ICS 35.020
CCS L 70

团　　体　　标　　准

T/GDCSA XXX-2026

智能合约安全基本要求

Basic Security Requirements for Smart Contracts

（征求意见稿）

2026-XX-XX 发布　　2026-XX-XX 实施

广东省网络空间安全协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由北京神州绿盟科技有限公司提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：XXX。

本文件主要起草人：XXX。

智能合约安全基本要求

1 范围

本文件规定了区块链智能合约安全基本要求，从智能合约的安全设计、代码安全、访问安全、数据安全、环境安全五个方面提供了智能合约安全基本要求。

本文件适用于指导、规范区块链智能合约的开发、部署、运行及测评。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 43572-2023 区块链和分布式记账技术 术语

GB/T 43579-2023 区块链和分布式记账技术 智能合约生命周期管理技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

注：区块链被设计用来抵抗篡改，并创建最终的、确定的、不可变的账本记录。

[来源:GB/T 43572-2023,3.6]

3.2

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

注：智能合约可以在法律上代表合同条款，并在适用司法管辖区的法律下产生可强制执行的义务。

[来源:GB/T 43572-2023,3.72]

4 智能合约安全基本要求逻辑架构

本标准将智能合约的安全分为安全设计、代码安全、访问安全、数据安全和环境安全，他们相互关联、相互依存，构成了智能合约完整安全防护体系。安全设计从源头规避系统性风险，代码安全确保智能合约自身无漏洞，访问安全控制对智能合约的合法访问，数据安全保护智能合约数据的机密性、完整性和隐私性，而环境安全为智能合约运行提供稳定保障。具体逻辑架构如下图 1 所示：

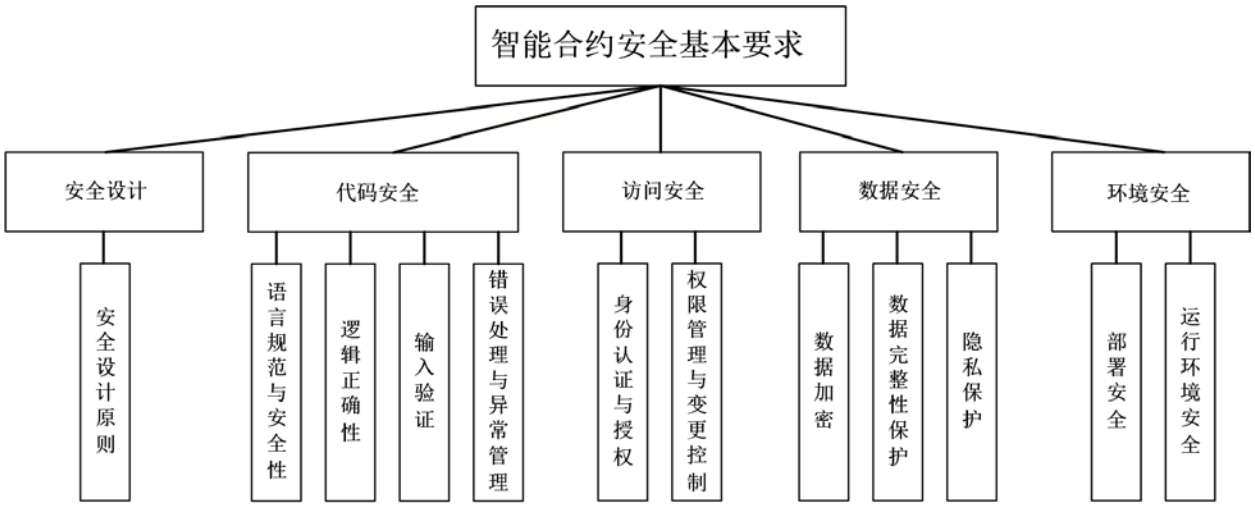

图1 智能合约安全基本要求逻辑架构

5 智能合约安全基本要求

5.1 安全设计

5.1.1 安全设计原则

a) 应遵循最小权限原则，在智能合约的架构设计与权限分配中，确保所有实体（如用户、合约、系统组件）的权限被严格限定于其职责所需的最小必要范围。
b) 应遵循攻击面最小化原则，在满足业务需求的前提下，通过架构设计尽可能减少智能合约与外部环境不必要的交互点与信息暴露范围。
c) 应采用纵深防御策略，在智能合约的代码、访问控制、数据校验及运行环境等多个层面协同部署安全措施，构建冗余互备的防御体系。
d) 应遵循默认安全原则，确保智能合约的初始状态、默认配置及失败处理模式均处于安全状态，例如异常情况下的状态回滚与访问拒绝。

5.2 代码安全

5.2.1 语言规范与安全性

a) 应使用经过充分验证、具有良好安全特性的智能合约编程语言进行开发，避免使用存在已知严重安全漏洞的语言版本或特性。
b) 应遵循该语言的安全编码规范，严格遵循代码格式规范，确保代码可读性与可维护性，便于后续审查与排查潜在问题。

5.2.2 逻辑正确性

a) 智能合约的业务逻辑应精确反映其设计意图，避免逻辑漏洞如条件判断错误、循环终止条件不当等，杜绝可能导致意外行为或资产损失的逻辑缺陷。
b) 对于涉及资产转移、权限变更等关键操作的逻辑，应进行严谨的数学建模与验证，确保其在所有可能的输入情况下均能正确执行，防止因逻辑偏差引发的漏洞利用。

5.2.3 输入验证

a) 对所有外部输入的数据，包括用户输入、其他合约调用传入的参数等，应进行全面、严格的验证，验证内容应涵盖数据类型、格式、取值范围、合法性等方面，确保输入数据符合预期且不会破坏合约逻辑。
b) 对于不符合验证要求的输入，应采取合理的拒绝处理机制，并记录详细的错误信息，以便后续分析与溯源，防止恶意输入干扰合约正常运行。

5.2.4 错误处理与异常管理

a) 在智能合约中合理设置错误处理机制，针对可能出现的各类异常情况，如资源不足、外部调用失败、数据不一致等，应定义明确的错误处理流程，确保合约在遇到异常时能够准确地处理，避免陷入不可预知的状态或导致系统崩溃。
b) 对于关键操作，应在执行前后进行状态检查与校验，利用断言等机制及时捕获逻辑偏差或错误状态，及时终止异常操作并给出明确的错误提示，便于开发者快速定位与修复问题。

5.3 访问安全

5.3.1 身份认证与授权

a) 应采用安全可靠的身份认证机制，对调用智能合约的用户、合约或其他实体进行准确的身份识别，如通过数字签名、加密密钥等技术手段验证身份合法性。
b) 应依据最小权限原则，严格限制不同身份主体对智能合约功能与数据的访问权限，明确授权范围，确保每个主体仅能执行其被授权的操作，防止越权访问与操作引发的安全风险。

5.3.2 权限管理与变更控制

a) 应建立完善的权限管理体系，对权限的分配、修改、撤销等操作进行详细记录与审计，确保权限变更过程可追溯。在进行权限调整时，需经过严格的审批流程，避免因权限管理失误导致安全漏洞。
b) 应对智能合约中的关键功能与数据访问点，设置多层次的访问控制策略，如结合时间限制、调用次数限制等动态因素，增强访问控制的灵活性与安全性，适应不同场景下的安全需求变化。

5.4 数据安全

5.4.1 数据机密性保护

a) 对智能合约中涉及的敏感数据，如用户隐私信息、资产密钥、商业机密等，在存储与传输过程中应采用经过认可的加密算法进行加密处理，确保数据的保密性与完整性。
b) 根据数据的重要程度与应用场景，合理选择对称加密与非对称加密算法的组合使用，在保证加密强度的同时，兼顾加密解密效率，以适应智能合约在区块链环境中的性能要求。

5.4.2 数据完整性保护

a) 为防止智能合约数据在存储、传输与处理过程中被篡改，应采用数据完整性验证机制，如哈希算法、数字签名等技术，对关键数据进行完整性校验。在每次数据读取或更新操作时，均需验证数据的完整性，一旦发现数据被篡改，立即采取相应的措施，如回滚操作、记录异常并报警等，确保数据的真实可靠性。
b) 应定期对智能合约的数据存储结构进行备份与一致性检查，通过对比备份数据与当前数据的完整性校验值，及时发现并修复潜在的数据损坏或篡改问题，保障智能合约数据的长期可靠性与可用性。

5.4.3 隐私保护

a) 在智能合约设计阶段，充分考虑用户隐私保护需求，采用隐私增强技术，如零知识证明、同态加密等，在不泄露用户敏感信息的前提下，实现智能合约的业务功能，确保用户在参与区块链系统时的隐私权益得到有效保障。
b) 对于涉及多方数据共享的智能合约场景，应明确数据共享的范围、目的与条件，通过制定严格的隐私政策与数据共享协议，规范数据共享行为，防止用户隐私数据在未经允许的情况下被过度收集、使用或传播。

5.5 环境安全

5.5.1 部署安全

a) 在智能合约部署前，应对合约代码进行彻底的静态安全分析与测试，利用专业的智能合约安全分析工具扫描代码中的潜在漏洞，如整数溢出、重入攻击、随机数生成漏洞等，并对发现的问题进行修复。同时，对合约的依赖项进行严格审查，确保所依赖的库、框架等组件不存在已知安全漏洞，避免因第三方组件问题引入安全隐患。
b) 智能合约的部署过程应遵循安全的部署流程，在安全的部署环境中进行操作，如使用安全的编译工具、部署节点等，防止在部署过程中合约代码被篡改或遭受中间人攻击。
c) 智能合约部署完成后，对合约的部署状态进行验证，确保合约已正确部署且初始配置符合安全要求。

5.5.2 运行环境安全

a) 区块链平台应为智能合约提供安全可靠的运行环境，包括但不限于安全的虚拟机、稳定的共识机制、有效的网络通信安全防护等，虚拟机应具备良好的隔离性与安全性，防止不同合约之间相互干扰或恶意攻击，确保每个合约在独立、安全的沙箱环境中运行。
b) 应定期对区块链平台的运行环境进行安全更新与维护，及时修补系统漏洞，提升运行环境的整体安全性。
c) 应对智能合约的运行状态进行实时监控与审计，及时发现并处理异常的合约行为，如异常的资源消耗、频繁的外部调用等，保障智能合约在安全、稳定的环境中持续运行。

参 考 文 献

[1] GB/T 43579-2023 区块链和分布式记账技术 智能合约生命周期管理技术规范
[2] T/SIA 029-2021 区块链智能合约一般要求
[3] 智能合约安全指南（2020年云安全联盟大中华区发布）