慢雾：面向香港稳定币发行人的智能合约实施指南

原创 慢雾安全团队 慢雾科技 2025年07月22日 15:25 福建

随着《稳定币条例》的正式通过，香港金融管理局(HKMA) 于 2025 年 5 月 26 日发布了《持牌稳定币发行人监管指引（草案）》，旨在确保本地稳定币生态的稳定、安全与合规运作。该指引详尽列明了持牌稳定币发行人必须持续遵守的监管要求与运营标准。

近期，越来越多机构就智能合约的合规实施问题向慢雾安全团队(SlowMist) 咨询。为协助发行人更好地理解和部署合规的智能合约体系，我们特别发布了《面向香港稳定币发行人的智能合约实施指南》，以提供清晰的技术路径与实践建议，支持香港稳定币生态的健康发展。

第一部分 基础架构与合规策略

本部分旨在为稳定币系统奠定高层架构的基石，这些架构决策完全由香港金融管理局(HKMA) 框架中最根本的要求驱动。在此处做出的选择将决定整个实施路径，确保从设计之初就将合规性深度嵌入技术栈中。

1. 底层分布式账本的选择

监管指令

持牌人必须评估其所使用的底层分布式账本技术(DLT) 的稳健性。此评估涵盖安全基础设施、对常见攻击（如 51% 攻击）的抵御能力、交易最终性保障以及共识算法的可靠性[1]。

慢雾(SlowMist) 技术解读

这并非一项简单的技术偏好选择，而是一项核心的合规任务。对底层区块链的选择必须经过正式的尽职调查，整个评估过程也需被详细记录，以便在监管审查时提供充分理据。底层账本的选择过程实际上为整个稳定币系统的安全性与稳定性奠定了基调。

香港金管局对账本稳健性的强调，实质上是在劝诫发行方避免采用未经市场验证、中心化程度过高或安全性存疑的新兴区块链。证明其安全性与稳定性的责任完全由发行方承担。如果发行方选择了安全性尚未被广泛验证的链，就必须设计并实施额外的补偿性控制措施。

实施指南

- **优先选择成熟的公有链：** 建议优先选用如 Ethereum、Arbitrum 等成熟且具备高安全性的公有区块链。这类网络凭借其久经考验的韧性、庞大的验证节点网络以及持续的公众监督，具备天然优势。其高昂的攻击成本（经济安全性）可直接回应监管对抵御 51% 攻击及保障交易最终性的关切。
- **替代方案的严格评估：** 若考虑采用联盟链或其他类型的分布式账本，必须开展一项严谨且可量化的对比分析，例如慢雾安全审计，以证明其安全标准不低于，甚至优于主流的公有链。

- **风险评估文档：**评估报告必须全面覆盖其抵御常见攻击的能力、共识算法类型，以及与代码缺陷、漏洞、漏洞利用及其他威胁相关的风险[2]，并详细分析这些风险如何对稳定币的发行、赎回及日常运营构成潜在影响。此文档是向监管机构证明技术选型审慎性的关键文件。

2. 核心代币标准与监管功能扩展

监管指令

监管文件并未指定某一特定的代币标准（如 ERC-20）。然而，文件强制要求实现一系列核心管理功能，包括铸币(mint)、销毁(burn)、升级(upgrade)、暂停(pause)、恢复(resume)、冻结(freeze)、黑名单(blacklist)、白名单(whitelist) 等操作[3]。

慢雾(SlowMist) 技术解读

香港金管局事实上定义了一个功能远超 ERC-20 标准的"监管增强型"代币标准。该标准不仅要求具备基础的代币流转功能，更强调操作安全性、权限可控性和风险可追溯性。为了在满足合规要求的同时最大限度地保障安全性，最高效且最稳妥的开发路径，是采用经过广泛审计、社区公认的标准库（如 OpenZeppelin），并在此基础上进行功能扩展。

实施指南

- **基础标准：**采用 ERC-20 作为基础标准，以确保代币的同质化和在更广泛生态系统中的互操作性。
- **功能扩展：**必须集成以下功能模块，以满足监管要求：
  - **Pausable：**用于实现对所有代币活动的全局暂停与恢复功能，这是应对重大安全事件的核心工具。
  - **Mintable：**用于实现持牌发行人需通过受控流程铸造新代币，并确保代币发行量严格对应足额法币储备资产。
  - **Burnable：**提供销毁代币的功能。在具体的实现中，此功能将是受严格权限控制的，而非允许任意用户自行销毁。
  - **Freezable：**用于暂停特定账户的代币转移功能（如涉及可疑交易）。
  - **Whitelist：**用于实施额外的安全措施，仅允许通过尽职调查和批准的地址参与核心操作（如接收新铸代币[4]）。
  - **Blacklist：**用于实现对涉及非法活动（如洗钱、欺诈）的地址实施交易禁令，禁止其发送 / 接收代币。黑名单管理需与 AML / CFT 系统联动，实时监控可疑交易。
  - **AccessControl：**这是实现精细化、基于角色的权限管理系统的基础。所有管理功能都必须通过此模块进行权限控制，以满足职责分离的要求[5]。

3. 主要合规模式：黑名单与白名单的选择

监管指令

关于持续监控，反洗钱 / 打击恐怖分子资金筹集(AML / CFT) 的咨询文件提出了多种措施，其中包括“将被识别为受制裁或与非法活动相关的钱包地址列入黑名单”，或者采取更严格的“对稳定币持有人的钱包地址实行白名单制，或采用闭环模式”[6]。

慢雾(SlowMist) 技术解读

这是整个系统架构中最为关键的决策点，它直接决定了稳定币的开放性、实用性以及合规操作的复杂性。

- **黑名单模式：**一种“默认开放”的模式。所有地址默认可以自由交易，只有那些被明确识别并添加至链上黑名单的地址，才会被限制。
- **白名单模式：**一种“默认关闭”的闭环模式。任何地址，除非经过发行方明确的尽职调查和批准，并被添加至链上白名单，否则无法持有或接收代币。

尽管白名单模式提供了 AML（反洗钱）控制能力，但对于一个旨在被广泛使用的稳定币而言，严格的白名单制度意味着稳定币只能在预先审查过的参与者之间流转，这使其更像一个封闭的银行账本系统，而非一种灵活的数字货币。

因此，同样被监管明确提及的黑名单模式，结合监管所要求的强大链下分析工具，构成了一种更为平衡的方案。它既满足了监管要求，又保留了资产的实用性。

在设计上，系统可以被构建为可升级的，或同时实现两种模式，以便在未来监管收紧或业务模式变更时，能够平滑过渡或切换至白名单模式。

实施指南

- **黑名单模式（默认推荐方案）：**
  - **优点：**具有更高的实用性，能够与广阔的去中心化金融(DeFi) 生态系统无缝互操作，为用户提供更低的使用门槛和更流畅的体验。
  - **缺点：**合规性高度依赖于强大的、实时的链下监控分析能力，以便及时发现并封堵非法地址。
  - **实现方式：**在智能合约的转账函数中，增加逻辑检查，确保交易的发送方(from) 和接收方(to) 地址均未被记录在黑名单中。
- **白名单模式**
  - **优点：**提供最高级别的 AML / CFT 控制，实现了事前预防，而非事后补救。
  - **缺点：**极大地限制了稳定币的通用性和采纳率，为管理白名单带来了巨大的运营开销，可能使其难以成为一种被广泛接受的交易媒介。
  - **实现方式：**在智能合约的转账函数中，增加逻辑检查，要求交易的发送方(from) 和接收方(to) 地址都必须存在于白名单中。建议开发专用 Web 用户后台系统进行操作，增加操作的便利性。

第二部分 智能合约实现

本部分为智能合约的核心功能提供了一份详尽的蓝图，将复杂的监管要求转化为具体的代码级逻辑、安全模式和操作协议。

1. 设计精细化的访问控制系统

监管指令

高风险操作的设计必须"防止任何单一方能够单方面执行相关操作（例如，通过**多重签名**协议）"[7]。不同操作的职责应被充分隔离。

慢雾(SlowMist) 技术解读

这意味着，一个强大且基于角色的访问控制系统(RBAC) 是强制性的。任何形式的单一"所有者"或"管理员"私钥，都是不合规的。

实施指南

必须定义一系列清晰的角色，并将这些角色分配给不同的、由多重签名钱包控制的实体或员工，以实现职责分离，最大限度降低单一故障点或合谋操纵的风险[8]。每个角色应仅限于特定职能，所有操作需多签名授权，并确保无单一员工同时持有多个高风险角色。所有操作需记录日志，并接受年度第三方审计，权限分配由管理员或董事会监督。

- **MINTER_ROLE**：负责处理稳定币的铸币(mint) 操作，包括在收到有效发行请求后创建代币单位，并确保铸币与储备资产池的相应增加匹配。
- **BURNER_ROLE**：负责处理稳定币的销毁(burn) 操作，包括在收到有效赎回请求后销毁代币单位。
- **PAUSER_ROLE**：负责暂停(pause) 稳定币的操作，例如在检测到异常事件（如安全威胁）时临时停止转账、铸币或赎回。
- **RESUME_ROLE**：负责恢复(resume) 稳定币的操作，例如在暂停事件解决后重新启用转账、铸币或赎回。
- **FREEZER_ROLE**：负责冻结(freeze) 和解除冻结(remove freeze) 特定钱包或代币的操作，例如在检测到可疑活动（如洗钱风险）时临时冻结资产。
- **WHITELISTER_ROLE**：负责管理白名单(whitelist)，包括添加或移除允许的钱包地址，例如限制铸币仅限于白名单地址。
- **BLACKLISTER_ROLE**：负责管理黑名单(blacklist) 和移除黑名单(remove blacklist)，例如将可疑钱包列入黑名单以阻止转账。
- **UPGRADER_ROLE**：如果采用可升级模型，负责升级(upgrade) 智能合约，例如更新合约代码以修复漏洞或添加功能。

表 1：基于角色的访问控制矩阵(RBAC Matrix)

下表提供了一个清晰、直观的规范，供开发人员和审计人员使用，明确地将每个特权操作映射到其所需的角色和控制类型。

操作	角色	类型
铸造代币	MINTER_ROLE	多重签名钱包
销毁代币	BURNER_ROLE	多重签名钱包
暂停合约	PAUSER_ROLE	多重签名钱包
恢复合约	RESUME_ROLE	多重签名钱包
冻结/解冻地址	FREEZER_ROLE	多重签名钱包
白名单管理	WHITELISTER_ROLE	多重签名钱包
黑名单管理	BLACKLISTER_ROLE	多重签名钱包
升级合约	UPGRADER_ROLE	多重签名钱包

2. 发行（铸币）机制

监管指令

发行必须是“审慎和稳健的”。铸币必须“与相关储备资产池的相应增加相匹配”。发行人应仅在收到资金和有效的发行请求后向其客户发行[9]。

慢雾(SlowMist) 技术解读

智能合约本身无法也无需强制执行“完全储备”的要求。相反，它扮演的是一个受控账本的角色，其中铸币权限是关键的控制点。完全储备的合规性是一项发生在链下、可通过审计验证的操作流程。监管将铸币行为与“有效的发行请求”和“收到资金”这两个链下事件绑定。因此，链上的铸造函数必须被设计为只能由一个能够验证这些链下条件已满足的可信实体（即发行人自己）调用。

实施指南

- **前置检查：** 函数在执行铸币前，必须检查目标地址 to 是否处于黑名单或被冻结状态。
- **操作流程**：
  - **链下尽职调查：** 客户完成所有必需的链下客户身份识别(KYC) 和客户尽职调查(CDD)流程[10]。此外，AML / CFT 法规要求，对于建立业务关系或进行超过特定阈值（如 8,000 港元）的偶尔交易的客户，必须执行 CDD[11]。
  - **资金接收：** 客户将等值的法币资金转入发行人指定的银行账户。
  - **内部验证：** 发行人的内部系统确认收到资金，并相应更新储备资产的会计记录。
  - **链上执行：** 运营团队创建并签署一个多重签名交易，调用智能合约的铸造代币函数，将新铸造的稳定币发送到客户预先注册并经验证的钱包地址。

3. 赎回（销毁）机制

监管指令

持牌人必须在收到有效的赎回请求后，“在切实可行的范围内尽快并在收到请求后的一个营业日内”处理[12]。储备资产的提取必须“与流通中的指定稳定币面值的相应减少相匹配”[13]。

慢雾(SlowMist) 技术解读

赎回是一个涉及链上与链下交互的两步过程。在赎回过程中，考虑到法币转账可能失败的风险，代币的销毁操作必须在确认法币结算之后进行，而非在此之前。这样可以保护发行人，避免其因一笔最终失败的赎回而提前销毁代币。

如果发行人先销毁代币，而银行转账失败，将导致其承担无对应资产的负债；反之，如果发行人先支付法币，却无法销毁对应的代币，也将蒙受损失。

因此，在赎回操作中，用户需先将代币转移至由发行人控制的指定地址，随后发行人在完成法币支付后再执行销毁。此模式允许用户将其代币“锁定”以供赎回，而发行人仅在履行完法币支付义务后才销毁代币，从而为双方提供了一个更安全的操作流程。

实施指南

- **赎回准备：**用户首先需要先将要赎回的代币转移至发行人控制的指定地址。
- **操作流程：**
    - **链下请求：**用户通过发行方的平台提交一个链下赎回请求。在处理请求前，发行人必须对客户进行适当的客户尽职调查(CDD)。
    - **系统验证：**发行人的系统验证请求的有效性，并检查用户是否已在链上完成了相应的代币转移操作。
    - **法币支付：**发行人将等值的法币转账至用户预先注册并验证的银行账户。
    - **链上销毁：**在确认法币转账成功后，持有 BURNER_ROLE 的多重签名钱包调用销毁函数，从指定的地址中销毁相应数量的代币。

4. 实施紧急控制：暂停与冻结

监管指令

合约必须支持暂停、恢复、拉黑、移除黑名单、冻结、解除冻结等操作。这些是事件管理框架的关键组成部分[14]。

慢雾(SlowMist) 技术解读

监管文件将“暂停”和“冻结”作为两个独立项目列出，这表明监管机构期望发行人具备灵活、分层的事件响应能力。**暂停**是应对重大危机（如合约被利用）的一种手段，而**冻结**则是处理特定法律或合规问题（如针对单个账户的法院命令）的精确工具。两者在功能上截然不同，必须分别实现：

- **暂停(Pause)：** 一个全局性的“紧急停止开关”，可瞬间中止合约的所有核心功能，包括转账、铸币和销毁。
- **冻结(Freeze)：** 一种账户级别的限制措施，可阻止某个特定地址发送或接收代币，但不会影响网络中其他地址的正常活动。

实施指南

- **暂停功能：** 仅由持有 PAUSER_ROLE 的多重签名钱包调用，用于全局中止合约功能。触发条件包括检测到异常事件（如网络攻击或储备资产不匹配），需董事会或高级管理层批准。恢复功能由独立的 RESUME_ROLE 处理，以实现职责分离。
- **冻结功能：** 由持有 FREEZER_ROLE 的多重签名钱包调用，用于针对特定地址的转账限制。触发条件包括可疑活动（如 AML 警报或法院命令），需链下验证后执行。解除冻结由同一角色处理，但需额外审计验证，发布相关公告，以防止滥用。

5. 地址筛选与黑名单机制

监管指令

持牌人应采取措施，例如“将被识别为受制裁或与非法活动相关的钱包地址列入黑名单”[15]。这是持续监控的核心控制手段，发行人应采用区块链分析工具等技术方案，以识别与非法或可疑活动相关的交易[16]。

慢雾(SlowMist) 技术解读

这必须是一个在链上强制执行的机制。仅仅在链下发出警告是不够的，必须在协议层面阻止交易的发生。黑名单的要求使持牌人需要采用实时的区块链分析工具 / 服务（如 MistTrack、Chainalysis、Elliptic）。合规团队利用这些工具得出的结论，安全地转化为由多重签名签署的交易，以更新链上的黑名单。

实施指南

- **函数实现：** 实现黑名单添加、黑名单移除功能的函数，并且仅由持有 BLACKLISTER_ROLE 的多重签名钱包调用。
- **转账限制：** 禁止加入黑名单的地址转移 / 接收代币。
- **操作流程：** 分析工具发出警报，触发内部合规审查，合规团队审查确认后，由 BLACKLISTER_ROLE 多签钱包发起黑名单添加交易。

6. 智能合约的可升级性

监管指令

稳定币相关的所有智能合约架构可能采用“可升级性”[17]。每当智能合约进行“升级”时，都必须进行审计[18]。

慢雾(SlowMist) 技术解读

可升级性设计是监管框架中对技术灵活性和风险管理的核心要求。它允许发行人在不中断现有合约状态的情况下更新逻辑，以应对漏洞修复、功能扩展或监管变更。

然而，这也带来了高风险：升级过程可能被滥用，导致合约行为意外变更或引入新漏洞。因此，升级必须被视为高风险操作，设计时应防止单一方单方面执行（如通过多重签名协议），并与基于角色的访问控制系统(RBAC) 集成。

监管强调的审计要求意味着，升级不仅是代码替换，更是嵌入严格变更管理流程的受控事件，确保新逻辑合约在部署前经过第三方验证，无漏洞或安全缺陷。

实施指南

- **代理模型：**对于 EVM 类型的智能合约来说，可以采用成熟的 ERC-1967 代理模型以实现可升级性。
- **权限控制：**升级函数必须仅由持有 UPGRADER_ROLE 的多重签名钱包调用。
- **变更管理流程：**根据监管要求，在提议任何升级之前，必须完成一个严格的变更管理流程，其中包括对新的逻辑合约进行全面的、独立的第三方安全审计。

7. 用于分析和报告的链上事件日志

监管指令

持牌人必须建立稳健的“信息和会计系统”，以“及时、准确地记录所有业务活动，包括链上和链下信息”，并“保留适当的审计追踪”[19]。

慢雾(SlowMist) 技术解读

智能合约是所有链上活动的主要事实来源。它必须为每一次重要的状态变更发出详细的事件(Events)，以便链下系统进行日志记录、监控和生成报告。这些事件在区块链上创建了一个不可篡改且永久的日志。该日志是所有链下监控、会计和报告系统的主要数据源，为审计提供了坚实的基础。

实施指南

除了 ERC-20 标准的要求的转账(Transfer)、授权(Approval) 事件外，合约必须为所有管理行为和状态变更定义并发出自定义事件：

- 代币铸造 / 销毁(Minted / Burned) 事件
- 合约暂停 / 恢复(Paused / Resume) 事件
- 黑名单添加 / 移除(BlacklistAdded / BlacklistRemoved) 事件
- 白名单添加 / 移除(WhitelistAdded / WhitelistRemoved) 事件
- 地址冻结 / 解除冻结(AddressFrozen / AddressUnfrozen) 事件
- 特权角色变更(RoleGranted / RoleRevoked) 事件
- 合约升级(Upgraded) 事件

第三部分 运营安全与生命周期管理

本部分详细阐述了围绕智能合约的、至关重要的运营安全程序。这些程序与代码本身同等重要，是实现全面安全和合规的必要条件。

1. 安全密钥管理架构

监管指令

这是监管文件中规定最为详尽和严格的领域之一。持牌人必须对私钥的整个生命周期实施强有力的控制，包括生成、存储、使用、备份和销毁[20]。“重要种子和/或私钥”（例如，用于升级、角色管理、大规模铸币的密钥）需要采用更高级别的安全标准，包括在“气隙环境”(air-gapped environment) 中进行离线生成[21]，并存储在硬件安全模块(HSM) 中[22]。

慢雾(SlowMist) 技术解读

香港金管局实质上是在要求将“传统金融级别”的安全态势应用于加密原生操作。实施这种级别的密钥管理所带来的成本与复杂性是巨大的，它将成为任何持牌发行人的核心运营部分。这种安全模型远远超出了典型 DeFi 项目的实践标准。监管文件为密钥管理提供了一份详细清单，明确提到了 HSM（硬件安全模块）、气隙环境、密钥仪式和多重签名。这实际上强制要求构建一个纵深防御的密钥管理架构：由保存在硬件钱包中的账户作为多重签名钱包的签名者，而该多重签名钱包本身则持有智能合约上的管理角色。对于安全级别最高的角色，这些硬件钱包本身必须在指定的、具备物理安全性的气隙环境中进行管理。整个架构构建了一个用于抵御密钥泄露的多层防御体系。

实施指南

- **密钥生成：**必须通过一个有详细文档记录的“密钥仪式”(key ceremony)[23]，在一个物理安全的、与外界网络完全隔离的气隙环境中完成。
- **密钥存储：**所有管理角色都必须由多重签名钱包控制。这些多签钱包的签名者所使用的私钥，必须存储在 HSM 或其他的安全硬件钱包中。对于最关键的角色其对应的密钥必须保存在气隙系统中，与任何在线环境物理隔离。
- **密钥使用：**必须强制执行多重签名策略。对于涉及“重要私钥”的交易签名，可能需要相关人员亲自到场操作[24]。

- **备份与恢复：**密钥分片或助记词的备份必须存储在香港境内（或经监管批准的地点）的多个安全且地理上分散的位置，并采用防篡改的包装[25]。

2. 完备的部署流程与运行时监控

监管指令

持牌人必须聘请“合格的第三方实体审计智能合约”，审计频率至少为每年一次，并且在每次部署、重新部署或升级时都必须进行。审计必须确保合约实现正确、功能符合预期，并且在“高度可信的水平上”不存在任何漏洞或安全缺陷[26]。被许可方应实施措施监控助记词和 / 或私钥的使用情况（例如 IP 检查、行为监测、关键活动警报、设备筛查、链上监测、访问控制监测等）[27]。并且被许可方应采取适当措施监测威胁情报，以发现新出现的威胁。应对威胁情报进行分析，以便能够及时实施缓解措施[28]。

慢雾(SlowMist) 技术解读

部署流程和运行时监控是监管对技术风险管理框架的直接延伸，强调从源头防范漏洞并持续监测运营风险。部署前审计要求将智能合约视为关键基础设施，必须通过多层验证（如单元测试、独立审计和代码冻结）确保无缺陷，这反映了监管对“高度可信”标准的追求，以避免代码缺陷或漏洞利用影响稳定币的发行、赎回或日常运营。运行时监控则聚焦于实时威胁检测，结合私钥使用监控（如行为分析）和威胁情报分析，形成闭环响应机制。这不仅满足事件管理框架的需求，还确保系统能动态应对新兴风险。整体而言，此部分的技术实现需整合链上链下工具，形成可追溯的审计追踪，从而将被动防御转化为主动合规。

实施指南

在正式部署之前，必须制定并严格执行一份“部署前检查清单”：

- **全面测试：**确保单元测试覆盖率 95% 以上，核心代码覆盖率 100%，确保输出单元测试的覆盖率报告。
- **独立审计：**完成至少一家、最好是两家信誉良好的审计公司出具的独立安全审计报告。
- **代码冻结：**完成审计后，冻结代码直至上线，不再做任何代码改动。
- **回归测试：**在正式部署前，执行单元测试并进行回归测试。
- **合规签核：**获得内部合规团队的正式签核，确认合约逻辑满足所有相关监管要求。
- **部署演练：**准备详细的部署脚本，并在一个与主网环境完全一致的测试网上进行完整的部署演练。
- **授权部署：**由授权的钱包执行最终的部署操作。

完成部署后应采取适当监控措施，以对特权角色的使用情况以及新出现的威胁及时实施缓解措施：

- **链上活动监控：**监控管理角色的使用情况（例如，使用慢雾安全监控系统 MistEye 添加关键角色活动监测），及时发现未授权情况的发生。
- **威胁情报监测：**应及时发现新出现的威胁（例如，使用慢雾安全监控系统 MistEye 的威胁情报订阅），并对威胁情报进行分析，以便能够及时实施缓解措施。

3. 为业务连续性和退出计划提供技术支持

监管指令

持牌人必须制定一份“业务退出计划，以实现其持牌稳定币业务的有序清盘”[29]。该计划必须包括清算储备资产和向持有人分配收益的程序。

慢雾(SlowMist) 技术解读

这意味着智能合约从设计之初就必须考虑其自身的“退役”过程，它需要具备能够实现有序关停的状态与机制。退出机制的要求意味着，智能合约的生命周期并不在部署时终结，而是必须拥有一个明确定义的、协议层的“生命终结”协议。这对许多习惯于构建“永久”合约的开发者来说是一个新颖的概念，也由此推动了一种“为终止而设计”的思维模式。一个有序的清盘过程需要一份干净、最终且无争议的记录，明确在关停时刻谁拥有什么。如果在一个混乱的、仍在进行交易的状态下进行关停，这一目标将难以实现。因此，一个能够冻结合约状态的函数，就是这一监管要求的直接技术体现。链上状态由此成为清算人手中最终的、可审计的事实来源。

实施指南

- **制定业务退出计划：**计划涵盖可能导致有序终止的各类情形，并包含对这些情形实际发生或潜在发生的监测措施。
- **链上退出流程**[30]**：**
  - 应暂停智能合约以停止所有代币转移行为，以确保最大化储备资产变现收益、最小化对整体市场稳定的影响。
  - 依托赎回功能与白名单功能，协助稳定币持有人提交赎回申请。

第四部分 附录：监管要求交叉引用表

本表将智能合约系统的每一个技术特性直接映射到强制要求它的具体监管文本：

技术特性 / 协议	智能合约实现	核心监管要求	来源文件与段落
多重签名管理控制	所有特权角色都应分配给多签钱包	必须防止单方面行动；职责分离	Draft guideline on supervision of licensed stablecoin issuers, p. 20, 6.5.3
链上黑名单机制	转账前检查发起者与接收者是否为黑名单地址	必须封堵与非法活动相关的地址	Consultation paper on the proposed AML/CFT requirements for regulated stablecoin activities, p. 13, 3.6.2
气隙环境密钥生成	在物理隔离环境中进行密钥仪式生成多签成员私钥	“重要私钥”必须离线生成	Draft guideline on supervision of licensed stablecoin issuers, p. 22-23, 6.5.8(ii) & (iii)
HSM 密钥存储	多签成员的私钥存储在 HSM 或认证硬件钱包中	私钥应在安全存储介质（如 HSM）中得到保护	Draft guideline on supervision of licensed stablecoin issuers, p. 23, 6.5.8(iv)
全局暂停功能	完全停止发行/销毁/转账功能	必须具备暂停合约的能力以应对事件	Draft guideline on supervision of licensed stablecoin issuers, p. 20, 6.5.3
账户级冻结功能	转账前检查发起者是否已被冻结	必须具备冻结单个账户的能力	Draft guideline on supervision of licensed stablecoin issuers, p. 20, 6.5.3
可升级模型	智能合约可选使用可升级架构	升级是高风险操作，升级前必须经过安全审计	Draft guideline on supervision of licensed stablecoin issuers, p. 20, 6.5.2 & p. 21, 6.5.5
部署前强制审计	在部署新逻辑合约前，需获得第三方审计报告	每次部署或升级都必须进行审计	Draft guideline on supervision of licensed stablecoin issuers, p. 21, 6.5.5
业务退出计划支持	暂停所有代币活动并协助稳定币持有人提交赎回申请	必须具备有序清盘的计划和能力	Draft guideline on supervision of licensed stablecoin issuers, p. 42, 6.8.16
链上事件日志	为所有管理操作和状态变更发出自定义事件	必须保留适当的审计追踪	Draft guideline on supervision of licensed stablecoin issuers, p. 51, 8.1.1
			Draft guideline on supervision of licensed stablecoin issuers, p. 12, 3.4.1;

客户尽职调查(CDD)	铸币 / 赎回流程的链下前置步骤	发行和赎回前需对客户进行 CDD	Consultation paper on the proposed AML/CFT requirements for regulated stablecoin activities, p. 9, 3.2.1 & p. 10, 3.3.1

相关资料

[1]Hong Kong Monetary Authority. (2025, May 26). *Consultation paper on the proposed AML/CFT requirements for regulated stablecoin activities*. https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/20250526_Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf

[2]Hong Kong Monetary Authority. (2025, May). *Draft guideline on supervision of licensed stablecoin issuers*. https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/20250526_Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf

文中引用出处

[1]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.5

[2]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.5

[3]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 20, 6.5.3

[4]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 20, 6.5.3

[5]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.4

[6]Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf, p. 13, 3.6.2

[7]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 20, 6.5.3

[8]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.4

[9]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 10, 3.1.1

[10]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 12, 3.4.1

[11]Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf, p. 9, 3.2.1

[12]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 11, 3.2.3

[13]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 11, 3.2.5

[14]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 38, 6.8.2

[15]Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf, p. 13, 3.6.2

[16]Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf, p. 11, 3.4.2

[17]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 20, 6.5.2

[18]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.5

[19]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 51, 8.1.1

[20]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 22, 6.5.8

[21]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 23, 6.5.8(ii)

[22]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 23, 6.5.8(iv)

[23]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 22, 6.5.8(ii)

[24]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 24, 6.5.8(vii)

[25]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 25, 6.5.8(x)

[26]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 21, 6.5.5

[27]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 24 6.5.8(ix)

[28]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 34 6.5.20(ii)

[29]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 42, 6.8.16

[30]Consultation_on_Draft_Guideline_on_Supervision_of_Licensed_Stablecoin_Issuers.pdf, p. 42, 6.8.16

往期回顾

威胁情报：Solana 开源机器人盗币分析

慢雾：引领香港稳定币发行人合规与安全

慢雾受邀参加香港金管局与数码港联合主办的金融网络科技大会

130 亿资金去向成谜：鑫慷嘉 DGCX 骗局崩盘始末

GMX 被黑分析：4200 万美金瞬间蒸发

慢雾导航

慢雾科技官网
https://www.slowmist.com/

慢雾区官网
https://slowmist.io/

慢雾 GitHub
https://github.com/slowmist

Telegram
https://t.me/slowmistteam

Twitter
https://twitter.com/@slowmist_team

Medium
https://medium.com/@slowmist

知识星球
https://t.zsxq.com/Q3zNvvF

稳定币安全与合规研究系列 · 目录

上一篇 · 慢雾：引领香港稳定币发行人合规与安全

修改于2025年07月22日