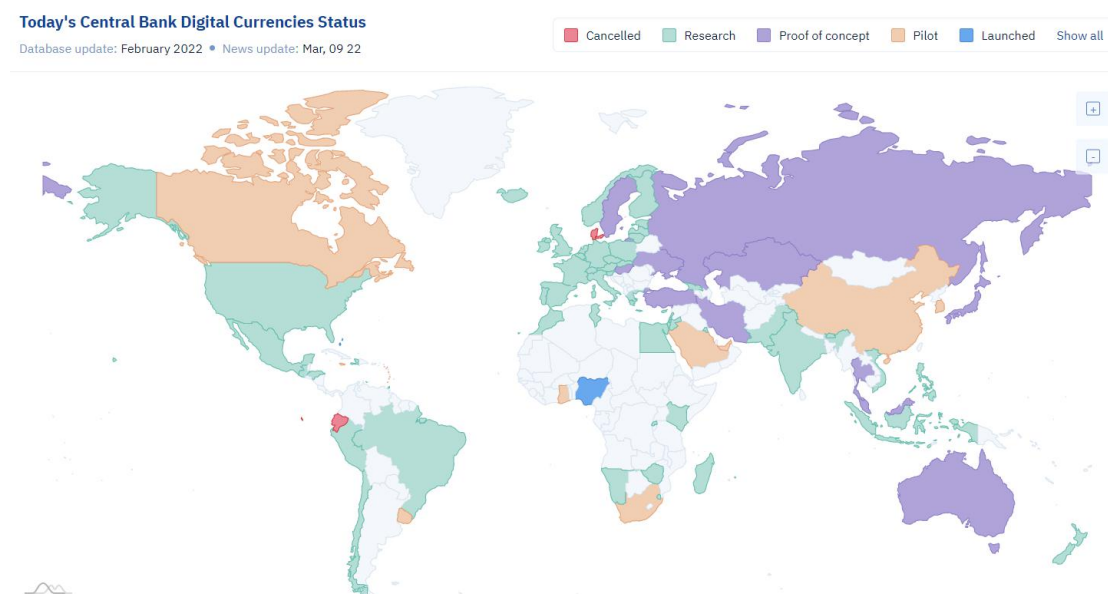


图 5-1 全球各国 CBDC 研发进度一览

2021年3月，东加勒比中央银行启动发行央行数字货币 DCash，覆盖圣基茨和尼维斯、安提瓜和巴布达、格林纳达及圣卢西亚四国，成为全球首个发行 CBDC 的货币联盟中央银行。未来，CBDC 有望持续促进支付结算融合、推进地区金融一体化。

### （一）央行数字货币发展概况

#### 1. 中国

中国人民银行数字货币计划从 2014 年成立研究小组到现在已七载有余，前期经历了漫长的理论初探、框架建立和研发设计流程。2019 年 6 月，Libra 白皮书发布后，数字人民币的发展进入快车道，目前已经在国内多个主要城市和重点场景进行了封闭测试。

中国人民银行法定数字货币体系的核心要素是“基于云计算的可信服务管理”，包括“一币、两库、三中心”。“一币”指数字人民币，为央行担保并签名发行的代表具体金额的加密数字串；“两库”指央行的发行库和商业银行的银行库；“三中心”包括登记中心、认证中心和大数据分析中心。其中，中国人民银行处于发行的中心地位，以双层模式投放数字人民币：第一层为央行向各商业银行投放，第二层为商业银行向社会公众兑换，该模式与传统纸币投放路径保持一致。由此可见，数字人民币不会对现有的移动支付方式产生冲击，可以有效拉近普通民众与数字化金融服务的距离，有望在较小的替换成本下实现成为主流通货和新金融基础设施的战略目标。

数字人民币是我国数字金融发展的核心要素，影响范围覆盖了金融与非金融主体。数字人民币创造出新的支付逻辑，将为商业银行、第三方支付机构、清算机构带来新的合作模式与市场博弈，也将为相关的技术和解决方案供应商带来新的商业机会。参与主体之间的协同合作与良性竞争将催化数字人民币交易的生态体系，为实体经济层面的企业与社会公众提供更具针对性、有效性的数字金融服务与产品支持。

2021 年 11 月 3 日，在香港科技金融周有关央行数字货币的圆桌论坛中，中国人民银行数字货币研究所所长穆长春介绍了目前中国数字人民币应用的最新进展。截至 2021 年 10 月 22 日，数字人民币累计交易金额达到 620 亿元，已

开立数字人民币个人钱包 1.4 亿个，对公钱包 1000 万个。另外，已经有超过 155 万个商家支持数字人民币钱包支付，累计交易笔数 1.5 亿余笔，涉及公用事业、餐饮服务、交通、零售及政府服务等多个领域。

但同时也应注意到，当前，我国数字人民币的监管机制仍在完善过程中，包括支付体系在内的数字人民币使用场景的规则体系等。在未来，中国人民银行仍将不断推进数字人民币的研发与应用工作，并将数字人民币对接我国金融监管框架。

## 2. 美国

2020 年 8 月，美国联邦储备委员会（以下简称“美联储”）公布了“Foo Wire”试验的一些发现，该试验使用 Hyperledger Fabric blockchain 软件开发。央行的研究人员表示，试验突显了 DLT 在某些支付用途上的潜力、系统实现的快速性、智能合同的潜在简单性，以及此类平台提供的功能范围。此外，波士顿联邦储备银行宣布，它将与麻省理工学院数字货币倡议的研究人员展开合作，以建立和测试一个“假想的”开源中央银行数字货币平台。2022 年 1 月，美联储发布了以“货币与支付：货币时代转型的美元”为题的白皮书。白皮书作为美联储与其相关利益者就 CBDC 进行公开讨论的第一步，明确了美国 CBDC 的定义、所处的经济背景、其潜在利益与风险。但该文件并无推进美 CBDC 政策的目的。在没有行政部门与国会的明确支持下（例如以具体授权法的形式），美联储不会做出发行 CBDC 的正式决定。

美国 CBDC 被定义为公众可以广泛使用的美联储数字负债，虽然尚未决定开展 CBDC，但是迄今为止的研究表明，美国对于可能设立的潜在 CBDC 有隐私保护、中介模式及可广泛转让及身份验证方面的要求，使该体系可以匹配美元的支付格局。具体而言，美国版 CBDC 重视消费者隐私权的保护，力求在保护消费者隐私权与提供必要的透明度防止犯罪中取得适当的平衡；在中介模式下，个人并不被授权直接开立联邦储备账户，私营部门将提供账户和数字钱包，以此方式促进 CBDC 的持有及支付的管理。作为美联储自身负债，中介模式将有助于利用私营部门现有的隐私及身份管理框架减少破坏美国现有稳定经济结构的可能性；美国版 CBDC 必须具备成为可广泛使用的支付手段的可能性，不同机构的客户可以随时使用 CBDC，使支付更有效率；最后，为了满足

打击洗钱和资助恐怖主义的严格要求，商业银行中间人需要核实进入商业银行的人的身份，正如银行和其他金融机构目前核实客户的身份一样。

美国同时展望了 CBDC 的广阔前景，美联储认为 CBDC 或成为美国支付系统的新基础，连接不同的支付服务，并在快速数字化的经济中保持安全、可靠的中央银行货币的核心地位。CBDC 将为广大公众提供广泛的数字货币使用渠道，更可能满足公众对于小额支付的需求（传统的支付系统不一定为网络小额交易设计）。不仅如此，作为国际市场的主导货币，美元的国际角色使其具有强大的国际影响力。目前，许多国家及联盟可能已经引入 CBDC，若现有的新型 CBDC 比美元纸币更具吸引力，美元的全球使用极有可能会随之减少，而美国 CBDC 有助于保持美元的国际角色，维护国际社会对于美联储机构的法治信任。

最后，美联储也提示到 CBDC 或许会从根本上改变美国的金融体系，当金融体系面对巨大压力时，大批其他形式的货币（包含商业银行的存款）将会快速转换成 CBDC，金融公司将会遭到更严重的挤兑。当前措施并不足以防止商业银行存款在恐慌中大量流向央行。因此，只有当研究表明 CBDC 对家庭、企业和经济整体的好处超出了下行风险，美国才会采取进一步的措施发展 CBDC。美联储将会在未来继续在公众及跨政府支持的背景下寻求 CBDC。

### 3. 日本

日本业已成为新一个开始探索 CBDC 可行性的主要经济体。自 2020 年 10 月发布“日本银行数字货币方法”以来，日本央行一直根据该方法进行试验，例如规定环境测试的要求和选择合作伙伴。当前，虽然暂无发行 CBDC 的计划，但是日本明确现阶段启动实验是一个必要的步骤。

起初，日本对于 CBDC 是否有必要存在更多持质疑的态度，由于民众能够安全使用现金，大多数的人持有银行账户，CBDC 的使用场景并未得到足够认可。但考虑到数字社会中支付和结算系统的本质，探索对于支付和结算的生态系统十分重要。因为它揭示了银行和非银行 PSPs 的作用、包括中央银行的公共部门应提供的公共物品以及平衡数据和隐私等方法。无论采纳 CBDC 与否，这些都是无法避免需要解决的问题。

随着科技发展，未来的支付和结算系统将会毫无疑问会变得更加便捷。现

代社会，随身携带金钱的风险已经降低，但是网上个人信息泄漏已成为令人担忧的问题。在这种情况下，安全与便利之间往往存在着权衡，中央银行和存款保险系统在减轻这种折衷方面起到了补充作用。如何保证安全与便利之间的最佳平衡，如何认定央行、银行和非银行 PSPs 在数字社会中应该扮演的角色都是日本央行需要考虑的问题。因此，日本意识到或许未来 CBDC 会成为解决办法的一部分。现在开始进行实验同时与众利益相关者交换意见极为重要。

#### 4. 加拿大

加拿大银行于 2021 年 7 月发布了关于 CBDC 可行性的研究报告。加拿大认可 CBDC 的有益之处，认为 CBDC 对于维持一个有竞争力和充满活力的数字经济是必要的。加拿大认为通过开发新的市场和应用程序，CBDC 可以增加福利；其次，CBDC 还可以限制滥用市场力量，避免支付和职能合同等新市场的协调失灵，从而达到减少福利损失的目的。

银行认可经济的数字化将继续发展，一般来说 CBDC 作为基本的外部支付选择可以约束市场。特别适用于在线交易的 CBDC 也将提供私人数字支付手段的替代办法，正如现金是销售交易的替代办法一样。为了有效地发挥外部选择地作用，加拿大 CBDC 需要特定的功能，以及商家接受和客户采用的特定关键水平。此外，作为一种竞争工具，CBDC 可能比大型科技公司在复杂多变的环境中制定新的竞争规则要简单，也比通过漫长而不确定的法律诉讼试图执行要简单。

最后，央行指出通过提供公开获取可编程货币等有前途的通用技术，CBDC 可以成为促进数字创新的工具。这一方面的好处及所带来的社会效益仍然有待观察，并需要更多的研究来确定是否由加拿大政府进行干预。

### （二）央行数字货币面临的挑战

在各国推进央行数字货币试点和研发的同时，央行数字货币需要考虑的合规风险不容忽视：

#### 1. 国内和国际层面面临法律适用和标准认同等问题

宏观角度，我国如何合规监管数字人民币同时面临国内和国际两方面挑战。国内层面，目前包括《中华人民共和国刑法》和《中华人民共和国人民币管理条例》在内的重要法律法规暂未对数字人民币流通，使用过程中可能产生



的法律问题的具体规定，数字人民币作为新兴技术产生的新生事物必然对现行法律体系产生一定影响。国际层面，各国对于数字货币的监管立场存在较大差异，在数字人民币以法币形式推出后，中国人民银行在未来不得不面对数字人民币多边标准认同、法律地位共识等更复杂的国际合作难题。同时，发行数字人民币将对国际金融现有流通体系造成一定冲击，甚或会产生对结算规则的冲击。

## 2. “冷钱包”成为央行数字货币反洗钱合规焦点

按照私钥的存储方式是否联网，可将数字货币的存储账户分为“冷钱包”和“热钱包”。冷钱包具有操作简便、交易安全等优势，但也使得大额数字货币的流转难以监控，脱离现有结算体系。

以我国数字人民币为例，对于央行数字货币的反洗钱合规焦点集中于冷钱包技术的“双离线支付”功能。在保持实时联网状态下，数字人民币和传统银行的电子支付或者是电子银行类似，属于传统账户体系，面临传统银行反洗钱相同的风险。由于我国的数字人民币定位为替代 M0，需要照顾部分难以实现网络覆盖地区，因此在设计上推出了“双离线支付”功能。易言之，如果两台手机在获取数字人民币后脱离现有的网络，依然可以通过 NFC 进行货币转移，而且只要保持与现有网络断开连接，该笔特定的数字货币流转便可能脱离现有的监管。这一点也是应予考虑的监管要点。

## 3. 全球范围的匿名交易与账户数量爆炸，违法犯罪行为隐蔽性增加

另一合规风险在于目前全球匿名账户开立数量过于庞大，非法交易、多户洗钱等监管缺位。核心问题在于账户介入主体多元，网络账户削弱传统属地管辖，使现阶段对于资金的监控出现现实障碍。目前的监管体系亟需形成跨链支付穿透调取等功能，揭开利用多个数字货币账户实现掩护资金非法移转的面纱。

## 二、司法存证——为公平正义

2017年8月18日，根据中央全面深化改革领导小组审议通过的方案，杭州互联网法院挂牌成立，集中审理浙江省杭州市辖区内基层人民法院有管辖权的六类涉互联网一审民事、行政案件。2018年8月9日，最高人民法院印发《关于增设北京互联网法院、广州互联网法院的方案》的通知，北京、广州两地互

联网法院正式成立。至此，中国互联网案件开启了集中管辖、专业审判的新篇章。

网络诉讼的普遍化使得电子证据成为司法电子文件管理的重要对象，区块链不可篡改、可追溯和去中心化等技术特性为电子证据保全提供了新的思路。近年来，最高人民法院不断深化司法体制改革和智慧法院建设。在智慧法院建设方面，最高人民法院紧跟互联网技术发展，建成全国统一司法区块链平台，创新在线存证方式，推动解决电子证据取证难、存证难、认证难问题。与此同时，各级法院积极探索，在司法实践中先于立法对通过区块链技术保存的电子数据效力予以广泛认可。

### （一）电子数据存证现状

最高人民法院早在 2018 年发布了《关于互联网法院审理案件若干问题的规定》，该司法解释第 11 条第 2 款规定电子数据如果可以证明其真实性的，法院应予确认，使区块链存证在司法应用中得到了实质层面的推进。

2021 年 6 月，《人民法院在线诉讼规则》发布，第 15 条至第 19 条对电子证据上链存储及证明力问题作了进一步规定。具言之，第 16 条规定电子数据上链并经技术核验后原则上认定为真实。第 17 条明确了法院对电子数据上链后真实性核查的判断方法，包括存证平台与存证技术的合规性、是否存在利害关系、是否存在技术手段不当干预等。第 18 条规定了转化型电子数据真实性判断方法，包括由数据上链一方当事人承担证明责任，由法官结合上链前数据的具体来源、生成机制、存储过程、公证机构公证、第三方见证、关联印证数据等情况综合判断。第 19 条衔接了现有专家辅助人制度与电子证据效力问题，当事人可以申请具有专门知识的人就区块链技术存储电子数据相关技术问题提出意见。

目前，电子数据存证已被广泛运用于诉讼活动，信息网络传播权纠纷及其他著作权纠纷案件占绝大部分。2021 年 5 月最高人民法院发布互联网十大典型案例中“杭州华泰一媒文化传媒有限公司诉深圳市道同科技发展有限公司侵害作品信息网络传播权案”<sup>①</sup>系全国首次对区块链电子存证法律效力进行认定的案件。该案同时明确了认定区块链存证效力的相关规则。

<sup>①</sup> 杭州互联网法院，(2018)浙 0192 民初 81 号。

原告华泰公司主张被告道同公司未经其许可在道同公司运营的“第一女性时尚网”中发表华泰公司享有著作权的作品，侵害了原告的信息网络传播权。华泰公司通过第三方存证平台对侵权事实予以取证，后该平台将相关数据计算成哈希值上传至比特币区块链和 Factom 区块链中形成区块证据链存证，以此向法院请求判令道同公司承担侵权责任。作为全国首例区块链技术电子存证著作权侵权案，在电子证据效力认定上，法院采取了以下步骤，在事实层面对区块链电子证据的审查判断做了详细论证：

1.存证平台资质审查。包括存证方与存证平台之间是否存在控股或其他利益关联关系（即中立性），是否通过国家网络与信息安全产品质量监督检验中心完整性鉴别检测。

2.取证技术手段的可信度审查。包括第三方存证平台所在服务器的安全性，第三方存证平台是否获得网站安全相关的认证及备案，取证固证人为篡改可能性。

3.区块链电子证据保存完整性审查。该阶段可进一步分为审查电子数据是否真实上传和审查是否为诉争的电子数据，主要技术手段为通过查看区块高度生成时间的时间逻辑和哈希值比对。

## （二）区块链电子存证的法律依据

现有的文献中存在将“电子存证”和“电子证据保全”概念混用的现象，但二者并非等同或替代的关系。电子证据保全和电子存证虽然都指向电子证据的提取和固定，却在时间和目的上有所区别。就时间而言，电子存证是一种瞬时性行为，一般发生在诉讼成立前的某个时间点；电子证据保全是一种持续性行为，贯穿电子证据整个生命周期。就目的而言，电子存证以电子证据的留存和取得为目的，旨在确保诉讼发生时有证据可用；电子证据保全则是为了保障电子证据的证据资格和证据能力，确保证据可以使用。<sup>①</sup>

在证据法学中，证据资格与能力以证据的“三性”即真实性、合法性和关联性为依托。在前述（2018）浙 0192 民初 81 号中，被告就原告提交的区块链证据提出了两方面质疑：区块链存证主体是否适格，以及区块链存证运行机制是否合法。因此，经由区块链存证的电子数据的证据资格应当接受真实性、合

<sup>①</sup> 聂勇浩，张妍：《基于区块链的电子证据保全模式研究——以广州互联网法院为例》，载《档案学研究》2021年第5期。

法性和关联性的检验。

### 1. 电子证据存证真实性的认定

电子证据存证的真实性认定是电子存证中有较大革新的部分，可以分为电子证据载体的真实性、电子数据的真实性以及电子证据内容的真实性。

#### (1) 电子证据载体真实性

电子证据载体的真实性，指电子证据的存储媒介在诉讼过程中不存在被伪造、编造、毁损，始终保持其同一性与完整性。在传统电子证据审查模式中，“易失真论”导致许多体系完备的电子数据被直接排除，而“唯科技论”则使许多虚假、被篡改的电子证据流入法庭。<sup>①</sup>区块链技术扩展了电子证据的载体外延，一方面基于共识算法的节点间信任关系，每个节点在参与记录的同时也验证着其他节点记录结果的准确性，即使某一节点遭到黑客攻击或病毒入侵，其他节点的数据并不会被更改或丢失；另一方面，时间戳技术使存证过程不可逆，从而使交易过程得到客观、准确地描述。

#### (2) 电子数据的真实性

电子数据是电子证据的存在形式，电子数据的真实性是指电子数据与原数据的一致性，要求电子数据与原数据相比不存在删除或增加。电子数据的真实性可进一步细化为产生、收集与传输三个阶段。

电子数据真实性是内容真实性判断的基础，而电子数据产生阶段的真实性，是保证后续阶段真实性的前提。虽然区块链电子存证在技术层面能保证电子证据载体的真实性，但是载体的真实性无法直接推导出数据本身的真实性。若要发挥区块链的技术优势，确保数据真实性，则需要在产生阶段确保电子数据“生成即上链”，生成于链下而后存储于链上的数据仍存在传统电子证据的验证困境。

在收集过程中，传统电子数据的收集过程主要面临载体安全风险与数据收集人员主观因素干扰两方面问题。区块链存证下的电子数据收集需要提前经用户认可并附有当事人合法的电子签名，一来通过确认当事人本人的操作来保证数据的真实有效，二来能基于去中心化的技术特性排除主观因素以及第三方存证机构篡改数据的风险。

<sup>①</sup> 张可：《论电子数据的孤证禁止规则：一个初步的探讨》，载《中国刑事法杂志》2020年第1期。

在传输过程中，传统电子数据需经多主体多介质转换，电子数据存在极高的被删改风险。为保障证据真实性，证据法理论要求证据在转移过程中应当形成完整的证据保管链条。然而实践中传统的电子数据传送过程无法保证传送链条的完整性，司法机关也因此可能因为电子数据的真实性降低而拒绝采信。区块链技术主要通过对电子数据进行加密和生成哈希值比对的方式保证传输过程的真实性。如果电子数据的整个生命周期一直严格遵循区块链存证系统的运行机制，全流程未有篡改的余地，那么可以真正在技术层面提高电子数据的证据效力。

### （3）电子证据内容真实性

电子证据内容真实性是电子证据真实性的核心问题，在长期司法实践中，电子证据内容真实性的证明问题无法得到有效解决，限制了电子证据在诉讼中的证明功能。以常见的著作权侵权纠纷为例，当事人需要对侵权网页进行抓取并存证。为了证明侵权网页的客观存在，有的当事人采取单方录屏的方式。但该固证方式并不能证明录屏前有无篡改网页数据行为，导致原本客观的证据掺入主观因素，增加了电子证据验真的成本与难度。而使用区块链存证技术的电子证据，一般可以逻辑推导出内容真实性。

然而需要指出的是，即使电子证据通过区块链存证后载体真实性与数据真实性得到区块链技术的强化，仍然存在证据内容与客观事实不一致的情形。

## 2. 电子证据存证合法性的认定

传统意义上的证据合法性，包括取证主体、程序、证据形式、证据保全与运用的合法性。<sup>①</sup>故，电子存证证据合法性的认定是一个机械对照法条的过程，不同于真实性与关联性的认定需要法官主观评判，电子证据存证只要符合法律规定，就应当认定具有合法性。

## 3. 电子证据存证关联性的认定

证据关联性作为证据的自然属性，取决于证据与待证事实间的逻辑联系，主要依靠法官的自由心证与逻辑判断。区块链电子存证使用技术手段对证据进行留存，在本质上不能确保或改变电子证据的关联性，仅能在部分应用场景下对证据的关联性认定提供参考。

<sup>①</sup> 刘方权：《双重视野下的证据合法性证明问题》，载《中国刑事法杂志》2015年第4期。

具言之，在电子证据关联性认定中，用于证明待证事实的电子数据，包括但不限于数据生成、修改等形成的时间等数据信息，及记录发送人和接收人 IP 地址、日志记录、源代码等痕迹信息。通过比对上述信息与区块链时间戳信息的同一性、比对电子证据上链后的哈希值等手段，可以在一定程度上强化证据链，保证电子证据的证明力。

### （三）国内法院区块链存证应用现状

#### 1. 北京互联网法院“天平链”

天平链是由北京互联网法院牵头，联合多家权威机构建设的司法联盟链。2018年9月9日，北京互联网法院“天平链”上线运行。秉持“中立、开放、安全、可控”的原则，北京互联网法院联合北京市高级人民法院、司法鉴定中心、公证处等司法机构，以及行业组织、大型央企、大型金融机构、大型互联网平台等20家单位作为节点共同组建了“天平链”。<sup>①</sup>

“天平链”通过利用区块链本身技术特点以及制定《应用接入技术规范》及《应用接入管理规范》，实现了电子证据的可信存证、高效验证，降低了当事人的维权成本，提升了法官采信电子证据的效率。

天平链在系统架构上属于联盟链，包括一级节点与二级节点。一级节点单位参与天平链共识、数据校验与记录，如北京高院、北京互联网法院、国家信息中心电子数据司法鉴定中心、中国电子商会等；二级节点单位则仅做数据校验与记录。

#### 2. 杭州互联网法院“司法区块链”

杭州互联网法院“司法区块链”为全国首个电子证据平台。该平台首次通过脱敏核、保真核双核双链技术，打造“全流程记录、全链路可信、全节点见证”的司法级别信任机制，确保了电子数据的真实性和合法性。通过区块链技术，将商业链、司法链跨链融合，有利于提升审判效率和审判效能。<sup>②</sup>

#### 3. 广州互联网法院“网通法链”智慧信用生态系统

2019年3月，广州互联网法院“网通法链”智慧信用生态系统正式上线。在“网通法链”系统建设中，“司法区块链”依托智慧司法政务云，联合法院、检察院、仲裁、公证多主体，集聚电信运营商、金融机构、互联网企业，为智

<sup>①</sup> 北京互联网法院：<http://tpl.bjinternetcourt.gov.cn:8080/tpl/#shen>.2022-1-21.

<sup>②</sup> 杭州互联网法院：<https://blockchain.netcourt.gov.cn/first>.2022-1-21.

慧信用生态系统提供区块链技术支持。

“网通法链”系统主要包括两部分。“可信电子证据平台”以规则制定为抓手，严格管理规范、技术要求、安全标准、存证格式，为当事人提交电子合同、维权过程、服务流程明细等证据线索“一键调证”提供支持。“司法信用共治平台”则围绕从源头减少审判执行增量，着力打造诉源治理“广州方案”。

#### （四）目前区块链存证存在的问题

##### 1. 司法区块链未完全实现“去中心化”

区块链系统可分为公有链、私有链及联盟链。公有链又称为开放区块链或无许可区块链，私有链和联盟链统称为有许可区块链。这三类应用在系统特性、组织架构与参与主体方面有很大差异性。由于目前我国法院应用的均为联盟链，上述互联网法院的司法区块链平台以联盟链的形式向特定组织开放，节点只有通过授权才能加入或退出，共识过程也受到预选节点控制，并未真正实现去中心化、发挥出区块链的优势。

联盟链本质上是一个多中心化的区块链系统，联盟链接入的成员均可查询和参与链内活动，但写入权限仅由参与群体内选定的部分高性能节点轮流完成。在联盟链中，只要控制 51% 的节点，仍有可能修改存储于链上的数据信息。<sup>①</sup>此外，在联盟链环境下，若法律主体不是区块链节点，则需要节点账户私钥代理其发送存证交易。因此若想维持电子证据的客观性，则需要证明电子证据和法律主体的关联性、需要证明代理人在发送交易前不存在数据篡改。<sup>②</sup>

##### 2. 未发挥出区块链技术“自我验真”的优势

为防止当事人提交前单方的编辑与删改行为，对于传统电子证据的鉴定或公证以补强证据效力成为实践中的惯常做法。

然而在区块链进入司法领域，这项革命性的技术却似乎并未对证据审查带来太多改变。在上文述及的杭州互联网法院“区块链电子证据效力认定第一案”中，虽然法官创新性地对区块链证据的审查判断路径进行了详细论证，但不难发现该案仍然沿用了传统的审查模式来评价区块链电子证据的可采性与证明力。区块链技术是一种可以自我验真的数据核验机制，电子证据经过区块

<sup>①</sup> 京东数科：《2020 京东区块链技术实践白皮书》，2020 年 10 月，第 134 页。

[http://www.chuangze.cn/third\\_down.asp?txtid=2982](http://www.chuangze.cn/third_down.asp?txtid=2982)，2022-1-21。

<sup>②</sup> 同上，第 135 页。

链技术的验证、加密后就能够证明该电子证据的真实性，因而是可以“技术自证”的。<sup>①</sup>在可以自我验真的前提下，司法资源是否可以节约在证据审查上的消耗，是否有必要继续因循传统证据审查的路径对区块链电子证据作双重验证值得探讨。

但不可否认的是，联盟链是客观条件限制下经权衡的最优解。公有链就目前来看并不适合在包括司法场景在内的场景中应用，在法院、检察院、公证机关、仲裁机构等不同主体之间既有案件往来，也有内部数据，公有链信息安全难以保证。同时，现有技术下公有链系统性能较低，难以满足高吞吐量业务场景的需求，应用受到较大限制。

### 三、他领域——风华尽显

目前我国区块链的产业链条已经基本形成，自上而下为：上游的区块链底层协议、硬件基础设施建设，中游的拓展性技术和解决方案，下游的行业应用，以及产业服务相关配套设施如监管合规服务、投融资、数据服务等。

#### （一）区块链+农业

早在 2020 年，中央一号文件《中共中央国务院关于抓好“三农”领域重点工作确保如期实现全面小康的意见》中就将区块链写入农业建设领域。在近年来的绿色农业建设中，区块链在我国农业农村方面的应用领域主要集中于两大板块，分别为要素端以及供应链管理端，要素端中，主要为农地征信及融资。而在供应端中，农产品安全溯源方面的应用最为广泛。

2021 年 7 月 19 日，农业农村部信息中心联合中国电信集团有限公司、山东省农业农村厅、潍坊市人民政府及坊子区委区政府，在山东省潍坊市坊子区举行“区块链+韭菜”试点项目启动暨合作协议签约仪式，标志着“区块链+”在农产品质量安全智慧管控上的应用迈出了开创性的关键一步。该项目是基于区块链在农产品质量安全等民生领域的应用，包括加强农产品全过程质量安全智慧管控，建立健全农产品质量安全追溯体系，重塑农产品质量安全治理制度机制等内容。

#### （二）区块链+防疫

<sup>①</sup> 胡萌：《区块链电子证据的效力分析与规范路径》，载《证据科学》2021 年第 1 期。



新冠肺炎疫情是一场大考。在新冠肺炎疫情防控常态化大背景下，时不时暴露出我国在应对公共突发卫生事件中的短板与缺陷。区块链基于自身技术特性，能满足包括但不限于信息共享、多主体协作、信息溯源等需求，对防控成本的降低、社会运行的稳定起到推动作用。

目前区块链应用于疫情防控的场景主要在公共预警、产品溯源、身份互认等方面。在公共预警领域，如山大地纬打造的“济南疫情防控平台”、链飞科技的“区块链疫情监测平台”，基于数据实时上链能够在最短时间内掌握疫情动态，打通数据孤岛，实现医疗机构间的数据共享与城市防疫的一体化治理。在产品溯源领域，北京微芯研究院的“北京冷链溯源平台”、蚂蚁集团的“防疫物资信息服务平台”依托区块链实现源头追溯，保证各节点溯源数据互认互信。在身份认证领域，包括微众银行的“粤康码”在内的各地防疫健康码大多应用了区块链技术，基于区块链技术的可信身份信息管理，结合分布式身份标识等技术，在实现身份验证的同时，避免数据泄露。

未来，区块链技术有望继续提升特定场景适应性，推动后疫情时代公共治理的创新应用。

### （三）区块链+碳中和

碳达峰、碳中和目标要求建立完善的碳足迹追溯体系和透明的碳排放交易市场机制，而区块链具有去中心化、防篡改、可追溯、全程留痕等技术特点，能够较完好的支撑碳足迹全生命周期的可信记录、碳排放全要素的可信流转，可为碳交易场景提供更安全、更高效、更经济的市场环境，以及可视、可信、可靠的监管环境。基于可信碳排放交易，未来也将培育出新兴的碳金融模式，为我国碳排放与碳中和目标提供有力保障。

例如，蚂蚁集团提出的蚂蚁链企业碳中和管理 SaaS 产品“碳矩阵”，基于区块链技术实现碳排放、碳减排、监管审计等过程公开透明，记录随时追溯查证，实现企业碳中和数据统一管理与数据可视化。

在“区块链+碳中和”领域国际标准的话语权争夺中，2021年5月，国家电网有限公司在电气电子工程师学会标准化协会（IEEE-SA）提交的国际标准提案《基于区块链的碳交易应用标准》正式立项。该标准也是 IEEE 首个“区块链+碳交易”国际标准，立足我国碳达峰、碳中和目标，依托国家电网开展的

“区块链+碳交易”创新探索典型成果和实践经验，总结提出区块链在碳交易领域的技术应用要求和规范，将帮助我国碳交易实现全生命周期溯源管理，解决碳交易多主体身份认证效率低、数据确权难等问题，通过分布式数据多方共同维护，保障碳交易数据可信共享，提升业务效率，为整个碳交易行业提供区块链技术指引和规范。

#### （四）区块链+金融监管

加密资产因其匿名化和去中心化已经成为洗钱、恐怖主义融资、赌博、诈骗等犯罪的理想工具，各主流国家即使允许加密资产投资与交易，也已将加密资产交易和风险管理作为重点监管领域。然而，对加密资产的金融监管面临调查取证难度大、违法犯罪手段专业性强、匿名化导致行为人身份信息确认难等特点。

在国内，以欧科云链为代表的一些企业已将区块链技术应用于金融合规与监管和警务合作领域。“链上天眼”产品运用“区块链+大数据”的技术框架，并结合机器学习、数据建模、相似度计算、特征工程等关键技术，将传统经济类案件的侦查方式应用到数字货币的相关案件面向合规部门以及监管机构提供资产安全保障及反洗钱服务，通过海量的地址标签库智能甄别高风险地址，及时识别链上风险，与监管部门共建链上安全。

据统计，作为第一代产品的升级版，“链上天眼 Pro”在 2021 年协助各地公安机关打击各类区块链相关案件 80 余起，协助公安机关、受害人冻结、追回资产 300 余亿元，广受各地公安民警好评。2022 年 1 月 10 日，“链上天眼 Pro2.0”发布，除实时监控、智能化分析研判等功能上的创新外，2.0 版本结合了此前数百起案件的分析研判经验，融合技侦战法与区块链大数据，精准追踪“涉案地址”、“交易特征”等信息，让数据发出专业声音，实现了数字货币案件的智能化追踪、一站式分析和取证研判。<sup>①</sup>

#### （五）区块链+信用证

信用证，是指银行根据进口人（买方）的请求，开给出口人（卖方）的一种保证承担支付货款责任的书面凭证。在信用证内，银行授权出口人在符合信用证所规定的条件下，以该行或其指定的银行为付款人，开具不得超过规定金

<sup>①</sup> 《欧科云链链上天眼 Pro2.0 正式上线，“三大创新突破”献礼人民警察》

额的汇票，并按规定随附装运单据，按期在指定地点收取货物。信用证自1997年最高人民法院出台的《国内信用证出台办法》引入国内，但国内信用证的业务量仍然较小，主要存在以下问题：1.国内信用证业务仅在同一家银行的内部开展，国内银行间的信用证业务的流转很困难；2.信用证业务流程需要大量银行工作人员手工完成，办理信用证业务的效率有待提高。3.传统信用证仅仅审核单据的真实性，而贸易单据的造价成本并不高，这就导致了实务中存在虚构贸易骗取信用证的问题。

“全员公开，无人篡改”的区块链技术有助于突破传统信用证业务的制约，建立平等互利、智能高效的电子信用证业务模式。区块链信用证系统主要包括三个部分：开证行业务系统、通知行业务系统、区块链网络。业务主要流程包括：申请人申请电开信用证，开证行业务平台受理；开证行业务平台将相关交易数据进行加密，通过业务系统与区块链接口写入区块链节点，区块链进行数据同步；通知行业务平台通过接口读取区块链数据；通知行业务平台节点对数据解密；通知行通知受益人，受益人确认后发货开单。

区块链技术降低了贸易造假的可能性，进而降低了交易风险；组织多个买方行和卖方行共同构建联盟链提升了结算融资服务效率。但是仍有部分法律问题值得关注：1.在跨行信用证业务方面，缺乏统一的区块链信用证行业标准，跨行办理和管理效率有待提高；2.人工操作过多，信用证业务流程仍不可避免地偶有出错的情形，有必要促进业务交易双方通过智能合约实现承诺协议自动执行，降低人工操作的出错率，提高业务办理的效率。

## 四、挑战——无处不在

### （一）企业整体合规意识欠缺

以《数据安全法》、《网络安全法》、《个人信息保护法》等法律为核心，《互联网信息服务管理办法》等行政法规和多项部门规章构建的区块链合规框架为区块链从业人员提供了业务合规指引。

首先应当明确，数字资产的本质是利用区块链技术通过区块记录信息并形成数据链条的特殊账本，符合《数据安全法》对数据的定义，属于《数据安全法》的调整对象。而数字资产的金融属性应当从属于数据属性，不能仅因为其在金融场景的应用就否定数字资产的数据属性。

近年来区块链概念存在被滥用于违法犯罪活动的情形，但区块链技术对数字经济发展和数据安全的正向作用不可否认。正因如此，上述法律规范构成的合规与监管体系是区块链产业商业模式规范化的一环，对提振市场信心，消解公众对新兴技术的误区有积极作用。

然而由于法律法规出台时间较短、企业甚至全社会对互联网合规意识不强、违法成本尚未显现、市场上数据合规专业人员等因素叠加，区块链从业人员的合规教育与企业内部的合规体系搭建目前普遍存在欠缺。大量企业内部未建立完善的数据合规体系或建立了相应的体系但在落实上存在疏漏，对外未履行备案登记等行政机关规定的义务。据笔者观察，在实务中大量互联网企业或涉及互联网产品和服务的企业对自身开展业务的合规要求不具备清晰的认知，仅基于自身对业务范围和产品内容的了解采取了有限的合规措施，忽视了大量风险的存在；在具体合规操作上缺乏体系化、制度化的内部流程，制定内部安全管理规章制度、风险应急预案时流于形式，导致日常经营合规存在重大隐患，甚至影响后续产品交易和企业融资。

目前我国对网络安全相关的违法犯罪行为规定了极高的法律责任。例如《个人信息保护法》第 66 条规定，违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，最高可处五千万元以下或者上一年度营业额百分之五以下罚款，并可责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。又如，《数据安全法》第 45 条规定，开展数据处理活动的组织、个人不履行数据安全保护义务的，最高可处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。鉴于此，区块链从业人员和互联网企业应当在专业人员协助下建立具有可操作性的内部合规体系，规范日常运营的数据处理，妥善履行备案、登记等行政机关规定的义务，尽早消除企业日常经营的合规风险。

## （二）区块链技术服务中立性与刑事合规风险的冲突

区块链从业人员与互联网企业需要尤其重视刑事合规风险的管控。从业者往往秉持技术中立的观点，主观上对刑事合规风险缺乏必要的警惕性，客观上

对日常经营活动中委托方的技术服务需求疏于审查和管理，导致涉嫌犯罪的案例屡见不鲜。

帮助信息网络犯罪活动罪（以下简称“帮信罪”）是区块链技术服务提供者在实务中最有可能被卷入的罪名。我国《刑法》第二百八十七条规定，帮信罪，是指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助的行为，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

本罪属于帮助犯独立成罪，根据《〈刑法修正案（九）〉释解与适用》，“增设本罪是为了更准确、有效地打击各种网络犯罪帮助行为，保护公民人身权利、财产权利和社会公共利益，维护信息网络秩序，保障信息网络健康发展”。

帮信罪入罪需要衡量三个标准：客观上实施了帮助信息网络犯罪活动的行为，主观上对他人利用信息网络实施的犯罪为明知，最后在情节上需要达到入罪标准。

首先，对于客观帮助行为，《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（以下简称“《司法解释》”）第八条对设立网站的犯罪行为进行了细化：以实施违法犯罪活动为目的而设立或者设立后主要用于实施违法犯罪活动的网站、通讯群组，应当认定为刑法第二百八十七条之一第一款第一项规定的“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”。以区块链技术服务中风险较高的搭建虚拟货币交易平台为例，区块链从业者需要关注是否存在或可能存在如洗钱、诈骗、传销、非法吸收公众存款等违法行为；其次，如果上游违法犯罪行为确能查证成立，则需要查证帮助行为是否直接与上游行为产生直接关联。

其次，对于主观层面，判断技术人员所提供的服务是否是“中立的技术服务”，要认定为中立的帮助行为，至少必须是“行为人并不追求非法目的”。《司法解释》第11条规定了帮助信息网络犯罪活动罪“明知”的认定标准，在“明知”认定的表述模式上采用了“详细列举+兜底描述+出罪空间”：为他人实施犯罪提供技术支持或者帮助，具有下列情形之一的，可以认定行为人明知他人利用信息网络实施犯罪，但是有相反证据的除外：

- (一) 经监管部门告知后仍然实施有关行为的；
- (二) 接到举报后不履行法定管理职责的；
- (三) 交易价格或者方式明显异常的；
- (四) 提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的；
- (五) 频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的；
- (六) 为他人逃避监管或者规避调查提供技术支持、帮助的；
- (七) 其他足以认定行为人明知的情形。

该条详细列举了几种具体犯罪行为的主要情形，并以“其他足以认定行为人明知的情形”作为兜底描述，留下其他犯罪行为的认定空间。

最后，对于帮信罪的入罪标准，《司法解释》第12条规定，“明知他人利用信息网络实施犯罪，为其犯罪提供帮助，具有下列情形之一的，应当认定为刑法第二百八十七条之二第一款规定的“情节严重”：（一）为三个以上对象提供帮助的；（二）支付结算金额二十万元以上的；（三）以投放广告等方式提供资金五万元以上的；（四）违法所得一万元以上的；（五）二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；（六）被帮助对象实施的犯罪造成严重后果的；（七）其他情节严重的情形。”“实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。”

### （三）反洗钱与反恐怖主义融资义务的履行

我国《反洗钱法》第三条规定，“在中华人民共和国境内设立的金融机构和按照规定应当履行反洗钱义务的特定非金融机构，应当依法采取预防、监控措施，建立健全客户身份识别制度、客户身份资料和交易记录保存制度、大额交易和可疑交易报告制度，履行反洗钱义务。”第三十六条规定，“对涉嫌恐怖活动资金的监控适用本法。”据此，反洗钱与反恐怖主义融资义务的履行主体为金融机构和特定的非金融机构。对于非金融机构的主体范围，第三十五条规定，由国务院反洗钱行政主管部门会同国务院有关部门制定。

2018年，中国人民银行发布《中国人民银行办公厅关于加强特定非金融机构反洗钱监管工作的通知》（银办发〔2018〕120号），明确“非金融机构”范围包括房地产开发企业和房地产中介机构、贵金属交易商和贵金属交易场所、会计师事务所、律师事务所、公证机构、公司服务提供商。这也是传统洗钱犯罪逐渐演变为金融行业与非金融行业并存、专业分工程度提升、手段多样化复杂化后国家对非金融机构监管疏漏的填补。

然而我国目前实行的《反洗钱法》于2007年实施，全文仅37条，操作性内容不强。同时，反洗钱行政法规、部门规章的缺位也使反洗钱法律框架存在疏漏，在监管实践中无法可依。这突出反映在以下方面：

一是“特定非金融机构”作为履行反洗钱义务的主体，其范围覆盖滞后于洗钱犯罪发展，具体义务不明晰。目前我国《反洗钱法》规定，特定非金融机构应当与金融机构履行相同的反洗钱义务，即“依法采取预防、监控措施，建立健全客户身份识别制度、客户身份资料和交易记录保存制度、大额交易和可疑交易报告制度”等。但由于非金融机构覆盖范围广泛、所处行业性质不同，导致特定非金融机构履行反洗钱义务时会存在差异。目前看来，对于区块链及加密资产方面的反洗钱制度，缺乏明确规定。

二是特定非金融机构面临认知与操作上的困难，一方面是由于特定非金融机构反洗钱组织架构缺失，各部门职责划分不清；另一方面是在行为人将目光投向非金融机构进行洗钱行为时，非金融机构及其从业人员却尚未建立起足够的警惕性，或是对反洗钱的必要性与重要性缺乏认知。区块链从业者可能会认为，对洗钱犯罪的防控主要是政府部门的职责和金融机构应当履行的义务，与自身无关，因而置身于反洗钱之外。

随着国家对反洗钱和反恐怖主义融资的不断重视，该领域在未来有较大立法空间，区块链从业人员与互联网企业应当及时跟进政策文件和法律法规的动态。同时，应当对从业人员进行反洗钱相关知识的培训，建立企业内部可疑业务报告制度和反馈机制，尽早消弭刑事合规风险。

#### （四）税收风险

我国对虚拟货币交易采禁止的态度迟滞了虚拟货币征税方面的相关规定。对交易的禁止并不意味着不会产生征税问题与税收风险，事实上，有相当一部

分公民从国外交易所进行虚拟货币交易并获得利润。

国际上已有较多对于虚拟货币交易征税的立法例。美国 IRS 早在 2014 年就发布文件要求对比特币征税，无论是出售还是交换可兑换的虚拟货币，还是使用虚拟货币作为交易手段支付商品或劳务，都将带来税收责任。日本国税局在 2017 年规定比特币交易的资本收益属于“杂项收入”，税率适用范围为 15%~55%。俄罗斯财政部于 2018 年声明，投资加密货币属于个人所得，适用个人 13% 的个人所得税税率。

2021 年 10 月 19 日，中国税务报发表文章《防范虚拟货币带来的税收风险》，引起行业轩然大波。文章称，从当前情况看，比特币等虚拟货币在全球范围内的交易很难在短时间内消失，未来发展的方向也无法确定。同时，在当前法律框架内，我国对于个人持有比特币等虚拟货币未受禁止，虚拟货币的交易被定义为“无效的民事法律行为”，却并未从法律上明确禁止。

文章指出，从税收角度上来看，对于国内企业和居民参与虚拟货币的境内外交易，我国应加强部门协作与国际多边监管合作，重点防范资金违规跨境流出和利用虚拟货币在境内外避税，并将虚拟货币账户纳入金融账户涉税信息交换之列。同时，我国应完善相关财产申报登记机制，对持有大量虚拟货币的用户进行实名登记与动态追踪。在罚没收缴、重组并购、破产清算等司法领域，要对虚拟货币的处置方式予以明确，避免国家税款流失。此外，税务部门应当主动与央行、金融监管、市场监管、公安司法等部门联动，严厉打击虚拟货币用于地下经济、走私、洗钱、逃税等非法行为。

我国现行税种中与虚拟货币相关的主要是增值税和所得税（包括个人所得税和企业所得税）。《增值税暂行条例》第一条“在中华人民共和国境内销售货物或者加工、修理修配劳务，销售服务、无形资产、不动产以及进口货物的单位和个人，为增值税的纳税人，应当依照本条例缴纳增值税”。学理上，虚拟货币在我国无法同国外立法例一样被认定为证券，可以认定为法律上的“物”——则相关交易行为可归类于税法上的“销售货物”，增值税税率为 17%；也可被视为无形资产——则相关交易行为应当按照销售无形资产缴纳增值税，增值税税率为 6%。

由于区块链技术的全球性和匿名性，虚拟货币交易中的偷税漏税问题在各



国的监管实践中较为薄弱。但监管的体系化、正规化与国际反避税、反洗钱与反恐怖主义融资合作的不断加深也增加了虚拟货币的税务合规风险。例如，由经济合作与发展组织（OECD）发起，全球多国参与制定的共同报告标准（Common Reporting Standard, CRS）旨在建立国际间的税收信息搜集与自动交换标准以打击国际逃避税行为。CRS的建立与落地，非法离境资产可能面临补税问题。

根据我国税收征管方面的法律规定，逃税的纳税人除了需要缴税款、滞纳金，还有可能被处欠缴税款百分之五十以上五倍以下的罚款，更严重的甚至可能面临刑事处罚。

## 第五章 致未来

本报告撰写的初衷即为综合整理 2021 年国内及境外区块链行业动态，除以全球监管与合规动态为核心外，也涵盖了区块链融资、大型企业的区块链技术应用、各国央行数字货币发展情况等板块，旨在为区块链从业者和其他潜在受众描绘更加综合全面、更具有国际视野的区块链技术应用场景。

在技术不断革新的当下，得益于党中央、国务院和地方各级政府对区块链技术及其应用场景的重视，我国区块链技术应用在国际上处于第一梯队。纵观全国，大部分地区都已经或正在着手将区块链应用推广至电子政务、城市大脑建设等公共管理领域。未来五年，区块链技术有望深度结合高水平精细化城市治理，真正实现“技术为民”的发展目标。

司法应用领域，《人民法院在线诉讼规则》的发布使电子存证技术的司法应用更加规范化。国内三大互联网法院继续联合其他节点单位接入联盟链，打造本区域可行电子证据存证平台；同时，吉林高院、山东高院、郑州中院等多家法院也开始发展电子存证。受制于区块链技术的发展水平，司法应用中存证效率和证据认定等方面仍有较大发展空间。

全球区块链合规与监管动态中，对全球经济有较大影响力的国家基本上采取了趋同的监管模式：一是根据加密货币的功能确定适用的法律制度，例如，若加密货币具备证券特征，则一般适用该国证券法律规范。二是在合规监管上，主要采取对从事加密货币业务主体增设行政许可、设置报告义务和信息披露义务等。三是在各界尤其关注的反洗钱与反恐怖主义融资问题上，部分国家专门设立行政机构负责可疑交易与加密货币业务主体的金融情报。由于我国对加密货币的交易采禁止态度，故暂时不存在监管上的压力，但在反洗钱与反恐怖主义融资领域的域外经验值得参考。

国际区块链产业动态中，区块链融资持续火热，加密货币、区块链解决方案受资本青睐的同时，NFT、隐私计算、技术融合也逐渐成为新的火热赛道。具有国际影响力的大型企业纷纷将区块链技术应用于供应链、企业内控、支付结算等领域。2021 年末，元宇宙概念受到热炒，但在资本趋之若鹜之余，仍需关注可能的法律风险及变现能力等问题。

研发和试点央行数字货币已经成为全球各主要经济体的共识。相较于 2020

年，2021年试点央行数字货币的国家的规模大幅增加，并有望助力地区融合、金融一体化。除央行数字货币外，区块链技术的商业应用图景也逐渐丰富，包括但不限于农业、疫情防控、碳中和、金融监管、国际贸易等领域。

但无论区块链技术在未来会发展出怎样的应用图景，区块链技术的多中心化、难篡改、自激励等特性注定了合规与监管是健康发展的核心。这不仅需要在立法层面针对新业态不断完善和细化规制措施，平衡监管与创新的冲突，更要求区块链从业者和互联网企业树立合规意识，完善企业内部合规制度与合规措施。我们相信，着眼全球视野，遵循规范理念，严守合规底线，区块链为数字经济赋能，提升政府治理必将发挥积极而重要的促进作用。

## 参考文献

- [1] 柯达.论区块链数字货币的非法集资刑法规制[J].东北大学学报（社会科学版），2020(06).
- [2] 聂勇浩, 张焱.基于区块链的电子证据保全模式研究——以广州互联网法院为例[J].档案学研究, 2021(05).
- [3] 张可.论电子数据的孤证禁止规则：一个初步的探讨[J].中国刑事法杂志, 2020 (01).
- [4] 刘方权.双重视野下的证据合法性证明问题[J].中国刑事法杂志, 2015(04).
- [5] 胡萌.区块链电子证据的效力分析与规范路径[J].证据科学, 2021(01).
- [6] 人力资源和社会保障部专业技术人员管理司.区块链工程技术人员区块链技术基础知识[M].北京: 中国人事出版社, 2021.
- [7] 中国网.欧科云链链上天眼 Pro2.0 正式上线，“三大创新突破”献礼人民警察 [EB/OL].<https://t.cj.sina.com.cn/articles/view/3164957712/bca56c1002001tkmk?sudaref=cn.bing.com&display=0&retcode=0>, 2022-1-10.
- [8] MAS.Project Ubin: Central Bank Digital Money using Distributed Ledger Technology[EB/OL].<https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin>, 2022-2-17.
- [9] Reed Smith Guide to the Metaverse(May 2021)[EB/OL].<https://fingfx.thomsonreuters.com/gfx/legaldocs/bdwpkwnyopm/MetaverseWhitePaperv2-compressed.pdf>.2022-2-21.
- [10] HM Treasury.Cryptoasset Promotions – Consultation (July 2020)[EB/OL].[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/902891/Cryptoasset\\_promotions\\_consultation.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902891/Cryptoasset_promotions_consultation.pdf), 2022-2-10.
- [11] CSA Staff Notice 51-363: Observations on Disclosure by Crypto Assets Reporting Issuers (11 March 2021)[EB/OL].  
[https://www.osc.ca/sites/default/files/2021-03/csa\\_20210311\\_51-363\\_observations-disclosure-crypto-asset.pdf](https://www.osc.ca/sites/default/files/2021-03/csa_20210311_51-363_observations-disclosure-crypto-asset.pdf), 2022-2-10.
- [12] Cryptoassets Taskforce: Final

- Report[EB/OL].[www.gov.uk/government/publications](http://www.gov.uk/government/publications), 2022-2-8.
- [13]PS19/22 Policy Statement: Guidance on Cryptoassets[EB/OL].<https://www.fca.org.uk/publication/policy/ps19-22.pdf>, 2022-2-9.
- [14]CSA Staff Notice 51-363: Observations on Disclosure by Crypto Assets Reporting Issuers (11 March 2021)[EB/OL].[https://www.osc.ca/sites/default/files/2021-03/csa\\_20210311\\_51-363\\_observations-disclosure-crypto-asset.pdf](https://www.osc.ca/sites/default/files/2021-03/csa_20210311_51-363_observations-disclosure-crypto-asset.pdf).2022-2-10.
- [15] 京东数科.2020 京东区块链技术实践白皮书 [EB/OL].[http://www.chuangze.cn/third\\_down.asp?txtid=2982](http://www.chuangze.cn/third_down.asp?txtid=2982), 2022-1-21.
- [16]陈丽珊.2021 年全球区块链投融资报告 [EB/OL].[https://mp.weixin.qq.com/s?\\_\\_biz=MzA3NjE4NjQ4NA==&mid=2650583777&idx=1&sn=3120f1d0a72de55d56eb295c8078f020&chksm=876d04fab01a8dec28a7483673d00591b62145387211233f7e327c9ff8324a87ebf00ac4252&scene=21#wechat\\_redirect](https://mp.weixin.qq.com/s?__biz=MzA3NjE4NjQ4NA==&mid=2650583777&idx=1&sn=3120f1d0a72de55d56eb295c8078f020&chksm=876d04fab01a8dec28a7483673d00591b62145387211233f7e327c9ff8324a87ebf00ac4252&scene=21#wechat_redirect).2022-3-13.