ICS 35.240
CCS L 70

DB31

上 海 市 地 方 标 准

DB31/T 1331—2021

区块链技术安全通用要求

General requirements of blockchain technology security

2021-12-07 发布　　2022-03-01 实施

上海市市场监督管理局　　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。

本文件由上海市经济和信息化委员会提出并组织实施。

本文件由上海市经济和信息化委员会、中共上海市委网络安全和信息化委员会办公室归口。

本文件起草单位：上海市信息安全测评认证中心、苏州同济区块链研究院有限公司、上海七印信息科技有限公司、上海墨珩网络科技有限公司、电信科学技术第一研究所有限公司。

本文件主要起草人：陈清明、顾敏、罗新辉、徐御、金铭彦、徐鑫、陈序、甘露、王一帆、阚肖庆、马小峰、吴鹏、陈小虎。

区块链技术安全通用要求

1 范围

本文件规定了区块链技术的技术架构、风险分析、安全要求等内容。

本文件适用于基于区块链技术的产品或应用的安全设计、开发、测试及维护。

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/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GM/T 0005 随机性检测规范

3 术语和定义

GB/T 25069 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位，通常由一系列交易和一些关于区块的元信息组成。

3.2

节点 node

具有特定功能的区块链组件。

3.3

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

3.4

共识机制 consensus mechanism

在分布式节点间达成共识的规则和程序。

3.5

智能合约 smart contracts

以数字形式定义的能够自动执行条款的合约。

3.6

对等网络 peer-to-peer network

一种仅包含对控制和操作能力等效的节点的计算机网络。

[来源：GB/T 5271.18—2018，18.04.05]

3.7

联盟链 consortium blockchain

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。

3.8

私有链 private blockchain

私有链的写入权限由某个组织或机构控制，数据读取权限受组织规定。

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)

CA 认证机构(Certificate Authority)

CAP 一致性(Consistency)、可用性(Availablity)、分区容错性(Partition)

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

DNS 域名系统(Domain Name System)

IPSec Internet 协议安全性(Internet Protocol Security)

P2P 对等网络(peer-to-peer network)

TLS 传输层安全性(Transport Layer Security)

5 区块链技术架构

为了便于分析，结合最佳实践和已知区块链风险分布情况，本文件提出区块链技术的三层技术架构，基础设施层将传统网络安全与区块链安全联系起来，协议层基于基础设施层提供的硬件或网络基础体系实现相应功能，并为扩展层提供相应功能的支持服务。协议层包含区块链技术的几大关键机制：共识机制、密码学机制、时序机制以及组网机制，协议层向下连接基础设施层，向上连接扩展层。扩展层通过调用协议层功能组件，可以提供多元化的服务与访问。三层技术架构如图 1 所示。

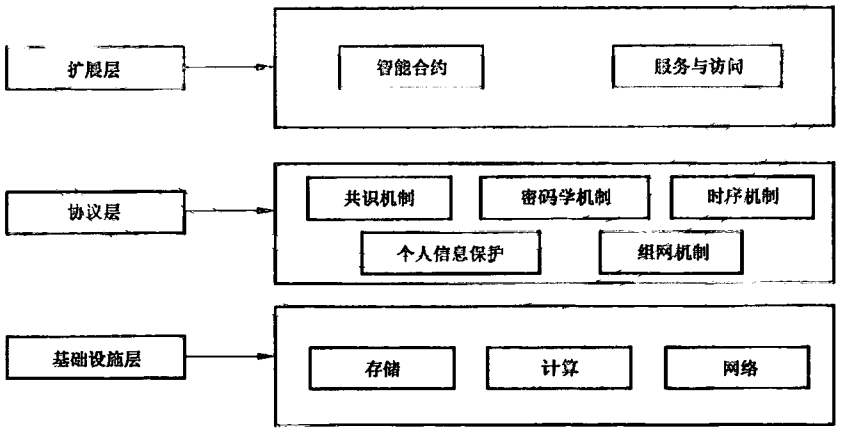

图 1 区块链技术架构

6 风险分析

6.1 基础设施层

6.1.1 存储

存储面临的安全风险主要为物理环境的安全风险，包括但不限于：

a) 设备遭盗窃和破坏；
b) 由雷击等恶劣天气导致的电流异常，设备出现故障；
c) 未提供备用电力供应；
d) 电磁干扰引起的设备故障。

6.1.2 网络

网络为区块链信息系统的运行提供必要的网络通信支持，安全风险包括但不限于：

a) 网络架构缺陷：
   1) 网络设备的业务处理能力无法满足业务高峰需求；
   2) 未实施网络区域隔离，导致网络的未授权访问；
   3) 未配置硬件冗余，导致网络不可用。
b) 通信传输不可靠：
   未对通信链路进行安全加密，导致数据泄露。
c) 网络攻击：
   1) DDOS 攻击；
   2) 病毒木马攻击；
   3) DNS 污染；
   4) 路由广播劫持。

6.1.3 计算

计算为区块链信息系统的运行提供必要的硬件设备支持，安全风险包括但不限于：

a) 设备配置不当：
   1) 未授权登录；
   2) 弱口令账户；
   3) 未启用审计。
b) 未对需要集中管控的设备进行集中管控。

6.2 协议层

6.2.1 共识机制

共识机制的安全风险包括但不限于：

a) 由共识机制自身设计漏洞导致的安全风险：
   1) 根据 CAP 准制，一个分布式系统最多只能同时满足一致性、可用性和分区容错性中的两条。因而共识机制可能面临可用性和一致性的选择，当节点或网络连接失效时，可能存在共识无法收敛、收敛时间较长超出可用范围、记录分叉等安全风险。
   2) 当攻击者算力达到一定比例时，存在恶意节点控制共识进程的安全风险。
   3) 攻击者采用双花攻击、女巫攻击等方式，达到双重支付、回滚记录、获得网络控制权等攻击目的。
b) 实际应用场景下的共识安全风险：
   1) 在联盟链的场景下，联盟参与者和节点数较少，联盟成员通过共谋，绕过共识机制的限制，任意修改链上数据；
   2) 不同的场景对安全性、扩展性、性能效率的需求不同，因共识算法选择不当可能导致安全风险。

6.2.2 密码学机制

密码学机制面临的安全风险包括但不限于：

a) 来自密码算法的安全风险：

1) 密码算法自身设计存在安全风险；

示例：如哈希算法面临碰撞威胁；

2) 密码算法开发实现中存在后门和漏洞。

b) 来自密钥的安全风险：密钥生成、分发、存储过程中因人员操作或管理不当带来的安全风险，包括密钥丢失被盗等。

6.2.3 时序机制

时序机制面临的安全风险包括但不限于：

a) 区块链节点未做时间同步，或时间同步过程被非法入侵，造成节点同步时间造成区块链共识协议的允许误差范围；

b) 时间戳不可信。

6.2.4 个人信息保护

区块链的个人信息保护是指通过密码学手段，保障用户身份、交易内容等个人信息安全。个人信息保护面临的安全风险包括但不限于：

a) 身份信息泄露的安全风险：用户的身份信息、物理地址、IP 地址与区块链上的用户公钥、地址等公开信息之间存在关联关系。

b) 交易信息泄露的安全风险：

1) 攻击者通过关联分析，可以推测出交易数据背后有价值的敏感信息；

2) 未授权节点访问交易数据。

6.2.5 组网机制

P2P 组网机制面临的安全风险包括但不限于：

a) 由 P2P 技术缺陷带来的安全风险：

1) P2P 网络节点准入要求极低，与专业服务器相比安全漏洞多、防护差，黑客容易针对少量关键节点发起网络路由攻击或者直接入侵，通过日蚀攻击获得利益；

2) 攻击者针对 P2P 网络缺少身份认证、数据验证、网络安全管理等机制的不足，发布有害信息，传播蠕虫、木马、病毒，实施 DDoS 攻击、路由攻击等。

b) 由设备故障导致的安全风险：因节点故障、网络连接断裂带来的组网安全风险，导致数据不一致、拒绝服务、节点隔离等。

6.3 扩展层

6.3.1 智能合约

智能合约面临的安全风险包括但不限于：

a) 合约内容的安全风险：

1) 编译语言不成熟，直接危害智能合约的执行和用户的个人数字资产；

2) 合约代码存在漏洞，导致交易依赖攻击、时间戳依赖攻击、调用深度攻击、可重入攻击、整数溢出攻击等安全风险；

3) 合约内容不符合相关法律规范。

b) 合约运行的安全风险：

1) 智能合约的运行环境没有与外部隔离，导致系统遭受攻击。
2) 在调用智能合约时涉及类型匹配、可容纳的交易数量限制、堆栈限制以及调用逻辑等。恶意攻击者可利用配置错误或者逻辑漏洞，对合约进行攻击。
3) 智能合约访问外部数据时，不能保证不同节点访问的数据的一致性和真实性，也无法避免数据提供节点恶意变更数据或被攻击引起单点失效的问题。

6.3.2 服务与访问

区块链的服务与访问面临的安全风险包括但不限于：

a) 由权限控制管理问题导致的安全风险：
   1) 非法用户接入。如未被标识用户从接口接入。
   2) 非授权访问。

示例：如非法用户进入网络或系统进行非法操作或合法用户超越授权范围进行操作。

b) 由区块链自身机制和开源软件导致的安全风险：
   1) 缺乏安全管理机构及监管审计机构参与管控区块链信息系统。区块链追求去中心化的设计，使得监管部门难以准确定位主体，从而出现监管盲区，导致数据泄露、非法交易等问题。
   2) 开源区块链软件因开发问题引发输入验证、API 使用、内存管理等方面的安全漏洞。

7 安全要求

7.1 概述

本章给出了基础设施层安全要求、协议层安全要求以及扩展层安全要求。除此之外，有助于理解安全要求的实现，在附录 A 和附录 B 中分别给出了协议层安全措施举例和扩展层安全措施举例。

7.2 适用范围

基础设施层、协议层、扩展层安全要求的适用范围如表 1 所示。

表 1 安全要求适用范围

序号	安全要求	适用范围
1	7.3.1	联盟链和私有链
2	7.3.2	联盟链和私有链
3	7.3.3	联盟链和私有链
4	7.4.1 a)	联盟链和私有链
5	7.4.1 b)	联盟链
6	7.4.1 c)	联盟链
7	7.4.1 d)	联盟链和私有链
8	7.4.1 e)	联盟链和私有链
9	7.4.2	联盟链和私有链
10	7.4.3	联盟链和私有链
11	7.4.4 a)	联盟链和私有链
12	7.4.4 b)	联盟链和私有链

表 1 安全要求适用范围（续）

序号	安全要求	适用范围
13	7.4.4 c)	联盟链
14	7.4.5 a)	联盟链
15	7.4.5 b)	联盟链和私有链
16	7.4.5 c)	联盟链和私有链
17	7.4.5 d)	联盟链和私有链
18	7.4.5 e)	联盟链和私有链
19	7.4.5 f)	联盟链
20	7.5.1.1	联盟链和私有链
21	7.5.1.2 a)	联盟链和私有链
22	7.5.1.2 b)	联盟链和私有链
23	7.5.1.2 c)	联盟链和私有链
24	7.5.1.2 d)	联盟链和私有链
25	7.5.1.2 e)	联盟链和私有链
26	7.5.1.2 f)	联盟链和私有链
27	7.5.1.2 g)	联盟链和私有链
28	7.5.1.2 h)	联盟链
29	7.5.2	联盟链和私有链

7.3 基础设施层安全

7.3.1 存储安全

应符合 GB/T 22239 规范中给出的安全物理环境相关要求。

7.3.2 网络安全

网络方面的安全要求包括：

a) 应符合 GB/T 22239 规范中给出的安全通信网络相关安全要求；

b) 应符合 GB/T 22239 规范中给出的安全区域边界相关安全要求。

7.3.3 计算安全

计算方面的安全要求包括：

a) 应符合 GB/T 22239 规范中给出的安全计算环境相关安全要求；

b) 应符合 GB/T 22239 规范中给出的安全管理中心集中管控的相关安全要求。

7.4 协议层安全

7.4.1 共识机制安全

共识机制方面的安全要求包括：

a) 应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击；

b) 应确保多个节点参与共识和确认，防止任何独立节点的恶意操作；

c) 应采用技术手段保证各节点账户记录的一致性；
d) 宜支持多种共识算法并实现共识算法可插拔，根据需求切换选择共识算法；
e) 宜提供根据网络规模、参与方数量、交易吞吐量等需求调整算法规模的功能。

7.4.2 密码学机制安全

密码学机制方面的安全要求包括：
a) 应采用满足国家商用密码相关规定的密码技术和服务，如国密算法 SM2、SM3、SM4 等；
b) 应使用非对称加密算法，用于信息加密、数字签名和登录认证等场景；
c) 应具备明确的密钥管理方案；
d) 宜使用第三方 CA 机构签发的数字证书来进行数字签名和签名验证等相关工作，确保信息的机密性、完整性和不可抵赖性；
e) 使用随机数时，应符合 GM/T 0005—2012 相关要求。

7.4.3 时序机制

时序机制方面的安全要求包括：
a) 应采用技术措施保证账本记录的时序一致性；
b) 宜使用由第三方时间戳服务机构产生的时间戳，使用可信时间源服务，保证时间戳可信性。

7.4.4 个人信息保护

个人信息保护方面的安全要求包括：
a) 应采用满足国家商用密码相关规定的加密方式来保护个人信息的处理、传输和存储；
b) 应提供数据变换技术，将个人敏感信息进行变换；

示例 1：如数据加密、敏感数据脱敏等手段。

c) 宜采用技术手段实现个人信息保护功能，将个人敏感信息存放到侧链上或链下，而不存储在公开的主链上等。

示例 2：如侧链技术、链下存储等。

7.4.5 组网机制安全

组网机制方面的安全要求包括：
a) 应提供节点服务器之间的身份认证；
b) 应支持动态加入和删除节点，且不影响业务的正常运行；
c) 应确保节点断线重连后，可与其他节点实现状态一致性；
d) 应在节点与节点之间建立安全的信息传输通道，支持国家商用密码实现的 TLS、IPSec 通信协议；

示例：如 TLS、IPSec 等协议。

e) 节点应对区块链网络中提交的相关信息进行有效性验证；
f) 应具备检测和防范恶意节点的机制，能够检测出网络中的恶意节点，并进行针对性的处理。

7.5 扩展层安全

7.5.1 智能合约安全

7.5.1.1 智能合约编写安全

智能合约编写方面的安全要求包括：
a) 应按照合约文本编写合约代码，确保合约代码与合约文本的一致性；
b) 应建立安全编码规范，智能合约源代码应符合规范要求，确保智能合约的安全性；

c) 智能合约应定义版本号，调用智能合约时应明确记录智能合约版本；
d) 智能合约应具有向后兼容性，智能合约升级或重新部署后，新智能合约能兼容或迁移原智能合约数据。

7.5.1.2 智能合约运行安全

智能合约运行方面的安全要求包括：
a) 应提供智能合约的升级和废止功能，应支持动态升级，智能合约的升级操作应记录在区块中，符合区块链交易要求、遵从交易执行的流程；
b) 应提供合约安全检测手段，确保及时发现和处置出现的问题，降低安全风险；
c) 应控制智能合约对外部环境的访问，控制隔离执行环境中的智能合约访问其执行环境之外的资源；
d) 当智能合约出现错误时，应提供智能合约冻结功能，冻结状态下的智能合约不能被继续调用；
e) 应提供运行载体，如虚拟机等，智能合约应在虚拟机等隔离环境中运行；
f) 对于与区块链信息系统外部数据进行交互的智能合约，外部数据的影响范围仅限于智能合约范围内，不应影响区块链信息系统的整体运行；
g) 应严格限制智能合约的部署，防止同链的其他合约以及本链以外的合约调用本合约引起的安全风险；
h) 宜提供有效的防范智能合约被恶意滥用的机制。如：多次调用无意义操作，从而造成 DDoS 攻击，使区块链信息系统瘫痪。

7.5.2 服务与访问安全

7.5.2.1 权限控制

权限控制方面的安全要求包括：
a) 接口应根据业务需求实施权限管理，防止未授权的访问和调用，针对不同的用户配置不同的访问权限；
b) 应设置操作限制，防止攻击者通过大量频繁操作，造成区块链服务性能严重下降；
c) 若支持多链架构的数据共享，应设计和实现多链架构的数据安全共享和隔离；
d) 应支持区块链节点版本升级，在升级前须在测试环境进行验证，保证升级过程中的业务平滑过渡；
e) 区块链节点版本应具有后向兼容性，区块链节点升级后仍支持旧版本的数据。

7.5.2.2 安全审计

安全审计方面的安全要求包括：
a) 应提供安全审计功能，对重要操作进行审计；
b) 所有操作行为应被记录，实现不可更改并可被查询，做到可审计、可追溯。

7.5.2.3 内容安全

内容安全方面的安全要求包括：
a) 区块链信息系统提供信息服务时，应建立审核机制，保证传播和存储的内容符合相关法律法规的要求；
b) 对审核发现的链上违法信息、不良信息，应保证能够追溯到信息发布节点。

附 录 A
（资料性）
协议层安全措施举例

为有效应对区块链协议层安全风险，表 A.1 列举了部分协议层安全措施。

表 A.1 协议层安全措施举例

文件条款	安全措施
7.4.1 共识机制安全	a) 加强共识协议在容错性上的设计，使得其可以容忍一定范围的节点物理或网络故障导致的非恶意节点断线和网络分区，并且能够抵御合谋攻击、女巫攻击等恶意攻击行为； b) 针对区块链网络中的未授权节点或恶意节点实施必要的节点/数据安全验证； c) 通过引入链外可信第三方的方式来增强联盟链的数据不可篡改性； d) 根据业务场景选择多种或可切换的共识算法
7.4.2 密码学机制安全	a) 使用满足国家商用密码相关规定的安全可靠的密码机制，密码实现过程中进行有效的代码混淆； b) 使用多种存储方式保障私钥安全
7.4.4 个人信息保护	a) 使用多通道、隔离账本，例如 fabric 的通道(Channel)机制，实现账本隔离，保护隐私； b) 使用群签名对身份匿名
7.4.5 组网机制安全	a) 采用核心节点冗余配置，保障在断网断线情况下的业务可用性； b) 合理设置对等网络节点的连接数目、更新机制、异常检测机制等

附 录 B
（资料性）
扩展层安全措施举例

为有效应对区块链扩展层安全风险，表 B.1 列举了部分扩展层安全措施。

表 B.1 扩展层安全措施举例

文件条款	安全措施
7.5.1 智能合约安全	a) 针对合约代码漏洞，采用形式化验证等方式进行合约代码安全性分析，在合约部署上线前尽可能消除漏洞，降低安全风险； b) 在智能合约运行环境中完成代码的执行与动态安全检测； c) 对区块链信息系统服务器进行定期漏洞扫描检查包括但不限于服务器本身的漏洞、区块链账本的漏洞、智能合约的漏洞，并对发现的安全漏洞和隐患提出修复方案并修复
7.5.2 服务与访问安全	a) 根据业务需求，做好接口的权限管理，防止未授权的访问和调用； b) 将每一次权限操作写入日志，尤其是敏感信息的查看和使用，以便复查和审计，做到可审计、可追溯； c) 按需将监管要求写进智能合约强制执行

参 考 文 献

[1] GB/T 5271.18—2018 信息技术 词汇 第18部分:分布式数据处理
[2] T/SHBTA 002—2019 区块链底层平台通用技术要求
[3] T/SSIA 0002—2018 区块链技术安全通用规范
[4] GM/T 0005—2012 随机性检测规范

上 海 市 地 方 标 准

区块链技术安全通用要求

DB31/T 1331—2021

*

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
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 1.25　字数 32 千字
2022 年 1 月第一版　2022 年 1 月第一次印刷

*

书号:155066·5-3927　定价　21.00 元

DB31/T 1331-2021

码上扫一扫　正版服务到