电磁频谱空间认知动态系统工业和信息化部重点实验室标准

COG 00002-2022

联盟链 监管系统技术要求规范

Consortium Blockchain-Technical Requirements Specification of Regulation System

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2022－XX－XX 发布　　2022－XX－XX 实施

南京航空航天大学
电磁频谱空间认知动态系统工信部重点实验室
发 布

目　　次

前　言

本文件按照GB/T 1.1-2020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。

本文件由南京航空航天大学和电磁频谱空间认知动态系统工信部重点实验室提出。

本文件由电磁频谱空间认知动态系统工信部重点实验室归口。

本文件起草单位：南京航空航天大学、电磁频谱空间认知动态系统工信部重点实验室、北京邮电大学、北京工业大学、山东大学、南京大学。

本标准主要起草人：王威，吴启晖，朱友文，郭少勇，公备，韩路，于东晓，张华，黄静，高飞，熊翱，毛云龙，徐明辉，郭嘉，李祖广，陈文彬，王梦莹，许文静，林功明，潘恒昌，孙珊，孙劲歌。

引　　言

联盟链是有特定准入规则的许可式区块链，相比于公有链，联盟链在效率和灵活性上更具优势，已成为我国区块链的重要发展方向。联盟链的安全风险将引发行业应用风险，目前对联盟链的应用仍存在监管缺失、监管信息不透明等问题。

本文面向联盟链系统与应用面临的安全风险，梳理联盟链监管要求，建立联盟链监管系统技术要求规范，用于明确和规范联盟链监管系统技术要求，为评价联盟链监管系统与服务提供指导。

联盟链 监管系统技术要求规范

1 范围

本标准规定了联盟链监管系统技术要求规范，包括如下内容：

a) 监管需求；
b) 监管框架；
c) 监管方法与要求；
d) 监管的隐私保护要求；
e) 监管权限管理要求；

本标准适用于：

a) 指导联盟链系统监管方建立健全监管机制；
b) 第三方评价联盟链监管系统服务能力。

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，仅所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。

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

GB/T xxx-xxx 信息技术 区块链和分布式记账技术 参考架构 （计划号：20173824-T-469）

GB/T xxxxx 信息安全技术 区块链技术安全框架 （计划号：20210998-T-469）

TD/T 3747-2020 区块链技术架构安全要求

JR/T 0184-2020 金融分布式账本技术安全规范

CBD-Forum-001-2019 区块链 隐私计算服务指南

CBD-Forum-002-2018 区块链 智能合约实施规范

TSIA028-2021-联盟区块链安全技术要求

T/CESA 1049-2018 区块链 隐私保护规范

DB43/T 1843-2020 信息安全技术 区块链数据安全技术评测要求

YD/T 3747-2020 区块链技术架构安全要求

CBD-Forum-002-2017 区块链 数据格式规范

3 术语和定义

ISO 22739:2020界定的以及下列术语和定义适用于本文件，为便于使用，以下重复列出了ISO 22739:2020中的一些术语和定义。

3.1

账本 ledger

按照时序方法组织的事务数据集合。

3.2

区块 block

一种包含区块头和区块数据的数据结构，其中区块头包含前一个区块的摘要信息。

3.3

区块链 blockchain

一个以区块为基本数据单元、按顺序储存的多副本的分布式账本技术。其中，区块是一段时间内的一组特定数据的集合，由区块头和区块体两部分组成；按顺序是根据区块产生的时间顺序排列，并且前后区块用密码技术保障顺序的安全性。区块链是分布式存储、共识机制、点对点通讯、密码算法等计算机技术在互联网时代的集成式创新和应用模式。

[T/SIA 007 术语 3.1]

3.4

实体 entity

信息和通信技术系统内部或外部的项目，例如个人、一个组织、一个设备、一个子系统或一组具有可识别的存在性的此类项目。

3.5

账户 account

参与交易的实体的账户表示。

3.6

节点 node

区块链中代表用户利益参与记账的计算机或智能设备称为节点。节点保存着自己的一份或者部分账本，通过算力或者份额投票的方式来解决共识问题，通过无信任的方式确保全体节点遵循的账本和自己的账本是一致的。

[T/SIA 007 术语 3.11]

3.7

共识 consensus

在分布式节点间达成区块数据一致性的认可。

3.8

联盟区块链 consortium blockchain

区块链由多个中心控制，系统由几个权威的机构共同分布式记账，这些节点再根据共识机制协调工作。

对特定的组织团体开放，一种仅有授权节点接入和使用的区块链部署模型。

3.9

智能合约 smart contract

存储在分布式账本中的计算机程序，其共识执行结果都记录在分布式账本中。

以数字形式定义的能够自行执行条款的合约。

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

3.10

时间戳 timestamp

时间变量参数，表示相对于公共时间参考的时间点。

[来源: ISO/IEC 18014-1:2008]

3.11

交易 transaction

工作流程的最小单元，即生成符合治理规则的结果所需的一个或多个操作序列。

3.12

事务 transaction

工作过程的最小单元， 是产生符合规则要求的结果所需的一个或多个动作序列。

3.13

链下 off-chain

与区块链系统相关，但在该区块链系统之外定位、执行或运行。

3.14

链上 on-chain

在区块链系统内定位、执行或运行。

3.15

监管方 supervisor

数据授权过程中负责实时监控授权行为是否违规的实体。

[示例：行政机关]

3.16

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

4 缩略语

下列缩略语适用于本文件

API：应用程序接口（Application Programming Interface）

SDK：软件开发工具包（Software Development Kit）

BaaS：区块链即服务（Blockchain as a Service）

PBFT：实用拜占庭容错（Practical Byzantine Fault Tolerance）

TPS: 每秒处理事务数（Transactions Per Second）

5 监管需求

为保障联盟链健康稳定运行，监管主体需要对已有的联盟链及其服务进行监管。

监管主体：联盟链的监管主体应为具有相关监管资质的省市互联网信息主管部门以及相关联盟链系统服务业务的主管部门。监管主体应遵循国家互联网信息办公室（以下简称：网信办）颁布的《区块链信息服务管理规定》开展本区域内联盟链信息服务的监管工作。

注：根据《区块链信息服务管理规定》，我国区块链的监管是以国家网信办为监管主体，以工业和信息化部为标准制定主体，以行业协会等为自律主体的三层监管架构。国信办作为监管主体，负责对提供各类区块链技术信息服务的服务商进行统一监管；工业和信息化部通过标准对技术方面实行监管；行业协会等进行自律性监管。

监管对象：在国家网信办区块链信息服务备案管理系统备案的，向社会提供基于联盟链技术服务的联盟链系统及其应用程序。

监管服务要求：监管机构应能从被监管联盟链获取用户身份信息；可通过监管平台实现对节点的权限控制；基于链上交易数据，可验证交易信息的合规性，追溯交易历史，并实现对多方交易行为的深度关联分析。

5.1 基本要求

符合条件的监管机构应在国家网信办备案，待审核通过后被赋予不同的监管权限，权限包括查看链上数据、更改区块内容、禁用链码等。

应支持监管机构灵活接入被监管联盟链，满足对链上节点、运行业务或联盟链提供的服务等进行安全审计和披露的要求。

应支持监管主体对监管权限的管理，包括但不限于更新监管规则，提取交易记录，按需查询、分析特定业务数据等。

应支持监管权限分层级管理，不同层级监管节点具有不同的监管权限，且高层级监管节点权限应包含低层级监管节点的所有权限。

应支持对监管权限的动态可调，监管主体可以禁用、激活以及删除特定监管节点。

应支持采用多种隐私保护技术，确保监管机构只能看到自己权属范围内的数据，保护用户数据隐私。

应支持监管信息和监管行为可信存证。

支持监管数据统计分析和可视化呈现。

5.2 分布式监管

应支持灵活的分布式监管方式，包括：

a) 支持分布式监管节点组成监管链，监管行为在监管链共享，实现监管信息共享、监管权限和监管行为相互监督、监管行为共识存证，保障监管的可信性。

b) 支持分布式监管节点接入监管平台，监管平台赋予不同监管节点不同的监管权限，并将监管节点的监管行为写入日志。

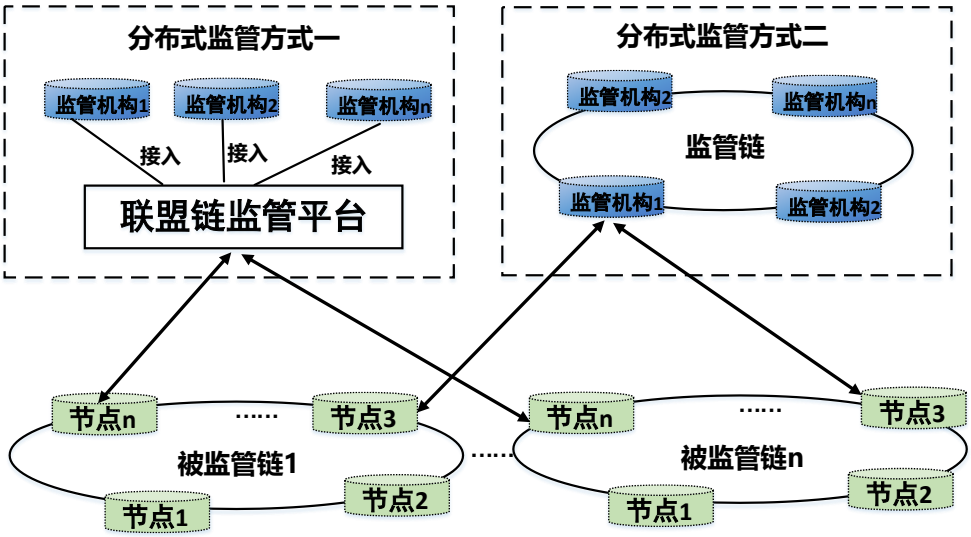

图1 分布式监管接入方式

5.3 穿透式监管

根据不同层级按需监管的要求，应允许上层监管机构对下层级联盟链的监管；

支持监管机构访问最底层数据，确保真实、准确、完整地采集交易信息，并建立信息分析和交易行为分析系统，实现穿透式监管。

应支持授权监管机构对违规交易区块的修改。

应支持对复杂交易特征的提取，识别隐藏的交易模式和特征。

5.4 全维度监管

支持对联盟链运行状态监管，包括但不限于联盟链底层架构、交易信息等。

支持对联盟链节点状态监管，包括节点位置、运行状态、信誉情况、网络连接情况等。

支持对钓鱼账户、交易所、矿池等不同账户的识别；

支持从交易发起到交易完成的交易全流程监管与溯源，监管机构基于同步的链上数据，通过大数据挖掘分析，实现端到端、跨机构和交易全流程的监管审计，追溯每一笔交易的历史痕迹，并监控关联节点的交易信息，防范风险事件的发生。

支持智能合约逻辑漏洞审查、运行状态监管等全生命周期监管。

支持监管机构对链上违规行为的处罚，对识别出的链上违规行为应支持恶意节点的剔除、违规区块的更改等操作。

5.5 监管权限管理

监管权限应严格审批和使用，应明确监管对象、方式、范围、规则等。

监管策略与权限应对被监管链透明，如发生策略更新或权限调整应在被监管联盟链上共识确认。

被监管链上信息的收集和使用应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，且不得违反对信息和服务安全和隐私保护的法律法规规定。

应支持对监管行为的存证，监管行为存证应包含具体的交易信息、监管行为、时间戳等。

应支持被监管链对超出监管权限的行为向上级监管机构申诉。

5.6 隐私保护

支持链上交易信息的多级别隐私保护，确保被监管联盟链上隐私信息只有拥有权限的监管节点才能解密，避免信息泄露。

支持拥有权限的双节点同时解密，增加隐私保护安全性。

支持多种类型的隐私保护技术应用，如零知识证明、安全多方计算等。

支持隐私保护策略升级。

6 监管架构

支持多种形式的监管接入，包括但不限于嵌入式监管、基于BaaS平台的后台接入式监管等，具体监管接入框架包括：

a) 嵌入式监管：即支持监管节点嵌入被监管联盟链，此监管方式不仅支持监管节点同步链上交易数据，也可使监管节点参与链上共识；

b) 基于 BaaS 平台的后台接入式监管：监管节点可获得 BaaS 平台的后端接口访问权限，基于 BaaS 平台获取在此平台上构建的联盟链交易数据，对交易数据解析后实现监管。

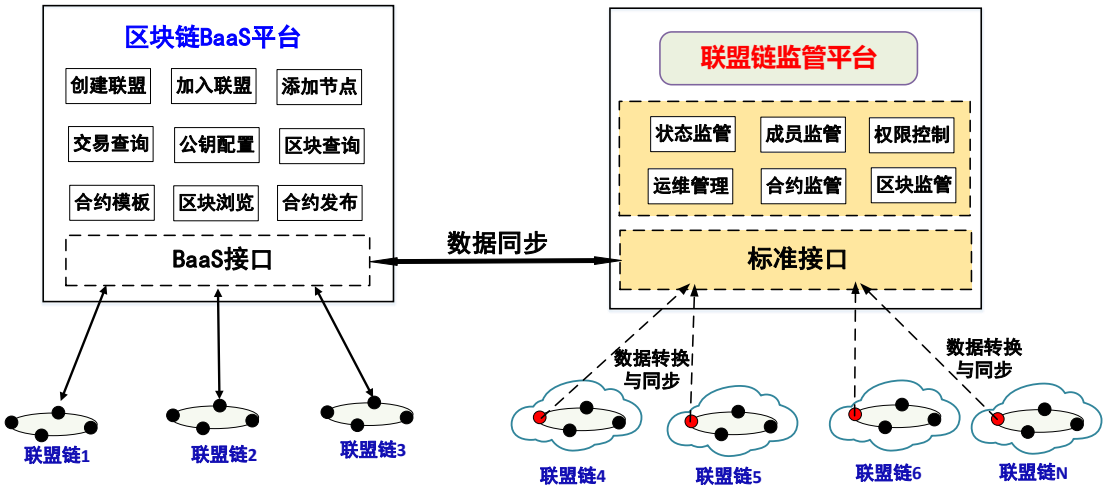

图2 联盟链监管一般架构

6.1 嵌入式监管架构

被监管联盟链应支持监管节点嵌入，各监管节点根据其职责权限，确定监管业务范围，对链上相关交易及数据进行审查和认证。

嵌入的监管节点可选择是否参与链上共识，如监管节点参与链上共识，则被监管链上交易共识前应先由被监管链审查，审查通过后再执行正常共识过程。

嵌入式监管节点如参与共识，则其权重应大于其余节点权重之和的一半以上，确保监管节点对交易具有一票否决权。

嵌入式监管节点如不参与共识，则应具备数据同步功能，可将链上区块信息全部同步至监管中心。

应支持监管节点权限调整和更新，嵌入式监管节点的权限更新应在被监管链上共识确认。

6.2 基于 BaaS 平台的监管架构

应支持监管机构接入 BaaS 平台，且应根据监管机构权限赋予其一定的 BaaS 平台操作权限，包括查看 BaaS 平台上运行的联盟链基本情况及相关交易数据、更改被监管联盟链节点及用户权限、查看链码及链码禁用等操作，实现对 BaaS 平台上运行联盟链的全方位监管。

应支持监管机构通过 BaaS 平台将区块数据按照标准格式同步至监管机构，构造被监管链的数字孪生体。

应支持 BaaS 平台通过标准化接口自动推送相关交易信息。

BaaS 平台上新建联盟链应在监管平台备案，备案信息包括业务主体、服务内容、服务对象、数据格式等。

6.3 监管服务流程

联盟链监管服务流程如图 3 所示。监管机构可通过 SDK 接口查询链上交易、数据、身份等信息，同时按需更新监管规则。基于监管规则，监管模块更新风险模型并配置监管告警模型，同时告警规则下发至被监管联盟链上各监管节点，监管节点依据告警规则对链上交易进行监控。如果区块链的监控项状态异常，则触发告警，并自动生成相应的告警信息反馈给监管平台，监管机构对异常信息进行处理，并对相应违规行为做出惩罚。为进一步优化风险评估模型，监管节点定时将链上数据同步至机器学习平台，机器学习平台对链上数据进行分析，并将分析结果反馈给监管模块实现风险模型的优化。

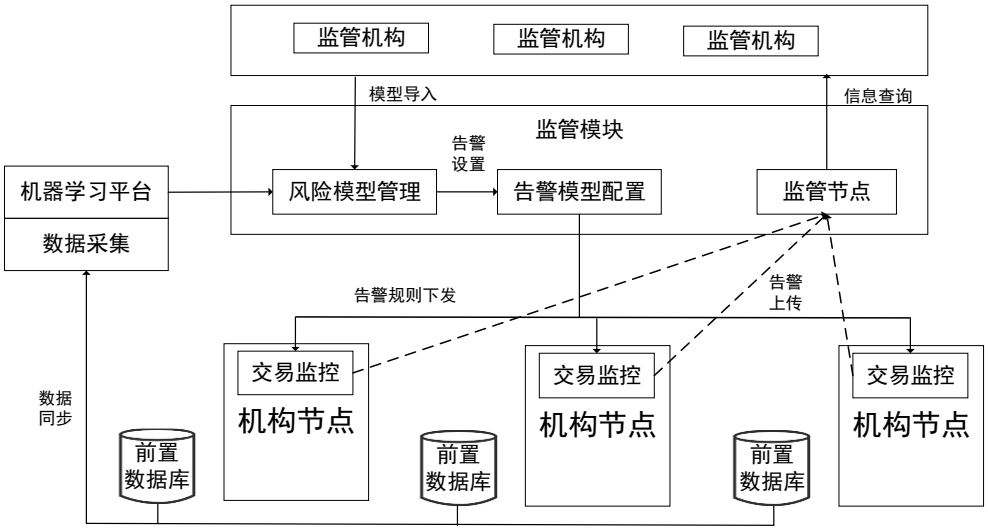

图3 监管服务流程示意图

7 节点和状态监管

7.1 基本要求

支持对联盟链运行状态、节点状态等监管，包括但不局限于：联盟链业务情况、节点位置分布、区块平均生成时间、最新区块生成时间、最新区块号、合约数量、共识算法、存储情况等。

支持对被监管联盟链运行状态数据的收集，并写入日志供测试或审查用，如异常应及时预警并处理。

支持节点准入和节点权限动态管理，支持对节点运行状态以及节点之间连接的监管；如发现部分节点运行异常，应在不影响服务运行的同时及时进行问题排查，在规定时限内将节点恢复至正常状态或启用备选节点，保障业务的政策运行。

7.2 联盟链及其系统用户身份监管

支持节点账户审核，包括节点账户身份审核和信用审核；

节点账户监管信息包括个人身份信息、证件照片或扫描件、个人征信情况等能够反映个人身份、现状、信用情况的信息；若节点拥有者为企业则账户监管信息包括：企业名称、营业执照、法人信息和企业信用等能够反映企业现状、信用情况以及法人身份、现状、信用情况的信息。

若节点账户监管信息发生了变更导致不能通过审核时，则监管节点向区块链上的其它各节点发出移除该节点的提议，其它各节点将屏蔽该节点，不与该节点发生交易。

支持身份信息变更，且应至少每六个月向监管机构更新一次。

7.3 节点运行状态监管

应对节点运行状态及节点与其他节点的连接进行监管；

应支持对节点的异常处理，如发现部分节点运行异常，应在不影响业务运行的同时及时进行问题排查，并在规定的时限内将节点恢复至正常状态或启用备用节点，保障业务正常运行；如果无法在规定时间内恢复节点，则应上报管理委员会；

如节点与其他节点连接异常，则应在不影响服务运行的同时，排查其他节点故障，且将情况上报管理委员会；

应收集系统运行中的状态数据，包括远端同步节点数、账本同步平均耗时、节点健康状态等，并写入日志供测试或审查，如异常应及时预警并处理；

如发现恶意或欺诈节点传播恶意损坏的账本数据，或有节点篡改账本，则应先定位节点位置，记录节点之前的信息，上报管理委员会。

8 交易监管

8.1 交易内容监管

8.1.1 基本要求

支持对区块链交易内容的安全及隐私审核，审核交易包含的信息中是否带有对区块链信息安全具有威胁性的木马、病毒等程序，是否带有泄露隐私的敏感信息。

支持交易存证，保证交易数据的原始与安全，通过电子签名、时间戳、哈希值等确认电子数据产生的提交者和提交时间，进行交易存证。

支持对交易内容的大数据分析，以识别异常交易行为。

支持监管方对特定交易内容的快速检索和定位。

支持授权监管方对存在违规消息区块进行修订，以删除链上恶意数据。

支持交易监管的统计显示，包括但不限于：交易次数、最新交易数据、交易频率(TPS)、峰值交易量、频繁交易账户、大额交易数等。

8.1.2 合规与合法性性监管

支持对区块内容的合规与合法性审核，包括是否包含法律、行政法规、规章禁止发布或者传输的信息。

支持对区块中包含的交易合法性审核，包括交易信息是否有违反市场监督管理法律、法规、规章，损害国家利益和社会公共利益，违背公序良俗等内容。

支持交易合规性审核，审核交易内容是否合规，比如一段时间内的交易总额、纳税比例等。

支持交易额度监管，根据交易额度界定大额交易或可疑交易，存在大额或可疑交易则进行记录并报告不符合行业规定的信息。

支持对交易发起人、接收人身份识别，对违规交易法人主体资质查询与权限管理。

8.2 交易行为监管

应支持监管机构对海量交易数据的解析，包含交易双方身份、具体交易商品或数据、交易发生时间、

交易金额等。

应支持监管机构按交易 ID、交易金额等筛查和追溯，基于海量交易数据实现交易关联关系分析，形成交易关联关系图。

支持对特定交易发起账户相关的交易关联追溯与分析，识别交易人的交易行为特征，如交易频次、平均交易次数、平均交易额度、大额交易数目等。

支持区块链用户身份推测与追踪，针对具有异常或非法行为的用户，推测其身份并追踪轨迹，减少利用区块链进行违法犯罪的行为。

支持异常交易模式发现和预警，如频繁交易、恶意刷单、虚假交易等，对短期内频繁进行交易的合约账户进行审核，判断其是否存在频繁回笼诈骗资金的可能性。

支持对交易评价的识别和关联，如恶意和虚假评价等。

9 智能合约监管

9.1 基本要求

应支持智能合约上线前的第三方安全审计，并保留审计记录，未通过审计的合约不能上线运行。

支持智能合约部署、调用、运行、撤销及合约调用时输入输出结果等实际运行过程监管，合约运行过程数据应存证记录。

支持按需将监管要求编码写入智能合约强制执行。

应能根据需要为监管机构提供交易行为统计数据，评价智能合约所提供服务的合规性。

9.2 合约静态监管

应对合约源代码进行安全审计，可通过人工阅读源代码和代码审计工具的方式，对联盟区块链编码安全进行测试分析，测试应覆盖超过 90%的代码。

应对源代码的词法、语法、语意进行静态分析，以减少源代码中存在的结构性错误、逻辑性错误、安全漏洞等问题。

支持对智能合约的形式化验证，消除合约中的歧义和不通用性，验证智能合约中函数功能的正确性和安全性。

支持对智能合约设计与业务逻辑一致性审计、编译环境审计及相关的应急响应机制。

应对业务逻辑、业务流程进行安全性测试和评估，评估交付物包括测试报告、测试用例集。

应支持多种主流智能合约语言的审计，包括但不限于 Go、solidity 等。

支持对智能合约执行效率的评估和优化。

支持对相似合约的挖掘，提取合约差异代码，实现对相似合约的分析、识别、关联。

9.3 合约动态监管

支持智能合约的部署行为监管，防止恶意部署智能合约。

支持对智能合约的动态监控，通过模糊测试、符号执行等技术手段对智能合约漏洞进行监测。

支持智能合约的冻结功能，防止智能合约漏洞持续影响系统。

支持智能合约升级，以修复智能合约漏洞。

支持将原合约数据迁移至升级更新、重新部署后的新合约。

支持智能合约的废止功能。

10 隐私保护

应满足交易金额和交易者身份地址对交易无关节点的隐私性。

支持对隐私保护方案的审计，审计内容包括隐私保护策略和隐私保护技术手段。

支持对隐私保护策略和隐私保护技术手段的合理性评估，包括对隐私保护原则的遵循程度，对不同隐私保护等级的风险防范要求匹配度，在当前环境下的适用性等。

支持隐私保护策略和隐私保护技术手段的执行过程监管，包括但不限于操作手册、操作记录等，确认执行过程遵循并实现既定的策略和技术手段。

支持对隐私保护策略和隐私保护技术手段的效果监管；确认隐私保护内容得到有效保护，达到既定要求。

支持对隐私保护策略的修改和变更，并按照新的规则实现隐私保护。

支持对不同隐私保护等级制定不同的监管和审计策略。

支持智能合约的隐私保护，包括但不限于合约代码本身的隐私和合约输入输出的隐私。

支持对隐私敏感数据创建可信执行环境，达到数据可用不可见。

参考文献

《区块链国家标准》 CBD-Forum-001-2017
《区块链技术安全通用规范》 TSSIA 0002-2018
《信息系统安全等级保护基本要求》 GB/T 22239-2019
《信息技术 区块链和分布式记账技术 参考架构》GB/T xxx-xxx
《信息安全技术 区块链技术安全框架》GB/T xxxxx
《金融分布式账本技术安全规范》 JR/T 0184
《区块链平台基础技术要求》 T/SIA 007
《联盟区块链安全技术要求》T/SIA 028—2021
《区块链 隐私计算服务指南》CBD-Forum-001-2019
《区块链 智能合约实施规范》CBD-Forum-002-2018
《区块链 隐私保护规范》T/CESA 1049-2018
《信息安全技术 区块链数据安全技术评测要求》DB43/T 1843-2020
《区块链技术架构安全要求》YD/T 3747-2020
《区块链 数据格式规范》CBD-Forum-002-2017