ICS 03.160
CCS S 922

四川省智慧城乡大数据应用研究会团体标准

T/ADEDS 01—2024

政务服务联盟区块链建设指南

Government Service Blockchain Technology Cross-Linking and Interaction Specification

2024－02－20 发布　　2024－03－01 实施

四川省智慧城乡大数据应用研究会　　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，迅鳐成都科技有限公司，四川省计算机研究院，四川迅鳐科技有限公司，成都交子区块链产业创新中心有限公司，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：张军，夏琦，解岩，乐益矣，陈瑞东，赵斌，熊红兵，方从刚，郑博，冯暄，曾铮，尹嘉奇，高建彬，夏虎，林晓东，李继涛，申谦，余庭山，姚敏，蔡友保，袁博，李晓寒，李凡，童亮，赵朋，张雨，徐菡，李秋芳，陈玲，苟斌，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，谢峰，李飞，缪春兰，王贝贝，陈庆，李子欣，刘洋洋，陈伟，唐文华，李宛霖，赖永波，陈利，冯新新，龚莎莎，陈绪阳，周玉瑗，张晨，陈亮，韩旭。

政务服务联盟区块链建设指南

1 范围

本标准提出了政务服务联盟区块链建设指南，主要包括政务服务联盟区块链总体架构、基础资源、底层组件、跨链交互、跨链监管等。

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、各地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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 42752—2023 区块链和分布式记账技术 参考架构

GB/T 30850.1 电子政务标准化指南 第1部分：总则

GB/T 30850.4 电子政务标准化指南 第4部分：信息共享

GB/T 30850.5 电子政务标准化指南 第5部分：支撑技术

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

区块链 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。

3.2

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。

3.3

业务链

根据政务服务平台公共应用场景的需要，结合业务需求拥有独立的数据存储、共识网络的区块链。

3.4

链操作管理系统

为各级各类政务服务联盟链提供统一配置管理与可视化交互的系统。

3.5

跨链监管系统

执行链操作管理系统调度，为各级各类政务服务联盟链与业务链提供统一跨链接入、动态组链、跨链交互、跨链监管服务的系统。

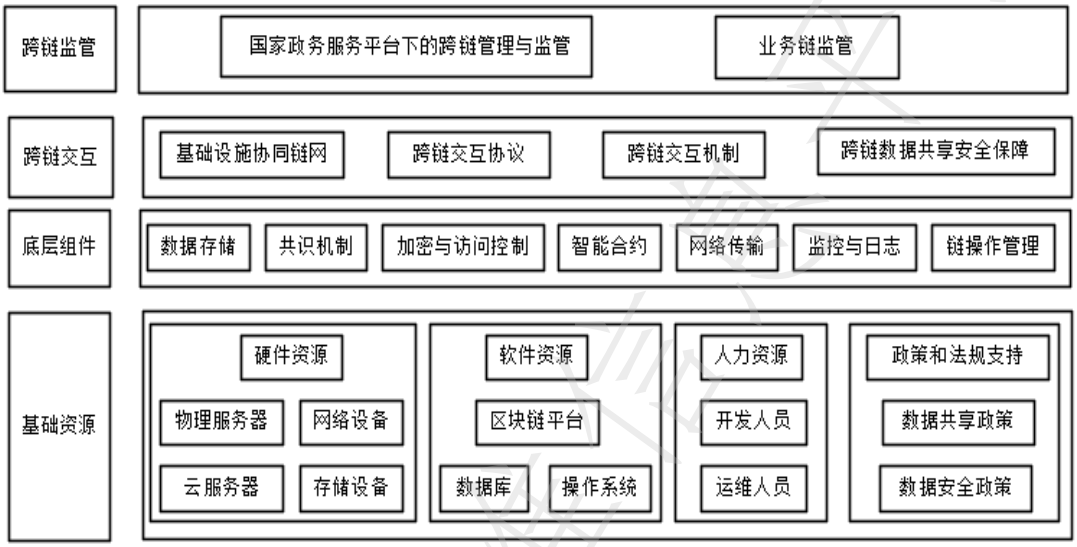
4 缩略语

下列缩略语适用于本文件。

COS：链操作管理系统，Chain Operation management System

CAS：跨链监管系统，Cross-Chain Audit Supervision System

5 总体架构



6 基础资源

6.1 硬件资源

a) 物理服务器

——应具备高性能的 CPU、足够的 RAM 和高速的 I/O，以满足大量交易和数据处理的需求；

——应具备物理安全措施，如机房的访问控制、视频监控等；

——为防止单点故障，应考虑部署多台服务器，实现负载均衡和故障切换。

b) 云服务器

——根据业务需求，能够快速增加或减少服务器资源

c) 存储设备

——应具备足够的存储容量，以满足长期的数据增长需求；

——高速的 SSD 可以提供更快的读写速度，满足高并发的交易处理；

——使用 RAID 或其他技术，确保数据的可靠性和持久性。

d) 网络设备

——应具备足够的网络带宽，以满足大量节点之间的通信需求；

——提供防火墙、入侵检测和防御系统，确保网络的安全性；

——网络设备应具备高可用性和故障切换能力

6.2 软件资源

a) 区块链平台

——平台应能够处理大量的交易和查询，满足政务需求；

——提供多种加密和签名机制，确保数据的安全性和完整性；

——支持智能合约和其他扩展功能，满足不断变化的业务需求。

b) 数据库

——数据库应具备高并发的读写能力，满足大量数据的处理；

——提供访问控制、加密和备份功能，确保数据的安全性；

——支持分布式和集群部署，满足数据增长的需求。

c） 操作系统

——操作系统应具备高可用性和稳定性，确保长时间的运行；

——提供用户和权限管理、安全补丁和更新，防止系统被攻击；

——支持多种硬件和软件资源，确保系统的正常运行。

6.3 人力资源

a） 开发人员

——开发人员应熟练掌握区块链开发语言 Solidity，并对区块链技术如智能合约、共识机制等有深入了解；

——应具备良好的团队合作精神，能够与其他人员有效沟通；

——能够独立思考，迅速找到解决方案面对开发中的问题和挑战。

b） 运维人员

——熟悉常见的操作系统，并了解网络基础，能够配置和管理网络设备；

——在系统出现问题时，能够迅速定位问题并采取措施，如恢复备份、重启服务等；

——与开发团队紧密合作，确保系统的稳定运行，并能够及时反馈和解决问题。

6.4 政策和法规支持

——为确保数据的安全性和系统的稳定性，应制定并遵循统一的安全标准和操作规范；

——为保证各政务联盟链之间的顺畅通信，需要制定和实施统一的技术标准和互操作性规范；

——为确保政务联盟链的透明性和可信赖性，应进行定期的审计，并确保所有操作都符合法规要求；

——为提高政府各部门对政务联盟链的理解，应开展相关的教育和培训活动。

7 底层组件

7.1 数据存储

a） 数据结构化标准

——使用 Merkle 树或其他公认的数据结构来组织和存储数据；

——数据结构应能够支持快速的数据验证和查询。

b） 数据完整性标准

——所有存储在联盟链上的数据必须通过加密哈希函数进行处理；

——数据的修改和添加必须经过数字签名验证；

——在各节点上的数据应满足最终一致性、完整性；

——应支持按照一定规则进行全部节点或部分节点的区块数据同步。

c） 数据安全性标准

——数据必须在存储前进行加密；

——数据访问必须进行身份验证和访问控制；

——定期进行安全审计和漏洞扫描。

d） 数据备份与恢复标准

——必须定期进行数据备份，并将备份数据存储在安全的位置；

——必须制定数据恢复计划，并定期进行恢复演练。

e） 数据共享与隐私保护标准

——数据共享必须基于用户的明确授权；

——使用零知识证明、同态加密等技术来保护数据隐私；

——数据的共享和访问必须遵循相关的法律和政策。

7.2 共识机制

a） 建立部门间共识机制，确保业务数据和操作记录的实时同步、完全一致；

b） 应支持不少于 2 类共识算法，选择适合联盟链特性的算法，如 PBFT、Raft 等；

c) 共识算法应保证各节点对上链数据打包区块的一致性；
d) 共识算法应支持在不可靠的网络环境中达成共识。

7.3 加密与安全访问控制

a) 加密算法
——应符合国家密码管理相关规范，如 GB/T 32918.2-2016、GB/T 32905-2016、GB/T 32907-2016；
——非对称加密算法应支持国家商用密码数字签名算法，如 SM2、SM9；
——杂凑算法应支持国家商用密码杂凑算法，如 SM3；
——对称加密算法应支持国家商用密码对称算法，如 SM4。
b) 访问控制
——所有访问政务联盟链的用户和节点都必须进行身份验证，确保只有授权的实体可以访问和操作数据；
——根据用户的职责和权限为其分配不同的角色，如管理员、审计员、普通用户等；
——基于用户的角色为其分配相应的权限，如读取、写入、修改等。确保用户只能访问其被授权的数据和功能；
——系统应能够检测并报告任何异常或未授权的访问尝试；
——根据实际需要和政策变化，定期更新访问控制策略，确保其始终满足实际需求；
——应采用最小化原则对敏感数据进行授权访问，限制数据暴露面；
——应支持用户身份、信息等敏感数据的脱敏处理。

7.4 智能合约

a) 应支持图灵完备的智能合约，包含算术运算、关系运算、逻辑运算、条件运算、赋值运算等；
b) 应支持智能合约生命周期管理功能，包括部署、升级、冻结、解冻、销毁；
c) 应支持智能合约运行状态监测和事物异常回滚功能；
d) 应采用自主可控的智能合约执行引擎。

7.5 网络传输

a) 应支持节点间安全通信，传输数据涉及个人信息，应遵守国家个人信息保护相关规范，采用 加密传输等手段保障传输安全；
b) 应支持动态组网，包括动态加入网络、退出网络。

7.6 监控与日志

a) 应支持多维度的行为监测与跟踪能力，对象包括区块链服务器、网络流量、链上应用、数字证书等；
b) 应支持区块链账本监测能力，例如监测账本数据的访问、变更、同步等；
c) 应支持共识监测能力，例如监测所有共识节点的共识过程、共识历史等；
d) 应支持跨链、链上和链下数据的关联监测分析能力，例如通过标识对链上行为与链下行为进行关联分析，实现对操作责任人的精准追溯。

7.7 链操作管理系统（COS）

a) 应支持业务链与节点配置管理功能，包括业务链创建、配置、状态查询等；
b) 应支持跨链接入认证配置管理功能，如业务链与节点进出策略配置、认证管理等；
c) 应支持联盟链配置管理功能，例如联盟成员管理、成员权限管理等；
d) 应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；
e) 应支持链上数据监测与行为分析规则配置管理功能，例如链上用户身份与行为分析规则、应用交互监测规则、跨链数据监测规则、BaaS 操作监测规则、安全行为分析规则等；
f) 应支持多维度的态势呈现能力，例如跨链态势、应用态势、安全态势等。

7.8 跨链监管系统（CAS）

a) 应支持统一的跨链传输协议与接口；
b) 应支持链操作管理系统的跨链接入认证策略，执行业务链与节点的认证、加入、退出、跨链 权限分配等；
c) 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；
d) 应支持链操作管理系统的跨链监测策略，执行跨链数据监测、跨链业务监测、跨链安全监测等；
e) 应支持节点安全监测系统的接入与管理。

8 跨链交互

8.1 省本级、地市州及部门级基础设施协同链网

a) 应支持基于中继链、公证人、双向锚定等技术的基础设施协同跨链网络。
b) 应支持基于不同区块链内核所构建的同构及异构链之间的互联互通，打破区块链数据孤岛，助力不同联盟链可信互联，促进区块链产业生态可信融合。
c) 应支持跨链申请、授权等操作行为完整保存上链，交易过程记录本地账本，全流程自动、透明、可监督，支持事中校验、事后审计，保障多方权益。
d) 应支持跨链账本数据以及智能合约数据仅在所有者授权情况下才能进行访问，基于身份体系对跨链合约及账本查询和交易操作提供授权能力，在保护数据安全的同时，还保证数据的使用过程可以被追溯。
e) 应支持基于分布式身份体系的跨链系统治理，为各个接入的区块链配置通用身份标识，支持基于标识寻址发起跨链访问。
f) 应支持跨链事务一致性要求，包括：保障跨链交易在整个流程中的事务一致性；支持事务超时处理机制，在事务超时且不满足一致性要求时进行回滚处理；支持实时或周期性的事务检查机制。允许事务回滚失败时，通过第三方介入的方式保障事务一致性。
g) 应支持跨链可靠性和可用性要求，包括：应支持链间互操作组件出现故障后自动回滚；应支持无单节点故障，可采用多活或负载均衡方式；应支持跨链事务数据和配置的自动备份；应支持数据备份，并支持利用备份数据在系统故障时快速恢复业务环境；应支持账本增量或全量备份；链间互操作组件宜支持账本备份，可以为其他节点恢复数据。
h) 应支持跨链隐私保护能力，保证跨链交互数据安全可靠，跨链中继不记录对应链的数据信息，支持跨链组件点对点数据交互，防止隐私泄露，有效保护跨链数据隐私。
i) 应支持跨链接入安全要求，包括：应支持通过用户数字证书进行身份认证；应支持超时断开机制，超时后应断开用户会话或重新鉴别用户身份；应支持在用户认证失败达到指定次数后，阻止用户再次发起认证请求；宜支持动态口令卡、USB Key、指纹、智能卡认证进行身份认证，其配套设备和系统必须符合国家相关规定；宜支持双因子认证。
j) 应支持跨链数据传输和存储安全，包括：支持跨链交易端到端的完整性保护；支持跨链通信端到端传输过程中的加密保护；支持链间互操作组件账本本地数据的加密存储；跨链交易数据只能被目的方获取，其它方无法获取；支持区块链中的非授权数据无法被链间互操作组件访问。

8.2 跨链交互协议

8.2.1 应用要求

a) 数据共享与互通
——所有部门必须提供其使用的区块链系统的详细信息，以便进行有效的跨链集成；
——部门之间应确保数据的安全性和隐私性，在跨链协议中进行数据交换时，必须采取加密措施；
——各部门应指定专门的技术团队或人员，与跨链协议的实施团队紧密合作，确保数据互通的顺利进行；
——在数据交换过程中，各部门应确保数据的准确性和完整性，避免因数据错误或遗漏导致的问题；
——各部门应定期进行数据交换的测试和验证，确保跨链协议的稳定性和可靠性；
——部门之间应建立通信机制，及时报告和解决在数据交换过程中出现的任何问题；

——所有部门在参与跨链数据交换时，必须遵循相关的法律法规和政策指导，确保数据交换的合法性；
——各部门应定期对其数据进行备份，以防止在跨链数据交换过程中出现的任何数据丢失或损坏。

b) 业务流程协同

——在涉及多部门协同办理的政务服务中，如行政审批、证照发放等，必须采用跨链技术来实现业务流程的自动化和智能化；
——各部门应确保其业务流程与跨链技术的集成，以确保业务流程的顺畅执行；
——所有参与部门必须提供其业务流程的详细信息，以便进行有效的跨链集成和自动化处理；
——部门之间应建立通信和协作机制，确保跨链技术在业务流程中的顺利应用，及时解决任何潜在问题。

c) 提高数据安全性

——必须确保所使用的跨链协议具有高度的加密和安全机制，以保障政务数据在传输和存储过程中的安全性；
——进行政务数据的交换和存储时，必须充分利用区块链技术的不可篡改性，确保数据的真实性和完整性；
——各部门应定期进行安全审查和验证，确保跨链协议和区块链技术的稳定性和安全性；
——各部门应建立应急响应机制，以应对可能出现的安全威胁或数据问题，确保政务数据的持续安全。

d) 简化技术集成

——所有部门在技术集成和数据交换时，必须采用跨链协议作为统一的技术标准和接口；
——各部门应确保其系统和平台与跨链协议的兼容性，以简化技术集成工作；
——在进行技术集成时，部门应遵循跨链协议的技术规范和标准，确保数据交换的稳定性和安全性；
——各部门应定期参与跨链协议的技术培训和更新，确保技术团队对协议的深入理解和正确应用。

8.2.2 跨链交互协议 CCIP

统一协作链支持通过CCIP跨链交互协议识别业务链之间的交易行为，CCIP跨链协议是一套规则和协议，定义了不同链之间的跨链通信和交互方式，包括数据格式、消息传递规范、跨链验证机制等，以确保不同链的互操作性和安全性。

a) 数据格式

CCIP数据格式参见《四川省区块链技术应用标准规范》。

b) 消息传递规范

——跨链交易请求消息：定义跨链交易请求的消息格式，包括发送链和接收链的标识、交易数据等信息。
——跨链消息的传递：定义跨链消息的传递协议，包括消息的编码、序列化和解析规则，确保不同链上节点能够正确解析和处理跨链消息。
——跨链消息的路由和转发规则：定义如何根据目标链的标识将跨链消息路由到相应的目标链节点，确保消息能够准确传递到目标链。

c) 跨链验证机制

确定如何构建验证路径，以验证交易在源链和目标链之间的有效性。验证路径可以是默克尔树、验证人签名等。

8.3 跨链交互机制

接入机构向主管部门提出接入申请，并准备相应的服务器资源、运行环境及网络环境，开发好一个与本地业务链相匹配的跨链适配器。主管部门同意申请后，为接入机构分配跨链账户和用户，并部署跨链可信通道。接入机构在平台上配置其本地业务链并安装跨链适配器。主管部门负责监测业务链的运行情况，确保跨链交互的顺畅和安全。具体见《政务服务区块链技术跨链接入和交互规范》。

8.4 跨链数据共享安全保障

跨链数据共享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，应满足以下要求：

8.4.1 数据加密

8.4.1.1 数据传输加密

所有跨链传输的数据应经过加密处理，确保数据在传输过程中的机密性和完整性。密钥管理和交换应符合安全最佳实践。

8.4.1.2 数据存储加密

存储在链上或链外的数据应以加密形式存储，防止未经授权的访问。平台应采用数据库加密、文件加密、和硬件安全模块等安全措施。

8.4.2 身份验证和授权

8.4.2.1 身份验证

所有跨链参与方必须通过严格的身份验证，确保只有合法用户可以访问和操作数据。平台应采用双因素认证、数字签名或令牌等强身份验证方法进行跨链数据访问。

8.4.2.2 权限管理

应建立细粒度的权限管理系统，确保每个用户或组织智能访问其授权的数据。

8.4.3 合规性检查

所有跨链数据交互必须符合适用的法规和政府政策要求，并定期进行合规性审查，确保数据共享过程合法合规。平台应采用数据脱敏和匿名化、审计日志记录、访问控制列表等合规性检查方法。

8.4.4 安全传输协议

应选择适当的安全传输协议，确保数据在传输过程中的安全性。

8.4.5 数据审计和监控

8.4.5.1 实时监控

实施实时监控机制，以检测异常活动或者潜在的安全风险。设置实时警报系统，确保及时发现并应对威胁。

8.4.5.2 审计日志

记录所有关键数据传输和访问事件的审计日志，审计日志应包括时间戳、参与方信息、数据类型等详细信息。

8.4.6 数据备份和恢复

应建立有效的数据备份和恢复策略，以应对数据丢失或损坏的情况，确保数据的可用性和完整性。

9 跨链监管

9.1 国家政务服务平台下的跨链管理与监管

a) 应支持统一的跨链传输协议与接口；
b) 应支持链操作管理系统的跨链接入认证策略，执行业务链与节点的认证、加入、退出、跨链权限分配等；
c) 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；
d) 应支持链操作管理系统的跨链监测策略，执行跨链数据监测、跨链业务监测、跨链安全监测等；

e） 应支持节点安全监测系统的接入与管理；
f） 应支持通过跨链监管系统(CAS)来实现省级与国家政务服务平台基础链的跨链交互与监管；
g） 应支持通过跨链监管系统 (CAS)来实现省各级各类政务服务基础链、业务链与省级政务服务联盟链的跨链交换与监管；
h） 省级及以下的各级基础链的跨链监管系统支持与安全管理中心审计级联互通，为政务数据提供链上链下全生命周期安全支撑。

9.2 业务链监管

各机构/单位需按照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。

具体服务标准见《政务服务区块链技术跨链接入和交互规范》。

a） 业务链应支持对自身区块链系统进行身份监测的能力，例如节点身份变更、用户身份变更证书状态监测等；
b） 业务链应支持对自身区块链系统进行行为监测的能力，例如节点访问、跨链交互、共识历史、应用交互、账本交互、BaaS 操作等；
c） 业务链应支持对自身节点服务器进行监测的能力，例如服务器资源状态、访问行为、操作行为等；
d） 业务链的安全监测能力应支持与国家政务服务平台一体化安全管理中心联动，为跨链数据安全与行为监测提供基础支撑。

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