

四川省智慧城乡大数据应用研究会团体标准

T/ADEDS 02—2024

政务服务区块链技术跨链接入和交互规范

Government Service Blockchain Technology Cross-Linking and Interaction
Specification

2024 - 02 - 20 发布

2024 - 03 - 01 实施

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 跨链可信通道 Cross-Chain Trusted Channel	1
3.2 跨链适配器 Cross-Chain Adapter	1
3.3 业务链 destination chain	1
3.4 源链 source chain	1
3.5 目标链 destination chain	1
4 缩略语	1
5 跨链原则	2
5.1 互操作性原则	2
5.2 安全性和隐私保护原则	2
5.3 数据标准原则	2
5.4 数据共享和访问	2
6 跨链技术	2
7 跨链接入流程和监管要求	2
7.1 跨链接入流程概述	2
7.2 跨链初始配置	4
7.3 跨链网络接入	4
7.4 跨链资源调用	5
8 跨链交互机制	7
8.1 智能合约开发	7
8.2 跨链交互发起	7
8.3 跨链交互执行	8
8.4 动态组链交互	8
9 跨链数据安全	8
9.1 链上数据管理	8
9.2 跨链机制安全要求	9
9.3 跨链交互安全保障	9
参考文献	11

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。

本文件由四川省大数据中心提出。

本文件由四川省智慧城乡大数据应用研究会归口。

本文件起草单位：四川省大数据中心，电子科技大学，四川省科学技术厅，德阳市政务服务和大数据管理局，成都市武侯区行政审批局，成都市规划和自然资源信息中心，四川省环境信息中心，四川省卫生健康信息中心，四川省省级住房公积金管理中心，成都星辰链网科技有限公司，迅鰩成都科技有限公司，成都交子区块链产业创新中心有限公司，四川省计算机研究院，四川迅鰩科技有限公司，中国电信四川公司，四川省电子政务运营中心，上海汉邦京泰数码技术有限公司，四川华西集采电子商务有限公司，大汉软件股份有限公司，浪潮软件股份有限公司。

本文件主要起草人：夏琦，张军，陈瑞东，乐益矣，解岩，赵斌，方从刚，张伟，郑博，冯暄，曾铮，高建彬，夏虎，毛云鹏，李继涛，邓忆德，阎洁，姚敏，蔡友保，高靡靡，袁博，李晓寒，张雨，童亮，赵朋，徐菡，李秋芳，陈玲，荀斌，陈璟，任墨海，姚刚，康友宏，文冠人，张文阳，陈松柏，黄康，吕一新，王鹏，吴亚泽，阮亚芬，李飞，缪春兰，王贝贝，陈庆，李子欣，刘洋洋，陈伟，唐文华，李宛霖，朱景熙，马江勃，任俊燊，冯新新，龚莎莎，陈绪阳，周玉瑗，张晨，陈亮，韩旭。

政务服务区块链技术跨链接入和交互规范

1 范围

本标准提出了政务服务区块链技术跨链接入和交互规范，主要包括跨链原则、技术、流程、监管、交互、安全等。

本标准适用于四川省各地各部门，政务服务相关技术公司和第三方服务机构等，为四川省省级区块链政务服务平台与国家区块链平台、各级各部门与省级区块链政务服务平台对接等提供标准化、规范化依据和协同化、一体化服务。

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/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 42752—2023 区块链和分布式记账技术 参考架构

C0167-2023 全国一体化政务服务平台区块链基础支撑平台技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

跨链可信通道 Cross-Chain Trusted Channel

跨链可信通道是构建跨链网络的关键组件，充当不同区块链网络之间的桥梁，使不同链之间可以进行信息数据的交互。用于接入机构的业务应用、业务链与跨链网络的连接，跨链网络由多个跨链可信通道相互连接组成。

3.2

跨链适配器 Cross-Chain Adapter

跨链适配器是连接不同区块链网络的关键组件，不同的区块链网络可能使用不同的协议、数据格式和交互规则，跨链适配器充当了解和适应这些不同规则的桥梁，使得不同区块链网络可以彼此交互。用于接入机构的业务区块链网络，调用本地服务获取链上数据资源。

3.3

业务链 destination chain

接入机构业务使用的区块链网络。

3.4

源链 source chain

在跨链协议中，主动发起跨链请求的一方。

[来源：GB/T 42570-2023]

3.5

目标链 destination chain

在跨链协议中，被动接收跨链请求的一方。

[来源：GB/T 42570-2023]

4 缩略语

下列缩略语适用于本文件。

CCTC：跨链可信通道，Cross-Chain Trusted Channel

CCA: 跨链适配器, Cross-Chain Adapter

CCIP: 跨链交互协议, Cross-Chain Interoperability Protocol

5 跨链原则

跨链接入应满足以下原则:

5.1 互操作性原则

政府服务系统之间必须具备互操作性, 以便无缝地共享数据和交互。

5.2 安全性和隐私保护原则

跨链接入应该确保数据的安全性和隐私保护, 包括身份验证和访问控制机制。

5.3 数据标准原则

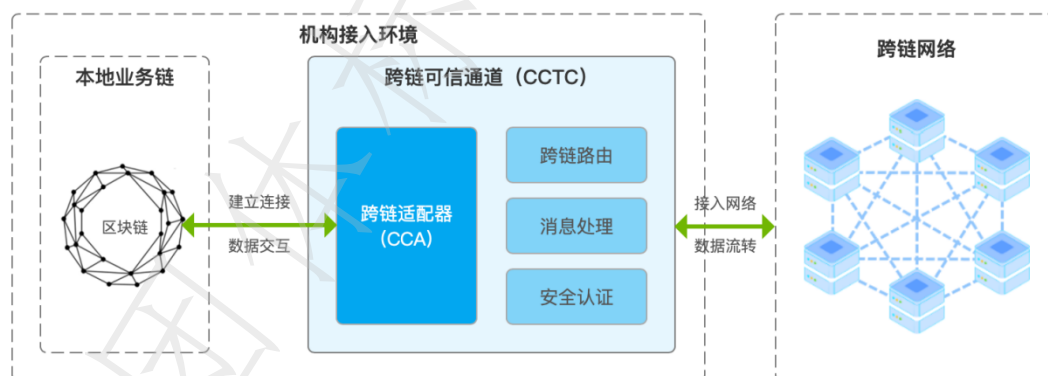
政府部门规定数据格式和标准, 以确保数据的一致性和可理解性。

5.4 数据共享和访问

政府部门定义数据共享和访问的规则和流程, 包括数据的共享权限和条件。

6 跨链技术

跨链接入应通过跨链可信通道、跨链适配器等实现, 由跨链可信通道组成跨链网络, 跨链适配器负责连接本地业务链, 并将信息数据通过跨链可信通道传递到跨链网络, 如图1所示。



7 跨链接入流程和监管要求

7.1 跨链接入流程概述

由接入机构向主管部门发起接入申请, 准备本地跨链接入的资源及环境, 并开发本地业务链的跨链适配器。主管部门为接入机构分配平台账户、发放账户密钥, 部署并分配跨链可信通道。接入机构通过平台配置本地业务链, 安装跨链适配器。主管部门部署跨链适配器并监测业务链运行情况。跨链接入的主要步骤如图2所示。

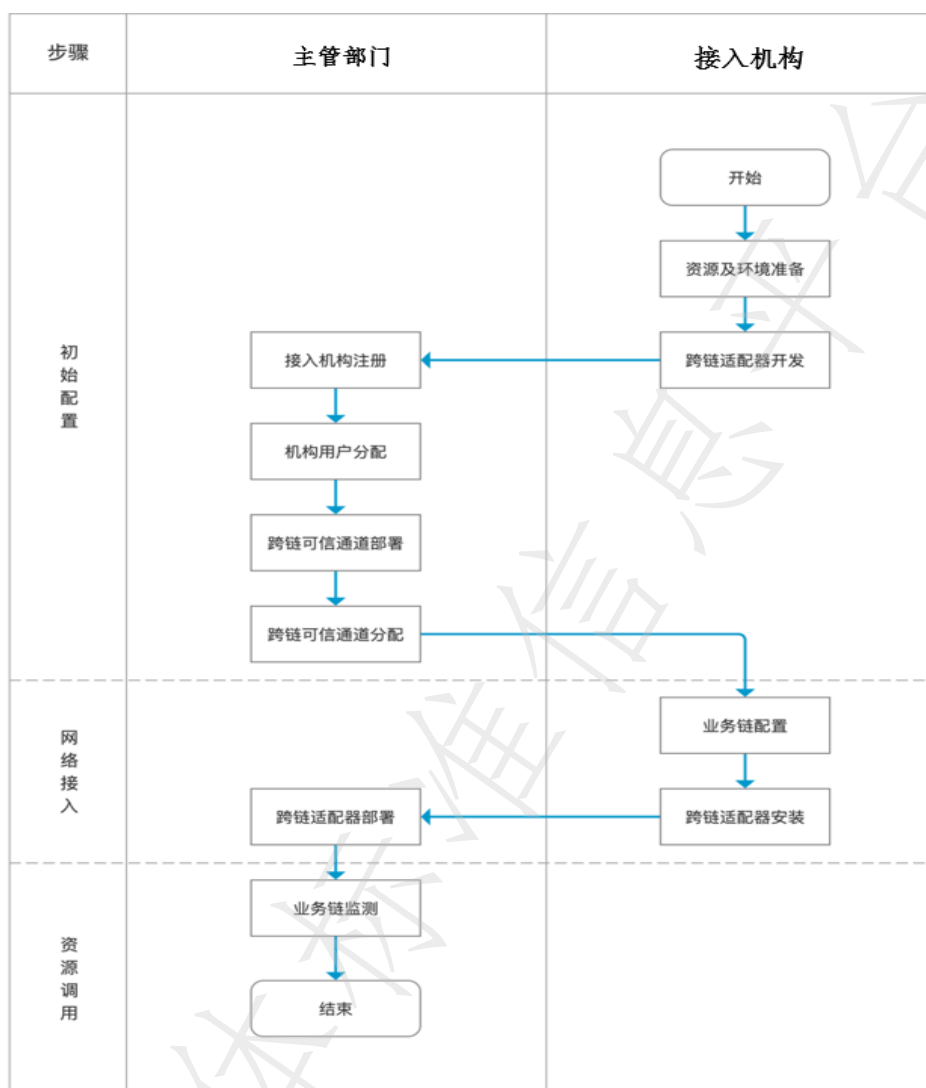


图2 跨链接入实施步骤图

- a) 资源及环境准备
接入机构为跨链接入准备服务器资源、运行环境及网络环境。
- a) 跨链适配器开发
接入机构按照跨链适配器开发规范开发与本地业务链相匹配的跨链适配器。
- b) 接入机构注册
主管部门为接入机构分配跨链账户，生成跨链账户密钥。
- c) 机构用户分配
主管部门为接入机构创建跨链平台用户。
- d) 跨链可信通道部署
主管部门将跨链可信通道部署至接入机构提供的服务器资源。
- e) 跨链可信通道分配
主管部门将跨链可信通道分配给相应的接入机构。
- f) 业务链配置
接入机构将本地业务链注册到跨链平台。
- g) 跨链适配器安装
接入机构将跨链适配器程序包上传至平台。
- h) 跨链适配器部署

主管部门将跨链适配器部署至接入机构的跨链可信通道。

i) 业务链监测

主管部门监测接入机构业务链运行情况。

7.2 跨链初始配置

跨链初始配置应满足以下要求：

7.2.1 资源及环境准备

由接入机构提供2台服务器资源供安装跨链可信通道使用，需连接电子政务外网并可访问本地业务区块链网络，具体配置及环境建议如下：

资源名称	配置	备注
服务器	CPU: 4核以上, 2.0GHz以上, 4M缓存; 内存: 16G 以上; 硬盘: 500G以上; 网卡: 高性能千兆网卡;	
网络环境	带宽: 100Mbps以上; 其它: 可访问本地区块链网络	
操作系统	系统版本: CentOS; 操作账户: root账号	

7.2.2 跨链适配器开发

接入机构根据本地业务链特点开发与之相匹配的用于连接该业务链的跨链适配器，跨链适配器与业务链一一对应。

跨链适配器作为不同区块链网络之间数据交换和格式转换的桥梁，需确保适配器能够实现跨链交互的逻辑和规则，同时保证性能和安全性。

7.2.3 网络环境准备

主管部门跨链平台运行在电子政务外网环境，各接入机构需按照跨链平台部署网络配置，将本地跨链可信通道的网络环境与主管部门网络映射双向联通，具体操作参考如下：

- a) 接入机构提供的部署跨链可信通道的服务器资源需具备电子政务外网网络环境，且可访问本地业务链网络；
- b) 接入机构提供的部署跨链可信通道的服务器资源需开放以下端口，以便主管部门 IP 访问跨链可信通道；
 - 9806：跨链可信通道入口，监听端口接收消息。
 - 9807：跨链可信通道出口，端口发送消息。
- c) 接入机构提供的部署跨链可信通道的服务器资源需开放访问外部地址的权限，即能访问主管部门 IP。

7.3 跨链网络接入

跨链网络接入应满足以下要求：

7.3.1 接入机构

a) 接入机构注册

由主管部门统一为接入机构分配账户，主管部门通过跨链管理平台为各接入机构注册，为其创建跨链账户作为唯一身份标识，并发放账户密钥用于跨链网络接入的身份验证。

字段名称	含义	备注
机构名称	接入机构的名称	
机构地址	接入机构的地址	
机构联系人	接入机构的联系人	
机构联系方式	接入机构的联系方式	
机构跨链账户	接入机构的跨链网络唯一身份标识	由主管部门定义

上表（续）

字段名称	含义	备注
跨链账户密钥	接入机构接入跨链网络的身份验证密钥	由主管部门发放

b) 机构用户分配

由主管部门通过跨链管理平台统一为各接入机构创建登录用户，创建完成后将用户名/密码等信息告知各接入机构。

字段名称	含义	备注
用户名	接入机构的跨链平台登录用户名	由主管部门定义
密码	接入机构的跨链平台的用户密码	
所属机构	接入机构	

c) 跨链可信通道部署

接入机构资源到位后由主管部门在接入机构提供的资源上部署跨链平台的跨链可信通道。跨链可信通道通过内部调用适配器获取链上信息，通过各方适配器自主调用业务链，调用过程需要完成签名验证等一系列安全认证。

d) 跨链可信通道分配

由主管部门通过跨链管理平台统一为接入机构分配跨链可信通道，配置通道基本信息及连接IP地址、端口信息。

7.3.2 跨链网络接入流程

实现跨链网络接入需要确保不同区块链网络能够连接、通信和协作。通过不同区块链网络之间的跨链网络接入，为后续的跨链交互和数据共享打下了基础。

接入机构登录主管部门跨链应用系统进行业务链配置及跨链适配器安装（注：访问跨链应用需要电子政务外网环境，且完成相关网络环境配置）。

a) 业务链配置

由接入机构通过跨链应用将本地业务链添加到跨链网络中。

字段名称	含义	备注
业务链标识	业务区块链的唯一标识	跨链平台生成
业务链名称	业务区块链的名称	
所属机构	接入机构	
业务链类型	业务区块链技术类型，如Fabric、FISCO-BCOS或其它	
业务链用途	业务区块链的用途，如存放证照数据信息等	可提供多个用途
业务链节点数量	业务链的共识节点、记账节点数量、其他节点数量	
业务链区块高度	业务链区块高度	

b) 跨链适配器安装

各接入机构的跨链适配器开发完成后，将代码包上传至跨链平台中，并将跨链适配器关联对应的本地业务链。

提供跨链适配器的如下信息：

字段名称	含义	备注
适配器标识	接入机构的适配器唯一标识	跨链平台生成
适配器名称	接入机构的适配器名称	
所属业务链	接入机构适配器对应的业务链	
所属机构	接入机构跨链账户	

c) 跨链适配器部署

跨链适配器安装完成后由主管部门统一部署，与跨链平台进行联合调试。

7.4 跨链资源调用

跨链资源调用应满足以下要求：

7.4.1 跨链适配器使用

跨链适配器使用应满足以下要求：

各接入机构可以根据跨链开发标准规范实现一个本地业务链的跨链适配器，并通过跨链适配器将本地业务链接入跨链网络，跨链适配器与业务链一一对应。

a) 业务链访问

各接入机构根据本地业务链的结构及技术特性开发可访问业务区块链的服务，集成区块链SDK或相关API，获取业务链资源。

b) 跨链调用类型

跨链资源调用按照业务目标及链上操作内容等分为以下几种跨链调用类型：

1) 业务链监测

跨链平台获取已接入业务链的信息和状态，监测区块链运行情况。

2) 跨链读数据

接入机构根据业务需求，按照约定跨链读取其他机构业务链上的数据资源。

3) 跨链写数据

接入机构根据业务需要，按照约定跨链将数据写入其他机构的业务链。

7.4.2 业务链监管

各接入机构需按照以下服务标准提供本地业务链相关信息，通过本地跨链适配器向跨链平台开放相应服务。

a) 业务链信息服务

各接入机构提供本地业务链网络信息服务。

1) 服务名称

业务链区块链信息服务；

2) 输入信息如下：

字段名称	含义	备注
业务链名称	本地业务链名称	

3) 输出信息如下：

字段名称	含义	备注
操作结果	调用操作结果，如成功、失败	
结果描述	调用操作结果描述，如失败原因	
业务链信息	业务链名称：业务链名称 所属机构：业务链归属机构名称 共识方式：业务链共识方式 运行状态：业务链的运行状态 区块高度：业务链的区块高度； 交易量：业务链的链上交易总数量；节点列表：业务链节点名称、类型、运行状态（运行中、停止等）	

b) 业务链节点详情服务

各接入机构提供本地业务链网络信息服务。

1) 服务名称

业务链节点详情服务；

2) 输入信息如下：

字段名称	含义	备注
业务链节点名称	本地业务链节点名称	

3) 输出信息如下：

字段名称	含义	备注
操作结果	调用操作结果，如成功、失败	
结果描述	调用操作结果描述，如失败原因	

上表（续）

字段名称	含义	备注
节点信息	节点名称：业务链节点名称 内存占用（%）：业务链节点服务器内存占用 Cpu占用（%）：cpu当前占用 节点状态：节点运行状态 Cpu（核）：业务链节点服务器cpu核数 Cpu（线程）：业务链节点服务器cpu线程数	

8 跨链交互机制

跨链交互机制应包含以下内容：

8.1 智能合约开发

各接入机构根据数据资源调用需求开发统一协作连的链上智能合约，以约定跨链的具体交互操作内容，确保跨链交互有效执行。

8.2 跨链交互发起

通过跨链交互发起，不同机构和单位能够安全、高效地共享数据和资源。跨链交互发起应包含以下流程：

数据跨链调用

数据需求机构的跨链业务应用通过跨链可信通道提供的服务调用其他机构的数据资源。

a) 服务名称

数据跨链调用服务

b) 输入信息如下：

字段名称	含义	备注
调用类型	跨链数据调用类型，如查询、交易等	
调用用途	跨链数据调用的用途，如信息验证、资料补充等	
路由地址	调用数据资源所在的地址路径，格式为接入机构标识：业务链标识：数据资源标识	
智能合约	使用的智能合约标识、版本等信息	
跨链账户	数据调用方的跨链账户	

c) 输出信息如下：

字段名称	含义	备注
调用结果	跨链数据调用操作结果，如成功、失败	
调用结果描述	跨链数据调用操作结果描述，如失败原因	
调用任务编号	跨链数据调用的任务编号	用于通过任务编号获取结果数据资源

8.2.1 跨链结果返回

通过跨链结果返回，数据需求机构能够获取他们在跨链交互中所需的数据和资源。

数据跨链调用服务采用异步通信方式，数据需求机构调用数据跨链调用服务后，需通过此服务获取返回的需求数据资源。

a) 服务名称

跨链结果返回

b) 输入信息如下：

字段名称	含义	备注
调用任务编号	跨链数据调用的任务编号	

c) 输出信息如下：

字段名称	含义	备注
任务结果	跨链数据调用操作结果，如成功、失败	
任务结果描述	跨链数据调用操作结果描述，如失败原因	
调用任务信息	跨链数据调用的任务编号、路由地址	
结果数据资源	跨链数据调用的结果数据资源列表，如{字段 1 名称: 字段 1 值, 字段 2 名称: 字段 2 值,}	可通过数据提供方所配置的数据资源表对照返回字段信息

8.3 跨链交互执行

跨链交互执行是推动区块链互操作性和数据共享的关键环节，为不同区块链网络之间的协作和创新提供了技术支持。

8.3.1 跨链交互协议数据构造

跨链跨链可信通道将接受到的跨链调用请求构造为CCIP跨链交互协议的数据结构，并交由统一协作链进行处理。

8.3.2 跨链交互行为共识

统一协作链接收CCIP数据结构跨链交互请求，对跨链交互行为进行共识，并将共识结果上链存证。

8.3.3 数据资源调用服务

a) 业务链访问

各接入机构根据本地业务链的结构及技术特性开发可访问业务区块链的服务，集成区块链SDK，获取链上数据资源。

b) 链上数据交互

访问本地业务链上的数据资源，按照跨链交互请求提供所需数据。

8.4 动态组链交互

为确保跨链交互的有效性和可行性，必须满足以下动态组链功能的要求：

- 应提供灵活的参数设置和规则定义，以适应不同类型的交互和业务需求；
- 根据业务需求和网络状况自动调整跨链通信路径，确保数据传输的稳定和高效；
- 支持动态组链配置管理功能，例如动态组链场景配置、场景创建、组员管理等；
- 应支持链操作管理系统的动态组链策略，执行基于场景的不同业务链跨层级、跨架构重组。

9 跨链数据安全

9.1 链上数据管理

9.1.1 数据分类

以数据对象的类别为依据，在分布式数据平台中，区块链上链数据需包含以下类别：

- 账户数据：区块链事务的实际发起者和相关方的数据，区块中记录的事务信息均被关联到相关的账户之上；
- 区块数据：区块链网络的底层链式数据，用来将一段给定时间内发生的事务处理结果持久化为成块链式数据结构；
- 事务数据：区块链系统上承载的具体业务动作的数据；
- 实体数据：事务的静态属性的数据，包括发起方地址、接收方地址、事务处理发生额和附加数据；
- 合约数据：事务的动态处理逻辑的数据，包括处理逻辑的可执行代码，处理逻辑的执行结果；
- 配置数据：区块链管理平台系统正常运行过程中所需的配置信息，包括软件版本号和网络通信底层对等节点配置信息等。

9.1.2 数据存储

区块链管理平台数据存储设施须满足GB/T 22239—2019三级及以上要求，为抵御常见的针对区块链账本的攻击，需满足以下要求：

- a) 节点数据应具备加密存储能力；
- b) 支持全节点，提供独立的、完整的数据存储能力；
- c) 宜提供批量数据从链上下载到本地数据库的服务；
- d) 宜提供区块链浏览器，上链数据的数据查找、定位、统计功能；
- e) 宜提供数据的概率分析、回归分析等功能；
- f) 应支持设置用户访问权限，数据信息应进行安全保护分级；
- g) 应具备一定容灾性功能，应保证当任意不超过区块链平台声明数量的节点发生故障，整个系统工作正常；
- h) 数据存储服务保证存储空间可扩展，防止耗尽存储空间攻击，满足高可用性。保证数据查询和更新等操作的响应时间满足上层协议和应用的要求。

9.1.3 数据监管

区块链设计时应为国家监管部门预留监管接口，监管方的共识节点在接收到数据之后，对数据进行监管校验，将符合监管校验条件的交易数据发送至存储空间进行数据存储：

- 引入更复杂的校验协议，对交易的合法性、用户的身份、交易的目的等进行更深入的检查；
- 校验不仅限于监管节点，也可以由网络中的其他节点进行，以确保网络的完整性和合法性；
- 监管节点实施实时监控，并建立一个审计日志系统，记录所有活动，在需要进行回溯和审计；
- 在智能合约中内嵌监管规则，确保所有执行的合约都符合监管要求。智能合约可以自动执行特定的监管逻辑，例如交易限额、用户身份验证、资金来源和去向的监控等。

9.2 跨链机制安全要求

跨链机制安全要求包括：

- a) 跨链具有拜占庭容错性；
- b) 一个区块链能够接收和验证另一个区块链的数据。区块链不能否认自己发送信息的行为和信息的内容，区块链确保验证过程的正确执行，不可被篡改；
- c) 对于支持数据或信息跨链的系统，由一个区块链发起的以变更双方状态为目的的跨链请求，需要满足或者在源链和目标链都执行成功，或者在两个链都执行失败；
- d) 具备跨链事务仲裁机制；
- e) 跨链消息中的隐私数据需要事先得到相应区块链的授权；敏感的跨链数据需要只被接收方获取，其他区块链或者链外服务不能获取；
- f) 保证跨链的交易不应被恶意重播，不存在双重支付问题。

9.3 跨链交互安全保障

跨链交互涉及不同部门区块链网络之间的数据交互，需要确保数据的隐私性、安全性和交互的可信度，保障信息数据在不同区块链网络之间的安全传输和交换。

9.3.1 跨链安全性和可靠性

跨链交互采用严格的验证和确认机制，确保交互合法、有效，并保证交互数据的安全性。跨链交互信息在跨链平台及外部系统间流转时均经过加密处理。

联盟链中，联盟成员主要可以分为两大类：政府机构和外部企业，区块链节点虽然是联盟成员自主组成，但针对政务服务场景的特殊性，为了保证联盟链网络的公信力和可信度，应提出以下要求：

- 确保政府机构和外部企业在节点控制上的平衡。政府机构控制的节点数量应至少等于或多于非政府机构控制的节点，以保持权力平衡，避免任何一方过度主导；

- 所有节点操作者必须通过严格的身份验证程序，确保只有授权的实体可以参与到网络中。此外，需要对不同类型的参与者（政府机构和外部企业）施加不同级别的权限，以防止未经授权的数据访问或更改；
- 建立一个透明且可审计的治理结构，确保所有成员的权利和责任明确。决策过程应公开，以便所有参与者和公众都能理解和监督；
- 采用先进的加密技术和安全措施来保护数据，防止未经授权的访问和篡改。确保数据的完整性是保持链的可信度的关键；
- 实施定期审计，检查联盟链的运作是否符合既定的标准和规则。审计结果应公开透明，让所有成员和公众都能访问。

9.3.2 跨链隐私保护措施

在跨链数据传输中，可能涉及用户隐私和敏感信息。平台采用国密加密技术确保数据在传输过程中的安全性和保密性。

9.3.3 跨链认证与信任建立

在不同区块链网络之间建立信任机制，确保跨链交互的可信度。平台采用数字签名、加密证书等方式进行交互身份验证，防止恶意访问的干扰。

9.3.4 智能合约的审计与验证

如果跨链交互涉及智能合约，需要对合约进行安全审计和验证，确保合约的逻辑和规则是安全和可信的。

参 考 文 献

- [1] GB/T 5271 信息技术 词汇
- [2] GB/T 18391 信息技术 数据元的规范与标准化
- [3] GB/T 25069 信息安全技术 术语
- [4] GB/T 28458 信息安全技术 安全漏洞标识与描述规范
- [5] T/ SIA 0072018 区块链平台基础技术要求
- [6] DB51/T XXXX—2022 四川省区块链技术应用标准规范
- [7] T/GZBD 7-202 主权区块链上链数据规范

全国团体标准信息平台