中国区块链技术和产业发展论坛标准

CBD-Forum-002-2018

区块链 智能合约实施规范

Blockchain—Smart contract implementing specification

2018-12-18 发布　　2018-12-18 实施

中国区块链技术和产业发展论坛　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009 标准化工作导则 第 1 部分：标准的结构和编写给出的规则起草。

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这些专利的责任。

本标准由中国区块链技术和产业发展论坛提出。

本标准负责起草单位：众安信息技术服务有限公司、中国电子技术标准化研究院、深圳前海微众银行股份有限公司、厦门安妮股份有限公司、上海复星高科技（集团）有限公司、上海金丘信息科技股份有限公司、京东集团、易见供应链管理股份有限公司、浙江蚂蚁小微金融服务集团有限公司、中国平安保险（集团）股份有限公司、普华永道中天会计师事务所（特殊普通合伙）。

本标准主要起草人：瞿争、宋文鹏、李鸣、赵阳、范洪月、张健、吕国新、孙亮、孙琳、张开翔、徐磊、郝汉、杨胜、鞠鹏、洪蜀宁、韩峰、张林、王招军、齐宁宁、周海平、刘天成、孙曦、韩梅、冯承勇、王梦寒、张宝、郭亦卓。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛　秘书处）联系。

电话：010-64102801/2804

电子邮件：cbdforum@cesi.cn

通信地址：北京东城区安定门东大街 1 号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

区块链　智能合约实施规范

1　范围

本标准规定了区块链智能合约的实施规范，包括智能合约构建、触发、运行和评估过程。

本标准适用于：

a)　为计划使用区块链的组织建设区块链系统提供智能合约实施参考；

b)　指导区块链服务提供组织建立区块链系统智能合约的实现；

c)　为区块链系统建设过程中智能合约运行时环境的实现提供参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 18391.1-2002 信息技术 数据元的规范与标准化 第1部分：数据元的规范与标准化框架

CBD-Forum-001-2017 区块链 参考架构

3　术语和定义

GB/T 18391.1-2002、CBD-Forum-001-2017界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 18391.1-2002、CBD-Forum-001-2017中一些术语和定义。

3.1

区块链 blockchain

在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[CBD-Forum-001-2017，定义2.2.1]

3.2

数据类型 data type

由数据元操作决定的用于采集字母、数字和（或）符号的格式，以描述数据元的值。

[GB/T 18391.1-2002，定义3.25]

3.3

形式化验证 formal verification

用数学形式化方法对算法的性质进行证明或证伪的过程。

3.4

智能合约形式化验证 formal verification for smart contract

通过形式化的程序逻辑，证明智能合约程序是否满足给定的形式化规范。在满足规范的基础上，通过显式证明来验证结果的正确性。

3.5

标识符 identifier

数据元的唯一标识。

[GB/T 18391.1-2002，定义 3.33]

3.6

预言机 oracle machine

区块链与物理世界进行交互而存在的可信任实体。

注：预言机通常提供了智能合约在合约条款得到满足时运行的充分条件。

3.7

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

注 1：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。

注 2：本文件中，除非特殊说明，合约代指图灵完备的智能合约，即从智能合约代码、智能合约运行时环境均支持图灵完备。

[CBD-Forum-001-2017，定义 2.2.7]

3.8

图灵完备 Turing complete

一系列操作数据的规则（如指令集、编程语言、细胞自动机）按照一定的顺序计算并解决所有可计算的问题。

4 缩略语

下列缩略语适用于本文件。

DApp：分布式应用程序（Decentralized Application）

5 智能合约实施框架

智能合约实施框架包含合约构建、合约触发、合约运行和合约评估四部分，见图 1。

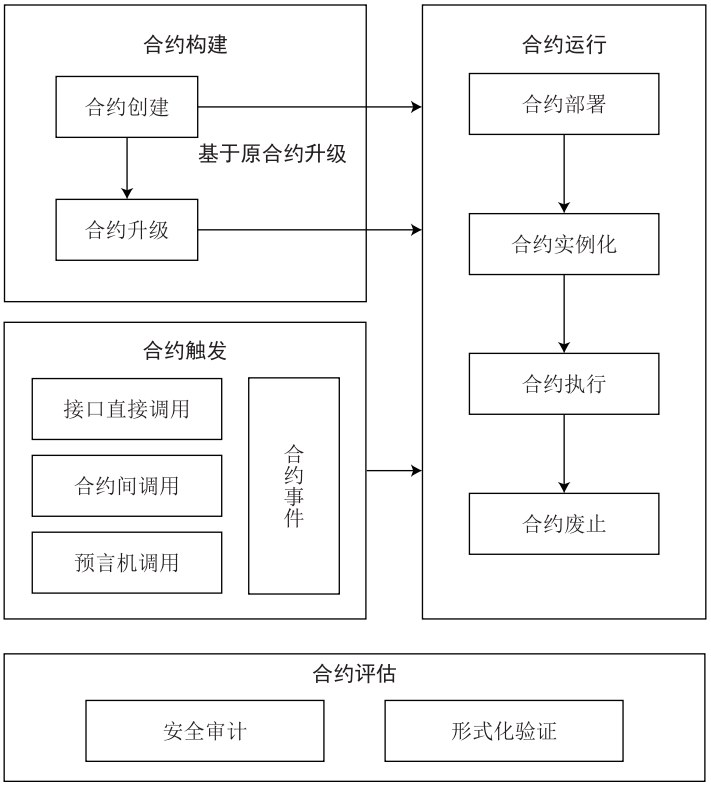

图 1　智能合约实施框架

6　实施过程

6.1　合约构建要求

6.1.1　合约编码规范

在编写智能合约代码时，应符合代码书写规范、逻辑要求等规范性要求。其中包括但不限于：

a)　书写规范：

1)　应使用已经广泛应用的安全技术和工具；

2)　合约和函数应模块化，逻辑简洁，避免逻辑性冲突，不宜使用过时的语法或用法，如分母为零、数值运算溢出、数组越界访问等。

b)　逻辑要求：

1)　对所有公共成员变量与函数的引用对象，进行对外暴露的风险分析；

2)　对所有条件选择语句和交易步骤进行完备性检查，满足条件动作描述的完备要求；

3)　避免已知的逻辑漏洞和低级的逻辑错误，如转账前余额未校验，未检查返回值的调用等。

6.1.2　合约语言约束

智能合约应使用已经广泛应用的合约语言，宜采用最新的稳定版本。合约语言的约束包含数据类型、计算类型和计算基本结构，见表 1。

表 1　智能合约语言约束

智能合约语言约束	应支持	宜支持
数据类型	string(字符串)、int(整型)、char(字符型)、boolean（布尔型）以及基本类型的数组类型	byte（字节型）、short（短整型）、long（长整型）、float（单精度浮点型）、double（双精度浮点型）等
计算类型	算术运算、关系运算、逻辑运算、条件运算、赋值运算	位运算、数据类型转换、HASH运算等
计算基本结构	顺序结构、分支结构和循环结构	异常结构处理、递归结构处理

6.1.3　合约版本定义

智能合约的每次修改应为独立版本，版本的定义方式可分为：

a)　代码中的定义：在源代码中通过区块链平台指定方式定义版本号；

b)　配置中的定义：在配置文件中定义版本号，该配置文件需要与智能合约代码一同部署；

c)　部署或升级中的定义：在部署或升级操作时定义版本号。

6.1.4　合约升级约束

智能合约的升级操作应由客户端发起、以接口调用的方式在区块链中提交，达成共识后生效，具体要求如下：

a)　升级操作应记录在区块中，符合区块链中交易要求、遵从交易执行的流程；

b)　智能合约升级后，应在区块链中保留前一版本；

c)　智能合约升级后，区块中记录的交易信息中应明确交易调用的智能合约版本。

6.2　合约触发要求

6.2.1　接口直接调用

直接调用是通过区块链接口，从外部直接触发调用。接口类型见表 2。

表 2　智能合约接口直接调用类型

接口类型	描述
创建接口	将智能合约的创建指令、相关代码和初始化参数传送至智能合约引擎，完成合约实例化。
调用接口	智能合约引擎根据发送者提供的参数，定位智能合约实例，加载合约代码，并执行合约指令。
查询接口	根据指定的智能合约寻址方式，查询智能合约实例的信息，包括合约代码，创建者，内部数据，合约状态等。
升级接口	根据指定的智能合约寻址方式和传入的数据，升级合约代码、内部数据和合约状态等，并将升级操作做为新的交易生成新的智能合约实例。
废止接口	根据指定的智能合约寻址方式，将指定的智能合约实例置为无效。

表 2　智能合约接口直接调用类型（续）

接口类型	描述
监管接口	为监管机构提供接口，供其按照监管规则进行操作。
获取环境常量接口	智能合约引擎在运行智能合约代码过程中，区块链系统应为智能合约引擎提供相关数据读取接口，提供的数据应为常量，不能被智能合约引擎修改。
查询日志接口	根据指定的智能合约寻址方式、交易标识和日志文件，查询合约运行时产生的日志。

6.2.2　合约间调用

合约间调用是指合约之间进行链上调用的过程。合约间互相调用时，宜使用“检查－生效－交互”模式。合约间调用可实现：

a)　将已部署的合约视为库，提供给其他合约使用；

b)　合约的多功能组合，如合约复用、合约升级、跨 DApp 交互等。

6.2.3　预言机调用

预言机调用是通过预言机可信实体获取智能合约执行的过程。预言机的调用接口要求如下：

a)　接口名称应明确接口功能，并具有可读性和可维护性；

b)　接口入参应明确参数的具体类型、数量和输入信息；

c)　接口返回数据应明确数据类型、数量和输出信息；

d)　接口描述文件应为预言机提供的结构化描述语言；

e)　接口协议应包含安全传输协议。

6.3　合约事件约束

6.3.1　合约事件类型

6.3.1.1　调用事件

调用事件是指由调用方主动对特定操作发起的调用请求，调用事件结构见表 3。

表 3　调用事件结构

属性	要求
调用事件名称	合约内唯一事件标识，事件名称应简短明确的描述事件功能。
调用事件入参	调用事件执行前应必备的参数条件，调用者可根据事件定义的入参类型和数量执行事件。
调用事件出参	在接受到调用方的调用请求以及入参后，执行返回给调用方的结果信息。应明确定义事件的出参类型和数量。

6.3.1.2 回调事件

回调事件是指对合约内事件实例的监听。在合约内部事件完成后，应将事件结果以消息的形式派发给事件监听方。回调事件结构见表 4。

表 4 回调事件结构

属性	要求
回调事件名称	合约内唯一事件标识，事件名称应简短明确的描述回调事件功能，便于外部调用者了解回调事件所承担的职责。
回调事件入参	需回调函数监听方应明确监听回调事件，并依据回调事件定义的格式处理消息。

6.3.1.3 信号事件

信号事件是指在构造事件中设定约束或触发条件，当条件满足时触发信号事件。事件以信号方式传递给信号监听方，信号事件结构见表 5。

表 5 信号事件结构

属性	要求
信号事件名称	合约内唯一信号标识，事件名称应简短明确的描述事件功能，便于外部调用者了解信号事件所承担的职责。
信号事件入参	信号事件约束条件为事件触发设立的触发阈值（如时间点、时间间隔、区块数等），当条件达到阈值要求则触发事件。

6.3.2 事件接口结构

事件接口结构为调用方提供接口的规范化说明。事件接口结构见表 6。

表 6 事件接口结构

属性	要求
接口名称	唯一的接口名称，使调用方明确接口调用功能。
接口入参	确定的入参类型和数目，使调用方明确接口输入信息。
接口出参	确定的出参类型和数目，使调用方明确接口接受信息。
接口描述文件	合约应提供结构化描述语言说明接口的声明内容，使调用方能通过描述信息使合约接口触发合约事件。
接口协议	合约应提供传输协议，使接口调用的数据传输到合约事件内，同时合约执行结果可回传给接口调用方。

6.4 合约运行过程

6.4.1 合约部署

合约部署是将合约代码部署到区块链网络节点的智能合约运行时环境中的过程。

6.4.2 合约实例化

合约实例化是将智能合约代码转换成运行环境可执行的格式的过程，该过程由智能合约运行环境自动完成。合约实例化应满足以下要求：

a) 系统应校验智能合约的实例化实体、通道写入策略和签名的验证；

b) 系统应将智能合约内容的 HASH 值写到区块链网络中；

c) 节点在运行智能合约前，应检查该智能合约和链上智能合约的 HASH 值的一致性。

6.4.3 合约执行

合约执行是执行智能合约业务逻辑的过程。合约在智能合约运行时环境中的执行结果应具备事务一致性。合约执行可视为合约状态的迁移，同时合约状态作为合约账户的属性保存在区块链网络上。

6.4.4 合约废止

合约废止是废弃已部署智能合约的过程。该过程以接口调用的方式，在区块链中达成共识后生效。合约废止应满足以下要求：

a) 调用智能合约废止时，应进行权限访问控制；

b) 智能合约废止后，应在区块链网络中保存被终止版本的智能合约代码。

6.5 合约评估方法

6.5.1 安全审计

智能合约的安全审计和评估对象包括智能合约设计及业务逻辑安全、源代码安全审计、编译环境审计及相关的应急响应等。

a) 设计及业务逻辑安全审计

对业务逻辑的安全评估可通过人工阅读文档和源代码的方式，对智能合约的业务流程进行安全性的测试和评估。编码规范参见“6.1 合约构建要求”章节。

b) 源代码安全审计

对源代码的审计可通过人工阅读源代码和代码审计工具的方式，对智能合约编码安全进行测试分析。

c) 编译环境安全审计

对编译环境的审计可通过人工观察智能合约编译器的名称和版本，识别有漏洞的版本。

d) 应急响应

发现智能合约漏洞后，应及时检查和修复智能合约源代码。

6.5.2 形式化验证

形式化验证可分为合约制定、形式描述、建模验证、代码生成和一致性测试五个过程，见图 2。

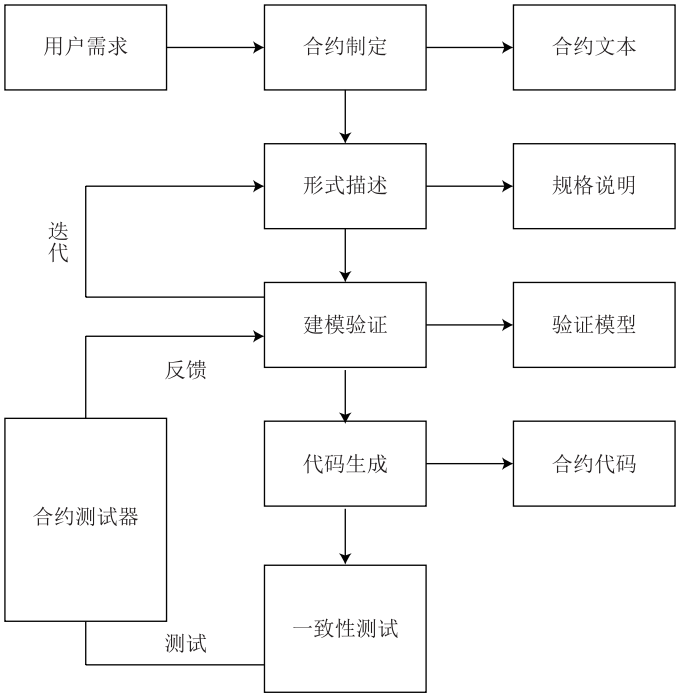

图 2　形式化验证活动图

a）　合约制定

根据用户需求及多方约定，使用非形式规范来设计合约，编写智能合约文本。

b）　形式描述

根据智能合约的模型描述和性能描述等要求，对合约文本进行形式化描述。

c）　建模验证

选择合适的建模语言和建模工具，对形式化描述的文档进行建模和验证。

d）　代码生成

通过模型驱动架构对待转换模型进行分析和解释，将验证模型生成符合形式化描述的标准化合约代码。

e）　一致性测试

一致性测试是指生成的合约代码与标准的合约文本一致的测试过程。主要包括模型检测、定理证明和等价性验证等方法。

参 考 文 献

[1] CBD-Forum-001-2017 区块链 参考架构

[2] OMG ® Unified Modeling Language ® (OMG UML ®) Version 2.5.1

CBD-Forum-001-2018

电话：010-64102801/2804
电子邮件：cbdforum@cesi.cn
网址：http://www.cbdforum.cn