ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 区块链信息服务安全规范

Information security technology—Security specification for information service of blockchain

（征求意见稿）

本稿完成日期：2021-1-15

XXXX-XX-XX 发布　　XXXX-XX-XX 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

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这些专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）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、中国电子技术标准化研究院、杭州趣链科技有限公司、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、浦东新区人民政府电子政务办、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、四川省信息安全测评中心、国家安全防范报警系统产品质量监督检测中心（北京）、中国汽车工程研究院股份有限公司、北京大学、清华大学、鼎铉商用密码测评技术（深圳）有限公司、联想（北京）有限公司、深圳市腾讯计算机系统有限公司、新华三技术有限公司、北京众享比特科技有限公司、北京百度网讯科技有限公司、国网区块链科技（北京）有限公司、泰康保险集团股份有限公司、浪潮电子信息产业有限公司、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、成都链安科技有限公司、京东数字科技控股股份有限公司、矩阵元技术（深圳）有限公司、蚂蚁科技集团股份有限公司、启明星辰信息技术集团股份有限公司、北京融数联智科技有限公司、北京小米移动软件有限公司、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、中国电子科技网络信息安全有限公司、北京人民在线网络有限公司、北京微智信业科技有限公司、中国电力科学研究院有限公司、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等。

本文件主要起草人：张潇丹、郭涛、蔡亮、刘贤刚、胡静远、周熙、韩冀中、姚相振、李伟、王惠莅、黄永洪、吕红蕾、史洪彬、周薇、刘总真、王宇航、陈晓丰、邵宇、郑佩玉、任泽君、陈妍、王永涛等。

引　言

由于区块链技术匿名性、分布式存储等特征，区块链信息服务在用户隐私保护、信息安全方面有优势，但其去中心化机制、链上信息难以修改等特征也为信息安全管理带来了挑战。由于区块链产业发展时间较短，信息安全管理措施和技术保障能力缺失缺位，进一步加剧了区块链上信息内容传播过程中的安全风险隐患。对此，国家相关部门高度重视，出台了《区块链信息服务管理规定》等一系列政策法规，规定了区块链信息服务提供者的信息安全管理责任。本文件针对区块链技术，面向提供具有社会化特征的区块链信息服务（包括联盟链和私有链），对区块链信息服务提出其应满足的安全要求和测试评估方法，适用于区块链信息服务提供者建立健全信息安全机制，并配备相应的技术保障措施，开展区块链信息服务安全建设，也适用于对区块链信息服务的安全评估。

本文件在撰写过程中参照在编标准《信息安全技术 互联网信息服务安全通用要求》中使用的“类、族、组件”的结构定义，针对区块链信息服务中涉及到信息生命周期的生成、处理、发布、传播、存储和销毁六个阶段，提出了安全要求和相应的测试评估方法。

信息安全技术 区块链信息服务安全规范

1 范围

本文件规定了联盟链和私有链的区块链信息服务提供者应满足的安全要求，包括安全技术要求和安全保障要求，以及相应的测试评估方法。

本文件适用于指导区块链信息服务提供者开展区块链信息服务安全建设，包括安全管理制度和技术保障措施等，也适用于指导对区块链信息服务进行安全评估。

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。

GB/T 25069 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T AAAAA—AAAA 信息安全技术 互联网信息服务安全通用要求

3 术语和定义

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

3.1

区块链技术 blockchain technique

一项新型的分布式集成创新技术，核心内容包括共识机制、分布式存储、点对点传输、智能合约、密码技术等技术。

注：“区块链”是对区块链技术的简称。

3.2

区块链信息服务 blockchain information service

指基于区块链技术或系统，通过互联网站、应用程序等形式，向社会公众提供的信息服务。

3.3

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

指向社会公众提供区块链信息服务的主体或者节点，以及为区块链信息服务的主体提供技术支持的机构或者组织。

3.4

联盟链 consortium blockchain

指通过权限控制对特定的组织团体开放的区块链，由联盟内部指定多个预选节点为共识节点，每个块的生成由所有的共识节点共识决定，其他接入节点在权限许可的情况下可参与记账，可通过该区块链开放的接口进行交易调用及限定查询。

3.5

私有链 private blockchain

指对特定的个人、组织或实体开放的区块链，特定的个人、组织或实体独享该区块链的读写权限。

3.6

时间戳 timestamp

用于辨识记录下来的时间日期的字符串或编码信息。

3.7

上链 on-chain

将相关数据写入到区块链系统中。

3.8

交易 transaction

在一定时间内的一条区块链上,一对一的链上事务性处理,每一笔都需要经过共识确认的状态迁移。

3.9

节点 node

提供区块链的所有功能或者部分功能的实体。

3.10

共识算法 consensus algorithm

区块链系统中各节点为达成一致采用的计算方法。

3.11

智能合约 smart contract

以信息化方式传播、验证或执行合同的计算机协议,其在区块链上体现为可自动执行的计算机程序。

3.12

归档 archive

指将链上数据转移到独立存储上。

3.13

恶意节点 malicious node

遭受非法控制的节点或存在虚假文件、共谋和不合作等问题的节点。

3.14

恶意交易 malicious transaction

由恶意节点发出的非正常交易。

3.15

恶意消息 malicious message

由恶意节点发出的消息。

3.16

许可证 license

用来授权软件使用的一个或多个副本。

4 符号和缩略语

下列缩略语适用于本文件。

IP	网际互联协议（Internet Protocol）
SM2	椭圆曲线密码算法
SM3	密码杂凑算法
SM4	分组密码算法

5 概述

5.1 区块链信息服务安全风险

区块链信息服务是互联网信息服务的一种特殊形式，基于区块链技术实现信息发布、交互、传播等相关功能属性，通过互联网站、应用程序等形式提供信息服务，在存储传播违法不良信息，实施网络违法犯罪活动，损害公民、法人和其他组织合法权益等方面存在一定安全风险。

5.2 安全要求模型

本文件基于区块链信息服务形式，从安全技术要求和安全保障要求两个方面，提出区块链信息服务安全要求模型，见图1。

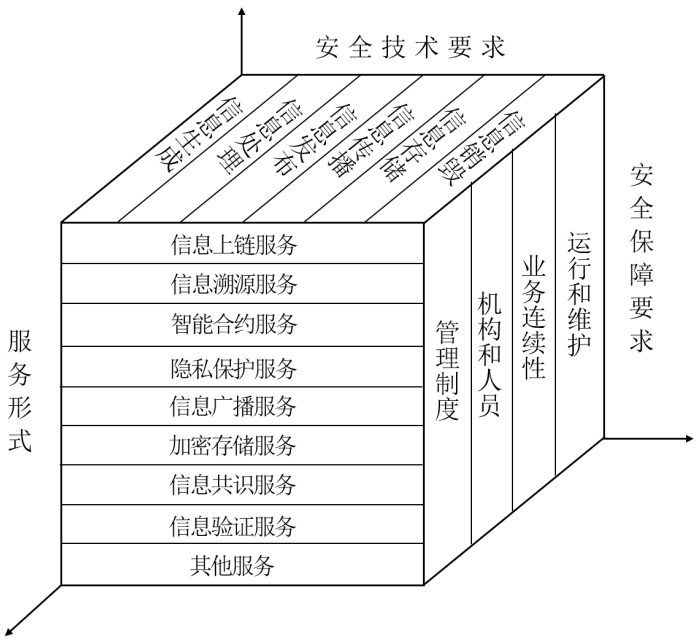

图1 区块链信息服务安全要求模型

服务形式方面，归纳了信息上链、信息溯源、智能合约、隐私保护、信息广播、加密存储、信息共识、信息验证等多种区块链信息服务形式。

安全技术要求方面，定义了信息生命周期，包括信息生成、信息处理、信息发布、信息传播、信息存储、信息销毁六个阶段，针对各阶段提出了面向开放性、交互性、影响力等特征的区块链信息服务的安全技术要求，涵盖了信息生命周期中的主要安全要素。

安全保障要求方面，从管理制度、机构和人员、业务连续性、运行和维护等四个维度，提出了区块链信息服务的安全保障要求。

本文件采用类、族、组件的层次化结构定义方法，提出区块链信息服务的安全技术要求和安全保障要求。

安全技术要求各类、族、组件对应关系见表1，安全保障要求各类、族、组件对应关系见表2。

表1 安全技术要求类、族、组件

类	族	组件
信息生成	区块链信息生成	交易信息规范
		交易信息采集规范
		交易追溯
	信息生成主体	区块链账户管理
		区块链节点管理
		信息溯源
信息处理	上链信息过滤	信息内容识别过滤机制
	信息分级分类	交易信息分级分类
		节点访问控制

表1 安全技术要求类、族、组件

类	族	组件
信息处理	共识机制	安全共识机制
	智能合约	安全智能合约
信息发布	信息上链前审核	审核制度管理
		审核程序管理
	信息发布流程	信息发布流程
信息传播	信息传播过程监测	链上信息安全审核
		信息安全监测预警
	安全事件响应处置	安全事件分级预案
		应急处置策略
信息存储	业务信息存储要求	用户个人信息存储
		账本信息存储
	日志存储	日志存储
信息销毁	信息销毁	信息销毁策略

表 2 安全保障要求的类、族、组件

类	族	组件
管理制度	安全制度	信息源制度
		信息审核发布制度
		信息识别过滤机制
	安全机制	监测预警机制
		投诉举报机制
机构和人员	组织机构	安全管理机构
		安全管理人员
	从业人员管理	人员配备
		人员管理
		人员培训
业务连续性	数据管理	数据保护
		数据存储
		数据销毁
	应急处理	信息溯源
		安全响应处置
运行和维护	服务运营	运营策略
	保障措施	设施设备保障
		网络安全保障

每一项安全技术要求和安全保障要求包括基本要求和增强要求，增强要求是对基本要求的增加和强化。区块链信息服务提供者应对提供的区块链信息服务所属产品类型、业务规模、节点规模等属性进行分析，选择相应的安全要求开展安全建设和评估活动。

区块链信息服务安全要求和测试评估方法在每个安全要求族中设置了“自定义组件”，区块链信息服务提供者可在安全建设和安全评估工作中自行添加组件并定义安全要求。

区块链信息服务安全测试评估的目的为区块链信息服务提供者开展安全建设和安全评估提供依据，主要包括安全技术测评方法和安全保障测评方法。

区块链信息服务的所属产品类型、业务规模和节点规模等属性与安全等级之间的对应关系见附录 A。同时区块链信息服务提供者可根据区块链信息服务及其产品的实际情况，通过组合多个组件包的方式确定特定产品的安全要求，详细内容参见附录 B。

在本文件中，**加黑部分**表示区块链信息服务应满足的**增强要求**。

6 安全技术要求

6.1 信息生成

6.1.1 区块链信息生成

6.1.1.1 交易信息规范

区块链信息服务提供者应：

a) 使用可信时间戳服务对节点授时，保证所有节点时间一致；
b) 使用真随机数、强伪随机数等随机数生成方式，保证随机数的随机性和不可预测性；
c) 使用数字签名来标识发送主体的身份；
d) 遵循密码管理规定对交易数据进行加密；
e) 对发送交易的接口有良好的设计规范，接口层隐藏底层数据的细节，并具有良好的可扩展性和兼容性；
f) 具备识别交易发送方身份的能力；
g) 采用哈希算法 SM3 或者其他安全措施确保发送交易的完整性；
h) 使用具备抵御破解能力的数字签名算法，支持国家商用密码数字签名算法，如 SM2 等；
i) 交易数据加密算法应具备抵御破解的能力，加密算法支持国家商用密码对称加密算法和非对称加密算法，如 SM2、SM3、SM4 等；
j) 在接口层对交易类型进行识别，并在执行层对交易进行分类处理。

6.1.1.2 交易信息采集规范

区块链信息服务提供者应：

a) 规范采集的交易信息，包括交易发起账户、交易接收账户、交易哈希、数字签名、交易类型和交易时间戳等；
b) 明确交易信息采集目的，保证采集的数据符合相关规范；
c) 在信息采集时默认对身份标识信息进行部分隐藏，同时提供全部显示手段；
d) 限定交易信息采集范围，对于隐私数据、加密信息不予采集。

6.1.1.3 交易追溯

区块链信息服务提供者应：

a) 对交易的相关信息，如交易发送方、接收方、交易生成的时间戳等数据进行记录与留存；
b) 提供查询交易信息和交易回执的接口；
c) 具备对采集信息源相关信息进行留存的技术能力，留存时间应不少于 6 个月；
d) 及时检测出任何一条被篡改的数据；
e) 通过 XXX 等方式，对交易信息进行有效追溯。

6.1.2 信息生成主体要求

6.1.2.1 区块链账户管理

区块链信息服务提供者应：

a) 具备创建账户的功能，保证每个账户具有唯一身份标识；
b) 创建账户时告知用户需妥善保管私钥；
c) 使用符合国家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，使用账户唯一标识标记发送方，且不暴露账户私钥部分；
e) 在交易体中携带数字签名保证不可抵赖性；
f) 按照 GB/T 35273—2020 中 9.1 相关要求，满足授权要求在获取账户信息前需告知用户并获得用户授权；
g) 应具备账户授权机制；
h) 应具备账户冻结、解冻、注销等功能；
i) 确保账户关联用户的真实身份信息，包括但不限于用户身份证号码、手机号码，用户遵循“前台自愿，后台实名”的原则。

6.1.2.2 区块链节点管理

区块链信息服务提供者应：

a) 通过证书等方式识别节点的身份；
b) 通过许可证等方式授予用户使用区块链信息服务的权利；
c) 保证节点的加入和退出需要经过共识；
d) 保证当证书失效或许可证过期时，节点失去共识能力；
e) 保证当节点发生故障时，系统具有吊销该节点证书的能力；
f) 支持节点证书和许可证更新后，节点重新获得共识能力；
g) 支持动态增删节点，增删节点时不影响业务正常运行；
h) 支持节点升级或系统升级，且不影响业务正常运行；
i) 当节点发生故障时，具备灾备节点切换的能力且不影响业务的正常运行。

6.1.2.3 信息溯源

区块链信息服务提供者应：

a) 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；
b) 对用户变更身份信息记录进行留存；
c) 定期核查并更新用户账户绑定的身份信息，确保其真实有效。

6.2 信息处理

6.2.1 上链信息过滤

6.2.1.1 信息内容识别过滤机制

区块链信息服务提供者应：

a) 保证具备对交易来源身份进行识别的能力；
b) 保证具备对交易的有效性和正确性进行验证的能力；
c) 识别恶意节点、恶意消息，并保证共识机制能正确完成；

d) 在被攻击节点数据与其他节点不一致时，采取有效机制删除被攻击节点或恢复被攻击节点数据；
e) 保证节点实现对重复交易的过滤；
f) 保证平台可根据实际情况对含有违法信息、不良信息的链和交易进行屏蔽查询；
g) 能够对恶意交易内容进行识别过滤，在接口层拒绝交易；
h) 对恶意交易的来源进行追溯；
i) 对恶意消息完成过滤后进行存证。

6.2.2 信息分级分类要求

6.2.2.1 交易信息分级分类

区块链信息服务提供者应：
a) 建立交易信息内容分级分类机制，分级分类对象包括交易的发送方、接收方、交易的执行类型等，明确交易的分级分类规则；
b) 采取相应技术手段，根据信息内容的敏感程度等方面对交易信息内容分级分类；
c) 明确不同级别信息内容面向的用户群体。

6.2.2.2 节点访问控制

区块链信息服务提供者应：
a) 对区块链中不同类型的节点设置不同权限，明确权限所对应的信息服务内容；
b) 具备对节点权限管理的技术能力；
c) 记录每次节点的权限操作；
d) 建立安全的节点授权机制。

6.2.3 共识机制

6.2.3.1 安全共识机制

区块链信息服务提供者应：
a) 使用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地进行；
c) 对加入共识机制的节点信息进行记录和身份验证，确保节点可追溯。

6.2.4 智能合约

6.2.4.1 安全智能合约

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管理，包括智能合约的创建、编译、部署、调用、冻结、解冻、升级和销毁等；
c) 对智能合约的安全性进行审核，使用智能合约漏洞检测等技术，保证智能合约的安全运行；
d) 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；
e) 在智能合约进行部署、调用、冻结、解冻、升级和销毁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。

6.3 信息发布

6.3.1 信息内容上链前审核

6.3.1.1 审核制度管理要求

区块链信息服务提供者应：

a) 建立用户账户注册信息审核制度，用户注册信息中不得含有违法信息、不良信息；
b) 建立上链前区块链信息内容审核制度，结合人工和技术手段，对节点发布的信息内容进行审核，不含有违法信息、不良信息。

6.3.1.2 审核程序管理

区块链信息服务提供者应：

a) 具备在信息上链前实施信息内容审核程序的能力，具备对信息先审后发的能力；
b) 对发布违法信息、不良信息的账户进行记录，对其发布信息进行存证；
c) 制定并实施信息内容审核程序；
d) 对信息内容进行分级审核；
e) 对重大事件等关键信息发布应进行及时安全审核。

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：

a) 明确普通信息、重大事件等关键信息的发布流程；
b) 根据区块链业务需要，对信息发布者公开或匿名处理；
c) 对重大事件等关键信息进行及时安全发布。

6.4 信息传播

6.4.1 信息传播过程

6.4.1.1 链上信息安全审核

区块链信息服务提供者应：

a) 建立区块链链上信息安全审核机制，采取包括人工审核、平台自动审核等技术手段，能够有效识别、及时停止发布、传输违法信息、不良信息；
b) 留存违法信息、不良信息的审核日志信息；
c) 对审核发现的链上违法信息、不良信息，能够追溯到信息发送节点。

6.4.1.2 信息安全监测预警

区块链信息服务提供者应：

a) 建立主动巡查等及时有效的监测机制，及时发现已经存在于区块链上的违法信息、不良信息，及时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，如发现运行异常节点及时排查预警；
c) 对监测链上违法信息、不良信息等相关信息进行存储；
d) 建立信息安全预警机制，能够对存在安全风险的信息内容提前预警；
e) 具备投诉举报渠道，包括有效的电话、电子邮箱、网页反馈入口等，及时接受投诉举报并予以处理；
f) 对区块链信息安全预警情况进行及时核查处置；

g） 对于举报的违法信息、不良信息，自接收投诉举报起，受理投诉时间不超过 24 小时；

h） 建立 7x24 小时投诉举报机制。

6.4.2 安全事件响应处置

6.4.2.1 安全事件分级预案

区块链信息服务提供者应：

a） 及时发现已经存在于区块链上的违法信息、不良信息，掌握信息的传播范围和影响力等信息；

b） 具备安全事件多级响应处置预案，明确安全事件各级响应处置要求。

6.4.2.2 应急处置策略

区块链信息服务提供者应：

a） 对安全事件及时响应并进行应急处置；

b） 配备相应的技术手段，对链上违法信息、不良信息进行处置；

c） 对发布违法信息、不良信息的节点进行干预，包括冻结、解冻、结束、开启和强制转移等方式；

d） 对安全事件响应处置过程进行留存证据，如记录响应处置人员、时间、对象、方式等关键信息。

e） 对区块链信息服务安全事件进行分级响应处置，并明确对违法信息、不良信息和信息发布账户的具体处置方式。

6.5 信息存储

6.5.1 业务信息存储要求

6.5.1.1 用户个人信息存储

区块链信息服务提供者应：

a） 对区块链用户的个人信息进行留存；

b） 使用多种方式协助用户进行私钥保管，包括软件存储、硬件存储等；

c） 参照 GB/T 35273—2020 中第 6 章的要求，制定用户个人信息保护规定；

d） 对用户重要敏感数据加密存储，保障用户信息的机密性；

e） 第三方存储用户个人信息时需告知用户并得到用户授权；

f） 对用户个人电子信息进行存储。

6.5.1.2 账本信息存储

区块链信息服务提供者应：

a） 对区块链信息服务中涉及发布、传播、共享等环节的业务信息进行存储；

b） 确保各节点存储账本数据的一致性；

c） 对账本数据进行加密存储，保证业务信息内容的完整性和保密性，设置数据访问权限；

d） 对账户数据、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；

e） 保证隐私数据保存在用户终端；

f） 在账本数据发生篡改时，保证节点具有异常恢复的能力；

g） 在机器存储空间不足时，保证区块链节点对数据进行归档；

h） 在未进行数据归档的情况下，节点不应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) 对区块链节点的网络消息收发、共识状态变更、区块打包验证流程、交易执行结果、区块生成、服务启停等日志信息进行存储；
b) 对节点启动、停止、增加、删除等操作日志进行存储；
c) 对节点证书有效期等日志进行存储；
d) 对节点授权情况进行存储；
e) 支持对日志信息的分级存储。

6.6 信息销毁

6.6.1 信息销毁

区块链信息服务提供者应：

a) 采取技术手段，使应销毁数据保持不可被检索、访问的状态；
b) 明确区块链系统废弃的方式、流程等关键策略要素；
c) 对区块链系统废弃过程记录，记录相关人员、时间、内容、方式等关键信息。

7 安全保障要求

7.1 管理制度

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) 制定信息采集规范，包括但不限于信息源采集范围、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；
b) 信息采集时应有明确授权；
c) 制定权限管理相关规范，包括节点权限和用户权限的分类规范，并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) 针对用户发布的文本、图片、音视频等信息内容制定透明的审核制度，包括信息是否合法合规等；
b) 针对用户发布的信息内容，制定与审核制度相适应的审核程序，明确审核轮次、审核策略、审核技术等审核程序关键要素；
c) 针对各类信息建立分级审核程序，对普通信息两级审核，对重大事件等关键信息多级审核；
d) 建立审核程序修订机制，对审核程序进行修订更新和版本控制；
e) 制定智能合约审核流程，包含对智能合约代码漏洞检测、形式化验证和安全扫描等；
f) 应建立信息发布审核制度修订机制，并对审核制度进行修订更新和版本控制；
g) 应配备与信息发布分级审核程序相适应的管理措施；
h) 建立与信息审核制度相适应的信息及时安全发布流程。

7.1.1.3 信息识别过滤

区块链信息服务提供者应制定交易信息规范和信息内容过滤规则等。

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) 制定区块链应急处理措施，当系统运行异常时，能及时对异常行为节点、存在安全风险的信息等预警并快速处置；
b) 制定共识机制应急处置措施，在区块链节点数不足以支持当前共识机制时，及时预警并处置；
c) 制定节点异常应急处置措施，在区块链节点发生异常时，及时预警并切换灾备节点。

7.1.2.2 投诉举报机制

区块链信息服务提供者应对区块链中的信息建立面向公众的投诉举报机制，并对举报及时受理，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：

a) 设立专职安全管理机构，指导区块链信息服务管理工作，组织开展区块链信息服务监督工作；
b) 提供与用户真实身份信息认证相配套的组织机构。

7.2.1.2 安全管理人员

区块链信息服务提供者应：

a) 配备与业务规模相适应的专职工作人员；
b) 配备处置区块链信息服务安全事件的人员。

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：

a) 在服务中提供与业务规模相适应的从事区块链信息服务安全相关的人员；
b) 配备与业务规模相适应，能够有效实施普通信息和关键信息审核的人员；
c) 配备与信息及时安全发布流程相适应的人员；
d) 配备与信息监测预警、核查处置和处置违法信息、不良信息相适应的人员。

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) 对数据和信息采取相应的防护措施，保证数据完整性且能抵抗篡改、重放等主动或被动攻击；
b) 具备信息发布相关日志存储的硬件资源和安全保护措施；
c) 具备用户个人信息保护和账本信息保护相关措施；
d) 采用密码技术保证节点间通信过程中敏感信息字段或整个报文信息的保密性，确保信息在存储、传输过程中不被非授权用户读取和篡改；
e) 在智能合约更新升级、重新部署后，具备能安全地将原合约数据迁移至新合约，原智能合约数据不丢失的技术保障；
f) 定期对账本信息进行查验，建立信息篡改后的修复机制；
g) 制定用户个人信息保护措施，采取如加密、去标识化等安全技术手段进行保护，不得泄露、毁损、丢失用户个人信息。

7.3.1.2 数据存储

区块链信息服务提供者应：

a) 制定用户个人信息和账本信息存储策略，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、账本信息和系统日志存储的硬件存储资源和设施设备；
c) 系统日志的留存时间应不少于 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) 制定系统日志存储策略，明确日志存储方式、存储流程、存储时效等关键策略要素；
f) 对交易内容进行留存，包括区块数据、账户数据、共识数据等。

7.3.1.3 数据销毁

区块链信息服务提供者应：

a) 具备信息销毁的相关技术能力；
b) 为区块链服务提供信息销毁权限，保障信息销毁有效实施。

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：

a) 制定区块链信息溯源规则；
b) 提供交易信息溯源的相关技术措施，且溯源信息的留存时间应不少于 6 个月。

7.3.2.2 安全响应处置

区块链信息服务提供者应：

a) 制定安全事件分级响应处置预案，定期开展安全事件应急演练；
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、不良信息数据库和异常行为用户列表，并定期维护更新。

7.4.2 保障措施

7.4.2.1 设施设备保障

区块链信息服务提供者应提供与业务规模相适应的设施设备资源保障，包括场地、设施、存储和网络资源等，允许区块链信息服务提供者使用第三方提供的设施设备并保障安全。

7.4.2.2 网络安全保障

区块链信息服务提供者应：

a) 配备实施禁止制作、复制、发布、传播违法信息、不良信息内容的技术保障；

b) 能够动态调整共识机制，确保区块链安全运行。

8 安全技术测评方法

8.1 信息生成

8.1.1 区块链信息生成

8.1.1.1 交易信息规范

8.1.1.1.1 基本要求

交易信息规范基本要求测评方法如下：

a) 测评方法：

1） 检测是否采用了国家法定的可信时间戳服务中心提供的可信时间戳服务；

2） 检测随机数生成算法所产生的随机数是否遵循密码管理要求；

3） 篡改数字签名，检测交易是否验签失败；

4） 检测交易数据加密算法是否满足对称加密和非对称加密算法的要求；

5） 检测发送交易的接口是否有可扩展字段；

6） 检测在交易发送过程中，是否对发送方的身份进行识别；

7） 检测发送的交易是否受到破坏，查看收到的交易是否和发送的交易信息一致。

b) 预期结果：

1) 采用国家法定的可信时间戳服务中心提供的可信时间戳服务；

2) 随机数遵循密码管理对随机数的要求；

3) 交易验签失败；

4) 加密算法满足相关要求；

5) 发送交易接口有可扩展字段；

6) 能够对发送方信息进行识别；

7) 收到的交易和发送的交易信息一致。

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

交易信息规范增强要求测评方法如下:

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满足国家商用密码要求；
   2) 披露交易数据加密采用的算法，通过代码审计等方式验证该算法是否满足国家商用密码要求；
   3) 发送不同执行类型的交易，查看是否通过不同的虚拟机执行交易；
   4) 创建不同的应用分区，执行不同的交易，查看不同分区的交易是否互不影响；
   5) 披露数字签名技术实现方法，验证该方法自身的安全性。
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；
   2) 采用的交易数据加密算法满足国家商用密码要求；
   3) 不同执行类型的交易通过不同的虚拟机执行；
   4) 不同类型的业务交易在不同的应用分区中进行；
   5) 数字签名技术实现方法是否存在安全性问题。
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 交易信息采集规范

交易信息采集规范基本要求测评方法如下：

a) 测评方法：
   1) 检测采集的交易信息字段；
   2) 检测交易信息采集数据是否符合相关规范；
   3) 在信息采集时是否对身份标识信息进行隐藏，是否提供技术手段显示全部信息；
   4) 检测数据采集范围是否包括隐私数据和加密信息。
b) 预期结果：
   1) 采集的交易信息包括交易发起节点、交易接收节点、交易哈希、数字签名、交易类型和交易时间戳；
   2) 符合相关规范；
   3) 能够隐藏身份标识信息，并提供技术手段显示全部信息；
   4) 不包括隐私数据和加密信息。
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 交易追溯

交易追溯基本要求测评方法如下：

a) 测评方法：
   1) 发送交易，查询交易，查看交易体中是否包含交易发送方、接收方、交易生成的时间戳、交易金额等字段；
   2) 通过查询交易接口查询交易信息，通过查询回执接口查询回执；
   3) 检查采集信息源相关日志存储时间是否不少于 6 个月；

4） 提交一条被篡改交易，检测是否能通过技术回溯检测出该交易；
5） 检测该平台是否具备交易追溯的能力。

b） 预期结果：
1） 包含预期字段；
2） 查询交易接口返回的结果包含以上预期字段，查询回执接口返回正确的回执；
3） 日志存储时间不少于 6 个月；
4） 能够回溯检测出被篡改交易；
5） 具有交易追溯能力。

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。

8.1.2 信息生成主体要求

8.1.2.1 区块链账户管理

8.1.2.1.1 基本要求

区块链账户管理基本要求测评方法如下：

a） 测评方法：
1） 创建账户，检测账户的身份标识是否具有唯一性；
2） 创建账户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） 检测密码算法是否满足密码管理规范；
4） 查看交易体中是否包含发送方的身份标识，且不包含私钥字段；
5） 检测交易体中是否包含签名字段；
6） 检测获取账户信息前是否有告知用户的相关提示和授权按钮。

b） 预期结果：
1） 账户创建成功，且账户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） 非对称加密算法的公钥满足国家管理规范；
4） 交易体中包含发送方的身份标识，且不包含私钥字段；
5） 交易体包含签名字段；
6） 有告知用户的相关提示和授权按钮。

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

区块链账户管理增强要求测评方法如下：

a） 测评方法：
1） 对账户授权，检测该账户是否具有权限；
2） 冻结账户，查看账户状态；注销账户，查看账户状态；
3） 注册用户后，检测后台是否可以查到用户的实名信息。

b） 预期结果：
1） 被授权用户具有相关权限；
2） 账户状态变为冻结；账户状态变为注销；
3） 后台可以查到用户的实名信息。

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 区块链节点管理

8.1.2.2.1 基本要求

区块链节点管理基本要求测评方法如下：

a) 测评方法：
1) 篡改区块链节点的证书或许可证，检测节点是否失效；
2) 模拟满足共识算法要求的故障节点数，增加节点，查看是否能新增成功；删除节点，查看是否能删除成功；
3) 篡改节点证书或许可证，发送交易，查看该节点区块高度是否和其他节点一致；
4) 宕机其中一个节点，吊销该节点证书，重启节点，检测该节点是否还能参与共识；
5) 新增节点时持续发送交易，查看交易是否发送成功；
6) 节点升级时持续发送交易，查看交易是否发送成功；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) 节点失效；
2) 新增成功，节点数加一；删除成功，节点数减一；
3) 该节点区块高度和其他节点一致；
4) 节点证书吊销成功，该节点不能参与共识；
5) 交易发送成功；
6) 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

区块链节点管理增强要求测评方法如下：

a) 测评方法：
切换灾备节点过程中向区块链持续发送交易，查看交易是否发送成功。

b) 预期结果：
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 信息溯源

8.1.2.3.1 基本要求

区块链信息溯源基本要求测评方法如下：

a) 测评方法：
检测区块链平台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：
区块链平台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。

8.1.2.3.2 增强要求

区块链信息溯源增强要求测评方法如下：

a) 测评方法：

1)

2) 修改用户身份信息，查看是否有身份变更记录；

3) 修改用户绑定的身份信息为真实的信息，查看是否修改成功；

4) 修改用户绑定的身份信息为不真实的信息，查看是否修改成功。

b) 预期结果：

1) 能查到身份变更记录；

2) 修改成功；

3) 修改失败。

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 上链信息过滤

8.2.1.1 信息内容识别过滤

8.2.1.1.1 基本要求

信息内容识别过滤基本要求测评方法如下：

a) 测评方法：

1）检测是否支持通过识别工具，识别指定交易账户的状态及基本信息；

2）提交双花交易，检测是否能通过；

3）提交包含恶意消息的交易，检测是否能通过；

4）通过随机向 N 个节点（满足共识算法要求的节点数）查询区块链数据，识别被攻击节点；

5）当发现被攻击节点后，经过一段时间后查询被攻击节点和其他节点数据，检测是否一致；

6）发送重复交易，检测是否全部交易均上链。

b) 预期结果：

1）能够识别交易账户状态及基本信息；

2）双花交易无法通过；

3）包含恶意消息的交易无法通过；

4）能够发现数据不一致节点，即被攻击节点；

5）被攻击节点数据与其他节点数据一致；

6）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。

8.2.1.1.2 增强要求

信息内容识别过滤增强要求测评方法如下：

a) 测评方法：

1) 发送恶意交易，查看其他节点是否对该交易进行共识；
2) 发送一些合法交易和恶意交易，查看返回结果，查看合法交易完整性；
3) 向节点发送恶意交易，在该节点上查询非法交易；
4) 向节点发送恶意交易后，在其他节点上查询非法交易。

b) 预期结果：
1) 恶意交易直接被拒绝，未传播到其他节点；
2) 合法交易的查询结果与发送时一致；
3) 能查到恶意交易的发送方；
4) 管理节点收到消息。

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。

8.2.2 信息分级分类要求

8.2.2.1 交易信息分级分类

8.2.2.1.1 基本要求

交易信息分级分类基本要求测评方法如下：

a) 测评方法：
1) 检测区块链平台是否能针对交易的发送方、接收方和交易执行类型设置不同的过滤规则；
2) 将交易过滤规则设为只能接收指定发送方的交易，发送来自不同发送方的交易，查看是否发送成功；
3) 将交易过滤规则设为只能接收指定接收方的交易，发送具有不同接收方的交易，查看是否发送成功；
4) 将交易过滤规则设为只能接收指定执行类型的交易，发送不同执行类型的交易，查看是否发送成功。

b) 预期结果：
1) 具有设置过滤规则的入口；
2) 和指定发送方一致的交易发送成功，其他交易失败；
3) 和指定接收方一致的交易发送成功，其他交易失败；
4) 和指定执行类型一致的交易发送成功，其他交易失败。

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

交易信息分级分类增强要求测评方法如下：

a) 测评方法：
使用不同级别的用户身份调用不同级别的交易接口，查看其权限是否一样；

b) 预期结果：
不同级别的用户对交易接口的权限不一样。

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。

8.2.2.2 节点访问控制

节点访问控制基本要求测评方法如下：

a) 测评方法：
   1) 检测区块链平台的不同类型的节点是否具有不同权限，检测其中一个类型的节点是否能进行另一种节点权限的操作；
   2) 进行节点权限操作，查看操作记录；
   3) 检测节点授权机制是否安全。
b) 预期结果：
   1) 该类型的节点无法进行其他类型节点权限下的操作；
   2) 查看到操作记录；
   3) 具有安全的节点授权机制。
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。

8.2.3 共识机制

8.2.3.1 安全共识机制

安全共识机制基本要求测评方法如下：

a) 测评方法：
   1) 披露区块链平台所采用的共识机制，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；
   2) 当恶意节点数少于容错节点数时，发送交易，查看节点的一致性；
   3) 当恶意节点数多于容错节点数时，发送交易，查看节点的一致性；
   4) 调用查询共识节点信息的接口，查看是否具有节点信息；
   5) 加入共识的节点是否经过身份验证。
b) 预期结果：
   1) 区块链平台实际采用的共识机制满足披露的共识算法规则；
   2) 当恶意节点数少于容错节点数时可以达成一致；
   3) 当恶意节点数多于容错节点数时无法达成一致；
   4) 能查到节点信息和身份；
   5) 节点经过身份验证。
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。

8.2.4 智能合约

8.2.4.1 安全智能合约

安全智能合约基本要求测评方法如下：

a) 测评方法：
   1) 检测智能合约的业务逻辑是否满足其披露的业务范围；
   2) 检测是否提供智能合约的全生命周期管理；
   3) 检测区块链信息服务提供者是否具有合约安全审计方案；
   4) 检测是否对智能合约的正确性进行审核；
   5) 查看部署、调用、冻结、解冻、升级和销毁等操作时，智能合约的接口是否具有签名字段。
b) 预期结果：

1） 智能合约的业务逻辑满足其披露的业务范围；
2） 具备对智能合约的全生命周期管理的能力；
3） 具有合约安全审计方案，如用例测试，第三方平台漏洞扫描等；
4） 对智能合约的文本和代码完成了形式化验证；
5） 部署、调用、冻结、解冻、升级和销毁等操作时，智能合约的接口具有签名字段。

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 信息内容上链前审核

8.3.1.1 审核制度管理

审核制度管理基本要求测评方法如下：

a） 测评方法：
1） 注册节点账户时，使用违法的名称、头像或简介，查看是否能注册成功；
2） 在发送的交易中包含违法字段，查看是否发送成功。

b） 预期结果：
1） 注册失败；
2） 交易发送失败。

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 审核程序管理

8.3.1.2.1 基本要求

审核程序管理基本要求的测评方法如下：

a） 测评方法：
1） 信息上链前是否经过内容审核；
2） 制造恶意节点，通过恶意节点向其他节点发送消息，查看节点日志中是否有记录；
3） 检测区块链平台是否具有信息内容审核机制。

b） 预期结果：
1） 信息上链经过内容审核；
2） 节点日志中有恶意节点的操作记录；
3） 区块链平台具有信息内容审核机制。

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。

8.3.1.2.2 增强要求

审核程序管理增强要求测评方法如下：

a） 测评方法：
1） 检测区块链平台是否具有交易分级的机制；
2） 检测区块链平台是否具有重大事件的安全审核机制。

b） 预期结果：
1） 区块链平台具有交易分级的机制；

2） 区块链平台具有重大事件的安全审核机制。

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

8.3.2.1.1 基本要求

信息发布流程基本要求测评方法如下：

a） 测评方法：

1） 发送普通交易，检测其发布流程；发送升级、部署合约等重要交易，检测其是否具有投票等流程；

2） 检测发送交易时是否能查看交易发送方公钥，且不包含私钥。

b） 预期结果：

1） 重要交易的发布流程需要经过投票；

2） 交易体中包含交易发送方公钥，不包含私钥。

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。

8.3.2.1.2 增强要求

信息发布流程增强要求测评方法如下：

a） 测评方法：

订阅重大事件，检测区块链平台的推送是否及时。

b） 预期结果：

区块链平台能及时推送。

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 信息传播过程

8.4.1.1 链上信息安全审核

8.4.1.1.1 基本要求

链上信息安全审核基本要求测评方法如下：

a） 测评方法：

1） 向区块链平台发送和传输违法信息、不良消息，检测平台是否能够成功检测并制止；

2） 查看区块链平台日志消息，查找违法信息、不良消息的相关信息。

b） 预期结果：

1） 区块链平台成功识别出违法信息、不良信息，并阻止信息发布；

2） 区块链平台可查询相关违法信息、不良消息的详细信息并保存。

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

链上信息安全审核增强要求测评方法如下：

a) 测评方法：
发送违法信息、不良信息，检测是否能追溯违法信息发送的具体账户。

b) 预期结果：
能够追溯到不良信息发送的具体账户。

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 信息安全监测预警

8.4.1.2.1 基本要求

信息安全检测预警基本要求测评方法如下：

a) 测评方法：
1） 发送违法信息、不良消息，检查平台是否能通过实时监测的手段及时检测出这些违法信息、不良信息，并对这些违法信息、不良信息的传播范围和影响力作相应判断；
2） 通过一定手段使节点运行异常，查看平台能否对异常节点和状态做实时监控，并及时预警；
3） 发送违法信息、不良消息，检测平台是否对异常的节点和相关消息进行日志级别存储；
4） 发送有安全风险的信息，检测平台是否可以对这些信息做出风险预警；
5） 确认平台是否提供有效的渠道，方便公众对违法信息、不良信息进行相关的投诉举报，并进行后续追踪。

b) 预期结果：
1） 能够实时监测出违法信息、不良信息，并对信息的传播范围和影响力做出评估；
2） 对异常节点和状态有实时监控和预警机制；
3） 对异常节点和相关信息有日志存储；
4） 能够对有安全风险的信息做出风险预警；
5） 提供有效的渠道让公众对违法信息、不良信息进行投诉举报，并进行后续追踪。

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。

8.4.1.2.2 增强要求

信息安全检测预警增强要求测评方法如下：

a) 测评方法：
1） 跟进区块链信息安全预警情况，检查是否可以及时进行处理；
2） 跟进对违法信息、不良信息的处理速度，确认公众投诉举报的相关违法信息的受理时间；
3） 确认可以进行投诉举报的时间节点，检查是否建立 7x24 小时投诉举报机制。

b) 预期结果：
1） 可以对区块链信息安全预警情况进行及时处理；
2） 公众投诉举报的相关违法信息的受理时间不超过 24 小时；
3） 建立 7x24 小时投诉举报机制，可以在任何时间进行投诉举报。

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 安全事件响应处置

8.4.2.1 安全事件分级预案

8.4.2.1.1 基本要求

安全事件分级预案基本要求测评方法如下：

a) 测评方法：
检查是否有安全事件分级响应处理预案，并对预案的详细内容做核对。

b) 预期结果：
具备安全事件分级响应处置预案，并且对安全事件分级规范、分级应急响应处置人员配备、处置流程、处置方式、处置时效等信息有所明确。

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。

8.4.2.1.2 增强要求

安全事件分级预案增强要求测评方法如下：

a) 测评方法：
检查是否有安全事件多级响应处理预案，并且各级响应都有相关处理要求。

b) 预期结果：
具备安全事件多级响应处理预案，各级响应处理要求有所明确。

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 应急处置策略

8.4.2.2.1 基本要求

应急处理策略基本要求测评方法如下：

a) 测评方法：
1） 检测是否可以对安全事件做出及时响应，并能做出应急处理；
2） 检测是否通过技术手段对上链的违法信息、不良信息做合理处置；
3） 检测是否可以对发送不良信息的节点进行干预，并检查具体干预方式；
4） 跟进具体的安全事件响应处理过程，检查是否对关键信息进行存证。

b) 预期结果：
1） 可以对安全事件做出及时响应和紧急处理；
2） 通过技术手段对违法信息、不良信息做出响应处置；
3） 通过冻结、解冻、结束、开启和强制转移等方式对发送不良信息的节点进行强制干预；
4） 对安全事件响应处理过程的记录响应处置人员、时间、对象、方式等信息进行存证。

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。

8.4.2.2.2 增强要求

应急处理策略增强要求测评方法如下：

a) 测评方法：
检查区块链信息服务安全事件的响应处置方式，对违法信息、不良信息和发布信息的节点的具体处置方式做具体核实。

b) 预期结果：
对区块链信息服务安全事件有分级响应处置机制，并且对违法信息、不良信息和发布信息的节点有明确的处理方式。
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 业务信息存储要求

8.5.1.1 用户个人信息存储

8.5.1.1.1 基本要求

用户个人信息存储基本要求测评方法如下：
a) 测评方法：
1） 检查区块链平台的用户是否保存了个人信息；
2） 检查可通过多种方式对私钥进行保管；
3） 检查用户个人信息保护的相关规定参照 GB/T 35273—2020 中 6.1，6.2，6.3，6.4 的相应要求；
4） 查看用户的个人敏感信息、隐私信息和重要数据等，验证信息被加密存储；
5） 使用第三方存储用户个人信息，检查用户是否被实时告知，并提供授权入口。
b) 预期结果：
1） 区块链平台的用户保存了个人信息；
2） 通过软件存储、硬件存储等多种方式对私钥进行保管；
3） 参照 GB/T 35273—2020 中 6.1，6.2，6.3，6.4 的相应要求对用户个人信息进行保护；
4） 用户的个人敏感信息、隐私信息和重要数据等被加密存储，保障用户的个人信息安全；
5） 用户个人信息被第三方存储时明确告知用户，并及时给用户提供了授权入口。
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 账本信息存储

8.5.1.2.1 基本要求

账本信息存储基本要求测评方法如下：
a) 测评方法：
1） 检查区块链信息服务中的存储信息，是否包含涉及发布、传播、共享等环节的业务信息；
2） 核对各节点的账本数据，检查是否一致；
3） 对账本数据进行访问，检查账本数据是否被加密；
4） 检查是否只在有数据访问权限时才能查询到账本的完整正确数据；
5） 查看账户数据、区块数据、配置数据、证书等数据，确认不同类型的数据分类别进行存储和管理；
6） 确认隐私数据的保存路径是否在本地。
b) 预期结果：
1） 涉及发布、传播、共享等环节的业务信息被存储；
2） 各节点保存的账本数据一致；

3） 账本数据被加密存储；
4） 没有数据权限时无法查询账本数据，有数据权限时可以查看完整账本数据；
5） 不同类型的数据被分类别进行存储和管理；
6） 隐私数据在链下本地存储，链上存储数据摘要。

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

账本信息存储增强要求测评方法如下：

a） 测评方法：
1） 对账本数据进行篡改，检查节点是否有异常恢复的能力；
2） 检查节点能够对数据进行归档；
3） 查看节点具体信息，是否包含本地存储的账本信息。

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的情况发生；
3） 节点留存本地存储的账本信息。

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

日志存储基本要求测评方法如下：

a） 测评方法：
1） 触发区块链节点的网络消息收发、共识状态变更、区块打包验证流程、交易执行结果、区块生成、服务启停等场景，检查日志信息是否存储；
2） 对节点启动、停止、增加、删除等操作，检查日志信息是否存储；
3） 检查节点证书有效期等日志是否存储。

b） 预期结果：
1） 网络消息收发、共识状态变更、区块打包验证流程、交易执行结果、区块生成、服务启停等场景的日志信息都成功存储；
2） 节点启动、停止、增加、删除等操作日志都成功存储；
3） 节点证书有效期等日志成功存储。

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。

8.5.2.1.2 增强要求

日志存储增强要求测评方法如下：

a） 测评方法：
检查区块链平台是否支持日志的分级存储。

b） 预期结果：

区块链平台支持日志的分级存储。

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。

8.6 信息销毁

8.6.1 信息销毁策略

信息销毁策略基本要求测评方法如下：

a) 测评方法：

1） 检测应销毁数据是否在区块链可见、是否可检索；

2） 明确区块链系统废弃方式、流程等关键策略要素；

3） 检查不同类型的区块链是否有不同的系统废弃策略；

4） 检查信息销毁过程中是否进行相应存证。

b) 预期结果：

1） 数据不可见，不可检索；

2） 区块链系统废弃方式、流程等关键策略要素信息详细明确；

3） 针对不同类型的区块链有不同的系统废弃策略；

4） 区块链系统废弃过程中，人员、时间、内容、方式等关键信息被进行及时存证。

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。

9 安全保障测评方法

9.1 管理制度

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测评方法如下：

a) 测评方法：

1） 查看信息采集规范，检查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的规范条目；

2） 是否在信息采集时有明确授权；

3） 查看权限管理相关规范，检查是否包括节点权限和用户权限分类相关规范条目，检查是否包括不同权限参与信息服务的要求。

b) 预期结果：

交易信息采集规范满足 6.1.1.1 中所述的要求。

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。

9.1.1.2 信息审核发布制度

9.1.1.2.1 基本要求

信息审核发布制度基本要求测评方法如下：

a) 测评方法：

1） 查看信息内容上链前审核制度，对是否包含文本、图片、音视频等进行审核；
2） 查看对节点发布信息的审核程序规则规范，检查审核轮次、审核策略、审核技术等审核程序关键要素是否明确；
3） 查看是否具备人工审核制度、非人工审核制度；
4） 查看平台对信息的分级审核程序，检查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；
5） 查看审核制度修订机制，检查是否包含修订更新和版本控制内容；
6） 查看信息发布流程，检查是否与信息内容审核制度和程序相适应；
7） 对于给定包含安全漏洞代码的智能合约，是否能检测出存在的漏洞。

b) 预期结果：
1） 具备审核制度，能够对文本、图片、音视频等进行审核；
2） 具备对用户发布信息的审核程序规则规范，明确了审核轮次、审核策略、审核技术等审核程序关键要素；
3） 具备人工审核制度和非人工审核制度；
4） 具备对信息的分级审核程序，对普通信息两级审核，对重大事件等关键信息多级审核；
5） 具备审核标准修订机制，能够对审核制度进行修订更新和版本控制；
6） 具备信息发布相关日志存储的硬件资源和安全保护技术措施；
7） 能够检测出智能合约的安全漏洞。

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。

9.1.1.2.2 增强要求

信息审核发布制度增强要求测评方法如下：

a) 测评方法：
1） 查看审核制度修订机制，检查是否包含修订更新和版本控制内容；
2） 查看是否具备与分级审核程序相适应的管理和技术保障措施；
3） 查看信息发布流程，检查是否与信息审核制度相适应，能否对信息及时安全发布。

b) 预期结果：
1） 具备审核标准修订机制，能够对审核制度进行修订更新和版本控制；
2） 具备与分级审核程序相适应的管理措施；
3） 具备与信息审核制度相适应的信息及时安全发布流程。

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。

9.1.1.3 信息识别过滤

信息内容识别过滤基本要求测评方法如下：

a) 测评方法：
查看交易信息规范、信息内容识别过滤规则和相关智能合约内容。

b) 预期结果：
具备交易信息规范、信息内容识别过滤规则和智能合约。

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。

9.1.2 安全机制

9.1.2.1 监测预警机制

应急处置机制基本要求测评方法如下：

a) 测评方法：
   1）提交风险内容，检查预警的时效和效果；
   2）在某节点进行异常行为，检查对该节点的预警时效和效果；
   3）检测达成共识时所需的最小节点数，检查是否与设定值一致；
   4）查看共识机制应急处置措施，检测在节点数不足以支持共识机制时，平台能否预警并进行处置；
   5）检测共识机制的真实性、合理性和容错性；
   6）检测节点发生异常时，平台能否预警并进行灾备节点切换。
b) 预期结果：
   1）对存在安全风险的信息内容能够及时预警；
   2）对信息发布行为异常的节点能够及时预警；
   3）最小节点数与设定值一致；
   4）具备共识机制应急处置措施，能在节点数不足以支持共识机制时进行预警并处置；
   5）具备真实、合理的共识机制，具备容错性设计；
   6）具备合理的灾备节点切换机制。
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。

9.1.2.2 投诉举报机制

投诉举报机制基本要求测评方法如下：

a) 测评方法：
   查看投诉举报机制规范，检测是否包含面向公众、对举报及时受理、记录处理情况的条款。
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。

9.2 机构和人员

9.2.1 组织机构

9.2.2 安全管理机构

9.2.2.1.1 基本要求

安全管理机构基本要求测评方法如下：

a) 测评方法：
   检查区块链信息服务提供者是否提供与用户个人信息保护和信息溯源相配套的组织机构保障。
b) 预期结果：
   具备相关组织机构保障。
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。

9.2.2.2 增强要求

安全管理机构增强要求测评方法如下：

a) 测评方法：
检查区块链信息服务提供者是否提供与用户真实身份信息认证相配套的组织机构。

b) 预期结果：
具备相关组织机构保障。

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。

9.2.2.3 安全管理人员

安全管理人员基本要求测评方法如下：

a) 测评方法：
查看业务规模，以及区块链信息服务安全管理和处置安全事件相关人员值班表。

b) 预期结果：
配备与业务规模相适应的安全管理人员。

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。

9.2.3 从业人员管理

9.2.3.1 人员配备

9.2.3.1.1 基本要求

人员配备基本要求测评方法如下：

a) 测评方法：
查看业务规模，以及从事区块链信息服务安全相关人员名单。

b) 预期结果：
配备与业务规模相适应的从业人员。

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。

9.2.3.1.2 增强要求

人员配备增强要求测评方法如下：

a) 测评方法：
1） 查看业务规模，以及对普通信息和关键信息审核人员值班表；
2） 查看业务规模，以及从事信息发布的相关人员值班表；
3） 查看信息监测预警、监测预警情况核查处置和处置违法信息、不良信息的相关人员值班表。

b) 预期结果：
1） 配备业务规模相适应的普通信息和关键信息审核人员；
2） 配备业务规模相适应信息及时安全发布的人员；
3） 配备与信息监测预警、监测预警情况核查处置和处置违法信息、不良信息的人员。

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。

9.2.3.2 人员管理

人员管理基本要求测评方法如下：

a) 测评方法：
查看业务人员相关管理制度，检查是否包括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与条款。

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。

9.2.3.3 人员培训

人员培训基本要求测评方法如下：

a) 测评方法：
1） 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；
2） 查看审核人员培训记录，检查审核人员是否定期参加培训；
3） 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：
1） 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；
2） 审核人员定期参加培训；
3） 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。

9.3 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

数据保护基本要求测评方法如下：

a) 测评方法：
1） 查看是否具备对数据和信息的防护措施规定，是否包含保证数据完整性、抵抗篡改、重放等攻击的条款；
2） 查看是否具备信息发布相关日志存储的硬件资源与相关措施规定；
3） 查看平台是否具备与用户个人信息保护和账本信息保护相关措施规定；
4） 查看是否采用密码技术，保证节点间通信过程中敏感信息字段或整个报文信息的保密性；
5） 查看智能合约迁移相关规范，查看是否具备原合约数据安全迁移相关条款，检测迁移智能合约后数据是否丢失；
6） 检查是否对账本信息定期查验，查看是否具备防止信息被篡改的措施；
7） 查看用户个人信息保护措施相关规定，检查是否具备不泄露、损坏、丢失用户个人信息条款。

b) 预期结果：
1） 具备对数据和信息的防护措施规定文件，包含保证数据完整性、抵抗篡改、重放等攻击的

条款；
2） 具备存储信息发布日志的硬件资源，具备相关措施规定文件；
3） 具备与用户个人信息保护和账本信息保护的相关措施规范文件；
4） 在节点通信中使用密码技术保证报文信息保密性；
5） 具备智能合约迁移相关规范，包含原合约数据安全迁移条款，检测原合约数据迁移后无丢失；
6） 具备定期查验账本信息的记录，具备防止信息被篡改相关措施；
7） 具备用户个人信息保护措施，具备不泄露、损坏、丢失用户个人信息等相关条款。

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。

9.3.1.2 数据存储

9.3.1.2.1 基本要求

数据存储基本要求测评方法如下：

a） 测评方法：
1） 查看用户个人信息存储和账本信息存储规范，检查是否包含存储方式、存储流程、同步方式等的条款，查看用户信息和账本信息存储后台进行验证；
2） 查看用户个人信息、账本信息和系统日志存储的硬件存储资源和设施设备；
3） 查看日志存储相关规定，查看系统日志创建时间，检查是否留存 6 个月前的日志。

b） 预期结果：
1） 具备用户个人信息和账本信息存储规范，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、账本信息和系统日志存储量与硬件存储资源和设施设备相适应；
3） 日志存储时间不少于 6 个月。

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。

9.3.1.2.2 增强要求

数据存储增强要求测评方法如下：

a） 测评方法：
1） 查看账本信息备份记录，检查密钥等关键信息备份周期；
2） 查看系统日志存储规范，检查存储方式、存储流程、存储时效要求，并在后台验证；
3） 查看交易内容留存日志；
4） 查看系统日志的备份记录，并在后台验证。

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） 制定了系统日志存储规范，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） 留存交易内容；
4） 系统日志有备份记录，与验证结果一致。

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。

9.3.1.3 数据销毁

数据销毁基本要求测评方法如下：

a) 测评方法：

1） 查看平台信息销毁权限，并对某数据进行销毁操作；

2） 检查数据销毁的方法和可复原程度。

b) 预期结果：

1） 能对某数据进行销毁，具备销毁权限；

2） 数据销毁依据相关规范进行，数据不可复原。

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。

9.3.2 应急处理

9.3.2.1 信息溯源

9.3.2.1.1 基本要求

信息溯源基本要求测评方法如下：

a) 测评方法：

1） 查看信息溯源规则；

2） 查看日志存储规定，查看交易日志创建时间，检查是否留存 6 个月前的日志。

b) 预期结果：

1） 具备信息溯源规则；

2） 交易信息日志留存时间不少于 6 个月。

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。

9.3.2.1.2 增强要求

信息溯源增强要求测评方法如下：

a) 测评方法：

查看是否具备对包含敏感词的信息进行追溯的相关技术和规范。

b) 预期结果：

具备配合相关部门追溯包含敏感词的信息的技术和规范。

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。

9.3.2.2 安全响应处置

9.3.2.2.1 基本要求

安全响应处置基本要求测评方法如下：

a) 测评方法：

1） 查看平台制定的安全事件分级响应处置预案；

2） 查看平台安全事件应急演练记录，以及演练周期。

b) 预期结果：

1） 制定了满足业务需求的安全事件分级响应处置预案；

2） 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。

9.3.2.2.2 增强要求

安全事件响应处置增强要求测评方法如下：

a） 测评方法：

查看多级处置预案修订更新时间和版本发布时间。

b） 预期结果：

对每级预案及时修订更新，版本控制良好。

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。

9.4 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测评方法如下：

a） 测评方法：

检查是否具备违法信息、不良信息数据库，检查数据库是否定期更新。

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。

9.4.2 保障措施

9.4.2.1 设施设备保障

设施设备保障的基本要求测评方法如下：

a） 测评方法：

1） 查看区块链信息服务提供者是否配备业务规模相适应的设施场地、设施、存储和网络资源；

2） 检查区块链信息服务提供者是否使用第三方提供设施设备，是否确保安全。

b） 预期结果：

1） 具备相关设施设备资源；

2） 能够确保使用第三方设施设备时保障安全。

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。

9.4.2.2 网络安全保障

9.4.2.2.1 基本要求

网络安全保障基本要求测评方法如下：

a） 测评方法：

检查区块链信息服务提供者是否具备实施实施禁止制作、复制、发布、传播违法信息、不良信

息的技术能力。

b) 预期结果：

具备相关技术能力。

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。

9.4.2.2.2 增强要求

网络安全保障增强要求测评方法如下：

a) 测评方法：

检查区块链信息服务提供者是否具备动态调整共识机制，确保区块链安全运行的能力。

b) 预期结果：

具备确保区块链安全运行同时，动态调整共识机制的能力。

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。

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要求和测试评估方法定义了两个安全级别，分别是基本级和增强级。通过区块链产品类型、业务规模和节点规模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或第三方安全评估机构开展安全建设和安全评估提供安全要求分级依据。不同产品类型的区块链信息服务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） 区块链产品类型为内容分发、数字版权、社交媒体、数据保护；

b） 区块链信息服务产品的业务规模达到大、中型企业规模要求；

c） 区块链平台节点规模达到一万以上。

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
产品类型	内容分发		✓
	数字版权		✓
	社交媒体		✓
	数据保护		✓
	其他	✓	
业务规模	大型企业		✓
	中型企业		✓
	小、微型企业	✓	
节点规模	一万以上		✓
	一万及以下	✓	

基本级应满足所定制组件中所有的基本要求。增强级应满足所定制组件中的基本要求和增强要求，若某组件中未定义增强要求，则应满足基本要求。基本级和增强级应满足的要求见表A.2区块链信息服务安全技术要求等级划分和表A.3区块链信息服务安全保障要求等级划分。

表A.2 区块链信息服务安全技术要求等级划分

安全技术要求			安全级	
			基本级	增强级
信息生成	区块链信息生成	交易信息规范	*	*
		交易信息采集规范	*	*
		交易追溯	*	*
	信息生成主体要求	区块链账户管理	*	**
		区块链节点管理	*	*
		信息溯源	*	*
信息处理	上链信息过滤	信息内容识别过滤机制	*	**

表A.2 区块链信息服务安全技术要求等级划分（续）

安全技术要求			安全级	
			基本级	增强级
信息处理	信息分级分类要求	交易信息分级分类	*	**
		节点权限管理	*	**
	共识机制	安全共识机制	*	**
	智能合约	安全智能合约	*	**
信息发布	信息内容上链前审核	审核制度管理	*	**
		审核程序管理	*	**
	信息发布流程要求	信息发布流程	*	**
信息传播	链上信息审核	链上信息安全审核	*	**
		信息安全监测预警	*	**
	安全事件响应处置	安全事件分级预案	*	**
		应急处置策略	*	**
信息存储	业务信息存储要求	用户个人信息存储	*	*
		账本信息存储	*	**
	日志存储要求	日志存储	*	**
信息销毁	信息销毁要求	信息销毁策略	*	*
注：“*”表示具有该要求，“**” 表示要求有所增强。				

表A.3 区块链信息服务安全保障要求等级划分

安全保障要求			安全级	
			基本级	增强级
管理制度	安全制度	信息源制度	*	*
		信息审核发布制度	*	**
		信息识别过滤机制	*	*
	安全机制	监测预警机制	*	*
		投诉举报机制	*	*
机构和人员	组织机构	安全管理机构	*	**
		安全管理人员	*	*
	从业人员管理	人员配备	*	**
		人员管理	*	*
		人员培训	*	*
业务连续性	数据管理	数据保护	*	**
		数据存储	*	**
		数据销毁	*	*
	应急处理	信息溯源	*	**
		安全响应处置	*	**
运行和维护	服务运营	运营策略	*	*
	保障措施	设施设备保障	*	*
		网络安全保障	*	**
注：“*”表示具有该要求，“**” 表示要求有所增强。				

附 录 B
（资料性）
区块链信息服务安全规范组件包定制示例

区块链信息服务安全要求和测试评估方法以组件的方式定义了具有开放性、交互性、动员力等特征的区块链信息生命周期六个阶段的安全要求。为了有效落实安全要求，开展特定区块链信息服务的安全评估工作，可通过组件包的方式，即组合不同的安全要求组件形成组件集合，实现特定服务形式的安全要求定制，对于提供多个服务形式的产品，可通过集成多个组件包的方式定制要求。几类常见区块链信息服务的组件包示例见表B.1：

表B.1 常见区块链信息服务形式的组件包

组件	服务形式							
	信息上链	信息溯源	智能合约	隐私保护	信息广播	加密存储	信息共识	信息验证
交易信息规范	✓	✓			✓			
交易信息采集规范	✓	✓			✓			
交易追溯		✓						
区块链账户管理				✓		✓		✓
区块链节点管理				✓		✓	✓	✓
信息溯源		✓						
信息内容识别过滤机制	✓				✓			
交易信息分级分类	✓				✓			✓
节点权限管理	✓				✓		✓	✓
安全共识机制	✓		✓		✓		✓	
安全智能合约	✓		✓		✓		✓	
审核制度管理	✓				✓			
审核程序管理	✓				✓			
信息发布流程	✓				✓			
链上信息安全审核	✓	✓	✓	✓	✓	✓	✓	✓
信息安全监测预警	✓	✓	✓	✓	✓	✓	✓	✓
安全事件分级预案	✓	✓	✓	✓	✓	✓	✓	✓
应急处置策略	✓	✓	✓	✓	✓	✓	✓	✓
用户个人信息存储				✓		✓		✓
账本信息存储				✓		✓		✓
日志存储	✓	✓		✓	✓	✓		✓
信息销毁策略	✓			✓		✓		

参 考 文 献

[1] GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法
[2] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
[3] GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范
[4] ISO 22739—2020 Blockchain and distributed ledger technologies — Vocabulary
[5] JT/T 0184—2020 金融分布式账本技术安全规范
[6] 金融分布式账本技术应用 评价指标
[7] 金融分布式账本技术应用 技术参考架构
[8] 信息技术 区块链和分布式记账技术 参考架构