ICS 35.240
CCS L70

DB36

江　西　省　地　方　标　准

DB36/T 1712—2022

政务区块链基础平台技术规范

Technical specifications of government blockchain basic platform

2022-12-13 发布　　2023-06-01 实施

江西省市场监督管理局　发布

目　次

前　言

本文件按照GB/T 1.1-2020给出的规定起草。

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。

本文件由江西省发展与改革委员会提出并归口。

本文件的起草单位：江西省信息中心、江西省生态环境厅、江西省应急管理厅、江西省住房和城乡建设厅、江西省审计厅、江西省卫生健康委员会、赣州市行政审批局、抚州市大数据中心、九江市数字经济发展中心、宜春市大数据发展管理局、吉安市大数据中心。

本文件主要起草人：杜军龙、何黎明、周剑涛、熊良、刘浪、文剑、张静、李苏发、吴屹、罗烈、熊少滨、钟毅、曾章琼、徐国平、钟露佳、张海洋、饶荣、冯军、周雨。

引　言

区块链技术作为一种集分布式数据存储、点对点传输、共识机制、加密算法等技术的新型应用模式，被认为是继大型机、个人电脑、互联网之后计算模式的创新，已被广泛运用于数字政府、数字金融、移动互联网等多个领域。为有效解决我省跨部门、跨行业、跨平台的政务信息共享等相关需求，迫切需要制定全省统一的政务区块链基础平台技术标准规范，以指导各地政务区块链基础平台的建设和管理，构建省、市政务信息流通新的桥梁，对全面提升省、市两级政务数据流转和互信十分必要。

本文件的起草工作在遵循国家相关法律法规、技术规范要求的基础上，充分考虑了全省政务区块链基础平台的现状及特点，用于指导政务区块链基础平台的建设和应用。

政务区块链基础平台技术规范

1 范围

本文件规定了政务区块链基础平台（下文简称“基础平台”）的术语和定义，设计了平台的整体架构，明确了平台建设的基本原则、技术要求、服务要求和管理要求，规范省、市两级基础平台的建设和使用。

本文件适用于指导江西省各级政务部门开展政务区块链基础平台建设和业务上链工作。

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 32905 信息安全技术 SM3密码杂凑算法
GB/T 32907 信息安全技术 SM4分组密码算法
GB/T 32915 信息安全技术 二元序列随机性检测方法
GB/T 32918 信息安全技术 SM2椭圆曲线公钥密码算法
GB/T 35273 信息安全技术 个人信息安全规范
GB/T AAAAA 区块链和分布式记账技术术语
GB/T BBBBB 信息安全技术区块链技术安全框架
GM/T 0006 密码应用标识规范
GM/T 0009 SM2密码算法使用规范
GM/T 0010 SM2密码算法加密签名消息语法规范
GM/T 0015 基于SM2密码算法的数字证书格式规范
GM/T 0054 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 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。

[来源：GB/T AAAA-AAAA,3.6]

3.2

节点 node

参与网络并存储账本记录的全部或部分副本的分布式记账技术设备或进程。

[来源：GB/T AAAA-AAAA,3.27]

3.3

政务区块链 blockchain for governmental affairs

利用区块链技术，通过透明和可信规则，实现政务数据跨部门、跨区域共同维护和使用，促进业务协同办理，提高政务服务效率。

3.4

联盟链 consortium blockchain

对特定组织团体开放的区块链，指节点通过管理员或管理机构授权后方可加入区块链，所有共识节点的区块链身份应互相知晓并可互相通信。

[来源：GB/T BBBB-BBBB，3.11]

3.5

业务链 blockchain for business

根据政务应用场景的需求，通过建立业务联盟链，形成拥有独立数据存储、共识网络及治理机制的逻辑链，该逻辑链既可以是业务子链，也可以是新建的业务链，且链与链之间相互独立。

3.6

隐私计算 privacy-preserving computation

指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，保障数据在流通与融合过程中的“可用不可见”。

3.7

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

[来源：GB/T AAAA-AAAA，3.72]

3.8

业务合约 business contract

政务区块链基础平台中，实现区块链业务逻辑的智能合约。

3.9

共识机制 consensus mechanism

区块链系统中通过数学算法实现不同节点之间对记账内容达成一致的方法，是区块链系统确认状态，节点间建立信任、协同合作的基础。

3.10

区块链管理系统 blockchain management system

基于区块链技术实现业务上链的信息化管理系统。

3.11

上链 on-chain

业务相关方向区块链系统发起一次请求，区块链节点将相关数据写入到区块链系统中。

3.12

图灵完备 turing complete

指一系列操作数据的规则（如指令集、编程语言）按照一定的顺序计算所有可计算的问题。

4 缩略语

下列缩略语适用于本文件。

IDE：集成开发环境（Integrated Development Environment）
EVM：以太坊虚拟机（Ethereum Virtual Machine）
WASM：WASM虚拟机（WebAssembly）
KV：键值对（Key Value）
CA：数字证书认证（Certificate Authority）
TPS：每秒事务处理量(Transaction Per Second)
SDK：软件开发工具包（Software Development Kit）
WWW：全球广域网（World Wide Web）
API：应用程序接口（Application Programming Interface）
TLS：安全传输层协议（Transport Layer Security）

5 基本原则

5.1 安全性原则

应按网络安全等级保护三级（或以上）要求建设。

5.2 集约性原则

应由省、市政务区块链管理部门统筹规划基础设施和平台建设，避免各级政务部门分散重复建设。省市间跨链应用建设应充分利用省、市区块链基础平台，各县（市、区）原则上不单独建设区块链基础平台。

5.3 兼容性原则

应基于当前主流的区块链技术体系，实现区块链平台兼容性升级，支持区块链平台与业务场景应用的相对独立，彼此升级互不影响。

5.4 可扩展性原则

应支持区块链节点、数据存储、分布式账本、智能合约、加密算法、共识机制等根据业务量平滑扩展。

6 整体架构

6.1 平台逻辑架构

政务区块链基础平台整体架构采用分层、解耦、复用的设计思想，平台逻辑架构分为基础资源层、区块链平台层、应用服务层，其逻辑架构如图1所示。

a) 基础资源层为区块链平台层和应用服务层提供计算、存储、网络等基础资源支撑。

b) 区块链平台层提供基础技术服务和核心能力输出。基础技术服务包括智能合约、共识协议、集成开发环境、隐私保护、密钥管理、虚拟机插件、存储设计、跨链技术等。核心能力输出主要为政务部门提供区块链平台运维管理等服务能力，包括运维管控、应用开发、数据服务、跨链服务、隐私计算等。

c) 应用服务层是为有业务上链需求的政务部门提供应用上链环境及接口，包括需新上链的政务区块链应用和需链改的传统政务应用。

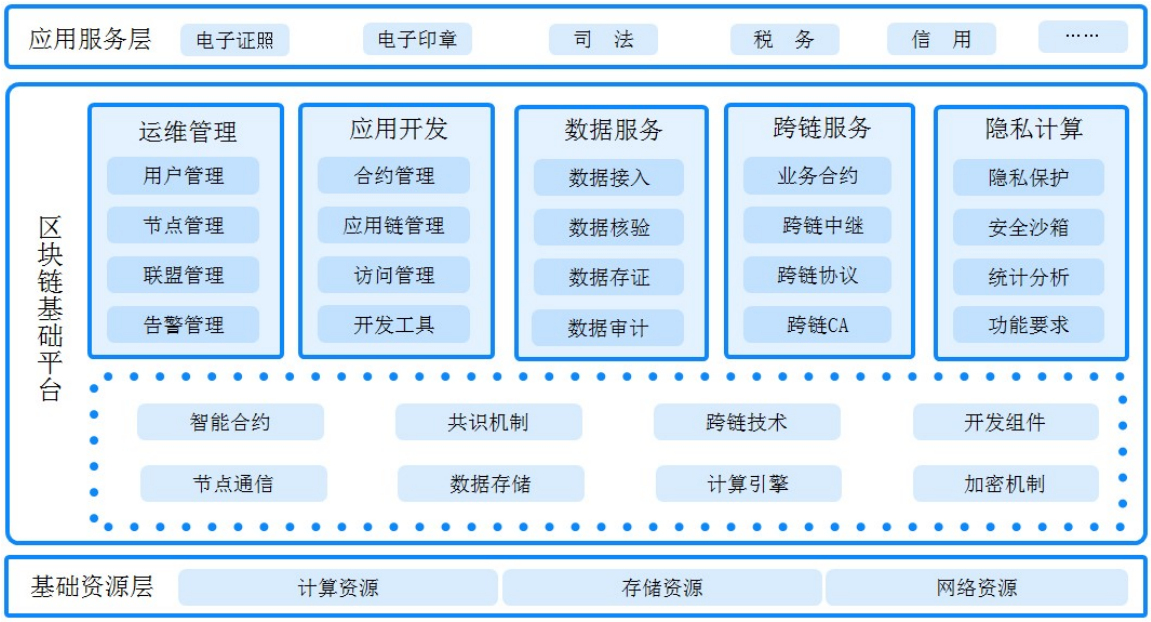

图1 政务区块链基础平台逻辑架构图

6.2 平台部署架构

政务区块链基础平台是应用上多方参与、分布式部署、灵活接入的公共性基础平台，包含省级基础平台、市级基础平台及区块链管理系统，其部署架构如图2所示。

a) 省级平台，包括省级基础链与省级业务链，主要用于满足省级政务部门业务上链需求。省级平台的部署与运维由省级政务区块链管理部门统一规划和管理。

b) 市级平台，包括市级基础链与市级业务链，主要用于满足市级政务部门业务上链需求。市级平台的部署与运维由市级政务区块链管理部门统一规划和管理。

c) 区块链管理系统。主要用于区块链管理平台的运维管理和能力开放，为各级政务部门提供区块链领域的服务能力，包括运维管控、应用开发、数据服务、跨链服务、隐私计算等。

图 2 政务区块链基础平台部署架构图

7 技术要求

7.1 节点要求

不少于当前构建区块链平台技术发展所需的最小化节点数服务要求。其中区块链节点中应包含至少1个监控管理节点，用于管理监控区块链的运行，同时能够获取链运行中权限变更的记录、能够获取需要审计的相关数据。

7.2 节点通信

保证节点之间能直接进行网络通信或能间接进行消息传递，基础平台的节点通信应具备以下功能：

a) 可动态配置节点通信的组网方式，单一节点故障应不影响节点的全网通信；
b) 节点通信应实现心跳等相关的技术机制，保证节点的在线状态，防止因节点网络离线造成的账本不一致；
c) 单个节点初始化完毕后，应具备完整的通信能力；
d) 新节点的加入对于全网中所有已加入的节点都等效可知，新的共识或者记账节点应在网络共识认可后才能加入；
e) 应支持节点动态退出，不同节点退出对于通讯层应是无感知的，且不影响系统通信能力；
f) 应保证下线节点重新加入网络后，账本数据同步和消息通讯能够正常进行，且下线节点重新加入共识后，应保证节点功能正常运行；
g) 应对节点在网络中的消息设置唯一的标识符；
h) 节点通信应与上层业务解耦。

7.3 数据存储

区块链中数据的分布式存储机制，基础平台的数据存储应至少满足以下要求：

a) 不同节点存储的区块链数据应保持完整性；
b) 涉及个人信息等敏感信息的数据，在存储时应遵守国家个人信息保护相关规范（符合 GB/T 35273-2020），进行加密存储；
c) 应支持不少于一种本地文件系统的存储引擎（如 KV 数据库存储），提供全量存储数据的唯一性证明；
d) 应支持历史状态数据的检索能力，能根据不同区块和不同的全局状态根哈希，构造出不同的全局状态历史树，进而查询到不同历史状态下的数据；
e) 应支持多复合条件进行链上数据的查询，如特定范围查询等。

7.4 计算引擎

基础平台的计算引擎应具备以下能力：

a) 提供基础平台运行过程中的计算能力；
b) 在基础平台的网络中，应能够被每个节点采用；
c) 应支持图灵完备的虚拟机技术、容器技术等；
d) 应支持多种类型的计算引擎，包括但不限于 EVM/WSAM 虚拟机在内计算引擎。

7.5 加密机制

为实现信息安全和隐私保护，基础平台的加密机制应符合以下要求：

a) 所使用的密码算法应符合国家密码管理部门的要求，应具有机密性、完整性、真实性、不可抵赖性；
b) 算法执行过程中需要使用随机数时，应按照国家密码管理部门的要求生成随机序列，并符合 GB/T 32915-2016 对随机性的要求；
c) 密钥管理应符合 GM/T 0054-2018 的要求，除公钥外，所有密钥不能以明文形式存储或传输；
d) 应使用符合国家标准的算法完成密码算法操作，具体标准包括：GM/T 0010、GM/T 0015 等；
e) 在需要使用对称加密算法的场景，应选择使用 SM4 等加密算法；
f) 需要使用非对称加密算法的场景，应选择使用 SM2 等加密算法；
g) 需要使用哈希算法的场景，应选择使用 SM3 等算法；
h) 应支持身份验证和鉴权功能，密钥更新后，原有密钥应不能继续使用。

7.6 共识机制

基础平台的共识机制应具备以下能力：

a) 共识算法应支持节点独立进行算法运算，不依赖任何其他节点数据和状态；
b) 共识算法应保证各节点对上链数据打包区块的计算能收敛并达到最终一致性；
c) 共识算法应声明在一定规模的节点环境下达成共识所需的理论时间，且该时间应能满足业务要求；
d) 应能在节点在线、节点离线、网络规模调整等情况下，不停止系统服务，替换原有共识算法并达成新的全网共识；
e) 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，整个平台运行正常；
f) 应具备抗攻击的能力，提供防止消息篡改的验证机制。

7.7 智能合约

基础平台的智能合约应具备以下能力：

a) 应提供编程语言支持，必要时可提供配套的集成开发环境；
b) 应提供智能合约冻结、解冻等功能；
c) 应提供智能合约运行的载体，如虚拟机等；
d) 在部署智能合约时应能指定版本号，部署成功的智能合约应具有唯一标识；
e) 应具备代码安全审查能力，如静态扫描、动态扫描、形式化验证等，防止代码缺陷引发的安全隐患；
f) 交易信息中应明确调用的智能合约版本，不同节点之间的相同智能合约应保证版本一致性；
g) 合约在所有参与共识节点上的执行结果应具备一致性。合约重复执行时，在初始条件不变的前提下，执行结果保持不变；
h) 对于与基础平台外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不应影响基础平台的整体运行；
i) 应支持对合约中交易进行监控，实时监测交易异常情况；
j) 应具备容错和异常终止功能，同时具有运行时间及资源占用可控性。

7.8 跨链技术

提供跨链服务，实现一个链到另一个链的通信。基础平台的跨链技术应具备以下能力：

a) 应支持多种跨链交互模式，支持同构和异构区块链跨链；
b) 应具备管理不同应用链之间跨链互通的能力，包括跨链互认证、跨链互操作等。
c) 应兼容多种异构区块链及跨链机制，保障良好的可扩展性，包括但不限于可信执行环境验证机制、公证人机制、侧链机制、多链机制等；
d) 应构建全局信任域，信任域由认证根、安全协议、可信环境、基于密码学的验证等机制构建，根据业务跨链流通需求设置跨链数据管理权限，保障分布式账本跨链的安全可信。

7.9 开发组件

开发组件支持上链业务开发方的活动，包括完成业务所需的开发环境管理、构建管理和测试管理等。

a) 开发环境应提供用于上链业务的开发环境和服务组合的工具，支持模块的开发；
b) 开发环境应支持开发服务相关的配置元数据的生成；
c) 开发环境应支持服务配置脚本和组件的编写或生成；
d) 构建管理组件应支持自动化构建软件包功能；
e) 构建管理组件应提供自动化编译功能及出错信息提示；
f) 构建管理组件应实现构建过程的审核流程；
g) 构建管理组件应支持多语言及多平台模式；
h) 测试管理组件应在测试环境与生产环境集成的情况下进行测试不应影响生产环境；
i) 测试管理组件应支持自动生成测试报告。

7.10 性能要求

在保证基础平台稳定运行的前提下，快速响应业务的上链需求和用户的访问查询需求，包括完成业务上链对智能合约的调用、链上数据查询、同步和确认等。

a) 在智能合约的调用上，交易上链成功率不低于 95%，交易延迟时间不超过 5 秒；同时在异常场景发生并恢复后仍能维持智能合约调用交易性能；
b) 在链上数据的查询时间效率上，不低于原有业务系统的查询时间效率，同时在异常场景发生并恢复后能快速还原查询效率；

c) 在上链数据同步性能上，交易同步应在块的共识完成前完成；且交易同步时，节点收到的冗余交易比例不高于申明的数值，节点同步并写入区块所耗费的时间应不高于出块时间；
d) 在交易确认时间上，单位时间内交易请求量不大于申明的 TPS 时，交易从发出到被确认处理完成的时间应不超过出块时间的 2 倍。

7.11 安全要求

平台安全应至少满足以下要求：
a) 区块链网络应遵循 GB/T 22239-2019 中规定的三级及以上物理和网络安全相关要求；
b) 应优先使用具有自主知识产权的关键技术和核心器件搭建政务区块链基础平台；
c) 应对基础平台数据进行合理的分类分级，对敏感数据的使用实施脱敏等保护措施，敏感信息应加密存储，具备权限管控，禁止非授权访问；
d) 应支持设置授权和安全规则授权用户访问和使用资源权限的功能；
e) 提供节点间通信加密和节点数据加密存储、节点主机安全加固、智能合约安全验证等安全策略；
f) 应考虑多种层次等级的安全威胁，包括但不限于身份管理类安全威胁、业务与应用类安全威胁、网络与信息安全威胁、终端类安全威胁、基础类安全威胁、管理类安全威胁等；
g) 应确保信息在存储、传输过程中不被非授权用户读取和篡改，可采用有权限的网络访问控制，在参与分布式账本节点之间构建虚拟专用网络，降低网络攻击造成的危害；
h) 应提供访问控制功能，依据安全策略控制用户对数据等客体的访问，按照权限最小化、相互制约原则，为账户分配访问权限。

8 服务要求

8.1 运维管理

8.1.1 用户管理

管理基础平台的的用户或账号。用户管理应至少具备以下功能：
a) 用户管理模块中支持用户注册、账号管理、权限配置等；
b) 应支持账户的冻结和解冻，冻结状态用户不允许发起交易。

8.1.2 节点管理

管理基础平台上的节点。节点管理应至少具备以下功能：
a) 应具备增加区块链节点、删除区块链节点的功能；
b) 应支持区块链节点管理账户权限体系；
c) 支持管理体系自定义，用户可根据不同应用场景设定节点权限等级和能力范围。

8.1.3 联盟管理

联盟管理应至少具备以下功能：
a) 应具备创建联盟链、删除联盟链、加入联盟链、退出联盟链等功能；
b) 应支持联盟链的管理，根据业务要求或用户隔离要求，多个联盟链间数据和业务隔离，保证联盟链间数据隐私和业务独立。
c) 应具备查看联盟链列表和属性信息，查看区块链节点和应用链列表信息等功能；
d) 应具备查看区块列表、区块信息、交易列表、交易信息等功能；
e) 应具备查看合约列表，查看合约信息等功能。

8.1.4 告警管理

告警管理应至少具备以下功能：

a) 实时监控区块链上各节点的状态，并针对异常情况进行告警；
b) 实时监控各联盟链的状态，并针对异常情况进行告警；
c) 跨链状态下，实时监控连接状态，并针对异常情况进行告警。

8.2 应用开发

8.2.1 应用链管理

基础平台应具备创建应用链、删除应用链、加入应用链、退出应用链等功能。

8.2.2 合约管理

基础平台应提供智能合约的全生命周期管理能力，包括合约编写、编译、部署、调用、升级、冻结、解冻和终止合约等。

8.2.3 访问管理

基础平台应具备访问控制、权限管理等功能。

8.2.4 开发工具

基础平台应能够提供简单、高效的合约集成开发环境，帮助开发者进行合约的编辑、编译、部署、调用、单步调试、单元测试、自动编解码等操作。

8.3 数据服务

8.3.1 数据接入

数据接入应至少具备以下能力：

a) 应支持多种数据源对接的能力，数据源地址可配置；
b) 支持自动获取待协作使用的数据详情；
c) 在协作业务运行过程中支持自动读取相关的数据；
d) 提供跨进程调用功能，为终端应用及用户层提供核心层接入服务。

8.3.2 数据核验

基础平台中，不同的区块拥有不同的全局状态根哈希。平台应支持根据不同区块和不同的全局状态根哈希，构造出不同的全局状态历史树，进而查询到不同历史状态下的数据。

8.3.3 数据存证

对于链上关键节点，如审批节点、流转节点、协作应用参与节点，平台应提供统一的上链存证及存证查看服务，以便于对数据使用链路的行为进行审计。

8.3.4 数据审计

数据审计应至少提供以下功能：

a) 系统具备记录用户访问日志，便于监管审计；
b) 应确保无法单独中断审计进程，无法删除、修改或覆盖审计记录

c） 审计记录的内容，至少应包括事件的日期、内容、发起者信息、类型、描述和结果等

8.4 跨链服务

省市之间、各设区市之间政务部门的跨链服务应支持同构链、异构链之间的相互通信，跨链示意图如图3所示。

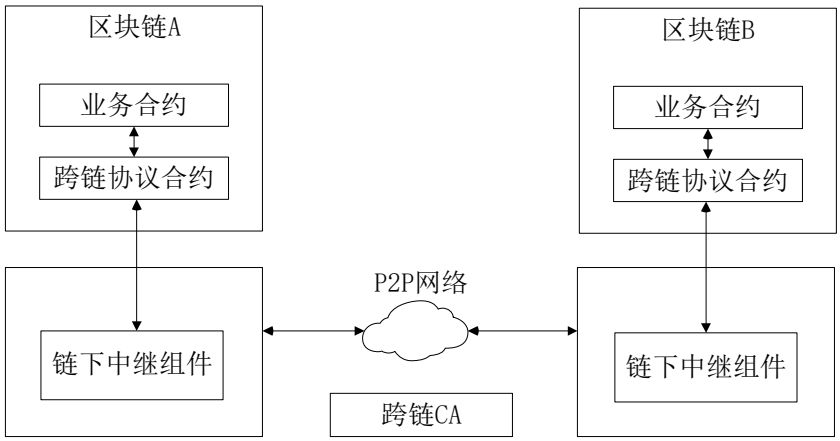

图3 跨链示意图

8.4.1 业务合约

跨链数据交互时，业务合约通过调用跨链协议合约的通讯接口，与其它区块链进行数据交互。应符合如下要求：

a） 业务合约上应具备跨链操作接口，支持主动查询跨链数据，主动发送跨链数据等能力；
b） 业务合约应具备对接收的跨链数据进行存储的能力。

8.4.2 跨链协议合约

跨链协议合约对业务合约提供跨链交互接口，可对区块链上出入的跨链数据实现编解码、数据完整性认证、跨链信任根锚定、跨链消息队列维护、以及跨链中继组件通讯等功能。

a） 具备对政务区块链上出入数据的编解码能力；
b） 验证政务区块链上跨链数据的完整性，防止跨链数据在传输过程中被篡改；
c） 支持跨链信任根锚定，支持信任根更新；
d） 维护跨链消息队列，支持业务合约发送和接收跨链消息，发送跨链事件；
e） 设置跨链数据上链接口，运行跨链中继组件，提交跨链数据；
f） 通知跨链中继组件上已产生的跨链请求。

8.4.3 跨链中继组件

跨链中继组件与跨链协议合约进行通讯，跨链中继组件应具备以下能力：

a） 监听来自跨链协议合约的请求消息；
b） 将跨链数据通过 P2P 中继网络路由发送，同时监听 P2P 中继网络的跨链请求，将跨链数据写入区块链上的跨链协议合约；
c） 应具备可信计算能力，能够根据跨链协议统一格式化跨链数据结构，并且生成第三方账本证明供远程区块链进行校验。

8.4.4 跨链 CA

跨链通讯时应分配区块链标识，由跨链CA作为跨链网络的可信身份信任根，给各区块链颁发可信证书，使得区块链之间、中继组件之间端到端安全可信地传输数据，并验证区块链身份是否合法。

跨链CA应由跨链CA运维方进行签发和管理：

a) 跨链 CA 运维方应由省级管理节点设立，并允许自签名 CA 在全局跨链网络中使用；
b) 跨链 CA 运维方应在完成对区块链配置方的认证后，再对区块链配置方签发区块链域名证书；
c) 区块链配置方应使用区块链域名证书私钥，签发区块链跨链证书，并发布区块链的类型、认证根等信息；
d) 应支持区块链域名证书的查询。

8.5 隐私计算

8.5.1 隐私保护

基础平台应支持秘密分享，同态加密，零知识证明等隐私数据保护技术，实现数据碰撞、数据查询、数据建模、模型部署等功能；

8.5.2 安全沙箱

保证参与数据分享的各方底层明细数据和原始数据均不出计算节点，所有的计算在隐私数据保护技术下进行，查询方仅能获取查询和计算的结果。

8.5.3 统计分析

应支持跨部门、跨层级的基础信息统计，统计信息包括但不限于子网状态、应用总量、数据总量、应用调用总量、数据资源分类统计量等，便于各级用户管理和快速查看。

8.5.4 功能要求

在实施隐私保护技术后，基础平台的隐私保护应具备以下功能：

a) 正确性：区块链业务访问输出具备与原业务系统访问输出结果一致；
b) 保密性：未经认证及权限许可的用户不能获知任意节点的敏感状态信息和交易的敏感数据；
c) 可认证性：区块链业务应用交易的发起方应为私钥的拥有者；
d) 可验证性：所采用的密码算法和协议具备可验证。

9 管理要求

9.1 省级平台管理

省级区块链基础平台由省级区块链管理部门统一规划，其职责包括但不限于:

a) 省级区块链管理部门在省级区块链基础平台上为省政务部门分配资源和权限，省级政务部门作为用户接入省级区块链，省级政务部门之间可以根据业务需要形成不同业务子链；
b) 省级政务部门提出节点资源申请、业务上下链等需求，省级区块链管理部门对省级政务部门的需求申请进行统一审批管理；
c) 省级区块链管理部门应为省市之间的跨链及各设区市间的跨链需求进行标准流程审批；
d) 省级区块链管理部门应对市级区块链建设情况及运行情况进行监督，定期采集各市级的区块链基础平台建设情况、使用情况等数据并在平台中进行展示、查阅。

9.2 市级平台管理

市级区块链基础平台由市级区块链管理部门统一规划，其职责包括但不限于:

a) 市级区块链管理部门在市级区块链基础平台上为市级各委办局分配资源和权限，市级政务部门作为用户接入市级区块链，市级政务部门之间可以根据业务需要形成不同业务子链；
b) 市级区块链管理部门作为管理节点应对所辖市级区块链上的节点资源申请、业务上下链等需求进行管理，同时市级政务部门之间建设业务链应向市级区块链管理部门报批；
c) 各县（市、区）政务部门应充分利用市级区块链基础平台，作为市级区块链基础平台的业务子链开展相关业务；节点资源可向市级区块链管理部门申请，批复的节点资源接入本地区块链。

9.3 省市间跨链管理

省级政务部门可向省级区块链管理部门申请，通过跨链模式发起业务流程同步和数据共享。在垂直方向，省市两级或多级单位之间形成纵向业务链，跨链服务应通过同级或上一级管理平台进行审批。

业务单位根据自身需求申请新的资源时，可向本地链管理单位申请资源，再将新节点接入到本地区块链基础平台。

9.4 平台接入管理

9.4.1 编码规范

业务合约编码安全及规范，应符合以下要求：

a) 遵循通用安全编程准则，包括输入验证、缓存溢出、安全调用组件和程序编译等；
b) 编写智能合约应参考目前比较成熟的框架和合约模板，不应从零开始编写所有代码；
c) 编码中应使用已经广泛应用的安全技术和工具；
d) 不应使用过时的语法或用法，同时应合理使用注释规则；
e) 函数应尽可能短而简洁，同时合约和函数应模块化，每个模块完成单一原子功能；
f) 涉及区块链账本信息变更的智能合约，必须有相应的差错处理约定，确保数据的正确性；
g) 提供开发语言无关的 API 接口，同时支持已广泛运用的编程语言的 SDK（编程语言包括但不限于 Java、C++和 Java Script 等常见的编程语言）。

9.4.2 应用接入

业务系统接入区块链基础平台，包括但不限于以下三种方式：

a) 业务系统直接通过 SDK 命令行与区块链基础平台进行交互；
b) 业务系统通过 Web 上集成的 SDK 与区块链基础平台交互；
c) 业务系统通过后端服务集成的 SDK 与区块链基础平台交互。

其中，第一种方式适用于系统管理员、维护人员进行技术维护，第二种、第三种方式适用于系统用户服务调用。

附 录 A
（资料性）
政务区块链典型应用场景

表A.1 典型应用场景

序号	应用分类	典型场景	场景描述
1	政务监管	司法存证	基于区块链技术构建法院、检察院、公安、司法等跨部门办案协同平台，各部门建立区块链节点，实现跨部门办案材料和数据全部上链，全流程留痕，保证数据全生命周期的可信。有效消除协作疑虑，提高协同办案效率。
2		溯源监管	使用区块链技术对重要监管产品的源头信息、交易信息、流通物流信息及终端消费信息进行分布式存储，防止人为的对追溯系统已经采集的追溯信息进行任意篡改，实现防伪认证和溯源建设的要求。
3		公共财政溯源	使用区块链技术将资金的划拨、流转、使用、验收考核结果上链。实现利用可追溯特性追踪财政资金的使用情况，利用智能合约优化财政征管机制，利用共识机制完善财政预算编制以及绩效评价，利用分布式账本技术建立财政收支的信息可公开机制。
4		资金监管	使用区块链技术将资金流转全生命周期中涉及到的各参与方组成闭环网络，围绕资金的事前信息共识、事中资金划拨、事后效果管理的信息上链，进行全方位、精准化、可追溯、防篡改的数字化、在线化管理。
5		危化品溯源	使用区块链技术实现对危险化学品进行全过程、全链条的信息化管理，打破不同部门的信息壁垒。此外，区块链技术可提高对危化品在物流过程中的监管能力，实现信息的不可篡改和可追溯。
6		电子票据	使用区块链技术将电子票据开具流转的全过程信息都被真实、全面地记录在区块链上，实现授权记录随时可查、全程可追溯，真正做到数据信息防篡改、防抵赖。在此基础上，可进一步实现状态共享、过程追溯及智能监管等功能的应用。
		工程管理	利用区块链技术对工程人员和设备进行区块链唯一身份标志管理，围绕人员、设备、车辆建立资产溯源和人员履历沉淀，便于对建筑工人、建筑设备、建筑材料等进行多维度、多视角综合评价。
7	政务服务	电子档案	参照《江西省档案馆电子档案移交与接收管理办法》，利用数字签名、时间戳和数字摘要等单项技术维护单个机构单份文件的真实性,应用智能合约技术,提升档案管理工作的自动化水平。
8		电子签章	参照《江西省电子印章管理暂行办法》，使用全流程证据上链，构建起电子签章从申领到使用、从使用到流转的闭环。让物理印章唯一性和电子签章（电子印章）安全性有机融合，既合规又便捷，确保在政务办事过程中电子印章的使用行为全程留痕。
9		电子证照	基于区块链技术构建电子证照全流程的信任体系，确保电子证照信息可信任且可追溯，让政务服务参与主体共同建设、共同监督，增强电子证照的安全性与可信度，提高办事效率。

参 考 文 献

[1] GB/T 22239-2019 信息系统安全等级保护基本要求
[2] GB/T 35273-2020 信息安全技术 个人信息安全规范
[3] JR/T 0184-2020 金融分布式账本技术安全规范
[4] JR/T 0193-2020 区块链技术金融应用 评估规则
[5] T/SSIA 0002-2018 区块链技术安全通用规范
[6] T/SIA 007-2018 区块链平台基础技术要求
[7] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[8] GB/T 32905-2016 信息安全技术 SM3密码杂凑算法
[9] GB/T 32907-2016 信息安全技术 SM4分组密码算法
[10] GB/T 32915-2016 信息安全技术 二元序列随机性检测方法
[11] GB/T 32918-2016 信息安全技术 SM2椭圆曲线公钥密码算法
[12] GM/T 0006 密码应用标识规范
[13] GM/T 0009 SM2密码算法使用规范
[14] GM/T 0010 SM2密码算法加密签名消息语法规范
[15] GM/T 0015 基于SM2密码算法的数字证书格式规范
[16] GM/T 0054-2018 信息系统密码应用基本要求
[17] 《可信区块链：安全评估指标与测试方法》