Dispute Settlement 争议解决, 2025, 11(11), 136-146
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.1111354

Hans汉斯

区块链证据的法律风险及控制

许莲成

湖北大学法学院，湖北 武汉

收稿日期：2025年10月11日；录用日期：2025年11月3日；发布日期：2025年11月13日

摘　要

区块链证据由于其自身优势，将在各部门法领域实现更加广泛的适用。但是，区块链自身具备的匿名性、不可篡改性、公开透明性为其带来巨大优势的同时，也造成了区块链证据取证困难、区块链犯罪频发、遗忘权和隐私权受侵害等法律风险；对此应采取相应风险控制手段，如加强区块链犯罪立法、加强主体隐私权和被遗忘权保护、完善区块链运用的法律监管制度等措施，以促进区块链证据的法律适用进程。

关键词

区块链证据，法律风险，风险控制

Research on Legal Risks and Regulation Method of the Blockchain Evidence

Liancheng Xu

Law School, Hubei University, Wuhan Hubei

Received: October 11, 2025; accepted: November 3, 2025; published: November 13, 2025

Abstract

The blockchain evidence, based on the blockchain technology, has a bright future in applying to different department law. The development of blockchain evidence in legal area is irresistible. However, as the traits of blockchain itself such as anonymous, unchangeable, unalterable, transparent have brought enormous advantages, it simultaneously has the potential to bring legal risks. for example, it might cause blockchain crimes, contradiction with the right to be forgotten, invade of the personal privacy and so on. In that case, we should take relevant measures to decrease and control the legal risks of blockchain evidence. For example, protecting the right of privacy, monitoring the operation of the blockchain evidence, establishing punishment measures to blockchain crimes, completing the procedure rules of the application of blockchain evidence, and so on, these methods will promote the application for the blockchain evidence in the future.

文章引用: 许莲成. 区块链证据的法律风险及控制[J]. 争议解决, 2025, 11(11): 136-146.
DOI: 10.12677/ds.2025.1111354

Keywords

Blockchain, Legal Risks, Control Methods

1. 引言

在社会秩序维持方面，法律是主体，技术是补充。这一哲理适用于对区块链技术证据的判断。技术本身的安全具有极大的不确定性，法律在处理新兴技术与社会关系的过程中不可或缺，因此区块链技术必须加以法律手段以控制其风险。

区块链技术下产生的各种证据并非完美无瑕，其存在诸多法律风险，如区块链技术本身具有的匿名性、不公开性使得区块链证据来源的审查、可信度的审查难度加大；此外，由于区块链去中心化、匿名性的特征易被不法分子加以利用，依托于区块链的跨国违法犯罪行为频发也是未来区块链相关立法、执法、司法方面需要应对的关键问题；区块链并非万能之匙，在知识产权领域、信息安全领域，链上信息的证据若在上链之初就为虚假或无著作权价值，此时区块链具有的不可篡改性可能造成知识产权泛滥、信息垃圾堆砌的局面，还有可能导致信息主体遗忘权、隐私权受到侵害的局面。对此我国应采取相应措施以控制区块链证据法律风险。

2. 区块链证据概述

(一) 区块链的概念和特征

(1) 区块链的概念

区块链是一种能够实现数据一致存储、难以篡改、防止抵赖的分布式账本技术(Distributed Ledger Technology) [1]。换而言之，区块链(Blockchain/Block Chain)是一种由多方共同维护，将数据区块以时间顺序相连的方式组合成的，并以密码学方式保证不可编辑和不可伪造的分布式数据库[2]。区块链依赖于分布式数据存储、点对点传输、共识机制、加密算法等计算机技术，其本身是一系列使用密码学而产生的互相关联的数据块。不需要借助任何其他的软件或平台就可以完成价值转移。

(2) 区块链的特征

1) 去中心化、去信任化

区块链所有节点权利义务对等，使得其不需要依赖第三方就能进行交易——即区块链技术可以实现无中介的交易。但是第三方权威机构的缺乏是导致区块链证据的重要隐患之一：区块链的去中心化可能导致国家、政府职能的弱化，此外，去中心化并非意味着区块链证据绝无可能出错，因此，中立的监管机构的存在仍是必要的。

2) 匿名性

隐秘性作为区块链的主要特征之一，有利于数据、隐私的存储和保护。但是区块链具有的匿名性在使交易更具有自由化的同时，也为违法犯罪活动提供了“隐身衣”。此外，就目前看来，区块链技术由于其自身还处于发展的初期阶段，其匿名性并不绝对，被黑客攻陷后存在破除匿名性特征的风险。

3) 不可篡改性

区块链记录的账本数据不可随意修改，由此避免了账目作假和重复支付等问题的出现。但同时区块

链不可编辑、不可篡改的特性不利于对于错误的修正和主体信息的删除。

4) 公开透明性

区块链公开透明的特性主要针对链上数据的公开透明，每一节点都记录和表达全数据库的信息，只需有对应密钥即可读取。但公开透明的特性使得信息主体的隐私权处于极大风险之中。

区块链技术为保证系统安全性及可验证性需要公开账本内容，导致恶意节点能够获取所有账户信息，通过聚类技术分析账本信息可以窥探区块链匿名账户与现实用户之间的身份关联关系。目前，数据隐私泄露已成为区块链及其衍生项目所面临的潜在问题[3]。恶意攻击者可以通过网络中安全性较为薄弱的节点监听智能合约的执行情况，窃取用户隐私信息等。

(二) 区块链的固有缺陷

区块链的固有特征导致其固有缺陷，区块链技术自身具备的特性，既是其优势，也是其带来法律风险的原因。首先，匿名性意味着用户的身份信息具有隐匿性，当非法用户利用区块链技术进行犯罪时，这一特性使得侦查机关对于犯罪主体的信息难以查找；此外，现有区块链技术的匿名性并不能得到完美实现，由于技术的不成熟，区块链的匿名性暂且无法完全实现，黑客恶意攻击时候，区块链宣称的匿名性有极大可能被获取，由此导致用户的个人信息泄露。其次，不可篡改性意味着信息数据一旦上链即永久存续，这一特性使用户无法有选择地删除个人信息，对被遗忘权存在一定程度的侵害。再者，公开透明性这一特性与匿名性存在一定的对立关系，用户信息在处于隐匿状态的同时，存在与链上每一个节点之中，这一机制同样可能造成个人信息的泄露。最后，去中心化的特性导致部分学者认为区块链技术的应用可以消除政府的信用背书和执法机构的监督管理，但笔者认为去中心化的特性并不意味着去中心化的运营，在区块链的运用过程中，政府的信用背书和依法监管不可或缺，因为依法监管是保证每一项新技术不产生对社会不利影响、保证技术灵活运用的重要支撑。

(三) 区块链证据适用的现实意义

对区块链技术为依托产生的区块链证据加以运用，是因为其潜在的巨大优势，区块链证据可能为各部门法律施行带来革命性创新。首先，在证据法领域，区块链证据有利于克服传统电子证据的缺陷；基于区块链技术的电子证据存证实践，可缓解电子证据原件困局，跨越中心化存证易篡改、难认定障碍，将当事人、法院、存证平台、相关数据提供方融合在一个司法证据系统内，形成数据流转的安全闭环，真正实现存证有保障、取证有效率、示证能感知、认证可量化。区块链证据引入证据法中，有利于丰富传统证据种类，改变纸本的电子证据认证程序繁琐的现状，对我国现有证据法律制度具有巨大的创新意义；此外，区块链证据中的智能合约，有可能改革合同订立的方式，智能合约立即执行、不可篡改的特点，对我国现有合同法律制度提出了挑战；区块链证据对于权利的登记和确定具有极大的便利性，对于知识产权、不动产等的认定具有创新意义。第二，在执行过程中，区块链证据有利于帮助法官查明事实，提升司法审判的可信度；区块链系统对智能合约具有执行的功能，当智能合约条件满足时，区块链系统将自动强制执行智能合约，这有利于解决诉讼过程中的执行难问题[4]。第三，在知识产权法领域，区块链证据有利于著作权、专利商标的确权与保护；文学艺术作品等已经创作上链之后，因区块链特性而无法被篡改，有利于作品的存续和权利保护。第四，在国际经济法领域，区块链证据可能促进新型国际支付方式的产生与运用。区块链技术应用于国际支付，可帮助运用主体降低成本，简化流程，大幅削减原有复杂的体系，提高资源分配和人才利用的效率，促进资金融通；对企业来说，可减缓其资金压力，更高效的对接厂商和客户；对市场来说，创新和创造的源泉充分涌流一直是其追求的目标，区块链的应用可激发市场活性。

总结：区块链证据之所以应当与法律适用各方面相结合，是因为其本身具有的强大优势，区块链技术证据的法律适用势不可挡，因此我们更应当对其潜在法律风险和控制手段进行研究。但同时，区块链

技术自身具备的特性，既是其优势，也是其带来法律风险的原因，详见表 1。

Table 1. Advantages and risks caused by the inherent characteristics of blockchain
表 1. 区块链固有特征导致的优势及风险

优势		区块链的特征		导致的风险
交易方便		去中心化		监管缺位
保护隐私	←	匿名性	→	犯罪溯源难
存证固证		不可篡改性		被遗忘权受侵害
信息流通		公开透明性		隐私权问题

3. 区块链证据的法律风险

区块链证据自身特性既为其带来巨大运用优势，同时也带来巨大法律风险，如区块链证据可能导致掩饰隐瞒犯罪所得、犯罪所得收益罪、破坏金融监管秩序犯罪、金融诈骗犯罪、逃汇罪；还可能导致公民隐私权、被遗忘权受侵害的局面；在调查取证环节，区块链证据具有取证困难的风险；其不可篡改的特征还可能造成知识产权泛滥且质量低下、信息垃圾堆砌的局面等。目前区块链证据的法律监管制度存在较多漏洞，涉及区块链金融的具体法律法规仅有《电子银行业务管理办法》《关于防范比特币风险的通知》《促进互联网金融健康发展的指导意见》等少数法规，且多以规章或规范性文件形式出现，尚且未达到全面有效的法律监管效果[5]。

(一) 区块链证据取证难

公钥、私钥的机制设置将使交易内容难以查明，区块链技术能够规避时间与地域的局限，为不法分子掩饰不法收入提供了途径和便利。区块链私密性会造成调取区块链证据较为困难、司法侦查过程中难以查找违法犯罪主体等问题。区块存储信息的保密性使得监管机关难以直接对交易活动进行审查和监管，匿名性意味着在开展监管、侦查工作时难以将用户与信息相对应，造成可能无法及时追踪到作案人的局面。此外，在合同法领域，当匿名智能合约产生法律纠纷时，难以查找出对方当事人。

(二) 不可篡改性致使遗忘权受侵害

被遗忘权[1]顾名思义即“被遗忘的权利”，是 GDPR 在被修正后增加的一种新型权利。“被遗忘权”是指：数据主体有要求数据平台及时删除关于其个人信息、数据的权利[6]。有学者认为，被遗忘权是指信息主体对已经发布在网络上的有关自身不恰当的、不相关的、过时的信息且可能会对该信息主体的名誉、荣誉造成不良影响时，要求信息控制者对相关信息予以删除的权利，属于人格权的一种[7]。

区块链的不可篡改性与被遗忘权有一定冲突：区块链信息不可编辑导致上链数据被锁定，当信息主体想遗忘而他人对该信息想记忆时，二者产生冲突时运用一般价值平衡理念难以适当解决；在出现信息输入有误的情形时，其不可篡改、不可编辑的特性造成错误和瑕疵无法被修改纠正的局面；若黑客等不法分子将国家秘密、商业秘密、谣言、诽谤、色情、个人隐私等非法信息编写入区块链，将无法直接对这些信息进行修改删除[8]，如 2013 年比特币区块链数据被发现嵌入非法色情信息[2]；美联储前主席伯南克的画像恶作剧被放置于区块链数据库中至今无法删除[3]；此外，在区块链智能合约中，合同条款一旦被记录在区块链中可以被系统自动执行且无法逆转，若合同本身是法律评价角度上的无效合同，双方当事人约定违法事项时，也不影响智能合约的执行，这对《合同法》等民事法律体系带来了巨大挑战。

[1]《欧盟数据保护通用条例》第 17 条。
[2]CNN 新闻 10 月 20 日的报道，则披露了执法部门是如何通过追踪比特币交易，顺藤摸瓜地追踪到遍布全球的该网站用户。多国联合行动捣毁了全球最大的暗网儿童色情网站“欢迎访问视频”(Welcome To Video)。
[3]本·伯南克(Ben Shalom Bernanke)，美国经济学家，前美国联邦储备委员会主席。

(三) 知识产权质量低下和信息垃圾堆砌

由于区块链不可篡改、不可编辑的特性，文学艺术作品等一旦上链，即产生记录，可以作为知识产权的凭证。然而随着区块链的普及，文学艺术作品、商标、专利的产生将会越来越多，因为上链内容的即时性和快捷性，知识产权的记录和登记数量将会十分庞大，而由于区块链技术仅有上链记录机制而缺乏相应审查程序和制度，必然会导致低质量知识产权作品泛滥、无意义登记的局面，反而不利于高质量知识产权的确权与保护。

2020 年 5 月 4 日，商标审判和上诉委员会裁定，石油和天然气公司不能向美国专利商标局注册“区块链钻井”商标，因为该短语“仅仅是对钻井技术的描述”[4]。由此可见，现实生活中，随意利用区块链证据申请知识产权保护的行为逐渐增多，这可能导致大量重复的权利申报，不利于知识产权的高质量保护。

(四) 公开透明性特征导致隐私泄露风险

根据中国区块链技术产业和发展论坛对区块链隐私的标准定义，隐私是指仅与个人利益相关且不需要强制公开的个人信息及个人领域，是指特性个人对信息和领域的秘而不宣、不愿第三人探知和干涉的事实和行为[5]。区块链公开性的特征极大程度增加个人信息泄露的风险，不仅有可能侵犯个人隐私权，更严重时不利于国家信息安全。

然而传统的隐私保护技术并不适用于区块链技术中，区块链数据存储在分散的节点，各节点众多且地位平等，没有中心化的监督和管控，难以针对分散的各个节点采取同等的监控，黑客很容易选取并攻陷较为薄弱的部分节点以达到入侵整个区块链数据库的目的。由此可见，区块链公开透明的特性在一定程度上与匿名性的特征是相悖的，因此在保护用户个人隐私的同时做到信息公开透明二者之间，需要法律的规范来保障这一平衡。

(五) 区块链证据安全性存疑——匿名性使违法犯罪活动溯源难

区块链技术为非法侵入计算机信息系统罪等新型计算机犯罪[6]、盗窃罪、传销、非法融资、诈骗等违法犯罪行为提供了反侦查的平台[9]，依托于区块链技术的虚拟货币的极大程度流通使得非法犯罪活动空间上升到全新高度，跨境犯罪将更难以溯源和调查，打击罪犯难度极大程度增加。

(1) 盗窃风险

2018 年日本虚拟货币交易所 Coincheck 被盗总值 5.3 亿美元虚拟货币；韩国最大虚拟货币平台 Bithumb 被盗总计 350 亿韩元比特币；根据网络安全公司黑炭 Carbon Black 于 2018 年 6 月发布的研究报告《暗网上的加密数字货币淘金热》：2018 年上半年全世界被盗的虚拟货币价值达 11 亿美元，虚拟货币交易平台是最易被盗窃的目标[10]。

(2) 网络传销

河南郑州 GBC 案[7]、陕西“消费时代 DBTC”大唐币案[8]、江苏“天合积分”案等极具相似性，皆属于利用区块链进行网络传销的犯罪[11]，可见利用区块链名义开展网络传销的行为十分猖獗。在河南郑州 GBC 案件中，范某经介绍加入 GBC 网络平台，以买卖虚拟货币可以获得高额收益为名义，诱使被害人持续投入资金、继续发展人员，其行为严重扰乱经济社会秩序，构成组织、领导传销活动罪。

(3) 集资、诈骗风险

据不完全统计，自 2016 年来，中国裁判文书网上公布的以虚拟货币为幌子的传销诈骗案件多达 180

[4]HughesWESTLAW 知识产权每日简报，2020，IPDBRF，0048.
[5]China Institute of Electronic Technology Standardization (2021) China Block Chain Technology Development Forum. http://www.cbdforum.cn/bcweb/
[6]例如非法获取计算机信息系统数据罪、破坏计算机信息系统罪、非法控制计算机信息系统罪等。
[7](2019)豫 0105 刑初 102 号审理法院：河南省郑州市金水区人民法院。
[8]全国首例“区块链”特大网络传销案。犯罪分子建立“消费时代”(DBTC)网络平台，以每枚 3 元的价格在“消费时代”(DBTC)网络平台销售虚拟的“大唐币”，并自行操纵升值幅度，通过网络发展下线。

余件，涉案总金额高达上千亿元人民币，其中，较为典型的浙江“深蓝积分”案[9]中，余某、熊某飞、熊某程、朱某聘请他人制作虚假宣传资料，通过微信宣传拉会员投资，让会员通过公司网络平台以高价购买产品，向会员赠送等值“深蓝积分”，并承诺短期内可获得高额回报，还可以投资购买公司对接外网平台的虚拟币，通过虚拟币的上涨获取更高额收益，而虚拟币的涨跌实则熊某飞通过后台操纵。余某等人短期内发展了全国近两千多名会员注册了九千多个账号，非法集资款项达到5938万元，犯罪行为人利用区块链技术进行犯罪活动，向不特定公众吸收或者变相吸收资金，危害金融秩序，其行为构成集资诈骗罪，还可能构成非法吸收公众存款罪。

福建“金砖储备资产货币”诈骗案[10]中，欧阳某某向被害人章某宣传“金砖储备资产货币”项目，谎称能够帮助章某投资该项目，诱使章某陆续向其指定的微信账号转账。欧阳某某收取上述款项后，通过ATM柜员机取款、转账、第三方支付及柜台取现等方式，将其中106万元分批次全部转出，并分散存入其本人或由其控制使用的银行账户，后用于个人开支，共造成章某经济损失数额较大，构成诈骗罪。

(4) 作为非法支付方式

依托区块链平台进行非法活动的佣金或报酬支付，区块链证据具有被用于其他违法犯罪活动的法律风险，例如通过区块链支付方式购买淫秽录像淫秽物品等，或卖方传播淫秽物品牟利且要求通过区块链平台支付、通过区块链行贿受贿、甚至雇凶买杀等。此外，美国兰德公司表明2015年发布的研究报告《虚拟货币对国家安全的影响：非国家实体部署可能性剖析》指出：恐怖组织利用虚拟货币提升其政治与经济实力具有较大的可能性[10]。

(5) 垄断风险

美国佛罗里达州地方法院，美国联合公司诉比特大陆公司案：依赖于可扩展区块链的加密货币技术的开发商对加密货币挖掘服务器的运营商，购买和销售加密货币的公司的创始人，加密货币交易所的运营商以及加密货币软件开发商提起了反垄断诉讼，指控他们通过控制其区块链来限制区块大小，并寻求禁令救济来操纵加密货币的价值。被告因未提出索赔而驳回，采矿服务器运营商因缺乏属人管辖权而被解雇，原告因进行管辖权发现而请求许可[11]。

(六) 区块链证据离不开中心化监管

区块链去中心化特性并不代表去中心化运用，区块链证据仍需官方的监管作为背书。若全然放弃政府信用背书的监管体系，完全依赖区块链证据自身去中心化的运营，区块链系统中的用户个人信息将可能被不法分子所侵犯。

根据市场经济运行规律。市场经济健康稳健运行，需要有效市场与有为政府相结合，国家宏观调控在克服市场固有缺陷方面的作用不可或缺。去中心化和自治性特征淡化了国家监管，对现存体制造成重大冲击，数字货币可能对国家货币发行权造成冲击，可能削弱央行调控经济的能力[12]；此外，监管部门尚未制定相应法律制度，增加市场主体法律风险。区块链证据要加以现实化，如房产的公证仍需要政府背书作为权威认证。因此区块链证据映射于现实生活中，仍需建立起政府为中心的、官方背书的区块链债权债务公示和资产公证体系。即使是具有去中心化特性的区块链，也需要政府部门加以监管和规制。

(七) 其他风险

区块链自身固有缺陷如容量不足、链上节点仍存在被攻陷可能等技术性缺陷同样是法律风险的重要来源，由此造成公众对区块链技术及其衍生产品明显信心不足，普遍表现为担忧无法兑现、价值起伏、区块链犯罪等。因此在技术层面也应当对此进行完善。

[9](2018)浙0782刑初2017号审理法院：浙江省义乌市人民法院。
[10](2019)闽09刑终172号审理法院：福建省宁德市中级人民法院。
[11]BITMAIN, INC., Roger Ver, Bitmain Technologies Ltd., Jihan Wu, Payward Ventures, Inc. d/b/a Kraken, Jesse Powell, Shammah Chancellor and Jason Cox, Defendants. CASE NO. 18-cv-25106-WILLIAMS/MCALILEY, Signed 03/31/2021.

上海 IDAX 案件[12]中，吴某、邓某发现全球“区块链”数字资产交易平台 IDAX 存在漏洞后，在平台上攻击该漏洞，造成 IDAX 平台的技术维护方某信息科技有限公司直接经济损失 4 万元。吴某、邓某二人违反刑法，对区块链平台中的数据进行非法操作，二人行为构成破坏计算机信息系统罪。

4. 域外区块链证据法律风险的控制经验及启示

(一) 保护遗忘权

欧盟最先提出“被遗忘权”的概念：“任何公民可以在其个人数据不再需要时提出删除要求”；随后在《数据保护指令》中首次书面写入“被遗忘权”；《欧盟数据保护通用条例》以欧盟法律的形式正式确立了被遗忘权，细化了被遗忘权的具体行使方式及限制条件。被遗忘权的具体适用最初是在 2014 年欧盟法院对“干萨雷斯诉谷歌”案件中，受诉法院作出的判决支持了干萨雷斯关于要求谷歌删除其关于拍卖信息的链接，至此，被遗忘权在欧盟通过司法判例正式确认[13]。

(二) 区块链匿名性犯罪的应对经验

到目前为止，仅有两个美国联邦地区法院解决了个人是否在虚拟货币兑换处的比特币交易记录中具体隐私利益的问题，分别是 Zietzke 诉美国(Zietzke II)[13]和 Zietzke 诉美国(Zietzke I)[14]。在每起案件中，地区法院都认为被告在其比特币交易记录中没有隐私利益的问题，因为交易是与第三方虚拟货币交易所共享的。美国第五巡回上诉法院认为存储在比特币区块链中的信息没有隐私利益，根据 Gratkowski 的观点：联邦特工使用强大而复杂的软件来分析比特币区块链没有侵犯宪法保护的区域，因为区块链上的信息没有宪法隐私利益。

在 United States 诉 Gratkowski[15]案件中，被告被判犯有接受儿童色情制品和访问网站意图观看儿童色情制品罪，被告提出上诉，反对驳回他关于隐瞒通过搜查令获得的证据的动议。上诉法院提出：被告使用虚拟货币从儿童色情网站购买和下载材料，对他位于区块链上的信息缺乏隐私权益，因此联邦特工使用软件来分析区块链并识别从该网站下载材料的用户并不违反第四修正案对不合理搜索的保护。由此可见，根据美国联邦法院观点，在区块链上的个人信息是记录违法犯罪信息时，并不受到保护，不可以侵犯隐私权作为抗辩。

(三) 启示

为促进区块链证据合法合规适用，从上层建筑的角度对区块链证据法律风险进行规制具有必要性。国家应完善区块链证据立法，目前规制区块链证据适用的法律法规较少，只在民法典、合同法中一笔带过，而针对性的专门法寥寥无几，且多为法律强制力较低的其他规范性文件。在区块链技术深入发展的同时，我们需要解决国家管理引导仍存在不足的问题。一方面，要发挥法律的底线作用，明确区块链法律主体及其相关权利义务和责任，最大限度降低可能发生的风险，补足法律漏洞；另一方面，要发挥法规的灵活性，积极改进相关制度政策，由政府主导，设立区块链发展规划和前沿技术领域的负面清单，从法律层面构建“安全防火墙”。

控制区块链证据的法律风险，不仅要加强立法执法司法，还要完善区块链监督审查法律制度。对于区块链可能侵害被遗忘权、隐私权的法律风险，应当加强隐私权、被遗忘权的保护方面立法并借鉴欧盟判例；对于利用区块链证据实施的违法犯罪行为，可以出台信息强制批露制度、监管措施，还可以设立类似于美国区块链特别工作组的技术性人才岗位加以侦查和打击；此外，各国针对区块链进行监管法律制度还有：纽约州金融服务局的 Bit License 规则、Fin CEN 对数字货币的监管制度等，这些规则可作为

[12](2019)沪 0120 刑初 435 号审理法院：上海市奉贤区人民法院。
[13]第 19-cv-03761 号，2020 年 WL264394 (N.D.Cal.2020 年 1 月 17 日)。
[14]426F.Supp.3d758 (W.D.Wash.2019).
[15]964F.3d307,310 (5thCir.2020).

我国监督制度的参考；对于利用区块链进行传销的犯罪行为的，应当加大对区块链技术及相关法律风险的普及程度，加深群众对区块链的理解，通过立法普法的形式，使得群众对利用区块链传销的行为具有进一步认识，以从根源上减少和杜绝利用区块链进行传销、诈骗的犯罪发生；针对区块链平台可能存在的无设立资格、违法投资行为、发布不实信息、投资者维权难度增大等法律风险，实施对应的惩戒和监管措施，实现政府的中心化管理和监控。

总的来说，即针对区块链不同法律风险，制定风险防范和风险规制的法律监管体系，建立规范的区块链适用法则，依据法律法规加以监管，维护信息安全与网络技术安全，依托法律监管体系，构建全方位监测、打击犯罪的法律管理制度。

5. 法律风险的控制措施

(一) 人格权的保护

(1) 隐私权的保护

对于区块链上的隐私权，笔者认为应当采用辩证的观点，对侵犯国家、社会、公众利益的区块链上信息，应当予以禁止和处罚，而对于没有社会危害性的个人信息和个人领域，应当予以保护，应当杜绝一刀切的武断做法。

(2) 被遗忘权的保护

我国首例“被遗忘权[16]”案是“任甲玉诉百度”一案，这是被遗忘权首次在我国司法案例中出现[14]。本案中，任甲玉曾任职于无锡某公司，在与该公司解除劳动关系后，任甲玉通过网络搜索自己名字，发现有自己和该公司的关联词条出现。任某认为该词条对自身声誉产生不良影响，遂向法院主张其“被遗忘权”，要求网页运营者删除其与该公司相关的关联词条。法院经审理认为原告主张的被遗忘权不具有受法律保护的必要性，并非侵权保护的正当权益，因此驳回任某的诉讼请求。[17]而笔者认为，随着区块链证据的普及和发展，我国应当重视被遗忘权的保护。被遗忘权最初产生是因为想要改过自新的犯罪分子，在日常生活中，公民往往希望公开有案底者的犯罪记录与信息，而改过自新的犯罪分子可能具有被遗忘的意愿，在司法实践中，如何平衡这一冲突具有较大难度，在完善对犯罪分子心理认证、社会危害性检查的同时，也要保护真正有改过自新愿望的有案底者。

(二) 完善区块链犯罪刑事处罚法律体系

区块链犯罪具有复杂性，利用区块链证据进行犯罪的行为往往导致数罪，如破坏计算机信息系统罪与传销罪并行、诈骗罪与非法集资罪并行等，笔者认为，认定非法控制计算机信息系统罪、破坏计算机信息系统罪、非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪等的重合交叉以及区分问题，具有一定的难度和复杂性，因此应当加强区块链犯罪的刑法领域研究，对区块链犯罪的行为进行准确地界定区分以达到准确定罪、精准处罚的目的。区块链证据的发展具有快速性，立法应当与时俱进，根据社会政治经济适当调整区块链犯罪法律体系，适应区块链时代的快速发展。

吸收各地打击区块链犯罪的法律经验：CoinHolmes 协助警方打击利用数字货币为电信诈骗洗钱的团伙[18]。电信诈骗团伙为了将非法所得的资金洗白，第一步先将黑币变为数字货币，利用多个假身份在 Huobi 交易所开户，并使用法定货币在交易所的场外交易平台购买 USDT，第二步将数字货币洗白为法定货币，并将所有洗白后的货币转移到平台外，最终转为“合法”货币。CoinHolmes 专门研发反洗钱系统，通过“关联交易分析”、主体识别，准确识别币商的身份，定位到相关币商信息，帮助警方抓获犯罪嫌疑人。

[16]我国《侵权责任法》规定网络用户利用网络服务实施侵权行为的，被侵权人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施，网络服务提供者接到通知后未采取必要措施的就损害扩大部分与网络用户承担连带责任。
[17]北京一中院(2015)一中民终字第 09558 号判决书。
[18]浙公网安备 33010802010441 号|浙 ICP 备 18022592 号-2|2022COINHOLMES|。

在刑事侦查过程中，执法机构应当加强与科技企业合作，联手打击犯罪活动。

为了避免区块链变成犯罪链，应当对其进行法治引导和有效的监测，利用法治的方法对区块链犯罪实施干预，以降低和控制其法律风险，实现合法合规的区块链证据适用。各国执法机构和监管当局加强国际司法合作，联合打击跨境区块链洗钱、逃汇等犯罪行为，及时查找、抓捕跨境犯罪分子，协同对不法分子采取资产冻结等措施；还可以与知名国际反洗钱和反恐融资的国际组织——FATF 进行合作，深度交流情报信息，学习共享反区块链犯罪的经验。

(三) 实行强制信息批露制度以实现中心化监管

区块链犯罪进行交易必须要经过区块链交易平台，而此交易平台作为去中心化的第三方平台，一般对代币发行方的项目是否真实的事实性不作任何审查和担保，或者即使有一定的担保，也存在担保不全面和无强制执行力的问题。因此，明确区块链数字货币金融交易的平台责任是监管的前提条件，笔者认为对于交易平台的监管可以实行属地管辖，在我国境内的交易平台必须及时将数据介入监管部门，监管部门对于异常数据、不真实数据可以直接采取相关措施。

当前区块链交易平台由于其去中心化的特性，导致其存在诸多不规范的行为，如故意隐瞒融资风险、夸大项目实际情况进行虚假宣传、不公开资金用途信息等，这导致了我国出现非法集资、传销等犯罪行为的逐渐增多。因此，对于中国境内的各种区块链证据平台及法人，有金融业务的，监管部门可以采取强制信息批露制度，要求区块链公司必须提供详细准确的项目资料，在项目实施过程中，项目发起人应当定期公开信息，项目资金必须专款专用，使每一笔资金的走向及时向投资者公开。

要完善区块链证据监督管理法律制度，出台切实可行的针对性区块链证据专用法，设置区块链运行规则和相应的监管及惩罚制度，坚决打击利用区块链证据进行投机的行为，设立中心化的监管机构全方位、全过程监督区块链交易活动，严厉处罚区块链违法犯罪行为，为区块链证据的适用提供具有政府官方背书的合法环境。去中心化的技术不等于不需要任何作为“中心”的监管机构，政府的公信部门应与相关高校、智库和科技企业联合，定期以政府名义出台我国区块链证据发展的风险报告，应当包括且不限于区块链犯罪情况、加密货币法律风险等，加强政府的中心化监管，才能使我国更加稳健地应对区块链技术的风险挑战。

建立侦查反应机制，基于现有常见的区块链刑事犯罪的不法用户个人，侦查机关可以制定不同的侦查反应机制，针对诈骗和传销类犯罪，侦查机关在侦查阶段，需要以最快的速度冻结犯罪分子的资金流转渠道，以便进行布控、抓捕，面对犯罪嫌疑人利用区块链证据进行非法集资等犯罪行为的，我国侦查机关可以联合数字货币平台或海外代币交易中心进行联合管控，共同监管、查控大额账户金融交易的资金流向，并由侦查机关掌控监管、控制犯罪所得的权力。

(四) 多重数字签名的身份认证程序

最高人民检察院提出：多重数字签名可以实现区块链参与方的身份认证，有利于打击区块链犯罪。区块链技术虽然可以追溯网络金融犯罪信息，但是其特有的隐名性和跨国存储特点不利于对犯罪分子真实身份信息的锁定和监控，通过引入多重数字签名等身份认证技术标识身份信息，编制有效智能合约代码约束上链记录存储和实名，对涉及大额交易的记录要求境内存储，可以有效应对网络金融犯罪的身份侦查问题，以达到惩治网络金融犯罪的目的。多重数字签名的身份认证程序，在保证区块链证据可追溯的同时，确保了参与者身份的安全性和透视化。

(五) 区块链证据的鉴定审查规则

区块链证据匿名性的特征导致其取证困难的问题，因此，在司法实践中，区块链证据的实际运用程序亟待完善。笔者认为：将匿名用户的区块链证据与用户法律身份相对应，需要完备的区块链证据审查、鉴定制度。此外，区块链证据如何合法取得也是区块链证据在司法适用中的一大难题。在民事审判领域，

杭州互联网法院针对当事人采用区块链技术进行固定证据、存证的合法性认定首开先河：在众多案件中，当事人通过杭州互联网法院司法区块链平台保全了被诉侵权文章，并采用区块链技术储存电子数据的方式证明数据的完整性和真实性 [19]。笔者认为，解决区块链证据取证困难的问题，可以采用制作笔录、全程录像的方式，将电子证据取证的做法类推至区块链证据当中，以提升区块链证据的可信度与合法性。同时辅之以证人证言和专家意见，以确定区块链证据所对应的主体。这种方式解决区块链匿名性导致的犯罪嫌疑人与区块链证据无法相对应的问题。同时，对于区块链证据应当进行更加严格的审查，鉴于区块链证据的复杂性，区块链证据有可能是犯罪嫌疑人故意留存的伪证，在司法适用中，应当完善区块链证据及其反证的效力，以准确地认定具有证据合法效力的定案依据。

(六) 完善国际立法

完善区块链证据的法律风险，应当加强反区块链跨境犯罪的立法完善：在国际经济法领域，应当完善国际税收法律制度，依法规制利用区块链技术逃税的行为，完善国际投资法律制度，监管利用区块链技术衍生的虚拟货币进行投资的行为，将国际数字货币投资向合法方向上引导，坚决打击利用区块链技术的投机行为；完善国际货币金融体系，进一步明确和构建区块链相关货币的地位与法律规制体系；完善国际知识产权制度，规定区块链上知识产权的审核标准和申报制度，杜绝知识产权质量低下的局面。

(七) 其他风险控制措施扩充

研发及完善区块链技术，从技术根源上弥补漏洞，促进区块链技术的更新和完善。目前区块链同态加密技术还不成熟、安全多方计算的隐私保护机制在实际应用中执行效率低下、智能合约无法加密和匿名化限制了其应用，这些技术层面的缺陷亟待完善。

6. 结语

控制区块链法律风险，应当建立成熟完善的区块链技术犯罪风险防控流程，从保护使用者隐私权、被遗忘权、防范和打击区块链犯罪、完善法律监管体系、完善国际立法等方面入手，促进区块链证据的合法发展进程。随着科学技术的日新月异，在区块链证据的法律应用过程将使我国司法改革进程更具有创新力和活力，通过对区块链证据进行全面的、前瞻性的风险控制法律措施，将使得区块链证据的适用逐步普及，为构筑高效、便民的法治社会注入动力。

参考文献

[1] 徐明星, 田颖, 李霁月. 图说区块链[M]. 北京: 中信出版社, 2017.

[2] 刘叶. 商业银行智能支付中的区块链应用研究[D]: [硕士学位论文]. 长春: 吉林财经大学, 2022.

[3] 王晨旭, 程加成, 桑新欣, 李国栋, 管晓宏. 区块链数据隐私保护: 研究现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119.

[4] 甘萌莹. 基于智能合约的“源储网荷”本地能源微网交易模型设计[J]. 通信电源技术, 2018, 35(6): 93-95+98.

[5] 张夏恒. 区块链引发的法律风险及其监管路径研究[J]. 当代经济管理, 2019, 41(4): 79-83.

[6] 田广兰. 大数据时代的数据主体权利及其未决问题——以欧盟《一般数据保护条例为分析对象》[J]. 中国人民大学学报, 2020, 34(6): 131-141.

[7] 张琬. 被遗忘权的制度建构研究[D]: [硕士学位论文]. 济南: 山东大学, 2022.

[8] 周瑞珏. 区块链技术的法律监管探究[J]. 北京邮电大学学报(社会科学版), 2017, 19(3): 39-45.

[9] 李蕤. 侵害公民个人信息犯罪之多重危害与侦查策略[J]. 中国刑警学院学报, 2014(1): 14-18.

[10] 兰立宏. 论虚拟货币的犯罪风险及其防控策略[J]. 南方金融, 2018(10): 33-40.

[19] “深圳市中研普华管理咨询有限公司、杭州华泰一媒文化传媒有限公司侵害作品信息网络传播权纠纷”杭州互联网法院(2019)浙0192民初2324号，浙江省杭州市中级人民法院(2019)浙01民终7668号。

[11] 张庆立. 区块链应用的不法风险与刑事法应对[J]. 东方法学, 2019(3): 72-86.
[12] 刘贞, 张强. 区块链技术在会计行业应用研究[J]. 农村经济与科技, 2020, 31(13): 131-132.
[13] 王红霞, 刘青哲. 《民法典》关于个人信息保护的亮点与适用[J]. 聊城大学学报(社会科学版), 2021(1): 116-122.
[14] 符彦姝. 浅谈大数据时代下的“被遗忘权” [J]. 北京印刷学院学报, 2020, 28(2): 17-20.