ICS 35.240
CCS L 04

YD

中华人民共和国通信行业标准

YD/T XXXX—202X

区块链智能合约安全技术要求

Security technical requirements for blockchain smart contract

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国工业和信息化部　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：深圳市腾讯计算机系统有限公司、腾讯云计算（北京）有限责任公司、成都链安科技有限公司、郑州信大捷安信息技术股份有限公司、国家计算机网络应急技术处理协调中心、中国移动通信集团有限公司、北京奇虎科技有限公司、电子科技大学、北京理工大学、西安邮电大学、蚂蚁科技集团股份有限公司、奇安信科技集团股份有限公司、北京邮电大学、中国信息通信科技集团有限公司、陕西省信息化工程研究院。

本文件主要起草人：李克鹏、武杨、郭铁涛、刘为华、刘献伦、刘颖、李力、苏庆慧、邵兵、郭锐、蔡庆普、张子剑、杨霞、杨勇、甘祥、张建俊、敖萌、苏蹦蹦、韩天乐、代威、梁军、卢洋、王宗友、蓝虎、郭文生、孙海泳、岳亮亮、邓岚膑、章书、王剑、彭晋、昌文婷、张屹、鲍旭华、黄亮、韩刚、张勇、尚进、于乐、程渤、赵帅、张祺琪、刘伟丽。

区块链智能合约安全技术要求

1 范围

本文件规定了区块链智能合约安全技术要求，包括区块链智能合约的安全技术框架、设计开发安全、测试验证安全、编译部署安全、触发运行安全、维护治理安全方面的技术要求。

本文件适用于指导区块链智能合约业务提供者、智能合约技术提供者、智能合约审计者等相关角色在区块链智能合约的设计、开发、测试、部署和运维等过程中进行安全保障，也适用于指导区块链智能合约系统的安全性评估。

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 25069-2022 信息安全技术 术语

ISO 22739:2020 区块链和分布式账本技术－术语（Blockchain and distributed ledger technologies—Vocabulary）

3 术语和定义

GB/T 25069-2022和ISO 22739:2020界定的以及下列术语和定义适用于本文件。

3.1

区块 block

区块链的基本组成单元，由区块头和区块数据组成。

[来源：ISO 22739:2020，3.2，有修改]

3.2

共识 consensus

在共识节点间达成区块数据一致性的认可。

[来源：ISO 22739:2020，3.11，有修改]

3.3

共识协议 consensus protocol

区块链中通过数学算法实现不同节点之间对交易达成一致的方法。

[来源：ISO 22739:2020，3.12，有修改]

3.4

区块链 blockchain

将区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

［来源：ISO 22739:2020，3.6，有修改］

3.5

节点 node

具有特定功能的区块链组件，可独立运行。

［来源：ISO 22739:2020，3.27，有修改］

3.6

交易 transaction

区块链双方或多方参与，并且会发生状态变更的一种区块基本组成单元。

［来源：ISO 22739:2020，3.77，有修改］

3.7

用户 user

参与产生区块链交易数据的个人、组织或进程。

［来源：ISO 22739:2020，3.3，有修改］

3.8

智能合约 smart contract

以运行在区块链中的软件程序形式存在的合约，合约由区块链部署、执行结果记录在区块链中。

［来源：ISO 22739:2020，3.72］

3.9

执行环境 execution environment

智能合约的执行容器，负责根据合约代码和用户发送的交易指令对区块链状态进行更新。

3.10

链上 on-chain

在区块链内定位、执行或运行。

［来源：ISO 22739:2020，3.54，有修改］

4 智能合约的安全技术框架

4.1 智能合约安全的整体逻辑架构

本文件围绕智能合约的生命周期，在智能合约的设计开发、测试验证、编译部署、触发运行、维护治理等各个阶段提出安全要求。

智能合约安全的整体逻辑架构，如图1所示。

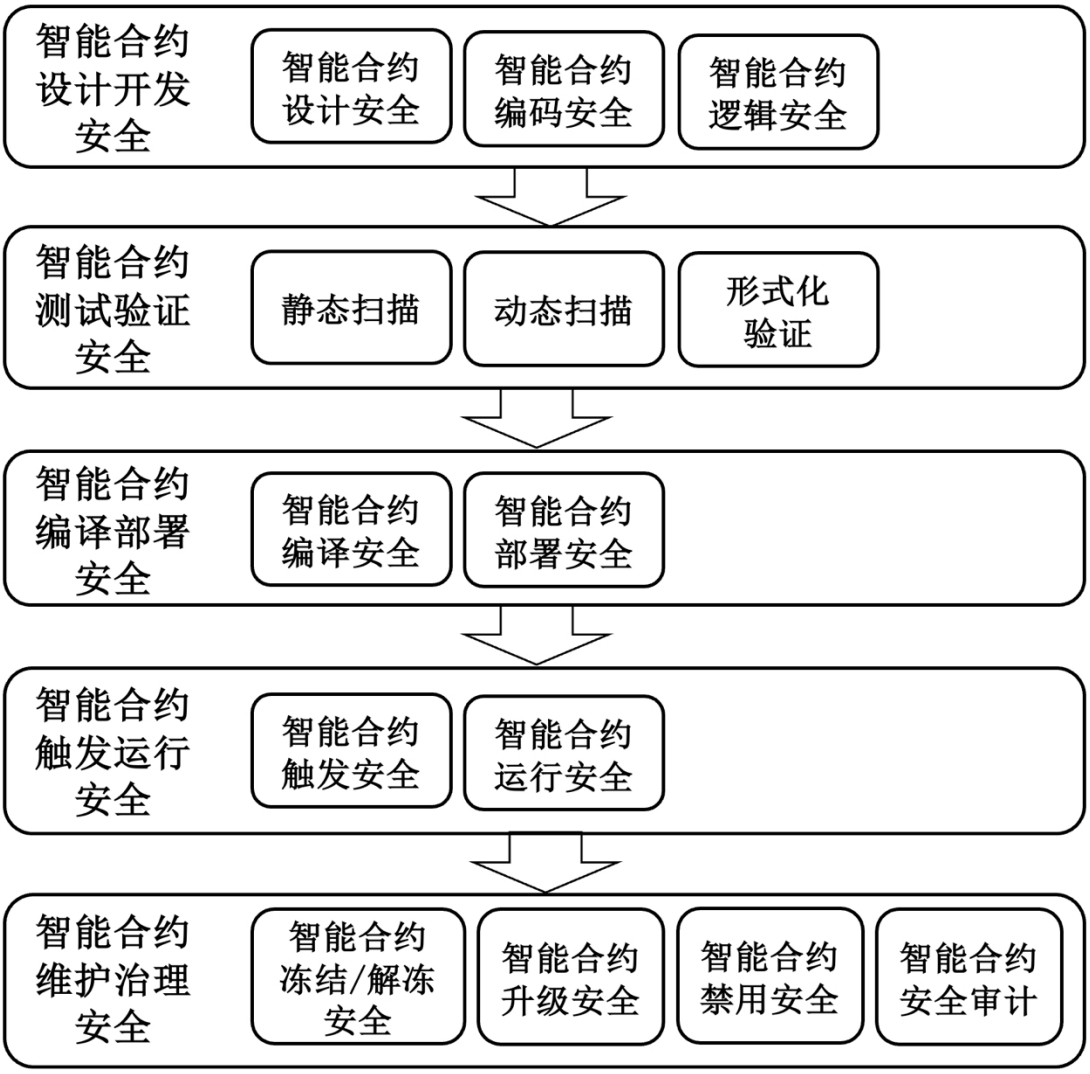

图1 区块链智能合约安全的整体逻辑架构图

智能合约全生命周期各阶段的安全要求，主要包括：

a) 智能合约设计开发的安全：主要包括智能合约的设计安全、编码安全、逻辑安全等；

b) 智能合约测试验证的安全：主要包括智能合约的静态扫描、动态扫描、形式化验证等；

c) 智能合约编译部署的安全：主要包括智能合约编译安全、部署安全等；

d) 智能合约触发运行的安全：主要包括智能合约触发安全、运行安全等；

e) 智能合约维护治理的安全：主要包括智能合约冻结/解冻安全、升级安全、禁用安全、安全审计等。

4.2 智能合约的角色定义

参与区块链智能合约的设计开发、验证测试、编译部署、运行和运维等过程的角色主要包括：

a) 智能合约业务提供者

智能合约业务提供者是指提供区块链智能合约业务的主体，主要负责链上部署运行、管理和维护区块链智能合约等，直接或间接地为区块链用户提供服务。

b) 智能合约技术提供者

智能合约技术提供者是指为智能合约业务提供者提供技术支持的机构或者组织，主要负责设计、开发、测试、配合维护区块链智能合约等，并提供相关技术支持和服务。

c) 智能合约审计者

智能合约审计者负责在区块链智能合约的供应和使用过程中执行审计。区块链智能合约审计通常覆盖运营、性能和安全，主要是检查相关的审计准则是否得到满足。

4.3 智能合约各角色的安全职责

4.3.1 智能合约业务提供者的安全职责

智能合约业务提供者的安全职责主要包括：

a） 对智能合约技术提供者提出安全需求，并查验安全需求的满足情况；

b） 执行智能合约服务的安全要求并保障智能合约业务的稳定，为智能合约的正常运行提供足够的资源；

c） 当智能合约服务出现异常时，能够及时修复异常，若自身不能处理，则及时联系智能合约技术提供者共同完成修复。

4.3.2 智能合约技术提供者的安全职责

智能合约技术提供者的安全职责主要包括：

a） 为智能合约业务提供者提供安全设计开发、测试验证的智能合约，并提供保障智能合约安全的支撑技术；

b） 为智能合约审计者提供审计的技术支撑；

c） 为保障智能合约业务的稳定运行提供管理运维支撑技术以及紧急情况下的处置方法。

4.3.3 智能合约审计者的安全职责

智能合约审计者的安全职责主要包括：

a） 遵循独立性、客观性原则，运用系统化和规范化的方法，通过监督、评价和咨询等方式，促进业务和技术提供者建立有效并持续完善的风险管理、内控合规和治理架构，实现区块链智能合约安全运行的业务目标；

b） 与智能合约技术提供者、智能合约业务提供者明确需要满足的智能合约审计服务和审计需求；

c） 当发现安全问题时，及时通知智能合约业务提供者进行整改；

d） 当发现不合规信息时，及时通知智能合约业务提供者进行屏蔽、访问限制等。

5 智能合约设计开发的安全技术要求

5.1 智能合约功能设计的安全技术要求

5.1.1 智能合约设计的安全性

智能合约技术提供者在智能合约设计安全性方面的要求如下：

a) 在设计智能合约代码时，应对整个合约的功能以及对外的交互进行安全设计，应规避因为设计缺陷所导致的安全问题；

b) 在智能合约设计时，应从多个来源收集输入事实，保证需求的可追溯性；

c) 在设计智能合约时，应对各个角色及其权限进行合理设计；

d) 设计的智能合约应具备防篡改和抗抵赖性，智能合约应完全按照针对合约约定的条件、事项和规则执行。

5.1.2 智能合约的处理错误能力

智能合约技术提供者设计的智能合约应具备处理或缓解错误/缺陷的能力，如提前终止能力或线上更新能力等，避免链上一直存在错误数据而不可更改的情况。

5.1.3 智能合约的敏感信息规避要求

智能合约技术提供者在设计智能合约时，为避免隐私或其他敏感数据泄露，在敏感信息规避方面的安全要求如下：

a) 对于处理隐私数据等敏感信息的智能合约，不应直接将敏感数据存储在链上；
b) 代码本身所包含的隐私数据或其他敏感信息，应进行加密或是将其转移至链下；
c) 加密算法应满足相关国家监管合规要求。

5.1.4 智能合约结果一致性的安全设计

智能合约技术提供者设计智能合约时，为保证各节点智能合约运行结果的一致性安全要求如下：

a) 智能合约中运行结果不应包含随机信息，否则有可能会导致结果不一致；
b) 在设计智能合约时应对时序的逻辑进行合理设计，即不同节点执行合约相同部分的先后次序可能是不同的，应避免由此产生的安全风险；
c) 在设计智能合约时，应不要有对先后顺序的依赖，如付款先后、申请先后等的依赖，以避免由于条件竞争导致的安全问题。

5.1.5 区块链平台的兼容能力的设计

当区块链平台升级时，智能合约技术提供者应评估原有智能合约在新升级平台的运行差异，并做兼容性方面的适配、调整，避免不兼容而导致的安全风险。

5.1.6 智能合约安全风险规避要求

智能合约技术提供者应在设计时考虑：智能合约在整个生命周期中存在不可更改、代码公开、分布式计算、运行环境不安全等情况，制定智能合约安全风险分析与风险管理规划，并对相关安全风险进行规避。

5.2 智能合约编码的安全技术要求

5.2.1 开发环境安全

智能合约技术提供者在智能合约编码过程中，在开发环境方面的安全要求如下：

a) 应对智能合约的开发、编译等工具定期进行更新，修复所存在的安全缺陷；
b) 在使用第三方工具和代码，以及安全部署更新前，应对其安全性进行评估，防止引入新的安全缺陷和风险。

5.2.2 明确变量定义

智能合约技术提供者在编写智能合约时，应明确定义变量的类型，以便确定变量的取值范围，防止变量溢出。

5.2.3 尽量避免直接嵌入底层语言

为防止高级语言的安全特性被绕过，智能合约技术提供者在编写智能合约时，应尽量避免底层语言（如汇编语言）的使用。除非智能合约高级语言无法实现的情况下（如对性能要求高或者运行环境要求使用底层语言等情况）而只能选择使用底层语言时，应充分知悉此安全风险并做好安全加固措施。

5.2.4 数学运算的边界条件

智能合约技术提供者开发的智能合约在进行数学运算时，应注意可能到达的边界条件。当赋值过大或过小导致可能发生溢出时，应支持对溢出进行正确处理。

5.2.5 避免不可靠输入

智能合约技术提供者在编写智能合约实现预定的功能或逻辑时，应避免引入不可靠输入。

5.2.6 错误处理

智能合约技术提供者在智能合约时，应使用安全函数。在智能合约中调用其他函数时，应对可能发生的错误进行处理以避免程序出错导致安全风险，包括捕获异常、处理错误返回值等。

5.2.7 合约代码库

智能合约技术提供者在使用智能合约代码库时的安全要求包括：

a) 应优先使用经过详细测试或第三方安全审计的可靠合约代码库；
b) 必须需仔细阅读代码库使用说明，在正确理解外部代码的情况下进行使用；
c) 不应使用未知源码的合约作为依赖。

5.3 智能合约的逻辑安全技术要求

5.3.1 身份验证

智能合约技术提供者开发的智能合约在对用户资产进行操作时，应对操作者身份进行验证，防止恶意操作。

5.3.2 权限管理

智能合约技术提供者开发的智能合约，当包含多个用户或者允许多个用户与其交互时，应对各用户所拥有的权限进行限制，对于冻结、禁用等操作，仅允许特定用户使用。

5.3.3 业务逻辑安全

智能合约技术提供者在智能合约业务逻辑的设计方面的安全要求包括：

a) 使合约代码实现与逻辑设计相符合，应避免歧义或者偏差存在；
b) 存在博弈机制的合约，应规避博弈设计中的缺陷；
c) 应规避“拒绝服务”（Denial-of-Service）风险；
d) 应规避“抢先交易”、“交易顺序依赖”的风险。

6 智能合约测试验证的安全技术要求

智能合约测试验证方面的安全技术要求如下：

a) 智能合约技术提供者在发布智能合约之前，应进行安全评估和测试，规避已知常见安全风险和隐患；
b) 智能合约技术提供者应修复已知的安全漏洞，并使用规范的安全测试，以协助开发者提高合约代码的安全质量；
c) 智能合约技术提供者宜进行函数可见性测试、合约限制绕过测试、调用栈耗尽测试、拒绝服务测试等；
d) 智能合约技术提供者若发现智能合约中漏洞，应能够采取恰当的方法使其安全地恢复；
e) 智能合约技术提供者应保证智能合约在测试环境中合约运行结果的正确性；
f) 智能合约技术提供者的安全测试应覆盖对合约代码或字节码进行常规漏洞检测、安全属性验证等；
g) 智能合约技术提供者应在发现智能合约漏洞后，及时修复和更新智能合约代码；
h) 智能合约技术提供者、智能合约业务提供者、智能合约审计者应对智能合约的业务逻辑、业务流程进行安全性的测试和评估；
i) 智能合约技术提供者、智能合约业务提供者、智能合约审计者应基于智能合约安全规则库和问题合约模式库实现智能合约的漏洞检测；
j) 智能合约技术提供者、智能合约业务提供者、智能合约审计者应支持对智能合约代码进行静态安全扫描，以便发现安全风险；
k) 智能合约技术提供者、智能合约业务提供者、智能合约审计者宜支持动态安全扫描，通过运行智能合约代码，根据运行状态来判断是否存在安全风险；
l) 智能合约技术提供者、智能合约业务提供者、智能合约审计者宜支持形式化验证，利用数学方法，确定程序的运行结果是否符合预期，验证智能合约代码的正确性。

7 智能合约编译部署的安全技术要求

7.1 智能合约编译的安全技术要求

智能合约技术提供者在智能合约编译时的安全要求如下：

a) 在编译智能合约时，应校验智能合约的编译实体和写入策略；
b) 应使用安全的共识算法，并通过第三方验证；
c) 应支持智能合约在区块链平台上编译检测；
d) 应使用已知的成熟的编译器；
e) 当发现编译器中的缺陷时，应及时更新以消除缺陷；
f) 编程语言的编译器应具备一致性；
g) 智能合约源码在编译成字节码后前后逻辑应一致。

7.2 智能合约部署的安全技术要求

智能合约技术提供者在智能合约部署方面的安全要求如下：

a) 智能合约的部署应由链上节点达成共识，防止产生恶意部署智能合约的行为；
b) 宜校验智能合约部署的完整性；
c) 应校验智能合约的执行权限和签名。

8 智能合约触发运行安全技术要求

8.1 智能合约触发的安全技术要求

8.1.1 直接接口调用安全

智能合约技术提供者在智能合约直接接口调用方面的安全要求如下：

a) 智能合约在直接接口调用时接口名称应明确接口功能，应具有可读性；
b) 智能合约的直接接口调用应执行规定的智能合约调用流程。

8.1.2 合约间调用安全

智能合约技术提供者在合约间调用方面的安全要求如下：

a) 智能合约的合约间调用，应丰富智能合约的内置方法和原生库实现；
b) 在涉及合约间调用时，应避免合约间调用可能存在的不确定因素安全风险，防止不受信任的外部合约引发的风险和错误出现；
c) 应选用恰当的限定词对智能合约的调用范围进行强制限制，防止外部调用，提高安全性；
d) 当与外部合约进行交互时，应以变量名称、方法名称或者是接口名称的方式明确标记交互是外部的，并在调用时考虑可能存在的不安全风险。

8.1.3 预言机调用安全

智能合约技术提供者在智能合约预言机调用方面的安全要求如下：

a) 智能合约在预言机调用时，接口协议应基于安全传输协议；
b) 预言机本身应通过第三方的安全性和可靠性评估；
c) 预言机的安全和可靠性评估应为定期进行的持续行为；
d) 如果发现预言机故意提供错误数据，应及时更正或者更换预言机；
e) 预言机提供的外部数据源的影响范围应仅限于智能合约范围内，不应影响系统的整体运行。

8.2 智能合约运行的安全技术要求

8.2.1 运行环境本身的安全性

智能合约技术提供者在智能合约的运行环境（执行智能合约的软件及硬件环境）本身的安全性方面的要求如下：

a) 应保证智能合约的运行环境提供确定性的功能执行、异常恢复、常规错误运行时监测和恢复等机制；
b) 应保障智能合约的运行环境满具备正确处理异常的能力，支持实时监测和状态回滚，支持合约正常终止。

8.2.2 运行环境依赖性

智能合约技术提供者在智能合约运行环境依赖性方面的安全要求如下：

a) 应保证智能合约中的核心逻辑尽量不依赖区块链系统中的信息作为参数；
b) 应保障智能合约核心逻辑对区块链系统参数的依赖是安全的。

8.2.3 规避恶意合约代码对运行环境底层的影响

智能合约技术提供者对运行智能合约的底层系统的安全要求如下：

a) 应保证运行智能合约的底层系统具备完备的拒绝服务防护；
b) 应保证运行智能合约的底层系统具备完备的虚拟机逃逸防护；

c） 应保证运行智能合约的底层系统具备完备的任意代码执行防护；
d） 应保证运行智能合约的底层系统具备完备的权限提升防护。

8.2.4 运行环境中不同合约的交互安全

智能合约技术提供者对于运行环境中不同智能合约的交互安全方面的安全要求如下：
a） 应提供权限管理的机制，以判断本次合约调用是否有权限修改相应的数据，包括提供根据用户信息和交易签名进行身份权限审查的功能（也可提供基于多密钥对的权限管理）等；
b） 对智能合约的接口应进行标准化定义并提供详细说明，并防止攻击者借用某合约身份对另一合约发起调用，从而绕过权限检查；
c） 智能合约的代码实现中，不应引入未知程序步数或执行时间的执行体，需支持合约能够在有限的程序步数和时间内完成执行；
d） 应避免使用智能合约中严重消耗资源的操作。

9 智能合约的维护治理安全

9.1 智能合约的冻结/解冻安全

智能合约技术提供者在智能合约的冻结和解冻方面安全要求如下：
a） 应提供智能合约冻结功能，当发现智能合约存在漏洞时可及时停止；
b） 在冻结智能合约时，应对其所能支配的资源进行有效限制，防止资源被恶意滥用；
c） 应提供智能合约解冻功能，当智能合约中的漏洞修复或者消除、转移后可恢复使用；
d） 在调用智能合约冻结和解冻功能时，应进行权限访问控制。

9.2 智能合约的升级安全

智能合约技术提供者在智能合约升级方面安全要求如下:
a） 应提供智能合约的在线升级功能,智能合约的每次升级应为独立版本；
b） 智能合约的升级操作应以接口调用的方式提交，达成共识后生效；
c） 对智能合约的升级操作应记录在区块中；
d） 应提供智能合约的版本控制功能，在智能合约升级到新版本后，能向前兼容旧版本合约，并能调用和访问旧版本的历史数据；
e） 应保证区块链平台升级后，智能合约仍能稳定运行。

9.3 智能合约的禁用安全

智能合约技术提供者在智能合约禁用方面安全要求如下：
a） 应提供智能合约禁用功能，废弃已部署的智能合约；
b） 调用智能合约禁用时，应进行权限访问控制；
c） 智能合约禁用后，可在区块链中保存被终止版本的智能合约代码，但不会再次执行；
d） 智能合约禁用时，应保证合约上的资产安全。

9.4 智能合约的安全审计

智能合约技术提供者、智能合约业务提供者和智能合约审计者在智能合约安全审计方面安全要求如下：
a） 智能合约技术提供者和智能合约审计者应对源代码进行审计，可通过人工审阅源代码和静态代

码审计工具等方式，对智能合约编码安全进行审计和分析，并保留审计记录；

b) 智能合约业务提供者对智能合约设计开发、测试验证、编译部署等过程进行安全审计以保证业务逻辑安全，并保留审计记录；应采取自身与第三方安全机构相结合的安全审计方式；

c) 智能合约业务提供者和智能合约审计者应对智能合约的编译环境进行审计，识别有漏洞的版本，并保留审计记录；

d) 智能合约业务提供者和智能合约审计者应对智能合约进行合规性审计，并保留审计记录；

e) 智能合约业务提供者和智能合约审计者应对智能合约中的个人隐私和商业秘密的保护措施进行审计，并保留审计记录；

f) 智能合约业务提供者和智能合约审计者应对源代码安全、二进制代码安全以及执行环境的安全进行审计，并保留审计记录。