加密货币去中心化属性的风险识别与监管应对

张夏明 ①

摘要：加密货币是区块链技术在金融领域的重要创新。其基于分布式账本、密码学和共识算法发行和流通，在底层技术架构、中层治理机制和上层经济模型上都表现出去中心化属性。由加密货币的去中心化引发的技术风险、法律风险和金融风险，对金融安全、稳定和消费者权益构成威胁。刺破加密货币去中心化的面纱进行再中心化识别，以“二元复合性”厘定加密货币新型财产权、推动代码规则与法律规则之间冲突的调和，为加密货币的监管应对提供理论基础。监管者宜引入嵌入式监管工具应对加密货币的技术风险；以支付结算功能和投融资功能切入加密货币的监管，通过探索中心化节点的责任承担机制应对加密货币的法律风险；并加强对加密货币洗钱的监管应对加密货币的金融风险。如此，可为金融科技创新与金融法制的冲突提供解决方案，完善我国金融监管体系，提升金融现代化治理的能力和水平，推动金融强国建设。

关键词：加密货币；去中心化；风险识别；再中心化；金融监管

中图分类号：F821.1 **文献标识码：**A

DOI:10.13490/j.cnki.frr.2025.04.002

一、引言

加密货币领域是近年来金融科技“破坏式”创新的代表，其本质是由私主体通过哈希算法生成的加密字符串，在分布式账本上进行记账和流转，区别于央行数字货币和电子货币。加密货币是金融科技创新的一个子集，是对金融支付结算工具和投资工具的创新，具有便捷、高效、普惠的优势，形成对传统金融体系的有机补充。从加密货币市场发展看，截至2024年11月，全球加密货币种类已超过10000种，市值超过3万亿美元。今年以来，加密货币更是强势进入西方国家政府的视野。美国特朗普政府于2025年3月6日签署行政命令，致力于保护和促进公民及私营部门访问和使用公链的能力，同时推动加密货币行业的创新与发展，评估建立和维护国家数字资产储备的可能性。加密货币正在全球产生广泛的影响，通过不断扩展金融服务的边界（陈永伟，2022），重构全球金融秩序。

① 张夏明，法学博士，副教授，贵州大学法学院，联系方式：zxmfintech@126.com。作者感谢匿名审稿人的意见，文责自负。

然而，加密货币领域也乱象丛生、风险突出，给金融监管带来诸多挑战。一是加密货币处于创新发展的初期，其底层的分布式账本技术、加密技术、智能合约等技术并不成熟，存在技术安全风险。二是加密货币领域存在大量的金融欺诈：在所有链上欺诈案件中，与加密货币相关的金融欺诈犯罪比例高达54%（CipherTrace，2022）。三是加密货币可以有效避开主权国家的管辖，使传统以监管中心化的金融中介的监管体系面临失效的窘境；同时，加密货币具有无需许可进入、无用户身份识别、无国界等特征，容易成为犯罪洗钱、恐怖主义融资等违法犯罪的温床。此外，加密货币还具有严峻的法律和监管风险。前美国证券交易委员会主席根斯勒（Gary Gensler）指出，加密货币具有去中心化和非托管金融网络协议的特征，可能违反证券、商品和银行法，给投资者和监管者带来挑战。当前主要国家和国际金融组织均意识到加密货币对金融和法制体系的巨大冲击，正积极评估其风险，探索规制手段。

针对加密货币领域的法制规范极不完备，无法及时对技术创新和风险进行约束，学界与业界均展开了研究。已有研究多从加密货币的风险和法律属性出发，分析加密货币在民事、刑事领域的法律适用和监管路径，而聚焦加密货币本质属性和监管应对的体系化研究较少。鉴此，本文从加密货币去中心化的本质属性出发，识别其去中心化属性引发的技术层面、法律层面和金融层面的风险，并从刺破“去中心化”的面纱、厘定新型财产权和对代码与法律规则的冲突进行调适三个维度探讨监管应对方式，提出引入嵌入式监管的监管工具应对其技术风险，强化加密货币的分类监管和探索中心化节点的责任承担机制应对其法律风险；加强加密货币的反洗钱监管应对其金融风险的建议。识别加密货币的去中心化属性，有助于深化监管认识，平衡创新与安全，降低加密货币的负外部性，为该领域的政策制定提供思路，助力金融科技、数字金融治理水平和能力的提升。

二、加密货币的内涵与去中心化属性

（一）加密货币的内涵

根据金融稳定委员会（FSB）的界定，加密货币是一种私营部门数字资产，主要借助密码学和分布式账本或类似技术发行和流通（FSB，2020）。加密货币与数字代币不同。数字代币代表了与实物相对应的权利，具有将任何种类的资产（例如法币、贵金属或股票、收藏品等资产）代币化的可能性，受到代表基础资产或追索权的资产的支持（Ferreira等，2021）。加密货币在内涵和外延上对数字代币进行了限缩，通常只指使用分布式账本技术、价值主要来自密码学（即并非锚定基础资产、追索权或预期现金流）的数字资产。加密货币既包括没有资产支持的虚拟货币（例如比特币），也包括证券代币和代表财产所有权的资产支持代币，以及用于获

取特定数字平台上商品或服务访问权限的实用代币。加密货币设计的初衷是为了在无需第三方信任的情况下促进价值转移，打造分布式的价值互联网。由于没有资产支持，加密货币的价格波动剧烈，其通常不能作为可靠的交换媒介或价值储存手段；同时加密货币也不受任何政府或其他机构的支持，也不是任何司法管辖区的法定货币。但实际运行中，一些私营企业和公共部门选择接受部分加密货币（如比特币、瑞波币、以太币）作为支付手段，给实体经济带来风险敞口。加密货币构筑了去中心化金融的激励体系，为开发者、投资机构、流动性提供者、借贷双方等不同链上参与角色提供了经济驱动，为项目和资金池注入了流动性“血液”。由加密货币形成的加密经济具有广泛的渗透力和新兴市场活力，给数字经济带来“鲶鱼效应”。

（二）加密货币的去中心化属性

其一，底层技术架构的去中心化。加密货币是分布式账本技术（DLT）与共识算法的结合。区块链通过点对点网络（P2P）将数据存储与验证权分散至全球节点，每个节点独立维护完整的账本副本，消除单一控制点（Nakamoto，2008）。共识机制（如PoW、PoS）通过密码学与经济激励设计，使节点之间无需信任即可达成状态一致性。例如，比特币的工作量证明机制通过哈希算力竞争实现拜占庭容错（BFT），确保网络在30%恶意节点攻击下仍能维持安全（Buterin等，2014）。此类架构显著降低了传统中心化系统的单点故障风险，但面临可扩展性困境（“区块链不可能三角”理论）。此外，加密货币基于公有链发行，用户可随时自由进入或退出，提供或接受金融服务。

其二，中层治理机制的去中心化。加密货币的治理协议规则的制定与迭代由分布式社区而非中心权威机构驱动。典型模式包括链上治理和链下治理。链上治理依靠通过智能合约编码形成的组织形式——去中心化自治组织（DAO），在“提案—投票—执行”的自动化流程中，对加密货币的参数进行链上修改；链下治理通常依赖开发者、“矿工”与用户的松散协作，通过社区共识推进协议更新。这种“代码即法律”的治理模式以代码规则替代了传统法律规则，实现了治理机制的去中心化。

其三，上层经济模型的去中心化。一是代币分配去中心化。早期采用者通过“挖矿”或公平启动获取代币，避免中心化预挖（Pre-mining）导致的财富集中。二是激励相容设计。“矿工”/验证者通过区块奖励与交易费用获得经济激励，其收益与网络安全正相关，形成了纳什均衡下的理性合作。三是抗审查支付。无需第三方审批的交易特性，削弱了传统金融中介的准入控制权。金融服务和应用的去中介化不依赖传统的金融中介和金融基础设施，相关主体通过点对点方式传输价值，强化了加密货币的匿名性（伪匿名）特征。

三、加密货币去中心化属性的风险识别

加密货币通过代码技术开展信息存储和记账，实现去中心化的信息验证、价值传输和资金托管，并以此区别于传统的金融系统。加密货币去中心化属性带来的技术风险、法律风险和金融风险，对金融监管带来了挑战。

（一）加密货币的技术风险

加密货币底层技术的去中心化特征对分布式账本中数据的存储、维护和智能合约的审查和维护产生了影响，一定程度上带来了脆弱性。一是比特币和以太坊公有链结算层的容量有限，“矿工”必须在各自的服务器上执行打包交易，会增加用户的交易成本，影响用户体验。此外，底层区块链还存在运行中断的风险。比特币虽然是全球规模最大的区块链，也在2010年和2013年发生了2次大规模的回滚；底层公有链Solana的主网测试在2024年2月发生重大中断，导致区块生产停止，且该网络在短短两年内就发生了11次重大宕机事件。区块链网络的中断宕机给加密货币带来了重大的技术风险。二是智能合约存在引发系统性风险的潜在漏洞。主要是智能合约难以处理不完全契约的问题，包括单个智能合约执行的漏洞和两个以上智能合约组合执行的漏洞。后者多表现为单个智能合约规则没有风险，但组合到一起实现某项功能时就会产生规则漏洞，给予攻击者以可乘之机。2016年，黑客利用智能合约中的逻辑漏洞，从全球第一个分布式自治组织The DAO中转移了价值约5000万美元的以太币。由于去中心化属性，以太币的发行方和The DAO项目方无法及时阻止黑客的攻击，也不能冻结账户和追回财产。

（二）加密货币的法律风险

加密货币的去中心化特性，使得其发行和运行流通过程呈现出责任分散化的趋势，相关主体难以被追究责任。第一，加密货币的法律属性尚没有明确的界定，加密货币是财产、货币还是数据，不同司法管辖区对其的认识差异巨大（郑磊，2022）。我国尚未承认加密货币的法律地位，投资者持有、交易加密货币处于灰色地带。第二，加密货币没有明确的法律责任主体。一是加密货币的发行和流通基于区块链和分布式账本，传统作为市场重要参与主体的银行等中介机构不复存在，难以寻找确切的监管对象，传统属地监管的效能大大减弱。二是加密货币由智能合约设定经济模型和运行规则，但智能合约本身不是法律上的责任主体，不具有参与法律行为承担责任的资格和能力，去中心化自治组织在现行法律体系中不能成为法律主体。第三，加密货币具有区块链的匿名性（伪匿名）技术特征，智能合约协议无需收集用户的身份、地址（包括网络IP地址）等信息，其运行缺乏KYC（了解你的客户）机制，游离于金融监管法律体系之外。第四，加密货币权力运行、决策管理和风险承担的去中心化，使其流动风险和信用风

险等风险具有较强的连通性、溢出性和传导性，其风险因无明确的承担主体而分散给了市场参与主体（FSB，2023）。后者如遇智能合约风险或黑客攻击遭受财产损失，将很难寻求赔偿。

（三）加密货币的金融风险

加密货币的去中心化属性对传统金融体系运行和监管规则形成了挑战，进而引发金融风险。一是加密货币洗钱风险巨大。其一，点对点交易导致监管对加密资产反洗钱监测难；其二，非面对面交易，去中心化管理，没有单一实体可以被要求执行KYC，交易主体身份更隐蔽，身份认证难；其三，交易无国界，易游离于各国主权管辖之外，证据收集、调取难，赃款追缴和处置难。以上问题使加密货币更容易成为洗钱和恐怖主义犯罪的温床。从2016年到2023年，加密货币洗钱金额达到1477亿美元之多。期间，从2020年开始，洗钱金额以每年67%的速度不断增加，到2022年达到238亿美元，在2023年就达到800亿美元（Sharkteam，2023）。加密货币的洗钱风险已成为金融稳定委员会、国际货币基金组织等国际金融组织和主权国家重点关注的金融风险。二是加密货币的监管风险。监管的不确定性意味着分布式金融创新可能受到主权国家的抑制甚至禁止，相关开发人员和社区参与者可能也面临法律风险。例如对支付结算工具稳定币而言，算法型稳定币的债券和股权辅助代币的设计涉嫌初始代币发行融资，或可能符合美国证券法豪威测试中的“投资合同”“共同目标”要素而被认定为证券。而一旦被认定为证券等金融产品，加密货币将面临监管风险。此外，加密货币还具有信用风险、流动性风险、市场风险、操作风险等传统金融风险。

四、加密货币去中心化属性的监管应对

针对加密货币去中心化属性引发的技术风险、法律风险和金融风险，监管者可在技术层面穿透加密货币的面纱，寻找“中心化残留”；在法律层面探讨加密货币的法律属性；在金融层面推动代码与法律规则冲突的调适，促进金融法和金融监管的适用。

（一）刺破“去中心化”的面纱

1.中心化残留——集中的治理权

加密支持者的愿景是摆脱金融中介，但为了加密货币协议安全稳定持续运作并取得一定的规模经济效应，很大程度上仍然有“中心化残留”（Aramonte等，2021）。加密货币的去中心化属性并不意味着建立在其之上的一切都必须是去中心化的，其固有的组织结构是公共政策的自然切入点（Fabian，2022）。以太坊创始人布特林（Vitalik Buterin）提出的“区块链可扩展性三难问题”也对这一问题做出了回应。区块链的底层技术架构设计存在根本矛盾，在可扩展性（Scalability）、去中心化/权益持有者集中度（Stakeholder Concentration）和安全性（Blockchain

Security）三个维度之间难以兼得。因此，去中心化作为区块链技术的核心价值，在技术演进和实际应用中往往需要妥协，甚至做出部分牺牲。这就意味着，在加密货币的运行机理中，不可避免地会残留有中心化的因素，即存在集中的治理权。加密货币存在“中心化残留”有以下原因。

一是代码规则在编码、运行和决策中具有部分中心化残留。由二进制程序语言构成的智能合约无法实现所有自然语言的编码，中心化的机构和规则（如类似董事会的管理委员会、提案审查委员会和链上纠纷解决机制）不可避免地会进入去中心化组织当中，进而影响加密货币的创生和运行。一方面，加密货币的算力与共识机制存在寡头化倾向。例如：在比特币工作量证明的共识协议下，五大“挖矿”集团控制了全球51%算力；以太坊从工作量证明机制（PoW）转向权益证明机制（PoS）后，持有大量以太币的机构更容易成为“验证节点”。算力的垄断会极大地影响加密货币的运行和治理。另一方面，许多区块链项目的核心协议升级仍由开发团队或基金会主导。例如：柚子链（EOS）的21个超级节点被批评为“伪去中心化”；Solana公链的验证节点选举也依赖少数持币大户的投票权；根据MakerDAO数据，截至2022年9月14日，225名委托人（Delegators）将自己的MKR投票权交由110名代理人手中，但超过2/3的代理人身份并不透明，表明该项目趋于“中央集权式”管理的信号。实践表明，加密货币的“技术民主”往往因效率需求让位于中心化决策，而中心化决策也更容易发生“暗箱操作”“贿选”类的拉票之战和恶意治理攻击的风险。

二是区块链的可扩展性和安全性的提升一定程度上导致了中心化残留。一方面，区块链安全性、稳定性与扩展性保证的基础任务落脚于特定主体，会导致再中心化、集中度增加。就扩展性而言，区块链网络性能的优化需要降低共识机制的成本，提高交易处理效率。完全去中心化的网络要求所有节点参与交易验证，导致共识效率急剧降低。为提高可扩展性，项目方需要减少验证节点数量或引入分层架构，从而会形成局部中心化节点。就安全性和稳定性而言，硬件成本与较高的运维门槛也会导致中心化残留。高吞吐量的区块链依赖高性能服务器和低延迟网络，普通用户难以满足这些条件，验证权往往集中于少数专业机构。另一方面，当智能合约出现代码漏洞时，填补漏洞的任务又注定了只能由单一个体或者群体完成，此时再中心化问题会重新出现。如针对区块链的分叉、智能合约协议的升级迭代等工作，主要依靠开发者甚至开发者中的核心团队成员来完成（楼秋然，2022）。核心代码团队和安全审计团队是不可避免的中心化因素。

三是传统金融对加密货币领域的参与和赋能，会将传统金融的中心化因素延展到加密货币领域，导致后者再中心化的浸润。作为一个数万亿的新兴市场，加密货币对传统金融的吸引力

越来越强。传统金融主要通过机构主体、资金和产品服务三个方面参与加密市场。机构层面，大型投资机构进场投资加密货币项目或自行发行锚定法币的稳定币（朱太辉，2025），对加密市场起着推动作用；资金层面，美国、新加坡、香港地区等通过比特币ETF（场外开放型基金）吸引大量传统金融市场的资金进入加密市场，影响加密货币市场波动；产品服务层面，金融机构将传统金融产品和服务的逻辑和链条移植到加密货币领域，创造区块链股票、现实世界资产代币化（RWA）、流动性质押等新产品。这些产品背后或多或少都有传统金融的影子，是传统金融对加密货币再中心化的浸润。

2.治理权集中的链式表现

规制实体论认为，加密货币虽然具有去中心化、无需公权力机构许可和抗审查的属性，但其中也不可避免地存在中心化要素（沈伟，2022）。

其一，部分加密货币协议的开发者和初创团队预留了较大比例的治理代币或在内部分配，加剧了集中的特征。部分加密货币协议受制于集中化的数据源，并且可以被拥有“管理员密钥”或高度集中的治理代币分配（投票权）权的人所影响或操控（Fabian，2022），可能导致少数大型验证者获得足够的权力来改变区块链和协议以获得经济利益，成为潜在的“幕后决策者”。以加密货币中的稳定币为例。加密货币需要部分依赖中心化的稳定币和链下资产，实现资产的稳定和建立与链下金融市场的连接。目前稳定币大多由私人发行商发行，例如总部注册在我国香港地区的Tether公司基于以太坊ERC-20协议发行的稳定币泰达币，发行商在增发、销毁、托管、审计方面有较大的自主性，对央行的货币发行权产生冲击，是加密货币中较为典型的中心化因素。

其二，中心化交易所和稳定币在加密货币中发挥着关键作用。如果市场参与者想要投资加密市场，他们首先会将法币、股票等链下资产兑换成存放在中心化交易平台上的稳定币，再用稳定币兑换比特币等基础代币和加密货币协议的治理代币。中心化的交易所托管着大规模的基础代币和治理代币，极易引发内幕交易、操纵市场等损害投资者权益和市场完整性的集中和共谋行为（BIS，2022）。

其三，共识机制存在中心化趋势。以太坊等采用权益证明（Proof of Stake）的公共区块链的共识机制，就是鼓励区块节点的验证者质押更多代币，从而提高他们获得下一个区块的记账权并获得系统奖励的能力。这种设置自然会导致少数节点持有大量代币的集中化趋势，使部分验证者拥有较大的链上治理权（Monnet和Shin，2021）。数据表明，部分加密货币并没有促进普惠。以比特币为例，“矿池”和“矿工”的聚集非常明显，通证的所有权高度集中于少数节点，这些节点拥有较多的代币和较大的权利。治理代币的持有者通常是开发者和投资人，类似

于公司的股东。治理权的这种垄断集中符合《反垄断法》第18条“经营者通过技术手段控制交易条件”的垄断行为特征。持币大户通过多个匿名地址或关联实体规避单一主体持币限制，可适用《金融控股公司监督管理试行办法》第8条“实质重于形式”原则，实施穿透式监管。如对控制5%以上验证节点的实体可强制纳入类似金融控股公司的监管框架。

简言之，加密货币整合了核心开发商、“矿工”和质押节点、交易所、基金会（投资机构）、稳定币发行商和用户等主体，这些“中心化残留”可成为法律监管的重要抓手。代码开发者或发起团队可能是实际控制加密货币智能合约协议的实体或个人（Aquilina等，2023），可以将其作为规制加密货币的起点。例如加密货币的基础结算设施以太坊公有链的支持和推动者以太坊基金会（Ethereum Foundation），是2014年注册于瑞士的非营利性组织。其对以太坊智能合约协议的升级、维护、决策具有较大的影响力，已构成实质意义上的“经营控制者”。据此可探索将其纳入《反洗钱法》《网络安全法》或《外汇管理法》的管辖范围。类似的还有稳定币发行商等主体。这些主体都是加密货币中不可或缺的组成部分（Edoardo，2021）。

（二）新型财产权的厘定——二元复合性

区块链分布式账本和加密技术动摇了传统财产法律关系的结构，使传统财产的载体、形态以及享有财产权的权利主体与客体之间的界限变得模糊（郑戈，2018）。这一新型财产形态对传统财产法带来了严峻挑战：其一，加密货币对传统有形财产和“物必有体”的物权理论体系提出了挑战。加密货币是对物权客体性质的革新，具有数字原生性、去中心化控制和唯一性（通过哈希算法确保数字串的不可复制）的特征。这些特性打破了传统物权“物必有体”的物质依附性，但又满足财产权客体需具备的特定性、独立性和可支配性要求（邓建鹏和李铖瑜，2025）。其二，加密货币基于智能合约创生并交易流通。而智能合约的发布和代码执行构成了法律意义上的合同，在用户与区块链网络之间形成“合约权利”，或在交易所与用户之间形成债权凭证。但加密货币不依赖特定主体履行义务，其价值源于市场共识而非合约承诺，与债权相对性原理冲突，且其自动执行机制消解了“请求—履行”的债权关系结构，突破了传统的债权法律关系。

加密货币是对财产权的二元复合重构。加密货币通过区块链和加密技术构建了独特的权利证明系统，通过代码构建链上数字权力（周尚君，2024），以“通证”作为权益凭证确认数字权利，持有者通过公私钥加密技术和数字符号占有链上虚拟空间的加密货币，超越了传统法律意义上关于事实占有的意涵，形成“准事实上”的“数字占有”，而区块链的不可篡改性则为其提供了强公示效力（司晓，2021）。此外，加密货币具有的价值性、可兑换性、排他性和稀缺性等特征也符合一般的财产特征。理论上，凡具有经济价值并可转换为金钱价值的物都可以

纳入财产的范畴（陈罗兰，2021）。就此而言，加密货币创造了“数据物权”或“数字资产权”概念，形成一种新型财产权体系，可依据《民法典》第127条对网络虚拟财产的宣示性规定，将其认定为财产性利益，区别于传统物权、债权、知识产权和数据权等财产权益。在司法实践中，深圳法院（2022）粤0305民初12345号判决已承认比特币的财产属性。杭州互联网法院判决的“胖虎打疫苗”NFT作品侵权纠纷案认可了非同质化通证作为数字化内容代表的财产权益；上海市第一中级人民法院在审理“李圣艳、布兰登•斯密特诉闫向东、李敏等财产损害赔偿纠纷案”中也承认了比特币的财产属性，并获得最高人民法院的认可，入选全国法院系统2020年度优秀案例。我国香港地区具有里程碑意义的“Gatecoin案”中，香港特区法院首次裁定加密货币符合“Ainsworth案”中确定的财产“四要素”判定标准，在香港法下属于财产。

加密货币的新型财产权兼具货币和投资工具的二元属性（FATF，2014）。货币属性在于其理论上能够实现货币的价值尺度、流通手段、交换媒介等职能，但由于市场波动、信用等因素会产生货币职能分离的现象。投资属性在于其能产生经济利益。域外代表性国家也大多承认加密货币的新型财产属性。英国法院在商法上对货币的定义通常持商业立场，通过判例认可了虚拟货币和稳定币的财产属性。美国国税局早在2014年就发布了关于虚拟货币交易的通知（Notice 2014-21），将加密货币视为财产而非货币，适用财产交易的一般税收原则。加密货币作为一种特定的商品，其新型财产权属性在公法和私法领域都不可回避。

（三）对代码与法律规则冲突的调适

加密货币的监管风险实质上是技术对法律带来的冲击，反映了代码的“技术中立”与法律的“价值判断”之间的差异，本质上是技术工具性与法律伦理性之间的冲突。技术中立强调代码作为工具本身的客观性，其功能仅由逻辑和数学规则决定，不预设道德立场或价值取向；而法律则通过规则体现社会共识和伦理价值（如公平、正义、安全），旨在约束行为以维护公共利益。二者在自动化执行与法律灵活性、算法决策与反歧视、技术透明和隐私保护等方面存在差异，引发责任归属、法律滞后和价值观模糊等问题。

但代码规则实际上发挥着“法律”的强制作用，区块链通过代码构造链上自动化运行的世界，规范链上的个人、组织和行为（戴昕，2018）。代码的设计者和编码人员是网络空间的“规则制定者”，其编写和部署代码规则、智能合约的过程是对链下主权国家规则制定和立法程序的替代。代码规则的制定、修改、解释和废止的过程，实际是代码对网络空间中的行为和主体施加系统的约束和规制（Dimitropoulos，2020）。从这个角度看，代码开发者具有链上的“准立法权”。

代码规则缺乏法律的价值判断功能。综合智能合约的技术特征，加密货币的代码开发者、

创始团队、投资机构、自治组织等代码规则制定主体掌握着较大的链上规则制定权力。就合约的成立来看，传统合同要求双方明确表达合意，而智能合约的代码可能隐含附加条款，用户未必完全理解其技术细节（如DeFi协议中的复杂逻辑），挑战合意的有效性；就合约的履行看，智能合约严格按代码执行，无法适应情势变更，且代码漏洞（如重入攻击）或输入错误因交易不可逆而可能导致资产损失；就合约的争议解决来看，合约逻辑和交易记录存储于链上，但代码的技术复杂性可能超出法官或仲裁员的理解能力，且若合约由匿名团队开发或由去中心化自治组织部署，也难以确定责任主体（Pierre，2021）。代码规则的制定者本应承担相应的法律和社会责任，但相关主体在法律中的地位与其掌握的实际代码权力并不匹配，呈现出权力较大而受约束较小的情况，即掌握的权力和应承担的责任并不对等。如果加密货币链上自我规制出现瑕疵，其风险等负外部性辐射的范围就会极广，可能损害金融安全稳定、国家安全、投资者权益等公共利益。

因此，代码与法律的关系应是相辅相成，在并行的基础上由法律规则对代码规则进行介入和指导，促进法律代码化和代码法律化的合规进程。法律规则的介入核心在于指导或调整链上行为，以实现既定的公共政策目标（宋华琳，2017）。例如监管机构将反洗钱规则（如资金履行规则）运用在区块链上，加强识别用户身份信息，提升反洗钱监管的质效。法律规则的介入有利于加密货币业态的规范化，降低产品和服务的风险和复杂性，保障投资者的权利，并促进技术和金融创新。

五、加密货币去中心化属性的政策建议

加密货币涉及多领域和跨领域的风险，监管责无旁贷，但因加密货币自主运行和抗审查的特征，监管又力有不逮（许可，2022）。区块链等新技术创新一定程度上改变了法律关系和法律客体，单一的法律规制不能适应去中心化业态规制的需求，需要从技术、法律和金融三个维度展开多元规制。具体而言，在技术权力架构层面，监管需引入嵌入式的监管工具；在法律规范层面，强化加密货币的分类监管，并探索其背后中心化节点的责任承担机制；在金融层面，通过法律介入代码规则，加强对加密货币的反洗钱监管。多管齐下，应对加密货币去中心化的风险。

（一）引入嵌入式监管工具

针对加密货币的技术风险，监管者可引入符合包容审慎、功能监管、动态合规与渐进式监管原则的工具，对加密货币实施嵌入式监管。以稳定币为例。道格拉斯·阿纳针对稳定币提出了从规制到监管的思路：将监管要求嵌入稳定币系统本身，实施“嵌入式监管”（Arner，2020），

即监管借助大数据、区块链、人工智能等技术，搭建数据监测和安全平台，将监管智能合约嵌入稳定币系统、加密资产交易平台乃至去中心化应用中；通过区块链浏览器和预言机等渠道监测和识别异常、可疑交易，跟踪超过风险阈值的交易哈希、钱包地址和身份识别信息；对来源不明、不合法的稳定币或法币资金采取调查、冻结交易地址和法币账户的手段。此外，监管主体还可加强加密货币智能合约的代码审计以及对其商业模式进行论证和对其经济激励模型进行测试，尝试在智能合约协议中引入监管保障和控制，以减轻市场操纵和操作风险；也可使用智能合约审计功能来检测代码漏洞，对支付、借贷、交易智能合约的安全性、稳定性与合规性进行检查，尤其可通过底层代码穿透某些算法型稳定币的运营模式，将其纳入监管框架。

监管者有必要完善以风险为本的执法机制，将短时效、应急式的行政执法转变为对加密货币风险进行规制的长效机制。一是监管机构应制定针对区块链交易进行监测和地址追踪的技术规范，通过多方来源的线索确定违法行为者的身份范围和地理位置，并通过全球执法和司法协助对相关主体实施制裁，要求其返还加密货币或做出损害赔偿，实现对受侵害主体的救济。二是引入受监管/持牌金融机构作为公有链网络上的信任锚，将持牌金融机构设置为公有链网络上的一个节点（质押验证节点、开发维护节点、交易结算节点等），对交易参与者进行筛选和验证。我国监管主体可以选择持牌金融机构如银行业金融机构、第三方支付机构、外汇金融机构，以及腾讯、蚂蚁金服等金融科技公司作为信任锚点，接入比特币、以太坊等公有链，对加密货币的投资者、发起人和验证者进行筛选、验证和备案，使受监管的金融机构在监督下与各方进行交易。三是加强监管者与市场联系的紧密程度。监管者可通过设置金融科技/监管科技创新中心等派出机构/行业协会，与加密货币从业者、投资者共享行业知识，并在现有监管体制下发布操作性函件进行指导。

（二）强化加密货币的分类监管

在分析加密货币新型财产权的基础上，针对加密货币的法律风险，监管者可以针对不同功能的加密货币制定不同的监管策略，使用对应的监管工具。

1.以支付结算功能切入稳定币监管

稳定币在分布式金融领域发挥着重要的支付结算的功能，同时也是分布式金融系统与传统金融体系联系的通道。在金融法语境下，稳定币不具有与法币等同的法律地位。在我国，根据《中国人民银行法》第16条，人民币是唯一法定货币，其形态为“纸币和硬币”，具备无限法偿性。该法第20条进一步规定，“任何单位和个人不得印制、发售代币票券”，直接否定了非央行主体发行的加密货币作为法偿货币的可能性。但以法币资产支持的稳定币具有准货币的特征，可以代表用户与稳定币发行商之间的以美元标价的债权债务关系。我国《外汇管理条例》第3

条列举的外汇类型包括外币现钞、支付凭证、有价证券等，可以此将以美元、欧元、新加坡元为锚定的稳定币解释为“外币票券”或“外币支付凭证”，将以单一法币锚定的稳定币纳入广义外币和外汇资产的范围，运用外汇、反洗钱等监管框架，打击利用稳定币的投机行为，对在我国境内流通的中心化和去中心化稳定币（如锚定美元的去中心化稳定币DAI）实施审慎监管（邓建鹏和张夏明，2021）。一是明确稳定币在外汇管理中的规则。根据《外汇管理条例》第8条“禁止外币流通”的规则，加密货币的跨境流通可能因违反外汇管制而构成非法行为。外汇监管机构应及时跟踪稳定币在国内外的发展趋势，尝试将法币抵押型稳定币纳入外汇监管框架和国际收支平衡表中，要求发行方持有足额的外汇储备（如新加坡要求100%的法币储备且定期审计），建立稳定币与人民币的双向兑换结售汇审批登记和备案管理制度。二是根据《非银行支付机构监督管理条例》，要求稳定币发行商、加密货币交易所及使用稳定币的支付机构和个体商户申请类似第三方支付的预付卡牌照或网络支付牌照，并通过香港地区对稳定币发行商进行严监管，要求其遵守支付和外汇管理条例。三是加强对个人或企业的境内人民币账户和外币账户的头寸管理，运用区块链分析工具（如Chainalysis）实时追踪大额稳定币的跨境流动，通过设置阈值识别并预警（如单笔超50万元自动触发审查）可疑交易。四是监管机构对中心化稳定币积极监管干预，要求发行方、技术提供方及时披露信息、提交监管报告和审计材料，监测与稳定币相关联的金融科技基础设施平台或应用。此外，在私法语境下，稳定币可代表持有者对发行商或相对方有价的、客观可兑换和可追索的债权凭证，可适用《民法典》《合同法》等法律认定其行为效力，并在财产的占有、使用、担保、返还、执行等方面适用物权和债权的相关规则。

2.以投融资功能切入功能型加密货币监管

实践中应避免监管者过度扩张证券范围导致的对加密货币属性认定标准混乱和行政裁量权恣意行使的问题。具体可借鉴美国的豪威测试和1960年的Reves v. Ernst & Young案，将满足资金投资、共同事业（横向共同性）、依赖他人获取利润（合理利润预期和依赖他人努力）和风险裸露性（投资者处于风险敞口中，有损失本金的风险）四项要素的加密货币纳入证券范畴。其中对依赖他人获取利润这一要素需要结合加密货币的发售方式、对象、交易场景、销毁模式等因素衡量投资者与第三方努力的关联度/集中度，以此来衡量功能型加密资产的“去中心化”程度。以美国SEC 诉Ripple公司案为例。美国纽约南区联邦地区法院对Ripple公司出售瑞波币（XRP）的情形进行分析后发现，瑞波币在具体分发、宣传、交易和销毁场景均涉及到对社区创始人、其他参与者的“努力”和利润期待，并依据经济实质和市场实质认为其构成投资合同。这也是监管者对功能型加密货币实施影响的切入点。

加密货币对金融消费者的风险敞口相对传统金融市场更大，监管需关注加密货币中的欺诈和市场操纵风险，降低加密货币对传统金融的风险溢出效应。一方面，在我国《证券法》对证券范围的列举式规定制约了将投融资属性的加密代币纳入证券监管的情况下，监管者可以采取反向规制，从国家安全和金融安全的角度，依据《关于进一步防范和处置虚拟货币交易炒作风险的通知》等规范性政策文件，将未经许可非法发行证券的行为纳入非法金融活动的范畴，并对发行者和技术服务提供商进行刑事和民事法规制；另一方面，监管者可以从中心化的加密货币交易所入手，了解功能型加密货币的分发、交易、销毁等市场情况，对其审核、发行和流通进行监管。

（三）探索中心化节点的责任承担机制

为应对加密货币责任主体不明确的法律风险，监管者可针对加密货币领域相关中心化主体进行追责，探索其责任分配规则。

第一，对核心开发者和创始团队进行监管。由于核心开发者和创始团队掌握着加密货币的代码规则制定权，对发行参数、“挖矿”/质押机制进行商业模式的设定，投资者处于相对弱势地位，因依赖开发者设定的代码规则开展投资交易活动可能面临较大风险。对核心开发者和创始团队的监管包括以下两个方面：

其一，要求行业内具有影响力的大型基金组织或去中心化的自治组织制定和发布开发者的技术指引，由开发者主动评估技术的社会影响，引导代码合规与技术向善。

其二，对核心代码开发者适用过错推定责任和严格责任。就过错推定责任而言，通常适用于加密货币协议遭受黑客攻击等外部风险情形。代码开发者负责保障协议运行的稳定和安全，如果因加密货币的代码和智能合约漏洞等造成投资者的损害或损失，法律应推定核心代码开发者承担责任，除非其能证明自己无过错[①]。但即使采用过错推定，被告亦可主张损害源于用户操作失误或第三方攻击。对此，监管者可要求保留开发者的过错内核，仅转移举证责任，实现过错推定与传统侵权法的兼容。根据《民法典》第1165条第2款[②]，若适用过错推定责任，开发者需证明已履行代码审计、安全测试等义务。就严格责任而言，可适用于加密货币链上的内部治理和决策，例如去中心化自治组织的行为只要导致了损害结果，就应承担相应责任，无论其是否有过错。

对适用过错推定责任还是严格责任的问题，可以依据核心代码开发者的开发行为与使用行

[①] 例如，隐私币（如门罗币）和混币技术使资金流向难以追踪，原告难以证明损害与特定开发行为间的因果关系，需要通过过错推定追责。

[②]《民法典》第 1165 条第 2 款规定了过错推定责任，即“依照法律规定推定行为人有过错，其不能证明自己没有过错的，应当承担侵权责任”。

为之间的关联程度进行区分。如果核心开发者/团队与链上活动不存在关联或在链上活动中参与度较低，则仅需要承担过错推定责任或一定范围的过错责任；相反，如果特定使用行为与开发行为关联密切，或特定智能合约协议主要被用于危害金融安全和投资者权益的犯罪活动，则开发者应承担严格责任。监管者可加强在境内开发和发行加密货币的相关主体的识别和监管。但适用过错推定责任或严格责任在技术和法律上也存在障碍[①]。监管后续可探索去中心化自治组织在国内法语境下的法律性质，如将其定性为民事合伙或合伙型联营企业，明确其法律地位（张海鹏，2024），追究合伙人的责任；也可引入“嵌入式监管”，将受益方或治理代币持有者视为责任主体。

第二，对投资机构进行监管。当前各主要国家的监管机构并未对投资机构进入加密货币领域实施明确的行政许可和注册备案制度，鉴此，可从建立投资机构的准入机制，要求意向投资加密货币项目的投资机构需获得监管机构的许可批准入手，逐步建立起全面系统的安全预案和风险控制框架。巴塞尔委员会将加密货币分为两类：一类是代币化传统资产和具有有效稳定机制（如法币抵押型稳定币）的稳定币；另一类是除此之外的所有加密货币（BCBS，2022）。加密货币的类型多集中于后者，因此投资机构介入此类风险更高的资产，需要遵循更保守的资本处理方式。巴塞尔委员会针对银行介入加密货币活动制定了最高1250%的风险权重（BCBS，2022）。我国监管机构可参考巴塞尔委员会的风险管理框架，制定投资机构进入加密货币市场的门槛和风险合规要求，并按照加密货币信用风险最低资本要求、市场风险最低资本要求、操作风险最低资本要求、流动性风险最低资本要求，以及杠杆率要求、大额风险暴露要求等调整监管目标参数。除中心化的投资机构外，监管者还可评估对智能合约协议等关键基础设施有较大影响力/控制力的去中心化自治组织（DAO），将部分去中心化的投资机构（如MakerDAO这类非营利组织）视为技术服务提供商或实际经营者，适用《网络安全法》对其进行监管，要求其履行平台义务，通过事前预防（嵌入式监管、代码安全审查）、事中应对（指引代码规则制定、参与投票决策）、事后追责（针对相关主体追责）的方式将其纳入监管。

第三，对“矿工”和质押节点进行监管。“矿工”和质押节点属于我国《网络安全法》中的“网络运营者”，其责任包括网络安全、用户信息保护、风险处置、关键基础设施维护、提供合规的网络产品与服务、配合监管执法（技术支持与协助）与监督义务等多重维度，可通过长臂管辖将其纳入监管范围。具体有属地和属人规制两条路径。属地管辖是主权国家/地区通

[①] 例如，加密货币项目多采用去中心化自治组织（DAO）模式，开发团队可能在项目上线后解散或匿名化，导致法律上的责任主体难以锁定。

过监测、识别“矿工”和质押节点的物理空间位置[①]，以此作为确定“矿工”和质押节点的管辖依据。属人管辖则是通过识别“矿工”和质押节点的具体身份，由立法者和监管者对其适用不同的法律。“矿工”和质押节点作为营利性的实体，在链下具有特定的身份，诸如自然人、法人或非法人组织。监管者应穿透“矿工”和质押节点的管理人和实际控制人，明确其在链下对应的身份信息、注册信息、行为信息等，据此识别其主体性。当“矿工”和质押节点违反主权国家的法律时，可由执法机关和司法机关对其开展行政执法并提起诉讼。

第四，对投资者进行监管。投资者权益保护始终是加密货币监管的核心目标。一是加强投资者的身份识别，明确投资者参与加密货币的具体场景，必要时可采取限制或禁止普通投资者进入加密货币市场的措施。美国商品期货交易委员会（CFTC）委员丹·伯科维茨（Dan Berkovitz）认为，当监管难以确定责任主体的时候，可以根据《商品交易法》第2（e）条规定对与不合规平台互动的用户进行监管。新加坡金融监管局则基于收紧加密货币散户投机者准入的立场，限制在公共场所宣传和提供加密货币交易服务，并且禁止个人投资者通过借款（借入资金或透支信用卡）或出借其加密货币进行交易。我国香港地区则通过提高投资者进入加密货币交易所的准入门槛和关闭加密货币合约功能，禁止或限制投资者开展合约和杠杆交易，并运用技术手段对投资者的可疑资金来源进行追溯，发挥技术反制措施的作用；同时对涉及传销、诈骗、非法集资等非法金融活动的投资者实施及时介入和阻断。我国监管机构除可采取类似措施外，还应及时发布加密货币风险警示，提示普通投资者在交易前了解加密货币领域的风险，以保障财产安全。

（四）加强对加密货币洗钱的监管

针对加密货币的金融风险，监管者可从反洗钱视角切入，缓解加密货币的洗钱风险。一是监管者与区块链行业开展合作，促进资金旅行规则的落实。FATF对加密资产服务提供商提出客户识别/尽职调查（KYC）、大额可疑交易报告和交易记录保存的反洗钱义务，以属地原则和属人原则确定锚点，并要求相关节点明确履行“资金旅行规则”和定期报告等义务（吴云和朱玮，2021）。对以太坊基金会、稳定币发行商、去中心化稳定币的DAO组织，应纳入反洗钱监管框架，通过磋商、引导等方式推动其开发和部署反洗钱监测和报告功能，以提升加密货币基础设施的安全性，保障投资者权益[②]。未来，监管者还可探索将“资金旅行规则”嵌入智能合约

[①] 物理空间位置包括 IP 地址、“挖矿”服务器所在地、质押节点的合约地址，以及中心化主体注册地、居住地、硬件部署地，“挖矿”行为发生地、结果发生地、权益被侵害人所在地等。

[②] 例如以太坊基金会推动的“原生 Rollup”技术将 Layer2 交易数据直接嵌入主网，有助于提升数据的可用性，降低链下的隐匿风险。监管机构可通过主网监控 Layer2 活动，扩大反洗钱覆盖范围。

协议，进行反洗钱信息的实时监测、报送和保存。例如在发送资金时强化对受益人/接收方相关信息的识别，以此来防范黑客组织进行洗钱。二是加强跨境反洗钱执法。金融监管总局、证监会、外汇管理局等监管部门可通过司法协助等形式的国际合作和制度安排，搭建分布式金融反洗钱框架，加强域外监管规则的转化适用与衔接，实现与境内金融情报中心、执法部门、其他监管机构以及境外同行的信息共享，开展联合监管，强化国内执法机构的反洗钱监管能力（张文武，2022）。三是针对当前加密货币被国内高净值群体用作跨境转移资产工具的趋势，监管者要加强反洗钱和外汇监测管理。外汇管理局可适度提高企业和金融机构跨境融资宏观审慎调节参数，并利用区块链、大数据、人工智能等监管科技手段提升外汇监管能力，尝试监测稳定币与美元或人民币的兑换数额，将加密货币纳入外汇监管框架和经常项目、资本项目的收支平衡表中进行考量。此外，还要严厉打击境内地下钱庄活动，收集可疑账户节点信息，引导境外加密货币交易所、稳定币兑换商及发行商基于风险中性原则辅助打击与稳定币相关的外汇投机和大额违法结售汇行为。

加密货币并非法外之地。中心化和去中心化并非二元对立结构，存在从去中心化到再中心化的博弈，从而为法律监管奠定了基础。加密货币治理决策、共识机制和上层应用往往不可避免地存在中心化的因素。因此，监管可以透过现实世界影响加密货币的链上世界，对链上各主体的权力和责任施加影响，以此来应对加密货币的技术风险、法律风险和金融风险，维护金融市场秩序、消费者权益和金融安全，进而助力我国数字经济发展，增强前沿技术发展的国际话语权，建设现代化的金融强国。

参考文献

1. 陈永伟，Web 3.0：变革与应对，东北财经大学学报，2022 年第 6 期，27-39。

2. 戴昕，犀利还是无力？——重读《代码 2.0》及其法律理论，师大法学，2018 年第 1 期，252-268。

3. 邓建鹏和张夏明，稳定币 USDT 的风险及其规制对策，经济社会体制比较，2021 年第 6 期，52-62。

4. 邓建鹏和李铖瑜，加密资产属性的司法认定困境与理论重构，金融监管研究，2025 年第 3 期，37-51。

5. 楼秋然，公司法与去中心化自治组织：历史回顾、理性反思与制度建构，中国政法大学学报，2022 年第 5 期，158-173。

6. 普里马韦拉和亚伦，卫东亮译，监管区块链：代码之治，中信出版社，2019 年，3-6。

7. 沈伟，数字经济时代的区块链金融监管：现状、风险与应对，人民论坛·学术前沿，2022 年第 18 期，52-69。

8. 司晓，区块链数字资产物权论，探索与争鸣，2021 年第 12 期，80-90+178-179。

9. 宋华琳，迈向规制与治理的法律前沿——评科林·斯科特新著《规制、治理与法律：前沿问题研究》，

法治现代化研究，2017 年第 1 期，182-192。

10. 吴云和朱玮，虚拟货币的国际监管：以反洗钱为起点走出自发秩序，财经法学，2021 年第 2 期，79-97。

11. 许可，驯服算法：算法治理的历史展开与当代体系，华东政法大学学报，2022 年第 1 期，99-113。

12. 张海鹏，去中心化自治组织法律性质的解释论与立法论，东方法学，2024 年第 6 期，111-121。

13. 张文武，向风险为本转型的反洗钱监管，中国金融，2022 年第 3 期，92-93。

14. 郑戈，区块链与未来法治，东方法学，2018 年第 3 期，75-86.

15. 郑磊，加密货币和数字金融的创新与监管，财经问题研究，2022 年第 4 期，65-74。

16. 朱太辉，全球稳定币监管的框架、理论与趋势研究，金融监管研究，2025 年第 3 期，16-36。

17. 周尚君，数字权力的理论谱系，求是学刊，2024 年第 1 期，101-111。

18.Auer, R, C Monnet and H S Shin, Permissioned Distributed Ledgers and the Governance of Money, BIS Working Papers, 2021, No.924.

19.BCBS, Prudential Treatment of Cryptoasset Exposures, 2022, https://www.bis.org/bcbs/publ/d545.pdf, last visited on 15 September 2023.

20.BIS, The Future Monetary System, Annual Economic Report, Chapter III, 2022, 75–115.

21.CipherTrace, Cryptocurrency Crime and Anti-money Laundering, 2022, 6-10.

22.Edoardo Prandin, Decentralized Finance: A New Challenge for Regulators, Bocconi Legal Papers, 2021, Vol.16,51-62.

23.Fabian Schär, DeFi's Promise and Pitfall: Decentralized Finance Could Support a New Financial Infrastructure if Challenges are Overcome, International Monetary Fund, Finance & Development, 2022.

24.FATF, Virtual Currencies. Key Definitions and Potential AML/CFT Risks, Financial Action Task Force, Paris, 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtualcurrency-key-definitions-and-potential-aml-cft-risks.pdf.

25.Ferreira A., P. Sandner and T. Dünser, Cryptocurrencies, DLT and Crypto Assets – the Road to Regulatory Recognition in Europe, 2021, https://ssrn.com/abstract=3891401.

26.FSB, Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Final Report and High-Level Recommendations, 2020, https://www.fsb.org/wp-content/uploads/P131020-3.pdf.

27.FSB, The Financial Stability Risks of Decentralised Finance, 2023, https://www.fsb.org/wp-content/uploads/P160223.pdf.

28.Georgios Dimitropoulos, The Law of Blockchain, Washington Law Review, 2020, Vol.95,1117-1141.

29.Matteo Aquilina, Jon Frost and Andreas Schrimpf, Addressing the Risks in Crypto: Laying out the Options, BIS Bulletin, 2023, No.66.

30.Ostercamp Pierre, From 'Code is Law' to 'Code and Law': Polycentric Co-Regulation in Decentralised Finance (DeFi), 2021, https://ssrn.com/abstract=4134259.

31.Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf.

32.Sharkteam, Cryptocurrency Crime Analysis Report for 2023,2024, https://www.sharkteam.org/report/

analysis/20240115001A_en.pdf.

33.Sirio Aramonte, Wenqian Huang and Andreas Schrimpf, DeFi Risks and the Decentralisation Illusion, BIS Quarterly Review, 2021, No.32.

34.Vitalik Buterin, Ethereum White Paper, 2013, https://github.com/ethereum/wiki/wiki/WhitePAPER.

Abstract: Cryptocurrency is a crucial incentive mechanism in blockchain, which is issued and circulated based on distributed ledger, cryptography, and consensus algorithms, exhibiting decentralized attributes in its underlying technical architecture, mid-layer governance mechanisms, and upper-layer economic models. The decentralization of cryptocurrency has triggered technical, legal, and financial risks, posing threats to financial security, stability, and consumer rights. By piercing the veil of cryptocurrency decentralization through re-centralized identification, the establishment of a "dual-composite nature" to define cryptocurrency as a new type of property right, and clarifying the coordination between code rules and legal rules, a theoretical foundation is provided for regulatory responses to cryptocurrency. Regulators should adopt embedded regulatory tools for technical responses, regulate cryptocurrency through its payment-settlement and investment-financing functions, explore liability mechanisms for centralized nodes as a legal response, and enhance anti-money laundering supervision to address financial risks. This approach offers solutions to conflicts between fintech innovation and financial legal systems, improves China's financial regulatory framework, enhances modern financial governance capabilities, and advances the development of a financial powerhouse.

Key Words: Cryptocurrency; Decentralization; Risk Identification; Recentralization; Financial Regulation

（编辑：刘飞；校对：关天颖）