

团体标准《智能合约安全基本要求》编制说明

一、工作简况

1.1 任务来源

《智能合约安全基本要求》由广东省网络空间安全协会归口。

1.2 主要起草单位和工作组人员

本标准由北京神州绿盟科技有限公司牵头，广东电网有限责任公司计量中心、广东省网络空间安全协会、广东新兴国家网络安全与信息化发展研究院、广东关键信息基础设施保护中心、广州华南检验检测中心有限公司、网安联认证中心有限公司、国源天顺科技产业集团有限公司等多家单位共同参与编制。

1.3 主要工作过程

(1) 2025年8月，标准正式立项，协会组织参与本标准编写的人员启动项目，成立规范编制组，确立各自分工，对标准进行调研，听取各单位的相关意见；

(2) 2025年9月-12月，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿；结合各参编单位的反馈意见，修改形成标准草案第二稿；

(3) 2026年1-3月，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变的同时，针对用户群体，做到可操作、可用与实用。

2.2 文档结构

《智能合约安全基本要求》标准文档分为前言、范围、规范性引用文件、术语和定义、智能合约安全基本要求逻辑架构、智能合约安全基本要求、参考文献等部分内容。

2.3 整体格式

整体格式根据 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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总及整个各方意见过程中，对各编写组成员提交部分，根据 GB/T 1.1-2020 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4 标准名称英文翻译

标准的名称“智能合约安全基本要求”翻译为 Basic security requirements for smart contracts。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 智能合约安全基本要求逻辑架构

本章主要介绍了智能合约安全基本要求逻辑架构。内容将智能合约安全划分为安全设计、代码安全、访问安全、数据安全和环境安全五个相互关联、相互依存的方面，其中安全设计从源头规避系统性风险，代码安全确保合约自身无漏洞，访问安全控制合法访问，数据安全保障数据的机密性、完整性和隐私性，环境安全为合约运行提供稳定支撑，并通过逻辑架构图展示了这一完整安全防护体系的逻辑架构。

2.7 智能合约安全基本要求

本章主要介绍了智能合约安全的五大核心要求：安全设计强调遵循最小权限、攻击面最小化、纵深防御和默认安全等原则，从源头规避风险；代码安全要求使用经过验证的语言并遵循安全编码规范，确保逻辑正确性，并对输入验证、错误处理与异常管理做出明确规定；访问安全通过身份认证与授权机制，结合权限管理与变更控制，确保对合约的合法访问；数据安全涵盖数据机密性保护、完整性验证及隐私保护，综合运用加密、哈希、零知识证明等技术手段；环境安全则关注合约的部署流程安全和运行环境的稳定性，包括代码审计、虚拟机隔离和实时监控等，这五个方面共同构成了智能合约的完整安全防护体系。

2.8 参考文献

本章主要引用了三项关键文档，包括国家标准《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》用于指导智能合约从设计、开发、部署到维护的全生命周期安全管理，引用《T/SIA 029-2021 区块链智能合约一般要求》作为智能合约基本功能和安全性的一般性技术规范依据，同时参考了《智能合约安全指南》(2020年云安全联盟大中华区发布)中关于智能合约安全漏洞分析、最佳实践和风险评估的专业指引，这些文献共同构成了本章节内容的重要理论基础和技术支撑。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无采用国际标准和国外先进标准情况。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。本标准是在遵循我国《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的基础上，对智能合约这一特定领域的指导开发、部署、运行及测评工作进行的专项补充和细化，在智能合约的具体落地指引。

六、重大分歧意见的处理经过和依据

《智能合约安全基本要求》编制过程中未出现重大分歧。

七、标准性质的建议

建议《智能合约安全基本要求》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

建议本标准发布后，相关行业协会、联盟组织可开展标准的宣贯培训工作。鼓励智能合约应用的开发和运营企业，依据本标准开展安全体系的自查、建设与优化。建议第三方测评机构可将本标准作为开展智能合约应用安全评估时的重要参考依据。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《智能合约安全基本要求》
标准编制组
2026年3月