ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 42571—2023

信息安全技术
区块链信息服务安全规范

Information security technology—
Security specification for blockchain information service

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　概述 …… 3
5.1　区块链信息服务概述 …… 3
5.2　区块链信息服务安全风险概述 …… 3
6　安全技术要求 …… 3
6.1　信息生成 …… 3
6.2　信息处理 …… 5
6.3　信息发布 …… 5
6.4　信息传播 …… 6
6.5　信息存储 …… 7
6.6　信息销毁 …… 8
7　安全管理要求 …… 8
7.1　制度管理 …… 8
7.2　机构和人员 …… 9
7.3　业务连续性 …… 10
7.4　运行与维护 …… 10
8　安全技术要求测试评估 …… 11
8.1　信息生成 …… 11
8.2　信息处理 …… 15
8.3　信息发布 …… 17
8.4　信息传播 …… 18
8.5　信息存储 …… 21
8.6　信息销毁 …… 23
9　安全管理要求检查评估 …… 24
9.1　制度管理 …… 24
9.2　机构和人员 …… 26
9.3　业务连续性 …… 27
9.4　运行与维护 …… 30
附录 A（规范性）　区块链信息服务安全等级划分 …… 32
参考文献 …… 33

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院信息工程研究所、浙江大学、杭州趣链科技有限公司、蚂蚁科技集团股份有限公司、深圳市腾讯计算机系统有限公司、中国电子技术标准化研究院、重庆邮电大学、公安部第三研究所、国家计算机网络应急技术处理协调中心、中国信息通信研究院、浦东新区人民政府办公室、国家工业信息安全发展研究中心、中国科学院计算技术研究所、上海市信息安全测评认证中心、陕西省网络与信息安全测评中心、四川省数字经济研究中心、公安部第一研究所、北京大学、清华大学、北京东方通网信科技有限公司、国网区块链科技(北京)有限公司、中国电子科技网络信息安全有限公司、联想(北京)有限公司、北京百度网讯科技有限公司、启明星辰信息技术集团股份有限公司、浪潮电子信息产业股份有限公司、国家能源局信息中心、京东科技控股股份有限公司、中国电力科学研究院有限公司、泰康保险集团股份有限公司、深圳市纽创信安科技开发有限公司、新华三技术有限公司、成都链安技术有限公司、北京众享比特科技有限公司、兴唐通信科技有限公司、北京爱奇艺科技有限公司、北京数字认证股份有限公司、矩阵元技术(深圳)有限公司、北京融数联智科技有限公司、北京小米电子软件技术有限公司、郑州信大捷安信息技术股份有限公司、北京猿链网络科技有限公司、北京人民在线网络有限公司、北京天融信网络安全技术有限公司、深圳壹账通智能科技有限公司、标信智链(杭州)科技发展有限公司、浙商银行股份有限公司、中国汽车工程研究院股份有限公司。

本文件主要起草人：张潇丹、郭涛、蔡亮、王惠莅、胡静远、周熙、韩冀中、姚相振、李伟、陈晓丰、昌文婷、张瀚文、武杨、郑佩玉、王磊、邵羽、黄永洪、崔婷婷、吕红蕾、史洪彬、周薇、刘总真、王宇航、谢安明、刘贤刚、孙毅、陈妍、职亮亮、李仁刚、冯伟、刘为华、吴桐、安高峰、王海棠、黄得志、蒋蓉生、万晓兰、余宇舟、卢志刚、梅秋丽、邹超、朱岩、白健、樊庆君、王丹琛、高瑞、张美娟、臧铖、吴新勇、任泽君、黄婧祎、王文磊、张永强、庞舒恬、罗新辉、张媛媛、闫希敏、陈红、张素博、安立、王云浩、李克鹏、张虎、谢红军、李瑞荣、荆博、全代勇、王梦楠、符史健。

信息安全技术
区块链信息服务安全规范

1 范围

本文件规定了区块链信息服务提供者的安全技术要求和安全管理要求，描述了相应测试评估方法和检查评估方法。

本文件适用于对区块链信息服务开展安全建设、安全运行、安全管理和安全评估等服务。

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/Z 20986—2007 信息安全技术 信息安全事件分级分类指南

GB/T 25069—2022 信息安全技术 术语

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 40645—2021 信息安全技术 互联网信息服务安全通用要求

GM/T 0033—2014 时间戳接口规范

3 术语和定义

GB/T 25069—2022、GB/T 35273—2020 和 GB/T 40645—2021 界定的以及下列术语和定义适用于本文件。

3.1

区块链信息服务 blockchain information service

基于区块链技术或系统，通过互联网站、应用程序等网络平台提供的信息服务。

3.2

区块链信息服务用户 blockchain information service user

使用区块链信息服务的组织或个人。

注：区块链信息服务用户简称“用户”。

3.3

区块链信息服务提供者 blockchain information service provider

向区块链信息服务用户提供区块链信息服务的组织。

注：区块链信息服务提供者包括但不限于区块链业务运营者和区块链技术提供者。

3.4

时间戳 timestamp

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

[来源:GB/T 25069—2022,3.541]

3.5

上链 record on-chain

将信息写入到区块链的过程。

3.6

节点 node

具有特定功能的区块链组件,可独立运行的单元。

[来源:ISO 22739:2020,3.50,有修改]

3.7

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基本区块组成单元。

[来源:ISO 22739:2020,3.77,有修改]

3.8

共识 consensus

在分布式节点间达成区块数据一致性的认可。

3.9

智能合约 smart contract

存储在分布式账本中的计算机程序,由区块链用户部署并自动执行,其任何执行结果都记录在分布式账本中。

[来源:ISO 22739:2020,3.72,有修改]

3.10

归档 archive

将链上数据转移到独立存储设备的过程。

3.11

账本 ledger

区块链数据的载体。

3.12

双花 double spending

区块链或分布式账本中,通证或加密资产的控制权被错误地转移多次的行为。

[来源:ISO 22739:2020,3.33,有修改]

4 缩略语

下列缩略语适用于本文件。

DDoS:分布式拒绝服务攻击(Distributed Denial of Service)

IP:网际互联协议(Internet Protocol)

P2P:对等计算(Peer-to-peer computing)

SM2:椭圆曲线公钥密码算法(Public Key Cryptographic Algorithm SM2 Based On Elliptic Curves)

SM4:分组密码算法(SM4 Block Cipher Algorithm)

5 概述

5.1 区块链信息服务概述

区块链信息服务是互联网信息服务的一种特殊形式，其信息存储支持多种形式，包括链上存储、链下存储和链上链下相结合。区块链信息服务提供者包括但不限于区块链业务运营者和区块链技术提供者，其中区块链业务运营者是区块链信息服务主体，区块链技术提供者为区块链业务运营者提供技术支持。区块链信息服务中信息是经过加工处理的数据，数据是对信息的记录。

5.2 区块链信息服务安全风险概述

区块链信息服务在传播违法信息、不良信息，实施网络违法犯罪行为，破坏网络生态秩序等方面，存在与互联网信息服务相似的安全风险。区块链技术特征增加了违法信息、不良信息处置等信息内容安全管理难度，进一步加剧了区块链信息服务的安全风险。区块链信息服务安全风险主要包括：

a) 记录在区块链上的信息难以被修改和删除，导致违法信息、不良信息在上链后难以被有效处置；

b) 区块链分布式存储和去中心化的特征，数据存储在各节点服务器，导致违法信息、不良信息难以被清除；

c) 区块链上运行的智能合约存在代码漏洞、恶意调用、执行异常等问题，导致无法提供正常的信息服务；

d) 使用 P2P 网络、共识机制等技术构建区块链网络，面临网络攻击、节点故障、隐私数据泄露等安全问题。

6 安全技术要求

6.1 信息生成

6.1.1 信息生成过程

6.1.1.1 信息源要求

区块链信息服务提供者应：

a) 按照 GB/T 40645—2021 中 5.1.1.1 的规定对存储在链上和链下的信息源进行处理；

b) 使用符合 GB/T 32915—2016 中第 4 章的要求对随机数进行检测，保证区块链技术中使用随机数的随机性和不可预测性；

c) 使用符合国家标准或行业标准的密码技术，保证节点间通信过程中敏感信息字段或整个信息的机密性、完整性和真实性，确保信息在存储、传播过程中不被未授权用户读取或恶意修改；

d) 使用具备抵御破解能力并支持符合国家商用密码管理规定的数字签名算法，如 SM2 等；

e) 使用具备抵御破解能力并支持符合国家商用密码管理规定的数据加密算法，如 SM2、SM4 等。

注：本文件中“黑色宋体”条款表示区块链信息服务满足的增强要求。

6.1.1.2 信息采集

区块链信息服务提供者应：

a) 按照 GB/T 40645—2021 中 5.1.1.2 对用户个人信息、交易信息等信息进行采集，明确信息采

集目的，限定信息采集范围；

b） 通过接口等方式规范采集的交易信息，包括交易发起账号、交易接收账号、交易杂凑值、数字签名、交易类型和交易时间戳等。

6.1.1.3 信息追溯

区块链信息服务提供者应：

a） 符合 GB/T 40645—2021 中 5.1.1.3 的规定对存储在链上和链下的信息进行溯源；

b） 使用数字签名来标识交易发送主体的身份，识别交易发送账号；

c） 对交易信息进行记录，包括交易发送账号、接收账号、交易生成的时间戳等；

d） 提供查询交易信息和交易回执的接口；

e） 检测交易是否被恶意修改。

6.1.2 信息生成主体

6.1.2.1 账号管理

区块链信息服务提供者应：

a） 具备账号服务功能，保证每个账号具有唯一的身份标识；

b） 创建账号时告知用户妥善保管私钥，或提供私钥保护方法的建议；

c） 使用符合国家商用密码管理规定的非对称加密算法公钥进行身份认证；

d） 在发送交易时使用账号唯一标识标记发送账号，且不暴露账号私钥部分；

e） 在发送交易时携带发送账号的数字签名，保证抗抵赖性；

f） 采取加密、去标识化等措施对用户个人信息进行保护；

g） 对用户账号进行认证授权和账号权限的访问控制；

h） 对用户账号实施冻结、解冻、注销等处置措施；

i） 确保账号关联用户的真实身份信息，包括用户身份证号码、手机号码等。

6.1.2.2 节点管理

区块链技术提供者应：

a） 使用可信授时服务对节点授时，保证所有节点时间一致；

b） 通过证书等方式识别节点的身份；

c） 保证当证书失效或许可证过期时，节点无法参与共识活动；

d） 保证当节点发生故障时，节点证书处于失效状态；

e） 支持节点证书和许可证更新后，节点重新参与共识活动；

f） 支持动态增删节点，增删节点时不影响业务正常运行；

g） 支持节点升级或区块链系统升级，升级时不影响业务正常运行；

h） 具备灾备节点，在节点发生故障时通过切换灾备节点保证业务的正常运行。

6.1.2.3 信息生成主体溯源

区块链信息服务提供者应：

a） 按照 GB/T 40645—2021 中 5.1.2.3 对信息生成主体进行追溯，包括账号信息和节点信息等；

b） 采取技术手段获取节点的相关信息，包括创建时间、运行状态、节点 IP 地址、节点所有者身份信息等。

6.2 信息处理

6.2.1 信息识别要求

6.2.1.1 信息内容检测

区块链信息服务提供者应：

a) 按照 GB/T 40645—2021 中 5.2.1.2 对信息进行识别，包括交易信息、链上存储信息、链下存储信息等；

b) 具备技术手段对交易的有效性和正确性进行验证。

6.2.1.2 信息内容处置

区块链信息服务提供者应：

a) 通过屏蔽查询等技术手段，对检测出的违法信息、不良信息进行处置，并对处置过程存证；

b) 通过技术手段实现节点对重复交易的处理；

c) **对存在违法信息、不良信息的交易来源进行追溯**。

6.2.2 分级分类要求

6.2.2.1 内容分级分类

区块链信息服务提供者应：

a) 按照附录 A 对区块链信息服务安全等级进行划分，从安全风险、内容质量等方面对信息内容进行分级，从业务特征等方面对信息内容进行分类；

b) 按照 GB/T 40645—2021 中 5.2.2.2 的要求对用户进行分类；

c) **在接口层对交易类型进行识别，在执行层对交易进行分类处理**。

6.2.2.2 节点访问控制

区块链信息服务提供者应：

a) 对不同类型的节点和节点管理人员设置不同权限，明确不同权限所对应的节点操作内容；

b) 记录每次对节点读写和访问、节点管理人员身份变更和管理权限变更等操作。

6.3 信息发布

6.3.1 信息审核

6.3.1.1 信息内容审核

区块链信息服务提供者应在信息上链前对信息内容进行审核，确保信息内容不包含违法信息、不良信息：

a) 采取关键词检测、图像识别、语音识别等技术手段，对用户账号信息中包含的文本、图片、音视频等内容进行审核；

b) 采取关键词检测、文本相似度比对等技术手段，对上链信息中包含的文本等内容进行审核，包括但不限于交易信息；

c) 采取关键词检测、图像识别、语音识别等技术手段，对链下存储的文本、图片、音视频等内容进行审核。

6.3.1.2 信息审核程序

区块链信息服务提供者应按照 GB/T 40645—2021 中 5.3.1.2 制定并实施信息审核程序，并对上链信息重点审核。

6.3.1.3 共识机制

区块链技术提供者应：

a) 提供基于真实共识算法的共识机制，保证共识机制具有最终一致性和确定性；
b) 定期对共识机制的安全性进行查验，保证共识机制安全有效运行；
c) 对加入共识机制的节点进行记录和身份验证，确保节点可追溯；
d) 通过技术手段保障共识机制抵御 DDoS、双花攻击等网络攻击。

6.3.2 信息发布流程要求

6.3.2.1 信息发布流程

区块链信息服务提供者应按照 GB/T 40645—2021 中 5.3.2.1 的要求对信息进行发布，链上存储信息的发布应经过共识机制，并对相关日志进行存储。

6.3.2.2 发布权限管理

区块链信息服务提供者应按照 GB/T 40645—2021 中 5.3.2.2 的要求进行信息发布权限管理，包括但不限于对信息发布的用户和节点。

6.4 信息传播

6.4.1 功能管理

6.4.1.1 智能合约

区块链信息服务提供者应：

a) 在业务范围内提供符合其业务逻辑的智能合约；
b) 提供智能合约的生命周期安全管理，包括智能合约的创建、编译、部署、调用、冻结、解冻和升级等过程的安全；
c) 对智能合约的安全性进行审核，使用智能合约漏洞检测、静态扫描等技术，保证智能合约的安全运行；
d) 在智能合约进行部署、调用、冻结、解冻和升级等操作时需要用户通过电子签名等方式对相关操作进行权限验证授权；
e) 对智能合约的正确性进行审核，包括对智能合约文本和代码的形式化验证等。

6.4.1.2 激励机制

区块链信息服务提供者：

a) 可在业务范围内提供符合其业务逻辑的激励机制；
b) 不应提供与代币发行融资相关的服务，包括但不限于发行虚拟货币、代币交易等。

6.4.2 信息传播过程监测

6.4.2.1 信息安全监测

区块链信息服务提供者应：

a) 建立主动巡查等监测机制，发现区块链信息服务中的违法信息、不良信息，掌握信息的传播范围和影响力等信息；
b) 对链上节点运行状态和信息发布状态进行监控，发现运行异常节点。

6.4.2.2 信息安全预警

区块链信息服务提供者应对存在安全风险的信息内容进行预警，并对信息安全预警情况进行处置。

6.4.3 安全事件响应处置

6.4.3.1 安全事件应急预案

区块链信息服务提供者应制定安全事件应急预案，定期进行演练。

6.4.3.2 应急处置策略

区块链信息服务提供者应：
a) 采取屏蔽查询等技术手段，对链上存储的违法信息、不良信息进行处置；
b) 采取逻辑删除、关键词屏蔽等技术手段，对链下存储的违法信息、不良信息进行处置；
c) 配备相应的技术手段，对发布违法信息、不良信息的节点和账号进行处置，包括但不限于冻结节点、关闭账号等；
d) 对安全事件响应处置过程进行证据留存，记录响应处置人员、时间、对象、方式等关键信息；
e) 对安全事件进行分级响应处置，明确对违法信息、不良信息和信息发布节点和账号的处置方式。

6.5 信息存储

6.5.1 服务信息存储

6.5.1.1 用户个人信息存储

区块链信息服务提供者应按照 GB/T 40645—2021 中 5.5.1.1 的要求对用户个人信息进行存储，对个人敏感信息的传输和存储应按照 GB/T 35273—2020 中 6.3 的要求进行。

6.5.1.2 业务信息存储

区块链信息服务提供者应：
a) 按照 GB/T 40645—2021 中 5.5.1.2 的要求对业务信息进行存储；
b) 确保各节点存储账本数据的一致性；
c) 对账号数据、区块数据、配置数据、证书等不同类型数据进行分类存储、分开管理；
d) 在账本数据发生恶意修改时，保证节点具有异常恢复的能力；
e) 在机器存储空间不足时，保证节点对数据进行归档；
f) 在未进行数据归档的情况下，保证节点不删除本地存储的账本信息。

6.5.2 日志存储要求

6.5.2.1 日志存储

区块链信息服务提供者应：
a) 按照 GB/T 40645—2021 中 5.5.2.1 的要求对日志信息进行存储；

b） 对用户行为日志进行存储，包括用户登录、信息发布等；
c） 对节点行为日志进行存储，包括区块生成、交易执行结果、共识状态变更、服务启停等；
d） 对节点启动、停止、增加、删除、授权等操作日志进行存储；
e） 对节点证书有效期、节点许可证有效期等信息进行存储；
f） 结合业务对日志信息进行分类存储。

6.5.2.2 日志管理

区块链信息服务提供者应设置日志访问权限，并进行日志审计。

6.6 信息销毁

6.6.1 用户注销管理

6.6.1.1 用户账号注销

区块链信息服务提供者应按照 GB/T 35273—2020 中 8.5 规定的要求，对用户账号进行注销。

6.6.1.2 用户信息销毁

区块链信息服务提供者应：
a） 遵守 GB/T 35273—2020 中 8.3 和 8.5 规定的要求，删除确认注销的用户个人信息；
b） 采取技术手段，使链上待销毁用户信息保持不可被检索、访问的状态；
c） 对用户信息销毁过程存证，包括销毁人员、时间、内容、方式等关键信息。

6.6.2 业务和日志信息销毁

6.6.2.1 信息销毁策略

区块链信息服务提供者应对存储的业务信息和日志信息进行销毁：
a） 对链下存储的信息采取逻辑删除或物理删除等措施；
b） 对链上存储的信息采取技术手段使其保持不可被检索、访问的状态。

6.6.2.2 信息销毁记录

区块链信息服务提供者应对信息销毁活动进行存证，包括销毁人员、时间、内容、方式等关键信息。

7 安全管理要求

7.1 制度管理

7.1.1 安全制度

7.1.1.1 信息源制度

区块链信息服务提供者应：
a） 按照 GB/T 40645—2021 中 6.1.1.1 的要求，制定信息源和信息采集制度，明确信息发布者、发布内容和信息采集要求；
b） 制定用户服务协议、隐私保护协议等用户注册相关制度，明确区块链信息服务提供者和用户的权利义务；

c) 制定节点权限和用户权限管理制度，包括节点和用户权限的分类规范，明确不同权限参与信息服务的要求。

7.1.1.2 信息审核发布制度

区块链信息服务提供者应：

a) 按照 GB/T 40645—2021 中 6.1.1.2 的要求，制定信息审核和信息发布相关制度，包括信息内容规范、交易信息规范、信息审核流程、信息发布流程等；

b) 制定智能合约审核流程，包括对智能合约代码漏洞检测、形式化验证和安全扫描等。

7.1.2 安全机制

7.1.2.1 监测预警机制

区块链信息服务提供者应：

a) 制定监测预警机制，明确对异常行为节点、存在安全风险的信息等预警和处置方式；

b) 明确共识机制需要的最小节点数，在节点数不足以支持当前共识机制时预警并处置。

7.1.2.2 投诉举报机制

区块链信息服务提供者应建立面向公众的投诉举报机制，并对举报进行受理，记录处理情况。

7.2 机构和人员

7.2.1 组织机构

7.2.1.1 安全管理机构

区块链信息服务提供者应设立信息服务安全管理机构，指导区块链信息服务安全管理工作，组织开展区块链信息服务监督工作。

7.2.1.2 机构管理人员

区块链信息服务提供者应在组织机构中配备与业务规模相适应的安全管理人员，包括安全管理机构负责人员、工作人员、安全事件处置人员等。

7.2.2 从业人员管理

7.2.2.1 人员配备

区块链信息服务提供者应在服务中提供与业务规模相适应的从事信息安全相关人员，包括技术人员、信息审核人员等。

7.2.2.2 人员管理

区块链信息服务提供者应制定从业人员管理制度，如关键岗位人员签订保密协议、相关离职要求等。

7.2.2.3 人员培训

区块链信息服务提供者应对参与区块链信息服务活动的相关人员建立培训制度，制定年度培训计划，组织实施培训与考核，教育培训内容应包括信息安全相关法律法规、政策措施、技术标准等。

7.3 业务连续性

7.3.1 数据管理

7.3.1.1 数据保护

区块链信息服务提供者应：

a) 制定用户个人信息安全保护措施，避免用户个人信息泄露、毁损、丢失；

b) 制定业务信息和日志信息的安全保护措施；

c) 在智能合约更新升级、重新部署后，将原智能合约数据迁移至新智能合约，并保证原智能合约数据不丢失；

d) 建立账本信息被恶意修改后的修复机制，并定期对账本信息进行查验。

7.3.1.2 数据存储

区块链信息服务提供者应：

a) 制定用户个人信息、业务信息的存储策略，明确信息存储方式、存储流程、同步方式等关键策略要素；

b) 配备用户个人信息、业务信息和日志信息存储的硬件存储资源和设施设备；

c) 保证日志的留存时间不少于 6 个月；

d) 对存储的账本信息进行备份，对密钥等关键信息定期备份；

e) 制定日志存储策略，明确日志存储方式、存储流程、存储时效等关键策略要素；

f) 对交易信息进行留存，包括区块、账号、共识等相关信息。

7.3.1.3 数据销毁

区块链信息服务提供者应制定对链上、链下存储的数据销毁或处置的管理要求，并进行数据销毁权限管理。

7.3.2 应急处理

7.3.2.1 信息溯源

区块链信息服务提供者应按照 GB/T 40645—2021 中 6.3.2.1 的要求制定信息溯源的相关机制与流程，对交易信息、用户信息、节点信息等进行追溯。

7.3.2.2 安全响应处置

区块链信息服务提供者应：

a) 按照 GB/T 20986—2007 中 5.2 规定的安全事件分级方式，制定安全事件分级响应处置预案；

b) 根据实际情况对安全事件分级预案进行修订更新和版本控制。

7.4 运行与维护

7.4.1 服务运营

7.4.1.1 运营策略

区块链信息服务提供者应建立违法信息、不良信息相关数据库和异常行为用户列表，并定期维护

更新。

7.4.1.2 投诉举报处理

区块链信息服务提供者应按照 GB/T 40645—2021 中 6.4.1.2 对投诉举报进行处理。

7.4.2 安全设施管理

7.4.2.1 设施设备管理

区块链信息服务提供者应提供与业务规模相适应的资源保障，包括场地、设施、设备等，允许区块链信息服务提供者在保障安全的前提下使用第三方提供的设施设备。

7.4.2.2 网络安全管理

区块链信息服务提供者应采取措施保障区块链信息服务网络安全，使网络处于稳定可靠运行的状态。

7.4.3 外包服务管理

7.4.3.1 使用第三方服务

区块链信息服务提供者：

a) 应制定使用第三方服务时遵循的安全管理规范，并通过协议、合同等形式明确合作方式和权责划分；
b) 作为责任方，应确保使用的第三方服务和接口满足信息服务安全要求；
c) 在委托第三方处理用户个人信息时，应符合 GB/T 35273—2020 中 9.1 的要求。

7.4.3.2 提供第三方服务

区块链信息服务提供者应对于提供的服务制定相应的安全规范，保证服务和接口的安全。

8 安全技术要求测试评估

8.1 信息生成

8.1.1 信息生成过程

8.1.1.1 信息源要求

8.1.1.1.1 基本要求测评方法

信息源要求基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：
   1) 检测是否对发布信息来源和信息内容进行标识、检索和筛选；
   2) 采用符合 GB/T 32915—2016 中第 4 章随机性检测方法检测随机数生成算法产生的随机数；
   3) 抓取节点之间的通信包，查看是否采用密码技术，核查通信消息的机密性、完整性和真实性，使用未授权用户读取和修改信息。
b) 预期结果：
   1) 采取标识、检索、筛选等措施，对发布信息来源和信息内容进行处置；

2） 生成的随机数通过随机性检测；

3） 使用密码技术保证交易信息机密性、完整性和真实性，信息存储和传播过程中未授权用户无法读取和修改。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.1.1.2 增强要求测评方法

信息源要求增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 披露数字签名采用的算法，通过代码审计等方式验证该算法是否符合国家商用密码管理规定，披露数字签名技术实现方法，验证该方法自身的安全性；

2） 披露交易信息加密采用的算法，通过代码审计等方式验证该算法是否符合国家商用密码管理规定。

b） 预期结果：

1） 采用的数字签名算法满足国家商用密码要求，数字签名技术实现方法未存在安全性问题；

2） 采用的交易信息加密算法满足国家商用密码要求，交易信息加密技术实现未存在安全性问题。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.1.2 信息采集

信息采集基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检测采集的用户个人信息中是否包含 GB/T 35273—2020 中 3.2 定义的个人敏感信息字段，检查用户个人信息和交易信息采集方法，检测是否在信息采集前对采集范围进行限定；

2） 检测采集的交易信息字段，查看是否包含交易发起账号、交易接收账号、交易杂凑值、数字签名、交易类型和交易时间戳等信息。

b） 预期结果：

1） 采集的用户个人信息中不包含个人敏感信息，在信息采集前对采集范围进行限定；

2） 采集的交易信息包括交易发起节点、交易接收节点、交易杂凑值、数字签名、交易类型和交易时间戳等信息。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.1.3 信息追溯

信息追溯基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 查看已发布链上和链下信息日志，查看是否包含发布时间、发布用户等字段；

2） 检查交易信息中是否包含数字签名字段，是否通过数字签名关联到交易发送账号；

3） 查看交易日志，查看是否包含交易发送账号、接收账号、交易生成时间戳等字段；

4） 提交一条被修改交易，检测是否有提示和日志记录。

b） 预期结果：

1） 具备信息发布日志，日志中包含发布时间、发布用户等字段；

2） 交易信息中包含数字签名字段，数字签名关联到交易发送账号；

3） 具备交易日志，交易日志中包含交易发送账号、接收账号、交易生成时间戳等字段；

4） 检测出被修改的交易，并记录相关日志信息。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2 信息生成主体

8.1.2.1 账号管理

8.1.2.1.1 基本要求测评方法

账号管理基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 创建多个账号，检测每个账号的身份标识是否具有唯一性；

2） 创建账号过程中查看是否具有告知用户妥善保管私钥的相关提示；

3） 检测非对称加密算法的公钥密码算法是否符合国家商用密码管理规定；

4） 查看交易中是否包含发送账号的身份标识，检查是否包含私钥字段；

5） 检测交易中是否包含发送账号的数字签名字段；

6） 检查是否采取加密、去标识化等技术措施对用户个人信息进行保护。

b） 预期结果：

1） 账号创建成功，且账号的身份标识具有唯一性；

2） 具有告知用户妥善保管私钥的相关提示；

3） 非对称加密算法公钥满足国家商用密码管理规定；

4） 交易信息包含发送账号的身份标识，且不包含私钥字段；

5） 交易信息包含数字签名字段；

6） 使用加密、去标识化等技术措施。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2.1.2 增强要求测评方法

账号管理增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 查看是否对账号进行认证授权和权限访问控制，被授权用户可以进行特殊功能或接口访问，未授权用户无法进行特殊访问；

2） 冻结、注销账号，查看账号状态，检测能否对冻结账号解冻；

3） 注册用户后，检测后台是否可以查询到用户的真实身份信息。

b） 预期结果：

1） 对账号认证授权，被授权用户具有相关权限；

2） 账号状态变为冻结或注销，能解冻已冻结账号；

3） 查询到用户的真实身份信息。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2.2 节点管理

8.1.2.2.1 基本要求测评方法

节点管理基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检测是否采用了可信授时服务，时间戳服务规范应遵循 GM/T 0033—2014；

2） 修改区块链节点的证书，检测节点是否失效；

3） 修改共识节点的证书或许可证，发送交易，检测该节点是否参与共识；

4） 宕机其中一个共识节点，检测该节点证书是否有效；

5） 对吊销证书或证书失效的共识节点重新颁发证书，检测该节点是否参与共识；

6） 新增或删除节点时持续发送交易，查看交易是否发送成功；

7） 节点升级时持续发送交易，查看交易是否发送成功，在系统升级时持续发送交易，查看交易是否发送成功。

b） 预期结果：

1） 时间戳服务规范遵循 GM/T 0033—2014；

2） 节点失效；

3） 该节点不再参与共识；

4） 节点证书失效；

5） 该节点重新参与共识；

6） 交易发送成功；

7） 交易发送成功。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2.2.2 增强要求测评方法

节点管理增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

在切换灾备节点过程中持续发送交易，查看交易是否发送成功。

b） 预期结果：

交易发送成功。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.1.2.3 信息生成主体溯源

信息生成主体溯源基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检测是否具备用户真实身份信息核验的技术或系统，查看用户行为日志和节点日志，修改用户身份信息，查看是否有身份变更记录；

2） 检测是否能获取节点创建时间、运行状态、节点 IP 地址、节点所有者的身份信息。

b） 预期结果：

1） 具备用户真实身份核验技术或系统，记录用户使用区块链信息服务日志和节点日志，能查询到用户身份信息变更记录；

2） 能获取节点创建时间、运行状态、节点 IP 地址、节点所有者的身份信息。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2 信息处理

8.2.1 上链信息识别

8.2.1.1 信息内容检测

信息内容检测基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检查是否建立违法信息、不良信息样本特征库，查看信息内容识别过滤系统或技术文件，检查是否对链上、链下存储的文本、图片、音视频等形式违法信息、不良信息进行识别和过滤；

2） 提交无效或错误的交易，如双花攻击等，检测是否能通过验证。

b） 预期结果：

1） 具备违法信息、不良信息样本特征库，具备对不同形式链上、链下存储的违法信息、不良信息识别过滤能力；

2） 无效或错误的交易无法通过验证。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.1.2 信息内容处置

8.2.1.2.1 基本要求测评方法

信息内容处置基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 指定一条交易信息，检测是否能对其进行处置，并对处置过程存证；

2） 发送重复交易，检测重复交易是否均上链。

b） 预期结果：

1） 采取屏蔽查询等技术手段处置特定信息，并对处置过程存证；

2） 重复交易只有一条上链。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.1.2.2 增强要求测评方法

信息内容处置增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检测是否能对特定交易信息来源进行追溯，包括信息内容、发送用户和日志信息等。

b） 预期结果：

对发送交易信息来源进行追溯，包括信息内容、发送用户、发送日志、行为日志等。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.2 分级分类要求

8.2.2.1 内容分级分类

8.2.2.1.1 基本要求测评方法

内容分级分类基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 查看信息内容分级分类规范文件或系统，检查是否按照信息的安全风险、信息内容质量等方面对信息内容进行分级，按照区块链信息服务的业务特征等方面对信息内容进行分类，检查不同级别、类别信息管理方式；

2） 查看用户分类规范文件或系统，检查不同类别的用户是否具备不同操作权限。

b） 预期结果：

1） 按要求对信息内容进行分级分类，并采取不同管理方式；

2） 对用户进行分类，不同类别用户具备不同操作权限。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.2.1.2 增强要求测评方法

内容分级分类增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检查是否在接口层对交易信息进行识别，检查是否在执行层对交易信息进行分类。

a） 预期结果：

在接口层对交易信息进行识别，在执行层对交易信息进行分类。

b） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.2.2.2 节点访问控制

节点访问控制基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检测是否对不同类型的节点和节点管理人员设置不同权限，检测只具备节点查看权限的管理人员是否能对节点进行其他操作，检测不具备节点管理权限的用户能否对节点进行操作；

2） 进行节点方法操作、节点和节点管理人员权限修改操作，查看操作记录。

b） 预期结果：

1） 对节点和节点管理人员具备不同权限，只具备节点查看权限的节点管理人员只能查看节点信息，不具备节点管理权限的用户无法对节点进行操作；

2） 查看到操作记录。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.3 信息发布

8.3.1 信息审核

8.3.1.1 信息内容审核

信息内容审核基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 查看用户账号信息审核技术系统，检查是否使用关键词检测、图像识别、语音识别等技术进行信息内容审核；

2) 查看上链信息审核技术系统，检查是否使用关键词检测、文本相似度比对等技术对上链的文本信息进行审核；

3) 查看链下存储信息审核技术系统，检查是否使用关键词检测、图像识别、语音识别等技术进行信息内容审核。

b) 预期结果：

1) 具备用户账号信息审核技术和系统；

2) 具备上链文本信息审核技术和系统；

3) 具备链下存储信息审核技术和系统。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.1.2 信息审核程序

信息审核程序基本要求的测评方法、预期结果和结果判定如下。

a) 测评方法：

查看信息审核记录，检测是否对信息内容实施先审后发，查看信息发布日志，检测是否对发布过违法信息、不良信息的账号、节点及发布的信息进行记录，检查不同类别信息是否分级审核，查看是否具有重大事件相关操作记录，如节点增删操作，合约冻结、解冻操作等。

b) 预期结果：

对信息内容先审后发，记录信息发布账号、节点及发布信息，对不同类别信息分级审核，具备重大事件的安全审核能力。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.1.3 共识机制

共识机制基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 披露区块链所采用的共识机制，通过代码审计的方式检测共识机制是否与披露的共识机制相符合，模拟恶意节点数多于或少于容错节点数的情况并发送交易，查看节点的一致性；

2) 查看共识机制安全性查验日志；

3) 检测加入共识的节点是否经过身份验证，使用具备合法身份证书的节点加入网络，查看是

否能正常共识，使用具备非法证书的节点加入网络，查看是否能正常共识；

4） 模拟 DDoS 攻击，查看是否具有限流、IP 过滤等措施抵御攻击，模拟双花攻击，同时发送两笔重复交易，查看交易是否成功，校验交易结果。

b） 预期结果：

1） 实际采用的共识机制满足披露的共识算法规则，当恶意节点数少于容错节点数时可以达成一致，当恶意节点数多于容错节点数时无法达成一致；

2） 具备定期查验共识机制安全性日志；

3） 加入共识的节点应经过身份验证，具备合法证书的节点可以正常共识，不具备合法证书的节点无法进行共识；

4） 具备抵御 DDoS 攻击的措施，共识机制正常运行，具备抵御双花攻击的措施，两笔重复交易只有一笔成功。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.2 信息发布流程要求

8.3.2.1 信息发布流程

信息发布流程基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

查看信息发布日志，检查是否对日志进行存储和保护，对重大事件等关键信息是否制定信息发布流程并实施，检查链上信息是否经过共识机制处理并查看相关日志记录。

b） 预期结果：

具备信息发布日志并对日志进行存储保护，具备关键信息的发布流程并及时安全发布，链上信息发布经过共识机制处理，具备相关日志。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.3.2.2 发布权限管理

发布权限管理基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检测是否对信息发布用户和节点进行权限管理，查看权限变更日志。

b） 预期结果：

具备信息发布用户和节点的权限管理与权限变更日志。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4 信息传播

8.4.1 功能管理

8.4.1.1 智能合约

8.4.1.1.1 基本要求测评方法

智能合约基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 检测智能合约的业务逻辑是否满足区块链信息服务提供者披露的业务范围；

2) 检测是否提供智能合约创建、编译、部署、调用、冻结、解冻和升级的全生命周期安全管理技术或系统；

3) 检测是否具备合约安全性审核技术或系统，如漏洞检测、静态扫描等技术；

4) 使用没有智能合约操作权限的用户进行智能合约部署、调用、冻结、解冻和升级等操作并查看结果，对用户授予智能合约操作权限后，进行部署、调用、冻结、解冻和升级等操作并查看结果。

b) 预期结果：

1) 智能合约的业务逻辑满足区块链信息服务提供者披露的业务范围；

2) 具备对智能合约的全生命周期安全管理的技术能力；

3) 具备对智能合约安全审核技术或系统；

4) 未授权时，用户无法进行部署、调用、冻结、解冻、升级和销毁等操作，授权之后，用户可以进行相关操作。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.1.1.2 增强要求测评方法

安全智能合约增强要求测评方法、预期结果和结果判定如下。

a) 测评方法：

检测是否采取形式化验证等技术手段对智能合约的文本和代码正确性进行审核。

b) 预期结果：

采取形式化验证等技术手段，对智能合约的文本和代码正确性进行审核。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.1.2 激励机制

激励机制基本要求测评方法如下：

a) 测评方法：

检查区块链信息服务中是否提供与代币发行融资相关的服务。

b) 预期结果：

不提供与代币发行融资相关的服务。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.2 信息传播过程监测

8.4.2.1 信息安全监测

信息安全监测基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 检查是否能具备对区块链信息服务的监测机制，查看信息监测日志；

2) 检测是否实时监控节点状态，检测是否能发现运行异常节点。

b） 预期结果：

1） 监测发现存储在链上和链下的违法信息、不良信息，具备信息监测日志；

2） 对节点和信息发布状态进行监控，能发现异常节点。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.2.2 信息安全预警

8.4.2.2.1 基本要求测评方法

信息安全预警基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

查看信息安全预警机制，检查是否按照该机制进行信息安全预警。

b） 预期结果：

对有安全风险的信息做出风险预警。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.2.2.2 增强要求测评方法

信息安全预警增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

跟进信息安全预警情况，检查是否进行处理。

b） 预期结果：

对信息安全预警情况进行处理。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.3 安全事件响应处置

8.4.3.1 安全事件应急预案

安全事件应急预案基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检查是否制定安全事件应急预案，检查是否定期开展演练。

b） 预期结果：

具备安全事件应急预案，定期开展安全事件应急演练并记录演练情况。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.3.2 应急处置策略

8.4.3.2.1 基本要求测评方法

应急处置策略基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

1） 检查是否采取屏蔽查询等技术手段，对链上存储的违法信息、不良信息进行处置；

2） 检查是否采取逻辑删除、关键词屏蔽等技术手段，对链下存储的违法信息、不良信息进行处置；

3） 检测是否对发送违法信息、不良信息的节点进行冻结，是否对发送违法信息、不良信息的账号进行关闭；

4） 查看已发生安全事件记录，跟进具体的安全事件响应处理过程，检查是否对响应处置人员、时间、对象、方式等关键信息进行存证。

b） 预期结果：

1） 具备处置链上违法信息、不良信息的技术手段；

2） 具备处置链下存储的违法信息、不良信息的技术手段；

3） 对发送违法信息、不良信息的节点进行冻结，对发送违法信息、不良信息的账号进行关闭；

4） 对安全事件响应处置过程的记录，包含响应处置人员、时间、对象、方式等关键信息。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.4.3.2.2 增强要求测评方法

应急处置策略增强要求测评方法如、预期结果和结果判定下：

a） 测评方法：

检查是否对安全事件进行分级响应处置，核实不同级别安全事件中对违法信息、不良信息和发布信息的节点、账号的处置方式。

b） 预期结果：

具备安全事件分级响应处置机制，对不同级别安全事件中发现的违法信息、不良信息和发布信息的节点、账号具备明确的处置方式。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5 信息存储

8.5.1 服务信息存储

8.5.1.1 用户个人信息存储

用户个人信息存储基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检查用户个人信息存储前是否获得用户授权，检查用户个人信息保护规定是否满足GB/T 35273—2020 中 6.1、6.2、6.3、6.4 的要求，查看用户的个人敏感信息、隐私信息和重要数据存储方式，检查敏感信息是否被加密存储，检查区块链信息服务是否使用第三方服务存储用户个人信息，若使用，检查用户是否被实时告知，检查是否对用户个人信息进行分级分类存储。

b） 预期结果：

存储用户个人信息前已获得用户授权，满足 GB/T 35273—2020 相关要求，对用户敏感信息加密存储，在第三方服务存储用户信息时明确告知，对用户个人信息分类存储。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.1.2 业务信息存储

8.5.1.2.1 基本要求测评方法

业务信息存储基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 检查是否存储业务信息，是否具备保障业务信息完整性和保密性相关技术措施；
2) 核对各节点的账本数据，检查是否一致；
3) 查看账号数据、区块数据、配置数据、证书等数据存储方式，确认不同类型的数据分类分级进行存储和管理。

b) 预期结果：

1) 存储业务信息，并具备技术措施保障业务信息的完整性和保密性；
2) 各节点保存的账本数据一致；
3) 不同类型的数据被分类别进行存储和管理。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.1.2.2 增强要求测评方法

业务信息存储增强要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 对账本数据进行修改，检查节点是否有异常恢复的能力；
2) 检查节点是否对数据进行归档，查看数据归档后节点存储空间是否变大，节点是否能继续正常发送交易；
3) 查看节点具体信息，对未归档的节点，查询历史交易和区块数据，检测是否包含账本所有信息。

b) 预期结果：

1) 节点具有异常恢复的能力；
2) 节点可以对数据进行归档，避免机器存储空间不足等情况，归档后节点能继续正常发送交易；
3) 未归档节点包含账本所有信息。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.2 日志存储要求

8.5.2.1 日志存储

8.5.2.1.1 基本要求测评方法

日志存储基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 检查是否存储日志信息，是否具备保障日志的完整性、保密性和可用性相关技术措施；
2) 检查是否存储用户登录、信息发布等用户行为日志；
3) 检查是否存储区块生成、交易执行结果、共识状态变更、服务启停等节点行为日志；

4） 对节点启动、停止、增加、删除等操作，检查日志信息是否存储；

5） 检查是否存储节点证书有效期、节点许可证等信息。

b） 预期结果：

1） 存储日志信息，并具备技术措施保障日志的完整性、保密性和可用性；

2） 存储用户行为日志；

3） 存储节点行为日志；

4） 存储节点启动、停止、增加、删除等节点操作日志；

5） 存储节点证书有效期和节点许可证。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.2.1.2 增强要求测评方法

日志存储增强要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检查是否结合业务对日志进行分类存储，在业务系统中查看不同日志分类。

b） 预期结果：

对日志信息进行分类存储。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.5.2.2 日志管理

日志管理基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

查看日志管理相关系统，检测是否设置日志访问权限，查看是否具备日志审计记录。

b） 预期结果：

设置日志访问权限，并进行日志审计。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.6 信息销毁

8.6.1 用户注销管理

8.6.1.1 用户信息注销

用户信息注销基本要求测评方法、预期结果和结果判定如下。

a） 测评方法：

检测是否能对用户账号进行注销，符合 GB/T 35273—2020 中 8.5 的要求。

b） 预期结果：

按照 GB/T 35273—2020 中 8.5 要求对用户账号进行注销。

c） 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.6.1.2 用户信息销毁

用户信息销毁基本要求测评方法如下。

a) 测评方法：

1) 查看用户管理相关系统，检测是否能对注销用户的信息进行删除；

2) 检查是否具备使得链上用户信息不可被检索或访问的技术手段；

3) 查看用户信息销毁日志，检测日志中是否包含用户信息销毁相关时间、人员、内容、方式等。

b) 预期结果：

1) 对注销用户信息进行删除；

2) 具备相关技术手段，使得链上用户信息不可被检索或访问；

3) 具备用户信息销毁日志，包含时间、人员、内容、方式等关键信息。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.6.2 业务与日志信息销毁

8.6.2.1 信息销毁策略

信息销毁策略基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

1) 检测能否对链下存储的业务信息和日志信息进行销毁；

2) 检测能否使得链上存储的业务信息和日志信息不可被检索或访问。

b) 预期结果：

1) 能对链下存储的业务信息和日志信息进行销毁；

2) 具备相关技术手段，使得链上存储的业务信息和日志信息不可被检索或访问。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

8.6.2.2 信息销毁记录

信息销毁记录基本要求测评方法、预期结果和结果判定如下。

a) 测评方法：

查看信息销毁日志，检查是否包括时间、人员、内容、方式等关键信息。

b) 预期结果：

具备信息销毁日志，包含时间、人员、内容、方式等关键信息。

c) 结果判定：

实际测评结果与预期结果一致则判定符合，其他情况判定不符合。

9 安全管理要求检查评估

9.1 制度管理

9.1.1 安全制度

9.1.1.1 信息源制度

信息源制度基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

1) 检查是否制定信息源规范和信息采集规范文件，检查规范文件中是否包含对信息源采集范围、采集方法、采集流程、信息类别、信息形式、采集渠道以及信息提供者等关键信息要素条款；

2) 检查是否制定用户注册制度文件，检查制度文件中是否在采集用户信息时有明确授权的条款；

3) 检查是否制定用户权限和节点权限管理相关规范文件，检查文件中是否包含节点权限和用户权限分类条款，检查是否明确不同权限参与的信息服务范围。

b) 预期结果：

1) 具备信息源和信息采集规范文件，规范文件中包含信息采集范围、采集方法、采集流程、信息类别、信息形式、采集渠道以及信息提供者等关键信息要素条款；

2) 具备用户注册制度文件，在采集用户信息时有明确授权；

3) 具备用户和节点权限管理规范文件，包含节点和用户权限要求，明确不同权限参与信息服务范围。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.1.1.2 信息审核发布制度

信息审核发布制度基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

1) 检查是否制定信息审核和信息发布相关制度文件，包括信息内容规范、交易信息规范、信息审核流程、信息发布流程等，检查规范文件中对是否包含文本、图片、音视频等进行审核，审核轮次、审核策略、审核技术等审核程序关键要素是否明确，结合区块链信息服务内容，查看是否具备人工审核制度、非人工审核制度，是否具备普通信息两级审核、对重大事件等关键信息的多级审核的条款，查看审核制度修订记录，包括文件修改记录等，检查是否包含修订更新和版本控制内容，查看不同级别审核程序是否具备不同的管理措施和技术措施，包括制定不同审核流程、配备不同审核人员；

2) 检查是否制定智能合约审核流程文件。

b) 预期结果：

1) 制定信息审核和信息发布相关制度文件，包含测评中涉及条款与内容；

2) 具备智能合约审核流程文件。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.1.2 安全机制

9.1.2.1 监测预警机制

监测预警机制基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

1) 检查是否制定监测预警机制文件，检查是否包含区块链信息服务监测方法条款，检查是否包含对异常行为的节点、存在安全风险的信息等内容的预警和处置方式；

2) 检查是否制定共识机制运行状态监测预警文件或条款，查看是否明确共识需要的最小节点数，检测在节点数不足以支持共识机制时能否预警并进行处置。

b） 预期结果：

1） 具备监测预警文件，对存在的安全风险能有效预警；

2） 具备共识机制预警文件或条款，能在节点数不足以支持共识机制时进行预警并处置。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.1.2.2 投诉举报机制

投诉举报机制基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否制定投诉举报机制文件或条款，检查用户是否可见，查看投诉举报受理及处理记录。

b） 预期结果：

具备符合要求的投诉举报机制。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.2 机构和人员

9.2.1 组织机构

9.2.1.1 安全管理机构

安全管理机构基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否设立了区块链信息服务安全管理机构，查看该机构成立证明材料，查看该机构负责的区块链信息服务安全管理工作记录，包括发布规章制度文件、安全事件处置记录等。

b） 预期结果：

设立了专职区块链信息服务安全管理机构，并组织开展区块链信息服务安全管理工作。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.2.1.2 机构管理人员

机构管理人员基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

查看安全管理机构人员名单，包括安全管理机构负责人和安全管理机构工作人员信息，查看人员值班记录等，查看从事区块链信息服务安全事件处置的人员名单和相关工作记录，包括安全事件处置记录、人员值班记录等。

b） 预期结果：

配备与业务规模相适应的安全管理机构人员。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.2.2 从业人员管理

9.2.2.1 人员配备

人员配备基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

查看从事区块链信息服务安全相关人员名单和工作记录，包括信息内容审核人员、应急响应处置人员、投诉举报受理人员等。

b) 预期结果：

配备与业务规模相适应的从事信息安全相关人员。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.2.2.2 人员管理

人员管理基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

查看业务人员相关管理制度文件，检查是否包含和关键岗位人员签订保密协议、离职要求等相关条款。

b) 预期结果：

具备相关业务人员管理制度文件与条款。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.2.2.3 人员培训

人员培训基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

查看人员培训相关制度，检查是否制定年度培训、定期组织培训与考核等相关条款，查看审核人员培训记录，检查审核人员是否定期参加培训，查看培训相关内容记录，检查是否包含信息安全相关法律法规、政策措施和技术标准。

b) 预期结果：

具备人员培训相关制度，制度中包含年度培训、定期组织培训与考核等相关条款，审核人员定期参加培训，培训内容包含信息安全相关法律法规、政策措施和技术标准。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3 业务连续性

9.3.1 数据管理

9.3.1.1 数据保护

9.3.1.1.1 基本要求检查评估方法

数据保护基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

1) 检查是否制定与用户个人信息保护相关文件或条款，是否包含技术保护措施条款，是否包含不得泄露、毁损、丢失用户个人信息条款；

2) 检查是否制定业务信息和日志信息安全保护相关文件或条款。

b) 预期结果：

1) 具备用户个人信息保护相关文件或条款，包含技术保护措施条款，包含不得泄露、毁损、丢

失用户个人信息条款；

2） 具备业务信息和用户个人信息保护相关文件或条款；

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.1.1.2 增强要求检查评估方法

数据保护增强要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否具备账本信息保护相关文件或条款，是否包含账本修复机制条款，是否包含账本信息定期查验条款。

b） 预期结果：

具备账本信息保护相关文件或条款，包含账本修复机制条款，包含定期查验账本信息条款。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.1.2 数据存储

9.3.1.2.1 基本要求检查评估方法

数据存储基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

1） 检查是否制定用户个人信息存储、业务信息存储策略文件或条款，检查是否包含存储方式、存储流程、同步方式等的条款，查看用户信息和业务信息存储后台进行验证；

2） 查看用户个人信息、业务信息和日志信息存储的系统，查看数据存储使用的硬件存储资源和设施设备情况证明材料，包括存储资源采购记录、数据存储记录等；

3） 查看系统日志创建时间，检查是否留存 6 个月前的日志，查看日志信息存储相关文件或条款中是否明确日志留存时间不少于 6 个月。

b） 预期结果：

1） 具备用户个人信息和账本信息存储规范文件或条款，条款中包含存储方式、存储流程、同步方式等，与后台验证结果相符；

2） 用户个人信息、业务信息和日志信息存储量与硬件存储资源和设施设备相适应；

3） 具备符合存储时限的日志，具备明确日志留存时间不少于 6 个月的文件或条款。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.1.2.2 增强要求检查评估方法

数据存储增强要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

1） 查看账本信息备份记录，检查密钥信息备份记录；

2） 检查是否制定日志信息存储规范文件，检查是否包含存储方式、存储流程、存储时效要求条款；

3） 查看交易信息留存日志，检查日志中是否包含区块、账号、共识等相关信息。

b） 预期结果：

1） 账本信息有备份，对密钥等关键信息定期备份；

2） 制定了日志信息存储规范，规定了存储方式、存储流程、存储时效要求，与后台验证结果一致；

3） 检查以日志形式留存交易信息，日志中包括区块、账号、共识等相关信息。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.1.3 数据销毁

数据销毁基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

查看链上数据处置相关规范文件或条款，查看链下存储数据销毁相关规范文件或条款，查看具备数据销毁权限人员和数据销毁记录。

b） 预期结果：

具备对链上待销毁数据处置和链下存储数据销毁的相关规范文件或条款，具备数据销毁权限管理能力。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.2 应急处理

9.3.2.1 信息溯源

信息溯源基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否制定信息溯源规范文件或条款，检查是否包含交易信息、用户信息、节点信息溯源流程。

b） 预期结果：

具备信息溯源规范文件或条款，包含交易信息、用户信息、节点信息溯源流程。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.2.2 安全响应处置

9.3.2.2.1 基本要求检查评估方法

安全响应处置基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否制定安全事件分级响应处置预案文件，查看近一年内安全事件应急演练记录。

b） 预期结果：

制定了满足业务需求的安全事件分级响应处置预案，并依据处置预案定期开展安全事件应急演练。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.3.2.2.2 增强要求检查评估方法

安全事件响应处置增强要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否制定多级应急响应处置预案文件，查看是否包含不同级别应急响应处置预案内容，检查文件修订更新时间和最新版本发布时间。

b） 预期结果：

具备多级应急响应处置预案，对各级预案进行修订更新，具备文件版本控制记录。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4 运行与维护

9.4.1 服务运营

9.4.1.1 运营策略

运营策略的基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

查看违法信息、不良信息数据库，结合区块链信息服务内容，检查是否包含文本、图片、音视频等数据库，查看数据库维护机制文件，检查数据库更新时间和历史更新记录。

b） 预期结果：

具备违法信息、不良信息数据库，数据库定期更新。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.1.2 投诉举报处理

运营策略的基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

检查是否制定投诉举报制度文件或条款，检查是否包含举报方式、受理时长等条款，查看投诉举报受理记录与处置记录。

b） 预期结果：

具备投诉举报制度文件或条款，包含举报方式、受理时长等条款，对投诉举报及时受理。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.2 安全设施管理

9.4.2.1 设施设备管理

设施设备管理的基本要求检查评估方法、预期结果和结果判定如下。

a） 检查评估方法：

查看区块链信息服务人员办公、节点布置、业务系统、数据存储等相关设施设备和场地介绍文件或条款，检查是否使用第三方提供设施设备，包括云服务等，若使用，查看与第三方签订的服务协议。

b） 预期结果：

具备相关设施设备资源，确保使用第三方设施设备时的安全要求。

c） 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.2.2 网络安全管理

网络安全管理基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

检查区块链信息服务是否完成网络安全等级保护测试评估，查看评估报告。

b) 预期结果：

开展网络安全等级保护测试评估。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.3 外包服务管理

9.4.3.1 使用第三方服务

使用第三方服务基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

1) 检查是否使用第三方服务，包括区块链技术服务、安全审核服务等，若使用，查看与第三方签订的协议或合同等证明材料，检查是否包含合作方式与权责划分条款；

2) 检查是否制定使用第三方服务安全保护规范文件，检查是否包含对第三方服务和接口的安全性保护措施，查看安全保护技术文件；

3) 查看委托第三方处理个人信息签订的相关文件或条款，检查是否超出已征得个人授权同意范围，是否明确责权划分，是否对处理情况进行记录。

b) 预期结果：

1) 具备使用第三方服务相关规范文件，与第三方签署的合同或协议中明确了合作方式与权责划分；

2) 具备对使用的第三方服务安全保护措施；

3) 未超出个人授权同意范围，已明确责权划分，对处理情况进行记录。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

9.4.3.2 提供第三方服务

提供第三方服务基本要求检查评估方法、预期结果和结果判定如下。

a) 检查评估方法：

检查是否提供第三方服务，包括区块链技术服务、安全审核服务等，检查是否制定提供第三方服务安全规范文件，检查是否包含对提供的服务、接口的安全要求条款。

b) 预期结果：

具备提供第三方服务相关安全规范文件，包含对服务、接口等的安全要求。

c) 结果判定：

实际检查评估结果与预期结果一致则判定符合，其他情况判定不符合。

附 录 A
（规范性）
区块链信息服务安全等级划分

区块链信息服务安全规范定义了两个安全级别，分别是基本级和增强级。通过区块链企业规模、业务范围、服务类型和数据类别等要素判断该区块链信息服务的影响力和发生安全事件后的危害程度，从而确定其应满足的安全级别，为区块链信息服务提供者开展安全建设和安全评估提供安全要求分级依据。区块链信息服务提供者在满足以下条件中的任何一种时，均需按照增强级开展安全建设和安全评估，见表 A.1：

a） 区块链信息服务提供者规模达到中、大型企业规模要求；

b） 区块链信息服务业务范围涉及音视频服务；

c） 区块链服务类型为内容分发、数字版权、数据保护等非社交媒体或非个人敏感信息类型；

d） 区块链信息服务数据涉及核心数据和重要数据；

e） 区块链信息服务用户规模达到 100 万以上。

表 A.1 区块链信息服务安全等级分级规则

分级要素		安全级	
		基本级	增强级
企业规模	大型企业		√
	中型企业		√
	小、微型企业	√	
业务范围	音频、视频		√
	文本	√	
	图片	√	
服务类型	内容分发		√
	数字版权		√
	数据保护		√
	其他	√	
数据类别	核心数据		√
	重要数据		√
	一般数据	√	
用户规模	100 万以上		√
	100 万及以下	√	
注：√表示区块链信息服务提供者应满足安全级别。			

参 考 文 献

[1] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
[2] GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范
[3] GB/T 37973—2017 信息安全技术 大数据安全管理指南
[4] JR/T 0184—2020 金融分布式账本技术安全规范
[5] 关于印发中小企业划型标准规定的通知(工信部联企业〔2011〕300 号)
[6] ISO 22739:2020 Blockchain and distributed ledger technologies—Vocabulary

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
区块链信息服务安全规范
GB/T 42571—2023
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.net.cn
服务热线:400-168-0010
2023 年 5 月第一版
*
书号:155066·1-72842

GB/T 42571-2023

码上扫一扫 正版服务到