

稳定币金融基础设施的法律识别与风险治理

柯 达

摘 要：稳定币金融基础设施是与稳定币相关的所有信息网络设施中，开展稳定币投放、赎回和资金转移业务，且具有系统重要性的支付系统。稳定币支付系统在系统运行者与稳定币发行机构分离的基础上，兼容单一币种的分散流通与不同币种的共同流通，其中的系统运行者与系统参与者均以非准入、非实名方式开展业务活动。现行的金融基础设施法律规范，仅能为应对稳定币支付系统的运行风险与结算风险提供一般规则，无法同时应对该支付系统滋生的洗钱风险。为应对运行风险，我国应建立既存区块链原生通证的国家储备、设置公益节点并鼓励系统运行者线下备案，要求拟发行稳定币的机构选择许可型公链作为稳定币投放、赎回及资金转移的基础设施。为应对结算风险，应细化稳定币支付系统的最终结算时点与最终结算效力，并构建储备资产的风险联动应对机制。为应对洗钱风险，应基于“日常性假名，可疑再识别”规则，确立稳定币发行机构与支付系统运行者的双重反洗钱义务。

关键词：稳定币；金融基础设施；支付系统；区块链；去中心化

〔中图分类号〕D922.28 〔文献标识码〕A 〔文章编号〕2096-6180（2026）03-0137-22

一、问题的提出：稳定币背后金融基础设施的“普罗透斯之脸”

稳定币（stablecoin）是依托区块链技术，通过特定资产、一揽子资产或纯粹算法的支持，维系其价值稳定的一种加密资产。^{〔1〕}基于对稳定币改善跨境支付、提供新经济增长点等潜力的认可，欧盟、美国、中国香港特别行政区等经济体近年来相继颁布稳定币或加密资产法律，以期进一步规范市场交易。与之不同的是，我国内地自2017年以来，对包括稳定币在内的所有加密资产（即

〔作者简介〕柯达，华东政法大学经济法学院副教授，法学博士。

〔基金项目〕贵州省2025年哲学社会科学规划年度重点课题“贵州省新兴行业治理现代化的法治保障研究”（项目批准号：25GZZD53）。

〔1〕 Financial Stability Board, Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations, 2020, p. 5. 按照是否受资产支持或受支持资产类型的差异，稳定币分为锚定法定货币资产的稳定币（即“法币稳定币”）、锚定其他金融资产或商品的稳定币、算法稳定币；由于法币稳定币在市场中占绝对主导地位，下文如无另外说明，“稳定币”均指锚定法定货币资产的法币稳定币。

虚拟货币)采取禁止式监管立场,任何投资活动如违背公序良俗均属无效⁽²⁾;由于稳定币具有极强的跨境流通能力,境外立法势必对我国现行监管带来一定挑战,因此不少业界或学界人士仍主张我国放开稳定币交易活动。然而,稳定币市场的间歇性“狂热”不仅忽视了境外立法深受非法律因素的利益驱动,特别是在鼓励创新与保护消费者之间形成的激烈博弈⁽³⁾;更掩盖了以往稳定币风险事件对金融稳定造成的冲击,如2018年的算法稳定币“Luna”运行崩溃,以及2022年的算法稳定币“Terra”崩盘、法币稳定币“USDC”的突发脱锚。

事实上,造成稳定币风险事件的根本原因,是其背后“金融基础设施”⁽⁴⁾的治理失序,例如没有人对风险事件负最终责任。稳定币的投放、赎回及资金转移,须依赖于以区块链为代表的“信息网络设施”⁽⁵⁾,进而呈现出稳定币发行者与记账者的分离;同时,“现实世界资产”(Real World Asset, RWA)通证化的推进,促使稳定币与其他加密资产或传统金融所依赖的信息网络设施建立起更紧密的互联互通联系。进一步看,稳定币的信息网络设施,在运作表现上较接近法定的金融基础设施范畴,因此采用金融基础设施的治理逻辑,便成了应对稳定币风险的可取选择。金融基础设施更是金融行业乃至整体社会经济正常运转的前提与基础,党的二十届三中全会通过的《中共中央关于进一步全面深化改革推进中国式现代化的决定》提出“建设安全高效的金融基础设施”;我国已在《金融市场基础设施原则》(下称《FMI原则》)的基础上,颁布《金融基础设施监督管理办法》(中国人民银行、中国证监会令〔2025〕第7号),重点强调了风险为本的治理路径;在日趋复杂的国际形势下,我国面临的主权挑战与跨境风险更为突出,我国相关监管部门已表示要“密切跟踪、动态评估境外稳定币的发展”⁽⁶⁾;而最新监管文件增设人民币稳定币的境外管辖规定⁽⁷⁾,表明我国仍然存在可控发展稳定币的空间与构建稳定币监管机制的必要。如何对稳定币金融基础设施进行风险治理,必将成为该监管机制要解决的核心问题。

基于信息网络设施的种类繁杂、重要程度各有差异,稳定币金融基础设施的风险治理问题,可进一步解构为以下两个递进且不可分离的方面:一方面,稳定币所依托的信息网络设施中,哪些属于法定的金融基础设施范畴,哪些仅为普通的信息网络设施;另一方面,若某一信息网络设

(2) 柯达:《虚拟货币“禁止式”监管:法理反思与制度优化》,载《华东政法大学学报》2024年第3期,第138页。

(3) Carlos Cantú, Jon Frost & Thomas M. Noone, *Some Perspectives on the Regulation of Stablecoins*, 87 Law and Contemporary Problems 129, 131 (2025).

(4) 我国现行法将国际上通用的金融市场基础设施称为“金融基础设施”,且其外延宽于金融市场基础设施。为确保本文提出的风险治理建议更具现实可行性,如无另外说明,下文均称为“金融基础设施”。

(5) “信息网络设施”是依托互联网络,开展数据采集、加工、存储、传输、检索等处理的软硬件设备的统称,其包括信息系统、网络设施等,在计算机行业内又被称为“信息基础设施”。但由于何谓“基础”在法律上存在一定争议,因此本文采用“信息网络设施”这一更中性的称谓。参见《计算机信息系统安全保护条例》(国务院令 第588号)第2条、《关键信息基础设施安全保护条例》(工信部联通信〔2024〕165号)第2条。

(6) 《中国宏观审慎管理体系的建设实践与未来演进——中国人民银行行长潘功胜在2025金融街论坛年会上的主题演讲》,载中国人民银行2025年10月27日, <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/5880408/index.html>。

(7) 《中国人民银行、国家发展改革委、工业和信息化部、公安部、市场监管总局、金融监管总局、中国证监会、国家外汇局关于进一步防范和处置虚拟货币等相关风险的通知》(银发〔2026〕42号)。

施被认定为金融基础设施，如何对其主要风险展开治理。目前，法学界主要围绕法律定性、是否要合法化、如何监管三个话题开展稳定币的法律研究，搭建了系统全面的稳定币监管理论框架。⁽⁸⁾其中，学界侧重于研究市场准入、储备资产管理、赎回权保障等“前台”内容，作为“后台”的基础设施治理尚未受到重视，进而不利于区分“稳定币的风险”与“稳定币基础设施的风险”。此外，学界已对区块链金融基础设施开展法律研究⁽⁹⁾，但相关技术原理主要以早期的比特币区块链为依据，尚未充分考虑技术的迭代更新。基于此，笔者先界定何谓法律意义上的稳定币金融基础设施，分析其主要风险，进而讨论现行法律规范能否适用于稳定币金融基础设施，最后提出相应的法律完善建议。

二、稳定币金融基础设施的法律识别

准确识别稳定币背后的金融基础设施范围是风险治理的前提与基础，并可避免因基础设施被“泛化”而徒增治理成本。因此，有必要先梳理稳定币的不同信息网络设施，识别其中哪些属于法定的金融基础设施，并分析其作为金融基础设施的特殊之处。

（一）稳定币“中心化”与“去中心化”信息网络设施的共存机制

稳定币的信息网络设施，为不同阶段的稳定币业务活动提供了“后台”支撑。就主流的稳定币产品而言，与稳定币直接相关的业务活动主要分为四类：其一，投放与赎回。稳定币发行机构在确定技术路线并推广宣传后，直接或间接面向公众发行稳定币，并可开展主动或被动赎回稳定币的业务。其二，资金转移。这是稳定币核心功能的行为展现，持有人将数字钱包中的稳定币转移至他人钱包中，依托“支付即结算”功能实现清偿债务等目的。其三，储备资产管理。向公众吸收的资金成为稳定币的储备资产，稳定币发行机构自行或委托第三方利用储备资产开展投资，以期实现储备资产的保值增值。此外，加密资产交易所、钱包服务商、金融机构等加密市场服务提供商，亦为公众提供稳定币的币种兑换、钱包开立与资金托管等服务。⁽¹⁰⁾

从行为表象上看，稳定币的业务活动与中央银行发行的法定货币或商业银行提供的银行存款高度相似，即包括发行、资金结算、调控等行为。但是，稳定币作为数字时代的新型数字资产，其业务活动实质体现为数据处理的过程；同时，稳定币业务活动又高度依赖于区块链技术，因此需要从信息网络设施视角进一步分析其运行机制。这些信息网络设施可以分为两类。

一类是开展稳定币投放、赎回、资金结算，以区块链为代表的“去中心化”信息网络设施。就主流稳定币而言，该类信息网络设施是支持智能合约可编程功能的“公共区块链”（下称公链）。

（8）邓建鹏、罗敬蔚：《论稳定币的本质属性、运行方式及风险防控》，载《新疆师范大学学报（哲学社会科学版）》2026年第1期，第114页。

（9）郑彧：《金融市场基础设施的历史进路及其监管应对》，载《国家检察官学院学报》2022年第4期，第168页；李晓楠：《区块链金融基础设施监管研究》，载《金融监管研究》2020年第10期，第85页。

（10）G7 Working Group on Stablecoins, Investigating the Impact of Global Stablecoins, 2019, p. 24.

该公链由专门的技术开发者设计，社会上的任何主体作为“节点”（node）自由加入参与区块链的运行，运行活动包括发行区块链的原生通证（native token）、验证链上数据、决定技术升级等。更重要的是，该区块链允许任何主体在链上另行加载具有自动执行功能的智能合约，稳定币便属于智能合约应用后的产物。当智能合约事先拟定的条件被满足时，区块链中的智能合约会自动投放或赎回稳定币，并记录稳定币相关交易数据，这些交易数据经节点验证后同样具有难以篡改的效果。^{〔11〕}

另一类是开展储备资产管理、不同币种兑换等业务活动的“中心化”信息网络设施。就储备资产管理而言，为实现稳定币币值稳定而投资的高流动性法币资产，均由传统的政府部门或金融机构发行，并经专门场所组织交易、托管或结算。受制于部门利益、技术水平等因素，这些储备资产的交易、托管或结算未依托于区块链，而是由分散在不同中心化信息网络设施开展。^{〔12〕}就不同稳定币或加密资产之间的兑换而言，目前“中心化交易所”在组织该类活动中占主导地位，如果用户在交易所开设专门的数字钱包，通过该钱包进行的交易事实上依托于交易所另行设立并运营的中心化信息网络设施，相关交易往往速度更快、成本更低。^{〔13〕}虽然目前有部分“去中心化交易所”在尝试组织不同稳定币或其他加密资产之间的兑换，但其市场规模极小，重要性远不及中心化交易所。尽管“跨链协议”“公证人机制”等技术手段也可以实现不同稳定币或加密资产所依托的公链之间的价值转移，但其仍须依赖于第三方的主观判断或干预控制，进而会引发额外的信用或运行风险^{〔14〕}，因此该类活动仍主要依托于中心化设施。

稳定币的信息网络设施之所以呈现中心化与去中心化的统合共存，是因为加密市场难以与国家主权绝对“割裂”。比特币所依托的区块链是最早的区块链技术实践，其在金融危机爆发、公众对传统法币体系不满的背景下诞生，以试图摆脱国家对货币的中心化控制。但由于比特币的市场价格波动极大，市场机构又不得不重新拥抱法定货币体制，即通过锚定由中心化主体发行的法币资产，来追求加密行业的币值稳定。^{〔15〕}

（二）重要支付系统：稳定币信息网络设施中的金融基础设施识别

稳定币业务活动的顺利开展，依赖于“中心化”与“去中心化”的信息网络设施，这些信息

〔11〕 Committee on Payments and Market Infrastructures, *Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework*, 2017, p. 3.

〔12〕 储备资产管理是稳定币监管框架的重点，因其会影响持有人对稳定币币值的信心。Daniel W. Borneman, *Banks Run in the Digital Economy: The Need for Stablecoin Regulation*, 47 Seton Hall Legislative Journal 52, 78 (2023).

〔13〕 不同于开展稳定币投放、赎回的区块链，该类信息网络设施开展的活动被称为“链下交易”（off-chain transactions），相关活动未被区块链记录。Bank of England, *Regulatory Regime for Systemic Payment Systems Using Stablecoins and Related Service Providers: Discussion Paper*, 2023, p. 87.

〔14〕 例如，2021年8月，跨链协议 Poly Network 确认遭到网络盗窃，引发公众对跨链协议安全性的质疑。Steven Schwarcz, *Demystifying Digital Currencies*, 87 Law and Contemporary Problems 1, 17 (2025).

〔15〕 柯达：《稳定币的“稳定”与“不稳定”》，载朱慈蕴、廖理主编：《清华金融法律评论》第3卷，法律出版社2020年版，第26页。

网络设施的运行者或参与者的数量、业务活动类型以及相应风险各有差异，因此需要根据法定标准，进一步识别哪些可纳入法律上的“金融基础设施”概念。根据《FMI 原则》的规定，金融市场基础设施是运行或参与机构之间用于清算、结算或记录支付、证券、衍生品或其他金融交易的多边系统⁽¹⁶⁾，我国《金融基础设施监督管理办法》还纳入了交易设施、基础征信系统两类。结合稳定币的技术特性，识别稳定币的金融基础设施应从“功能”与“地位”两方面展开。

在功能方面，由于稳定币属于转移法定货币资金的新型支付手段，只有从事稳定币投放、赎回、资金转移以及兑换交易的信息网络设施，可能被纳入金融基础设施中的“支付系统”或“交易设施”范畴，但无法归属于其他几类金融基础设施。对于支付系统，《FMI 原则》将其定义为“两个或多个参与者之间资金转移的一套工具、程序和规则”⁽¹⁷⁾。按照该定义，只有用于资金转移环节的稳定币信息网络设施才属于支付系统。但与传统法定货币不同，稳定币的投放、赎回和资金转移所使用的信息网络设施是一体的，投放、赎回本质上是发行机构与公众之间的资金转移。⁽¹⁸⁾对于交易设施，《金融基础设施监督管理办法》未提供具体定义，可参照现行证券期货法律将其定义为组织和监督交易，并实行自律管理的场所设施。⁽¹⁹⁾目前，不论是由中心化还是去中心化交易所提供，面向不同稳定币之间、稳定币与其他加密资产之间开展的场内或场外交易，均符合该交易设施的定义。此外，稳定币的储备资产管理由发行机构或其委托的第三方对外单独实施，其行为的单向性使其无法归入任一金融基础设施。需要注意的是，区块链可通过“支付即结算”实现确权效果，因此不存在单独认定结算系统、中央对手方或登记存管系统的必要。⁽²⁰⁾

在地位方面，目前只有符合系统重要性标准的信息网络设施才能被认定为金融基础设施中的“重要支付系统”。《FMI 原则》区分了“重要”与“非重要”支付系统，只有重要支付系统才能被认定为金融基础设施；同时，将重要支付系统推定为具有“系统重要性”，从而使其接受额外的宏观审慎管理，因此须根据系统重要性程度来判断某一支付系统是否为金融基础设施。至于何谓“系统重要性”，《FMI 原则》主要遵循“业务关联性”认定标准，即在金融领域可能引发和传递系统

(16) Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, Principles for Financial Market Infrastructures, 2012, p. 8.

(17) Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, Principles for Financial Market Infrastructures, 2012, p. 9.

(18) 国际清算银行与国际证监会组织认为，稳定币运行过程中的“转移功能”(transfer function)通常需要一套在参与者之间转让“硬币”(coin)的规则以及用于验证交易的机制，该功能属于金融市场基础设施应具有的功能。Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions, Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements, 2022, p. 4.

(19) 《证券法》第 96 条，《期货和衍生品法》第 79 条。

(20) 此外，从表象上看，稳定币的信息网络设施符合“交易数据库”的定义，即“集中保存交易数据电子记录的单位”。See Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, Principles for Financial Market Infrastructures, 2012, p. 9. 但是，交易数据库是为了防范场外衍生品交易数据缺失所致系统性风险而设立的；对稳定币而言，不论是中心化还是去中心化的信息网络设施，均不存在类似的数据缺失问题。

性中断。⁽²¹⁾同时,结合我国《金融基础设施监督管理办法》并参考欧盟的《系统重要性支付系统监管要求》,评判“系统重要性”的主要标准还包括:其一,支付业务规模及市场占有率;其二,支付业务的可替代性;其三,与其他金融基础设施的关联度;其四,跨境开展业务的国家或地区数量。⁽²²⁾传统上,一国由中央银行运营的大额支付系统,或由数家大型商业银行共同设立运营的零售支付系统均具有系统重要性,这些中心化的支付系统在本国的特定业务场景中具有独一无二的地位。但按此种划分标准,目前市场第一大稳定币“USDT”所依托的区块链只能“勉强”根据市场占有率成为金融基础设施。由于稳定币支付系统在底层技术上与传统支付系统存在根本区别,在判断某一稳定币的信息网络设施是否具有“系统重要性”时,应与其他同类型的支付系统,而不是与传统的中心化支付系统相比较。此外,为解决“区块链三元悖论”⁽²³⁾中的可扩展性问题,在一些区块链上形成了“第二层”(Layer 2)、侧链等另行处理链上交易的信息网络设施⁽²⁴⁾,这类信息网络设施同样应纳入“系统重要性”的认定范围⁽²⁵⁾。

与支付系统不同的是,交易设施是《金融基础设施监督管理办法》独有的金融基础设施,我国包括证券交易所、期货交易所等在内的现有交易设施均由政府机构特许设立,且主要经营业务在境内开展,其重要程度与前文所述的传统中心化支付系统相一致。就稳定币而言,其被频繁充当法定货币与其他加密资产之间的“交易对”,进而在加密资产交易所内产生了稳定币或其他加密资产之间的大量兑换交易。尽管目前数家加密资产交易所占据市场主导地位,但这些交易所均采用传统中心化信息网络设施,其面临的主要风险与传统交易所基本一致,因而不能像支付系统一样,在判断“系统重要性”上仅与同类信息网络设施作比较。此外,大部分加密资产交易所不仅组织跨币种交易,同时还开展吸收存款、发放贷款、销售衍生品、担保等业务,其事实上已成为综合金融服务提供商,而非单纯的交易设施。⁽²⁶⁾在此情况下,提供稳定币兑换交易的加密资产交易所作为交易设施,未符合“系统重要性”标准,因此下文仅论述“重要支付系统”这一类型的

(21) Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commission, Principles for Financial Market Infrastructures, 2012, p. 20.

(22) 《金融基础设施监督管理办法》第31条; Oversight Requirements for Systemically Important Payment Systems (EU) 2025/1355, Art. 3; 季奎明:《金融法制定中的基础设施统合规范论纲》,载《财经法学》2025年第4期,第86页。关于评价稳定币金融基础设施的跨境标准,可参见 International Organisation of Securities Commissions, Global Stablecoin Initiatives: Public Report, 2020, p. 28.

(23) “区块链三元悖论”是指区块链无法同时实现去中心化、安全性和可扩展性;公链如果要追求高度的去中心化、安全性,就必须牺牲可扩展性。

(24) Yannis Bakos & Hanna Halaburda, *Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance*, Computer Science, Business (2022), <https://www.semanticscholar.org/paper/Permissioned-vs-Permissionless-Blockchain-Tradeo%EF%AC%80s-Bakos-Halaburda/b5a7782b1220e134449fb14df66e86d4bc492997>, visited on 21 March 2026.

(25) 需要注意的是,“稳定币基础设施”的系统重要性标准,不等同“稳定币”的重要性标准。有学者指出,符合“全球”等重要性标准的稳定币商业模式更像是一种构想,而非可操作的现实。Iris H-Y Chiu, *Global Stablecoins Without a Future? Analysing Europe's Regulatory Defence in the Markets for Crypto-Assets Regulation as an Internationally-Leading Example*, 58 The International Lawyer 223, 233 (2025).

(26) Marco Dell'Erba, *Crypto-Trading Platforms as Exchanges*, 2024 Michigan State Law Review 1, 50 (2024).

稳定币金融基础设施。

（三）稳定币重要支付系统的主体行为解构

为更全面掌握稳定币重要支付系统的风险表现，特别是相较于传统支付系统的特殊之处，有必要先行剖析其参与者与运行者有哪些主体，这些主体为何、如何参与或运行支付系统。

首先，支付系统运行者与参与者的非准入化与非实名化。⁽²⁷⁾ 传统的支付系统一般由监管部门自行设立、特许设立或批准设立，少数国家还受历史因素影响存在由数家大型金融机构共同设立的情况，从而使支付系统的运行者及其开展的业务活动表现出极强的公共性。同时，某一主体如欲成为金融基础设施的参与者，进而开展资金清算结算等活动，需要符合特定的准入条件，并开立实名账户。⁽²⁸⁾ 对稳定币而言，开展投放、赎回、资金转移的重要支付系统主要为公链，任何主体在接入该区块链网络并成为节点后，均能成为系统运行者，根据特定的共识机制开展链上数据验证、系统升级等运行活动，进而获得相应的运行奖励。如果某一节点认为继续加入运行无法获得预期收益，亦能随时停止接入区块链网络。同时，区块链的钱包用户作为支付系统的参与者，可通过数字钱包生成相应的私钥及对应的公钥即“钱包地址”，据此发起稳定币的转让或接收，而开立钱包亦无须任何准入门槛。其中，稳定币持有人并不必然与钱包服务商形成财产权转移意义上的保管关系，其亦可将稳定币的私钥存储在钱包服务商无法控制或施加实质性支配的“非托管钱包”（unhosted wallet）之中。⁽²⁹⁾ 进一步看，不论是节点还是钱包用户，均可用假名化的钱包地址开展系统运行或交易；但同时，任何人都可查看某一钱包地址在何时开展了何种活动，以及该地址的稳定币等加密资产持有情况。

其次，稳定币发行机构与支付系统运行者的分离。在传统法币体系下，中央银行发行基于国家信用、面向所有公众使用的现金货币，并创造出同样体现国家信用、面向金融机构或其他大型机构使用的央行存款准备金，后者中的一大部分被用于金融机构或其他大型机构之间的清算结算。由于开展清算结算需要特定的货币存储媒介，中央银行为这些机构开立存放存款准备金的央行账户，并运行为这些机构之间开展清算结算的金融基础设施。从该意义上讲，中央银行既是货币的发行机构，又是货币账户的开立者，更是与清算结算相关的支付系统运行者。但就主流稳定币而言，发行机构只能选择已实际运行的特定区块链作为稳定币投放、赎回、资金转移的重要支付系统，而无法单方主导运行该区块链，更不必为稳定币的持有人提供数字钱包并履行托管职责；相反，发行机构仅能依据事先在该区块链所加载的智能合约开展若干交易限制，例如将特定钱包列

（27）在一些区块链（如比特币区块链）中，参与者即用户亦被称为“轻量节点”，该节点只有钱包与路由转发功能，且只能验证自己的交易。由于轻量节点不参与全局性的区块链系统运行，因此本文不将其视为与普通节点一样的运行者，而是将其作为普通的参与者看待。

（28）《银行业金融机构加入、退出支付系统管理办法（试行）》（银发〔2007〕384号）第8条。

（29）Tom Barbereau & Balázs Bodó, *Beyond Financial Regulation of Crypto-Asset Wallet Software: In Search of Secondary Liability*, 49 Computer Law and Security Review 1, 6 (2023).

入黑名单。⁽³⁰⁾

最后, 稳定币重要支付系统兼具“单一币种分散流通”与“不同币种共同流通”的互联互通功能。就同种支付手段而言, 传统法币体系下仅存在一家可开立结算账户并实现财产权转移的支付系统, 例如转移央行准备金的大额支付系统、转移银行存款的商业银行行内支付系统。对稳定币而言, 一方面, 稳定币发行机构可以同时选择多条区块链作为开展稳定币投放、赎回、资金结算的支付系统。例如, 稳定币“USDT”同时依托波场(Tron)、以太坊(Ethereum)、索拉纳(Solana)等多条区块链。发行人之所以同时选择不同区块链作为稳定币的支付系统, 主要是为了兼顾不同交易场景下的支付需求。例如, 以太坊上的稳定币交易侧重于安全偏好较强、效率要求较低的大额交易, 而波场上的稳定币交易侧重于效率偏好较强、安全要求较低的小额高频交易。进一步看, 稳定币持有人的钱包地址是基于特定的区块链生成的, 因此其持有的同种稳定币可能会分布在不同的区块链上流通; 同时, 某一区块链可能兼具金融基础设施功能, 以及由“去中心化应用”(DApp)提供、不用于支付的经济功能或社会功能, 例如镌刻区块链上的“铭文”。⁽³¹⁾

另一方面, 除了某一区块链创造的原生通证之外, 多个发行机构投放的稳定币或其他加密资产作为“衍生通证”, 可以在同一区块链上共存。某一区块链上的原生通证是该区块链能否正常运行的前提, 以以太坊为例, 之所以有人愿意成为该区块链上的运行者实施验证、记录交易等行为, 是因为运行者有机会获得由以太坊新创造的原生通证即以太币, 或由稳定币持有人支付作为“交易手续费”且已在市场上流通的以太币。由于以太币在加密市场上有升值空间, 以太坊的运行者可以在获得以太币后, 通过交易所或其他途径卖出而获得收益。在原生通证提供区块链运行激励的基础上, 稳定币或其他加密资产的发行机构对该区块链会建立“持续运行”的预期, 进而通过加载智能合约开展衍生通证的投放与赎回。

三、重要支付系统定性下稳定币金融基础设施的风险治理困境

区块链虽然在理论上是一种“去信任”应用, 但其作为一种金融基础设施仍须依赖社会个体的运行管理, 并会产生因个体信任引发的风险。下文以重要支付系统为核心, 分析现行法律制度能否有效应对稳定币金融基础设施的主要风险。

(一) 稳定币重要支付系统的主要风险

风险治理不仅是维护稳定币领域金融稳定的必要手段⁽³²⁾, 更是国际上对金融基础设施法律治理的核心方式。结合稳定币的技术特性, 重要支付系统的主要风险为运行风险、结算风险和洗钱

(30) 稳定币发行机构的相关操作, 均须依赖于加载于特定区块链的智能合约。关于智能合约在稳定币中的具体应用内容, 参见香港金融管理局《〈稳定币条例〉持牌稳定币发行人监管指引》第6.5.3条。

(31) 国际清算银行提出的“统一账本”(unified ledger)与“金融互联网”(finternet), 便是区块链多功能的具体应用展现。Agustín Carstens and Nandan Nilekani, Finternet: The Financial System for the Future, BIS Working Papers, 2024, p. 12.

(32) Financial Stability Board, High-Level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report, 2023, p. 7-8.

风险。其中，传统支付系统同样存在运行风险、结算风险，但其具体表现与稳定币存在差异，而洗钱风险则是稳定币情境下新增的风险。

其一，与传统支付系统性质相同但表现不同的运行风险。运行风险是因信息系统和内部处理过程中存在缺陷、人员不足或外部事件干扰，导致金融基础设施提供的服务减少、恶化或中断的风险。⁽³³⁾ 从内部视角看，运行者与参与者的准入缺位会加重稳定币重要支付系统的运行安全危机。如上文所言，任何主体均可随时成为区块链节点，自由加入或退出区块链的运行。人们之所以相信区块链上的数据以及链上流通的稳定币，根本上是信任有特定数量的节点足以正常维持区块链的运行。⁽³⁴⁾ 虽然维持大多数公链运行的节点分布在世界各地，一定程度上分散了运行风险，但仍存在某区块链的原生通证价格下跌或其他因素，导致节点数量缺失、区块链无法正常运行的可能性⁽³⁵⁾；同时，如果大多数节点分布在我国境外，还可能会损害主权层面的运行安全。从外部视角看，稳定币重要支付系统还可能依托“预言机”等技术，与其他区块链或中心化信息网络设施实现互联互通，这同样会放大外部网络攻击的安全损害效果，进而导致业务流程扩散层面的“跨类型风险”⁽³⁶⁾。

其二，与传统支付系统性质相同但表现不同的结算风险。由于信用风险、流动性风险均在结果上体现为参与者违约时面临的风险，“结算最终性”即“金融资产转让或债务清偿的无条件、不可撤销”⁽³⁷⁾能否实现，成为传统支付系统风险控制的关键。⁽³⁸⁾ 稳定币与其他加密资产一样，理论上可以实现全天候“支付即结算”，即在扣减付款人钱包余额的同时，增加收款人的钱包余额，其中不会出现传统法币因第三方介入导致的在途资金风险。⁽³⁹⁾ 但是，支付即结算并不意味着稳定币可以实时到账，更不意味着其背后的重要支付系统可以实现结算最终性。稳定币的结算，实质为节点验证交易并将其放入新区块，然后新区块会被添加到区块链中，从而使其承载的交易数据难以篡改。不过，主流区块链所采用的共识机制会导致“概率结算”效果。以采用工作量证明机制的区块链为例，由于矿工将创造出的数据区块向其他节点广播并请求验证的过程存在时延，同时时间内会形成数条尾部信息区块存在差异的数据链，某一条数据链上添加的区块越多，时间越长，先

〔33〕 Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commission, *Principles for Financial Market Infrastructures*, 2012, p. 94.

〔34〕 Paolo Saguato & Guido Ferrarini & Eric Pan, *Financial Market Infrastructures: The International Approach and the Current Challenges*, in Jens-Hinrich Binder & Paolo Saguato, *Financial Market Infrastructures: Law and Regulation*, Oxford University Press, 2021, p. 82.

〔35〕 区块链无法正常运行，会削弱其作为金融基础设施的可适用性。Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 New York University Journal of Legislation and Public Policy 837, 854 (2015).

〔36〕 张阳：《论金融市场基础设施风险治理的“三边机制”》，载《甘肃政法大学学报》2023年第3期，第7页；Hadar Y. Jabotinsky, *The Network Effects of International Crypto and DLT Regulation*, 57 Vanderbilt Journal of Transnational Law 1285, 1302 (2024).

〔37〕 Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, 2012, p. 64.

〔38〕 毛术文：《支付系统结算最终性法律保障研究》，载《中国支付清算》2022年第1辑，第9页；Hossein Nabilou, *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, 7 Business & Finance Law Review 139, 149 (2024).

〔39〕 徐忠、邹传伟：《区块链能做什么、不能做什么？》，载《金融研究》2018年第11期，第3页。

前交易被更改的可能性就越小，交易就越“确定”，最终成为提供最终结算效果的主链。此外，采用稳定币结算的金融基础设施，相较于法定货币或银行存款会带给参与者更大的外部信用风险，这是因为稳定币的实际价值与面值会发生偏离，偏离的大小取决于发行机构对储备资产的管理能力。⁽⁴⁰⁾

其三，稳定币情境下新增的洗钱风险。⁽⁴¹⁾ 该洗钱风险主要体现在以下三个层面：在底层技术层面，区块链所开展的稳定币投放、赎回、资金转移，以及节点接入区块链后的运行活动，均未必须要求相关主体提供实名信息。在存储媒介层面，即便稳定币发行人、交易所或钱包服务商要求用户进行实名认证，但稳定币重要支付系统仍允许用户在不与前述主体开展业务往来的情况下，通过非托管钱包完成点对点的资金转移。⁽⁴²⁾ 在叠加技术层面，由于区块链上的所有交易数据以假名方式对外公开，为避免部分钱包地址被识别实名身份，一些商业机构推出了“混币器”（Mixer）服务、“隐私币”（AEC）或通过“隐秘地址”（Stealth Address）以实现隐私增强功能，掩盖原本公开可查的直接交易链路。⁽⁴³⁾

洗钱是严重危害金融管理秩序、破坏打击犯罪效果的行为，而反洗钱制度的核心在于要求面向公众提供金融服务或出售特定商品的机构履行反洗钱义务。在传统法币体系下，金融基础设施的运行者不直接面向公众提供金融服务，即便其在基础设施运营过程中会处理涉及特定个人或金融企业的数据，但由此直接承受的洗钱风险程度，远小于金融基础设施的参与者，特别是金融机构。与传统金融基础设施不同的是，稳定币持有人可以通过非托管钱包等媒介，直接作为稳定币重要支付系统的参与者，无须像传统金融基础设施一样委托第三方主体处理交易⁽⁴⁴⁾，这使得稳定币重要支付系统及其运行者将直接承受洗钱所带来的不利后果。

（二）现行金融基础设施治理规范对稳定币的可适用表现

以《FMI 原则》和《金融基础设施监督管理办法》为代表的法律规范，为传统金融基础设施的风险治理确立了基本框架，因此可作为应对稳定币重要支付系统所致风险的法律依据。结合稳定币的技术特性，现行金融基础设施治理规范可以适用于稳定币的内容，主要体现在传统支付系统同样存在的运行风险和结算风险上。

首先，现行法可以通过市场准入规则，应对因技术层面缺乏准入而引发的内部运行风险。由

〔40〕 Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions, Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements, 2022, p. 19.

〔41〕 从表面上看，洗钱风险亦属于法律风险的一种，但在传统金融基础设施法律规范中，法律风险是指因合同效力、法定程序等事由导致无法履约的损失，其不包括各方参与主体是否遵守某一司法管辖区内的各种法律规定。Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, Principles for Financial Market Infrastructures, 2012, p. 18.

〔42〕 Financial Action Task Force, Best Practices on Travel Rule Supervision, 2025, p. 8; Rodrigo Coelho, Jonathan Fishman, and Denise Garcia Ocampo, Supervising Cryptoassets for Anti-money Laundering, FSI Insights on Policy Implementation, 2021, p. 18.

〔43〕 例如，美国一公司提供“Tornado Cash”混币器服务，允许客户进行无法追踪的加密资产转移。White House, Strengthening American Leadership in Digital Financial Technology, 2025, p. 103.

〔44〕 吴云等：《虚拟货币洗钱问题研究：固有风险、类型分析与监管应对》，载《金融监管研究》2021年第10期，第7页。

于大量金融基础设施由政府机构特许设立后运行，现行法的约束重点在于参与者准入。例如，《FMI 原则》要求金融基础设施应该具有客观的、基于风险的、公开披露的参与标准，支持公平和公开的准入，并应该识别、监测和管理由分级参与安排产生的实质性风险。⁽⁴⁵⁾ 但对稳定币而言，作为支付系统运行者的区块链节点可以自由加入或退出，而作为参与者的稳定币持有人也可以越过第三方中介直接发起交易，法律无法直接强制既有的区块链节点接受政府机构的监管。这种准入缺位实质上反映了稳定币重要支付系统的纯技术治理逻辑，即通过技术上带有激励性质的共识机制，实现系统内部的治理，以排除公权力与法律的干预。⁽⁴⁶⁾ 不过，稳定币受法币资产支撑，其金融基础设施与传统金融体系联系密切，因此无法完全摆脱外部权力与规范的影响。⁽⁴⁷⁾ 对于如何尊重区块链技术的作用，同时又不会引发基础设施之外的风险，现行法亟待提供更明确的解决方案。

其次，现行法可以针对互联互通引发的外部运行风险提供基本的治理框架。根据《FMI 原则》的规定，与一个或多个其他金融基础设施连接的金融基础设施，应识别、监测和管理与连接相关的风险⁽⁴⁸⁾；我国《金融基础设施监督管理办法》第 21 条则进一步强调了金融基础设施互联互通的法律基础，即其运营机构之间应当通过签订协议或公约等形式，明确各方权利、义务和责任，避免与所连接金融基础设施之间的风险传染。在前述三种稳定币基础设施的互联互通类型中，针对“不同币种共同流通”，基于区块链的开源属性，不论是在技术层面还是在法律层面均难以对该互联互通进行约束；而针对“单一币种分散流通”与“其他信息网络设施的互联互通”，稳定币的发行机构具有较强的选择与控制能力，因而具备适用现行法的基础条件。不过，因稳定币发行机构与支付系统运行者的分离，对于非兼任支付系统运行者的稳定币发行机构，法律上仍有必要对互联互通的类型与条件进行约束。

最后，现行法可为应对结算风险提供最终结算时间点和结算货币的基本规则。《FMI 原则》要求金融基础设施应最迟于生效日的日终提供清晰确定的最终结算，此外应首先使用央行货币进行货币结算。⁽⁴⁹⁾ 我国《金融基础设施监督管理办法》虽未提及类似的风险治理措施，但在支付系统相关规章中确认支付业务完成清算后具有最终性。⁽⁵⁰⁾ 对传统支付系统而言，法律层面的结算最终性并不等同于技术层面的结算最终性，因而前者是被拟制出来的，中心化的支付系统仍可能因遭

〔45〕 Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, 2012, p. 101, 105.

〔46〕 [美] 凯文·沃巴赫：《信任，但需要验证：论区块链为何需要法律》，林少伟译，载《东方法学》2018 年第 4 期，第 109 页。

〔47〕 Eric Alston et al., *Can Permissionless Blockchains Avoid Governance and the Law?*, 2 Notre Dame Journal on Emerging Technologies 1, 5 (2021).

〔48〕 Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, 2012, p. 109.

〔49〕 Committee on Payment and Settlement Systems & Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, 2012, p. 64, 67.

〔50〕 《大额支付系统业务处理办法》（银办发〔2016〕112 号）第 8 条、《人民币跨境支付系统业务规则》（银发〔2025〕248 号）第 35 条。需要注意的是，中国人民银行体系下的“清算”，实质为机构之间转移货币资金财产权的“结算”。

受网络攻击而撤销交易，因此要区分技术层面的最终性和法律层面的最终性。⁽⁵¹⁾对稳定币而言，其重要支付系统的概率结算特征亦能体现出最终性在技术层面与法律层面的分离，因此现行法可为其在法律层面的结算最终性提供基本指引。不过，我国支付系统的结算最终性规则由于效力等级较低，尚无法对抗《中华人民共和国企业破产法》（下称《企业破产法》）等破产相关法律规范中的破产撤销权、破产管理人代履行选择权、个别债务清偿无效等规定。⁽⁵²⁾与之相关的是结算货币的外部信用风险，由于稳定币的法律地位尚未得到界定，特别是与非银行支付机构备付金、货币市场基金份额的区别，如何监管其储备资产亦存在争议，进而给防范结算货币的外部信用风险带来了挑战。

需要注意的是，内部视角下的信用与流动性风险管理是现行金融基础设施法律规范的重点内容。在传统法币体系下，由于金融基础设施提供了多样化的清算结算模式选择，且存在与某类货币直接相关的托管或担保措施，其风险治理重于应对金融基础设施自身参与托管或投资的潜在损失，以及金融基础设施参与者没有充足资金履行义务，或到期无法履行义务的不利后果。但对稳定币而言，主流区块链仅提供双边开展的全额结算模式，其无涉多边共同展开清算或依赖于前一手方的资金，以及可能发生的流动性不足或交易违约。部分区块链虽然具有原生通证质押的功能，但该功能是为了确保节点能在“权益证明”共识机制下适当参与系统运行，而非为了应对前述信用或流动性风险。

（三）现行金融基础设施治理规范难以适用稳定币的表现

与传统支付系统存在的运行风险和结算风险不同，现行金融基础设施治理规范难以适用于稳定币存在的洗钱风险。在此情况下，传统反洗钱法律规范便有必要被引入，以此判断能否作为稳定币金融基础设施风险治理的适当依据。根据《中华人民共和国反洗钱法》（下称《反洗钱法》）等法律法规的规定，金融机构作为发挥资金融通功能的中介，是开展反洗钱工作的重点主体。其中，我国已根据反洗钱金融行动特别工作组（Financial Action Task Force, FATF）的要求实施“旅行规则”（Travel Rule），即代表交易发起人的金融机构应获取必要、准确的发起人与受益人信息，之后即时、安全地将这些信息传递至代表受益方的金融机构，并应要求提供给有关当局。⁽⁵³⁾2025年6月，FATF发布《旅行规则监管最佳实践》，重申稳定币等加密资产的服务提供商同样应遵守包括旅行规则在内的反洗钱规则。⁽⁵⁴⁾不过，以金融机构为核心的反洗钱规则同样难以应对稳定币重要支付系统的洗钱风险。

首先，将稳定币重要支付系统的运行者直接作为反洗钱义务主体，不具备法律适用上的可行

(51) Hossein Nabilou, *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations*, 7 Business & Finance Law Review 139, 140 (2022).

(52) 《企业破产法》第16条、第18条、第21条。

(53) Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, 2012, p. 17; 《中国人民银行办公厅关于进一步加强反洗钱和反恐怖融资工作的通知》（银办发〔2018〕130号）。

(54) Financial Action Task Force, *Best Practices on Travel Rule Supervision*, 2025, p. 2; 关于欧盟针对加密资产发布的旅行规则，See European Banking Authority, *Final Report on Guidelines on Information Requirements in Relation to Transfers of Funds and Certain Crypto-Assets Transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines)*, 2024.

性。按照传统反洗钱逻辑，稳定币服务商与稳定币的交易发起人或受益人有货币资金的往来，因此应履行反洗钱义务。但如上文所言，稳定币的发行机构仅能在稳定币的投放与赎回阶段才有可能识别交易者的身份；同时，稳定币的流通不一定要经过交易所或钱包服务商，交易双方通过非托管钱包亦能完成稳定币的财产权转移。⁽⁵⁵⁾ 在此情况下，区块链节点作为支付系统运行者，对所有稳定币交易开展数据验证等活动，其在客观效果上等同于传统反洗钱情境下商业银行从事的支付结算业务，因此同样具备开展反洗钱工作的技术条件。虽然我国现行法将清算机构纳入了履行反洗钱义务的主体范围⁽⁵⁶⁾，但稳定币重要支付系统允许运行者自由加入或退出，这使作为运行者的节点难以承担与传统金融机构相同的反洗钱义务。

其次，稳定币持有人使用规避反洗钱的非托管钱包、隐私币或混币器等“隐私增强型”应用，在技术层面与法律层面均无法受到限制。除了节点与钱包用户均难以被识别这一传统困境之外，基于公链的开源属性，任何主体均可以在区块链上基于智能合约开发隐私增强型应用，开发此类应用的类型、时间、主体等内容不会受到前置性的技术约束。即便稳定币所依托区块链的特定节点，从技术上可以拒绝验证涉嫌洗钱活动、基于隐私增强型应用而生的交易数据，但同时仍然会有其他不知晓此类情况的节点验证或广播该交易数据。这实质上体现了针对特定交易的反洗钱措施，与平等对待任何交易的区块链共识机制的矛盾。⁽⁵⁷⁾ 此外，与传统银行账户的开立须受到身份认证、账户数量限制不同，区块链上的数字钱包的开立不受任何限制，因此规避反洗钱措施的成本更低。尽管稳定币发行机构可以根据先前设定的智能合约将部分钱包地址纳入“黑名单”，进而实现该地址资金冻结的效果⁽⁵⁸⁾，但仍无法像传统金融机构一样直接划拨或转移钱包内的资金至其他主体，其治理效果较为有限⁽⁵⁹⁾。

最后，无法有效平衡反洗钱、隐私保护及财产处分自由。我国 2025 年新修订的《反洗钱法》对洗钱风险管理措施专门作出规定：一方面，对存在洗钱高风险情形的，金融机构必要时可以采取限制交易方式、金额或者频次，限制业务类型，拒绝办理业务等风险管理措施；另一方面，金融机构采取风险管理措施，应在其业务权限范围内按照有关管理规定的要求和程序进行，平衡好管理洗钱风险与优化金融服务的关系，不得采取与洗钱风险状况明显不相匹配的措施。⁽⁶⁰⁾ 对稳定币而言，如果区块链内设的智能合约自动根据外部提供的名单，对特定的钱包地址采取拉入黑名

(55) 在此种交易中，交易发起方与受益方对于稳定币发行机构而言均不是其“客户”，因为二者存在于稳定币的正常流通阶段，与发行机构之间未构建起任何合同关系。See Hong Kong Monetary Authority, Consultation Conclusions on Proposed AML/CFT Requirements for Regulated Stablecoin Activities, 2025, p. 6.

(56) 《银行卡清算机构管理办法》（中国人民银行、国家金融监督管理总局令（2025）第 2 号）第 6 条、《金融机构反洗钱和反恐怖融资监督管理办法》（中国人民银行令（2025）第 10 号）第 2 条。

(57) Bank of International Settlements, Annual Economic Report: The Next-generation Monetary and Financial System, 2025, p. 83.

(58) Katrin Schuler, Ann Sofie Cloots & Fabian Schär, *On DeFi and on-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10 Journal of Financial Regulation 213, 229 (2024).

(59) Iñaki Aldasoro et al., *Stablecoin Growth: Policy Challenges and Approaches*, 111 BIS Bulletin 1, 3 (2025).

(60) 《反洗钱法》第 30 条；北京清科博动科技有限公司诉招商银行股份有限公司北京清华园支行储蓄存款合同纠纷，北京金融法院（2021）京 74 民终 489 号民事判决书。

单等反洗钱措施，基于区块链地址上资金余额的公开性，这会在客观上增加稳定币合法持有人的假名被识别为真实身份，进而产生隐私被侵犯的可能。⁽⁶¹⁾同时，结合区块链上任何行为活动的不可撤销性，如果稳定币持有人的某一钱包地址被误判为具有洗钱嫌疑而被冻结，由于现行法未对稳定币钱包地址如何解冻、主张损害赔偿的对象作出明确规定，稳定币持有人的财产处分自由也可能会受到过分损害。

四、重要支付系统定性下稳定币金融基础设施的风险治理完善

面对稳定币重要支付系统的运行风险、结算风险和洗钱风险，现行法尚存进一步完善的空间。对此，有必要尊重技术先行构建的“适应性治理”⁽⁶²⁾逻辑，兼顾更广泛的社会效益，以减少稳定币运行活动带来的负外部性⁽⁶³⁾。下文分别就运行风险、结算风险和洗钱风险提出相应的治理完善建议。

（一）市场自治优先：既存支付系统的运行风险治理

针对稳定币重要支付系统在市场准入与互联互通方面的运行风险，应基于公共性视角，并依据“新老划断”原则开展风险治理。对稳定币而言，金融基础设施事实上是一种“半公共资源”（semicommons），其整合了作为私人资源的货币资金和作为公共资源的信息网络设施。⁽⁶⁴⁾据此，一方面，稳定币重要支付系统的运行者既可以是政府机构或具有政府背景的企业，亦可以是具有一定技术能力、通过基础设施运行获取相应收益的任何企业或个人。另一方面，运行者应以维护公共性为重，该公共性不仅体现在谨慎维护系统安全、防范运行风险上，更基于稳定币的极强跨境和匿名特征，体现在维护货币主权、数据主权以及识别担责主体上。如果维护公共性与追求己方收益相冲突，支付系统运行者必须优先维护公共性。

在公共性基础上，应根据“新老划断”原则，对既存的稳定币重要支付系统与将来拟设立的新系统采取区分式的风险治理。其原因在于，对既存的稳定币重要支付系统，法律无法通过强制手段迫使支付系统的运行者改变其行为模式，亦无法单方改变区块链在技术层面的运行机制。由于区块链应用程序本身无法被关闭，即便通过监管手段关停某一应用程序的网络接口，在新的网络接口被开发后，该应用程序也将继续运行。⁽⁶⁵⁾对于既定存在、已经被用于稳定币投放、赎回和资金转移的重要支付系统，应在尊重市场自治的基础上，通过以下措施防范运行风险。

〔61〕例如，2022年数字资产借贷平台 Celsius 提交破产申请，其披露了近50万用户的姓名和交易信息，加重了用户受盗窃或勒索的风险。See Shlomit Azgad-Tromer et al., *The Case for on-Chain Privacy and Compliance*, 6 Stanford Journal of Blockchain Law & Policy 265, 267 (2023).

〔62〕Esen Esener, *Adaptive Governance for Blockchain Networks*, 7 Stanford Journal of Blockchain Law & Policy 76, 99 (2024).

〔63〕Eric Alston, *Digital Currency Industry Self-Regulation: Not All Consensus Is Automatic*, 27 Virginia Journal of Law & Technology 1, 8 (2023).

〔64〕James Grimmelmann & A. Jason Windawi, *Blockchains as Infrastructure and Semicommons*, 64 William & Mary Law Review 1097, 1116 (2023).

〔65〕Primavera De Filippi et al., *Blockchain Technology and the Rule of Code: Regulation via Governance*, 92 George Washington Law Review 1229, 1238 (2024).

首先，建立既存稳定币区块链原生通证的国家储备机制。我国《金融基础设施监督管理办法》第5条规定，“对于涉及国家金融安全、外溢性强的金融基础设施，保持国家绝对控制力”，即系统重要性程度更强的金融基础设施应由国家主导运行。但由于既有主流区块链的节点分布于全球各地，稳定币重要支付系统同样由国家主导运行并不具有现实可行性。对此，可通过直接影响区块链原生通证的市场价格，间接影响区块链节点加入基础设施运行的行为选择；从兼顾安全与效率的整体视角看，原生通证价格的影响方式应是国家储备机制。⁽⁶⁶⁾ 该国家储备机制的运作类似于现行的外汇储备机制，即特定机构以国家名义在市场上买卖标的资产，以实现该资产的日常保值增值，并在特殊时期在市场上买卖以影响标的资产的价格。同时，作为国家储备的原生通证应具有代表性，例如占市场主要地位的稳定币币种在该原生通证依托的区块链上流通。⁽⁶⁷⁾

其次，设置专门机构作为“公益节点”，参与稳定币重要支付系统的运行。虽然对于稳定币所依托的区块链，相应节点从技术上看无法受到统一的控制或约束，但为了维护公共性，减少节点不当参与重要支付系统的运行给该稳定币乃至整个金融体系带来的损害，法律上应构建专门机构的节点储备机制。该机构通过原生通证的质押或者一定的算力，具备了接入特定稳定币重要支付系统的能力；在稳定币市场发生异常波动或交易所等市场主体出现网络攻击事件，给相应支付系统的声誉带来不利影响时，该机构可作为公益节点维持该区块链的正常运行。与我国资本市场上投资者保护机构不同，公益节点侧重于维护宏观层面的市场秩序、防范基础设施的运行风险。

最后，采用市场激励方式开展稳定币重要支付系统运行者的线下备案识别，以维护运行者之间竞争和参与者发起交易的公平性。一方面，法律上应采用市场补贴、税收优惠等激励方式鼓励系统运行者到特定机构进行备案登记。稳定币重要支付系统的运行者识别，不仅有助于在事前事中尽早防范运行风险，还有助于在事后及时定责，由此进一步确保所有参与者在基础设施运行过程中拥有开放和非歧视性的交易机会。⁽⁶⁸⁾ 另一方面，在运行者识别的基础上，可采用交易手续费补贴等方式确保交易的公平性，以进一步保障基础设施的公共性。按照纯粹技术治理的逻辑，为避免浪费网络资源和阻止恶意攻击，稳定币重要支付系统在技术上设置了网络越拥堵、交易手续费越高的运作机制，但也造成了某一运行者或参与者“一家独大”的持币集中化效果，这同样会带来运行风险。交易手续费补贴可以减少稳定币重要支付系统运行者的假名化导致的运行风险，同时不损害既存区块链的去中心化运作逻辑。

(66) [法] 普里马韦拉·德·菲利皮、[美] 亚伦·赖特：《监管区块链：代码之治》，卫东亮译，中信出版集团 2018 年版，第 204 页。

(67) 部分国家已针对占据加密市场总额更大的比特币开展了国家储备工作，例如美国白宫于 2025 年 3 月签署行政令，建立比特币战略储备，其来源主要为执法司法活动中收缴的比特币。*Stabishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile*, White House (6 March 2025), <https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/>.

(68) Samuel N., Weinstein, *Blockchain Neutrality*, 55 Georgia Law Review 499, 515 (2021).

（二）许可型公链嵌入：拟设支付系统的运行风险治理

对于暂未发行但计划发行稳定币的发行机构，应要求发行机构选择“许可型公链”（Public Permissioned Blockchain）作为稳定币投放、赎回、资金转移的重要支付系统，以防范运行风险。许可型公链是代码开源、数据公开、节点身份须验证但可自由加入或退出的区块链类型，其可用于构建通用、多用途共享基础设施的底层技术。^{〔69〕}相较于传统的公链和联盟链，许可型公链兼顾了激励机制下开放与安全的优势，并能在链上交易数据公开的同时确保数据的不可篡改。^{〔70〕}从风险治理角度看，除了共识算法的可靠性、对常见区块链攻击的抵御能力之外^{〔71〕}，法律上的许可型公链应符合以下要件。

其一，许可型公链满足无法由单方或少数几方联合控制的实质去中心化。去中心化是公链的“生命”，去中心化的实质不在于假名或匿名与否，而在于单方或少数几方能否控制区块链的运行，进而更改区块链已验证的数据，甚至撤销某一已实施的业务活动。尽管区块链在实际运行过程当中，出现了会影响中心化效果的核心开发人员等主体^{〔72〕}，但区块链的内在技术架构并未因该类主体的存在而发生改变，且该类主体的相关行为只能经节点认可后才能发生相应的技术效果。^{〔73〕}在域外，美国众议院已通过的《数字资产市场清晰度法案》遵循“基于控制的成熟度框架”，提供了区块链不受单方控制的判断标准，包括自动化编程运作、通证持有分散化、价值来源于使用和运作等^{〔74〕}，据此可采用区块链初创的中心化阶段施加证券监管、成熟的去中心化阶段施加商品监管的分类监管思路^{〔75〕}。此外，不宜将稳定币在结算效果上的特殊性作为认定区块链是否去中心化的标准。部分业内人士主张稳定币可以实现“支付即结算”，即全天候、实时、全额的结算模式，但是任何公链在理论上也可以采用其他清算结算方式。同时，运营时间方面也不是公链的特殊性，因为中心化的金融基础设施理论上也可以全天候运营，这取决于金融基础设施如何平衡安全与效率。

〔69〕 Monetary Authority of Singapore, Global Layer One: Foundation Layer for Financial Networks, 2024, p. 7; Monetary Authority of Singapore and Bank of International Settlements, Project Guardian: Enabling Open and Interoperable Networks, 2023, p. 12.

〔70〕 关于数字人民币的联盟链技术要素，参见柯达：《商业银行数字人民币业务：法律定性与制度完善》，载《华南理工大学学报（社会科学版）》2025年第4期，第85页。

〔71〕 香港金融管理局《〈稳定币条例〉持牌稳定币发行人监管指引》（2025年8月发布）第6.5.5条。

〔72〕 王延川：《“除魅”区块链：去中心化、新中心化与再中心化》，载《西安交通大学学报（社会科学版）》2020年第3期，第39页。

〔73〕 Amber Seira et al., *Governance of Permissionless Blockchain Networks*, FEDS Notes, <https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html>, visited on 21 March 2026.

〔74〕 Sec. 42, H.R.3633—Digital Asset Market Clarity Act of 2025. 有学者亦提出，成熟区块链所创造的“真正去中心化金融”，可以适当豁免于《银行保密法》的约束。See Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, 11 *Journal of Financial Regulation* 225, 231 (2025).

〔75〕 相似的是，美国证监会（SEC）曾提出“通证安全港”（Token Safe Harbour）提案，该提案旨在为区块链初始开发团队提供3年的证券法适用豁免期。See U.S. Securities And Exchange Commission, *Token Safe Harbor Proposal 2.0*, <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20>, visited on 21 March 2026.

其二，为确保常态化运行，许可型公链应由本国机构设计开发，节点参与运行须经实名认证，且满足数据篡改条件数量的节点必须分布在我国境内。虽然区块链的开发设计者对区块链的实际运行没有绝对控制权，但其在提出系统升级方案等方面具有较大影响力。例如，可供发行稳定币的“树图”（Conflux）区块链会不定期发布系统升级公告，提醒各区块链的节点定期予以技术升级，其事实上充当了“提案者”角色。为确保开发设计者提出的方案符合维护主权层面的公共性要求，用于稳定币流通的区块链同样应由本国设计开发。同时，为敦促区块链节点谨慎开展稳定币重要支付系统的运行，同时在运行风险事件发生后尽快确定担责主体，开展稳定币金融基础设施运行的任何机构或个人应经过真实身份认证。更重要的是，同样出于维护主权安全的公共性目标，区块链节点还须接受“地理位置认证”，在境外分布的节点数量不得高于满足数据篡改标准的数量。

其三，为尽早监测、识别与处置运行风险，许可型公链应提供监管嵌入与智能合约审计的功能。一方面，许可型公链应允许监管部门作为拥有特殊权限的节点，在链上实时监测与识别可能发生的运行风险，并在符合特定标准后及时予以处置。⁽⁷⁶⁾为兼顾个人信息保护，许可型公链应采用特殊技术手段，确保监管部门仅能识别符合要求的数据，避免过度处理个人信息。⁽⁷⁷⁾在符合公共紧急情况下，如果处于分散状态的节点难以就系统升级等事项达成一致，还应允许监管节点作为“决定性”节点，采取符合比例原则的系统运行活动。另一方面，应允许具有技术能力的行业自律组织作为拥有特殊权限的节点，对链上基于智能合约发行的稳定币相关交易或系统升级活动，开展智能合约审计。此种智能合约审计不仅需要考虑常见的运行风险，而且需要判断某一区块链运行活动的合规性，例如能否提供删除权等个人信息权益的技术实现路径，以及在跨境数据处理活动中是否支持数据的本地存储，进而避免智能合约的不可变更性引发额外的运行风险。

在选择符合以上条件的许可型公链后，稳定币发行机构还应遵守开展内外部互联互通的法定要求。实践中，稳定币区块链与外部其他信息网络设施之间的互联互通，须经具有一定中心化属性的技术手段或主体才可实现，由此导致外部网络攻击更加频繁。为防止此类互联互通因运行风险进一步发展为系统性风险，同一稳定币发行机构对同一稳定币所采用的区块链数量应受到限制。当然，如因流通量或交易场景扩大导致原有区块链的交易效率下降，稳定币发行机构应在监管部门批准后，另行增加稳定币所采用区块链的数量。此外，在开展内外部互联互通时，稳定币发行机构不得选择不符合我国现行法规定的区块链信息网络设施开展互联互通，由此直接阻断外部的运行风险。

（三）最终结算拟制：细化支付系统的结算风险治理规则

针对法律意义上稳定币结算最终性规则仍不明确，基础设施仍会受到外部信用风险威胁的情

〔76〕 Raphael Auer, *Embedded Supervision: How to Build Regulation into Blockchain Finance*, 811 BIS Working Papers 1, 2 (2019).

〔77〕 此种监管手段需要付出较高的运营成本，对此，可通过智能合约自动执行的“链间监管”与纯外部手段介入的“链外监管”予以协调配合。参见高昊昱等：《区块链安全监管研究综述》，载《通信学报》2025年第4期，第63页。

况，应进一步细化稳定币重要支付系统的结算规则。

第一，细化稳定币重要支付系统的最终结算时间点、最终结算的效力以及相应的保障措施。由于采用工作量证明机制的区块链存在“概率结算”现象，为确保稳定币的高效流通并保护收付款人的交易预期，应以收款人“到账”即公钥上显示的可支配资金余额出现变化，作为最终结算完成的时间点。这是因为到账意味着收款人享有完全自主支配财产权的能力；稳定币的最终结算完成后，如果稳定币的付款人出现被申请破产清算等情形，付款人的债权人不得取回已完成最终结算的稳定币。此外需要注意的是，对于发生在 Layer 2 或侧链上的稳定币交易，其最终结算不应以 Layer 2 或侧链上显示的结果为依据，而仍应以其所依托的主链所汇总的交易结果为依据；针对区块链通过公证人等技术手段应对概率结算⁽⁷⁸⁾，此种技术手段由于通过中心化主体接入外部数据实现，其不应具有法律意义上的结算最终性。

进一步看，为确保最终结算的持续实现，法律上不应认可通过区块链分叉或其他“回滚”方式的技术效果，而应继续认可之前已经根据特定共识机制进行的稳定币交易效力。实践中，如果盗窃等事件损害了区块链及其原生通证的声誉，部分节点会商议通过“硬分叉”方式撤销与此类事件相关、在某一段时间内开展的所有交易。在硬分叉情形下，原区块链分离出另一条新链，虽然新、旧区块链均承认分叉之前的数据区块，但运行新链的节点认定有效的新数据区块，将会被运行原区块链的节点认定为无效。⁽⁷⁹⁾ 例如 2016 年，以太坊上的大型智能合约项目“The DAO”被黑客攻击并盗取巨量以太币；之后，以太坊基金会组织发起系统升级，从而撤销被黑客窃取的以太币相关交易的效力。⁽⁸⁰⁾ 此种交易“回滚”只能临时解决盗窃等事件造成的声誉损失，但不能从根本上规避此类风险，反而会影响交易预期；同时，在稳定币的交易场景较为多元的背景下，如果贸然采取回滚措施，必然会引发一系列破坏加密市场乃至实体经济交易预期的连锁反应。因此，从法律上看，应继续认可“回滚”之前的原先交易行为以及相应稳定币财产权转移的效果，即便此类行为得到符合特定数量节点的认可。同时，如果确实发生错误转账、资金遭窃等情形，稳定币发行机构等中心化服务商可以依据合同约定或交易习惯，帮助稳定币的原权利人主张其合法权益⁽⁸¹⁾，但相关权益维护过程不应阻碍区块链上正常的数据验证等活动。

需要注意的是，稳定币重要支付系统在法律上拟制的结算最终性，不应违反行政或司法机关依法作出的强制性裁判或决定。例如，我国香港高等法院于 2024 年末受理了一起涉稳定币的电诈案件，原告向法院申请将两个持有涉案赃款的钱包地址进行冻结。法院虽然没有直接冻结钱包地址的技术能力，但其利用了区块链上所有假名交易数据公开的特性，在区块链上广播了其他钱包

(78) 姚前：《基于区块链的新型金融基础设施——理论、实践与监管》，中国金融出版社 2021 年版，第 201 页。

(79) [美] 阿尔文德·纳拉亚南等：《区块链：技术驱动金融》，林华等译，中信出版集团 2016 年版，第 94-95 页。

(80) 部分矿工因为拒绝运行同意“回滚”的软件补丁，进而继续在发生黑客窃取事件的原区块链上挖矿，后者又被称为“以太坊经典”(Ethereum Classic) 区块链，以区别于现在经过软件升级的“以太坊”(Ethereum) 区块链。

(81) 与银行账户不同的是，如果付款人将稳定币转错至另一钱包地址，且该地址的名义归属者恰好遗忘了该地址的存在，那么相应的稳定币实际上被“贮藏”，对于社会总体而言就会发生通缩的效果。

地址不得向受禁制令约束的钱包地址开展任何交易的“铭文”；违反该禁制令的任何人，可以被裁定藐视法庭罪、被判入狱或者被处罚款。⁽⁸²⁾

第二，针对稳定币作为结算货币面临的外部信用风险，应从协调基础设施的去中心化与币值管理的中心化视角，构建储备资产管理的风险联动应对机制。美国、中国香港特区等经济体的稳定币立法均涵盖了储备资产管理的要求，例如限制投资资产的类型、分离管理与托管主体、即时赎回法定货币等。管理储备资产的信息网络设施虽然不是法律意义上的金融基础设施，但储备资产能否确保币值稳定、相应信息网络设施是否安全可靠，同样会影响稳定币重要支付系统的平稳运行；如果储备资产发生信用风险，稳定币的市场价格将极有可能发生巨大波动，进而导致节点参与区块链运行的可获益程度发生变化。在此情况下，稳定币发行机构应审慎监测储备资产与基础设施之间的风险传导过程，如果储备资产发生风险事件，发行机构应及时作为节点接入区块链，参与稳定币重要支付系统的运行。

（四）双重主体协同：构建支付系统的洗钱风险治理规则

在现行金融基础设施法律规范对洗钱风险治理缺位、传统金融机构反洗钱规范难以适用于稳定币的情况下，应重构针对稳定币重要支付系统的反洗钱规范。重构反洗钱规范首先应解决的问题，是“了解你的客户”（know your customer, KYC）这一识别交易者的规则⁽⁸³⁾在稳定币重要支付系统中能否继续适用。KYC规则包含的实名认证要求，虽然有助于打击犯罪并维护金融安全，但是在交易所等中心化主体所提供的业务场景之外，KYC规则无法适用，特别是非托管钱包之间的交易。同时，区块链上的所有交易数据以假名方式对外公开，比传统金融交易更具透明性与可追溯性，只要能在假名与实名之间构建合理的关联关系，其同样能够实现KYC规则的治理目标。⁽⁸⁴⁾对于采用“通证”（token）技术的稳定币，其开展交易的基础不是身份验证而是余额验证，因此径行采用KYC规则有违稳定币的基本交易逻辑。在此情况下，不论是既存的还是将来拟设立的稳定币重要支付系统，更可取的是“了解你的交易”（know your trade, KYT）或“了解你的地址”（know your address, KYA）规则，即采取“日常性假名，可疑再识别”原则，以替代绝对意义上的实名制。

在该原则基础上，稳定币重要支付系统的反洗钱义务应由系统运行者与稳定币的发行机构协同履行。一方面，稳定币的发行机构应履行偏向于“主动”性的事前、事中反洗钱义务。具体而言，发行机构应在稳定币的投放、赎回等与客户开展直接交易的业务活动中，记录保存交易各方

〔82〕 Worldwide A-Plus Ltd. v. Holders of Wallet Address a.o., No. 2417, 2024, in the High Court of the Hong Kong Special Administrative Region Court of First Instance Action.

〔83〕 KYC规则与我国网络法《区块链信息服务管理规定》所要求的网络信息服务实名制存在相似之处，即要求区块链信息服务提供者对用户进行真实身份信息认证。参见《网络安全法》第24条、《区块链信息服务管理规定》第8条。

〔84〕 单从技术角度看，区块链可以通过零知识证明、预言机构建数字身份验证机制，从而在满足反洗钱要求的前提下最大限度地保护用户隐私。See Heather Yue Zhou, *Regulating Crypto Money Laundering: An Assessment of Current Regulatory Responses and Potentials for Technology-Based Solutions*, 8 Stanford Journal of Blockchain Law & Policy 142, 174 (2025).

的钱包地址、交易金额等重要交易数据；同时，在稳定币的资金转移过程中，发行机构应根据特定技术手段确保前述重要交易数据的可获取。发行机构如果自行发现某笔交易或某个钱包地址具有洗钱嫌疑，应按照洗钱嫌疑的风险危害程度，采取差异化的洗钱管理措施。实践中，诸多稳定币发行机构主要采取“黑名单”手段，即利用智能合约中的可编程性，阻止某个钱包地址中的交易，例如稳定币“USDT”“USDC”的发行机构均可采取该手段。在法律上，中国香港《打击洗钱及恐怖分子资金筹集指引（持牌稳定币发行人适用）》第5.10条规定，为防范稳定币被用于非法活动的风险，持牌人可采用适当的技术方案，在最初分销范围之外以持续方式筛查稳定币交易及相关钱包地址，将被识别到与制裁或非法活动有关的钱包地址列入黑名单。^{〔85〕}此外，国际清算银行（BIS）提出了“合规评分”作为黑名单的一种变体，即利用区块链上公开的交易数据评出合规的较高分值和较低分值，其中的较高分值表示与列入“允许列表”钱包相关联的稳定币，而较低分值则表示与列入“拒绝列表”钱包相关联的稳定币。^{〔86〕}

另一方面，稳定币重要支付系统的运行者应在稳定币发行机构履行主动性义务的基础上，履行偏向于“被动”性、监督为主的事后反洗钱义务，以实现反洗钱与隐私保护、财产权自由保护的平衡。包括施加黑名单反洗钱措施在内，所有在区块链上开展的行为活动都需要经系统运行者进行广播与验证后才能生效，因此系统运行者具有判断某稳定币交易活动在法律上是否合法有效，甚至拒绝无效交易的技术能力。同时，系统运行者如果判断稳定币发行机构采取的反洗钱措施不正确或采取的措施程度过当，亦可在技术上纠正此类不当措施，以实现反洗钱与财产权自由保护的平衡。进一步看，尽管理论上系统运行者对系统外部第三人须履行注意义务^{〔87〕}，但在反洗钱领域，此种义务应是被动性、非强制性的，即为了“补强”稳定币发行机构所施加的、存在一定激励效果的倡导性义务。具体而言，稳定币重要支付系统的运行者可另行搭建搜集、分析大额交易或可疑交易的信息网络设施，如果稳定币的发行机构采取的反洗钱措施与其自身判断的结论不一致，可以拒绝广播与验证。即便该措施经过其他系统运行者验证后仍产生相应的技术效果，但将来如果被采取措施的钱包主体向发行机构与节点主张救济权利，系统运行者可以凭借其拒绝验证豁免其法律责任，由此还能激励发行机构兼任支付系统运行者的职责。^{〔88〕}

此外，对于非托管钱包，已实施稳定币立法的经济体暂无针对性的反洗钱方案，其主要将“反

〔85〕 但是，黑名单制度也有缺陷，因为区块链的公钥地址可以随意创建，不法分子只须创建一个新地址即可绕过黑名单，因此有学者指出，应拉入黑名单的是某笔交易而非某个地址。See Christoph Wronka, *Money Laundering Through Cryptocurrencies: Analysis of the Phenomenon and Appropriate Prevention Measures*, 25 Journal of Money Laundering Control 79, 90 (2022).

〔86〕 如何防止合规评分被不当“污染”，同样是合规评分需要避免的不利影响。Iñaki Aldasoro et al., *An Approach to Anti-money Laundering Compliance for Cryptoassets*, 111 BIS Bulletin 1, 3 (2025).

〔87〕 汪青松：《区块链系统内部关系的性质界定与归责路径》，载《法学》2019年第5期，第141页。

〔88〕 稳定币发行机构具有作为节点参与基础设施运行的经济动力，即可以通过运行活动获取交易发起者支付的“交易手续费”，因此目前许多稳定币发行机构均推出了自研的公链。

洗钱不力”的责任归于稳定币发行机构等中心化主体。⁽⁸⁹⁾ 这一针对非托管钱包的洗钱风险治理方式并不完全合理，尽管稳定币发行机构可以针对非托管钱包实施更严格的旅行规则要求，但对于涉及多层嵌套非托管钱包的可疑交易，发行机构的监测能力亦相当有限。⁽⁹⁰⁾ 对此，应同样基于前述逻辑，由稳定币的发行机构与支付系统运行者协调承担。

五、结语

开展稳定币投放、赎回、资金转移业务，并具有系统重要性的支付系统，应属于法定的金融基础设施。针对稳定币重要支付系统的运行风险、结算风险以及洗钱风险，应基于公共性完善风险治理：其一，按照市场自治优先的原则，对既存稳定币重要支付系统的运行风险进行治理，包括建立既存稳定币区块链原生通证的国家储备机制、设置专门机构作为区块链上的公益节点、采用市场激励方式开展节点的线下备案识别；其二，要求暂未发行但计划发行稳定币的发行机构，应选择许可型公链作为稳定币投放、赎回、资金转移的基础设施，以防范运行风险；其三，细化稳定币重要支付系统的最终结算时间点、最终结算的效力以及相应的保障措施，并优化储备资产管理的法律规范；其四，要求稳定币的发行机构应履行偏向于“主动”性的事前、事中反洗钱义务，而支付系统运行者则履行偏向于“被动”性、重在监督的事后反洗钱义务。

区块链作为金融基础设施的底层技术之一，在跨境支付等缺乏互信的社会经济领域具有独特优势。在未来，区块链有望通过智能合约等应用，进一步促进金融或商品资产的流通，以提高金融经济服务的效率、可及性和可负担性。⁽⁹¹⁾ 不论将来我国仍仅探索发行离岸人民币稳定币，还是有条件放开稳定币的发行，均应以公共性为原则，打造自主可控的中国特色金融基础设施，充分发挥区块链的技术优势，并提供相应的风险治理保障。

Legal Identification and Risk Governance on Financial Infrastructure for Stablecoin

KE Da

Abstract: The financial infrastructure for stablecoin is the systemically important payment system that carries out stablecoin's issuance, redemption, and fund transfer in all information network facilities related to stablecoins. Based on the separation of system operators and stablecoin

(89) 《打击洗钱及恐怖分子资金筹集指引（持牌稳定币发行人适用）》第 5.10 条。

(90) Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions, 2026, p. 19.

(91) Monetary Authority of Singapore and Bank of International Settlements, Project Guardian: Enabling Open and Interoperable Networks, 2023, p. 6.

issuers, the stablecoin payment system is compatible with the decentralized circulation of a single money and the common circulation of different monies, in which system operators and system participants, conduct business activities in a non-access and non-real-name manner. The current legal framework governing financial infrastructure can provide general guidelines for addressing the operational and settlement risks associated with stablecoin payment systems, but it is unable to address the money laundering risks that such systems may pose. To address operational risk, the law should establish a national reserve of existing native blockchain tokens, set up nodes for public interest, and encourage system operators to file records offline. Besides, the institutions planning to issue stablecoin should choose public permissioned blockchain as the infrastructure for stablecoin's issuance, redemption, and fund transfer. To address settlement risk, the final settlement time point and final settlement effectiveness of the stablecoin payment system should be refined, and a risk linkage response mechanism for reserve assets should be established. To deal with money laundering risks, dual anti-money laundering obligations should be established between stablecoin issuers and payment system operators based on the "daily pseudonymity, suspicious re-identification" rule.

Keywords: Stablecoin; Financial Infrastructure; Payment System; Blockchain; Decentralization

(责任编辑: 楼秋然 汪友年)