ICS:35.240.99
L 70

团　　体　　标　　准

T/GDCSA 000-2024

政务区块链服务平台 数据交换与共享指南

Government service blockchain platform : Data sharing and exchange

（征求意见稿）

2024-XX-XX 发布　　2024-XX-XX 实施

XXXXXXXXX　　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。

本文件由数字广东网络建设有限公司提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：数字广东网络建设有限公司、广州中科易德科技有限公司、广东省科技创新监测研究中心、暨南大学、广东省技术经济研究发展中心、广东省药品监督管理局事务中心、中山大学软件工程学院、广州软件应用技术研究院、广州市智能软件产业研究院、广州执信网络技术有限公司、广东中科执信科技有限公司。

本文件主要起草人：徐延林、邓颂清、夏锐锋、李引、袁敏夫、邱舟强、陈丽丽、杨安家、黄海滨、何川、董雯雯、贺光玉、刘东成、王一龙、张晨。

政务区块链服务平台 数据交换与共享指南

1 范围

本文件规定了政务区块链服务平台的数据交换与共享的技术规范，包括需使用的相关技术，以及在数据交换与共享过程中必要的技术要求。

本文件适用于政务区块链服务平台的研发、测试、评估和验收等。

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 5271.1-2000 信息技术 词汇 第1部分：基本术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 42571-2023 信息安全技术 区块链信息服务安全规范

GB/T 42752-2023 区块链和分布式记账技术 参考架构

T/CCSA 410—2022 区块链辅助的隐私计算技术工具 技术要求与测试方法

3 术语和定义

GB/T 5271.1-2000、GB/T 37988-2019、GB/T 40685-2021、GB/T 42752-2023、GB/T 42571-2023、T/CCSA 410—2022界定的以及下列术语和定义适用于本文件。

3.1

数据 data

信息的可再解释形式化表示，以适用于通信、解释或处理。

[来源：GB/T 5271.1-2000，01.01.02]

3.2

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988-2019，3.1]

3.3

数据交换共享 data sharing and exchange

以数据作为流通对象，按照一定规则在参与各方中传递和使用的行为。

3.4

区块链 blockchain

使用密码技术将共识确认过的区块按时间顺序进行追加链接形成的分布式账本。

[来源：GB/T 42752-2023，3.12、3.6和3.10]

3.5

智能合约 smart contract

存储在分布式账本中的计算机程序。

[来源：GB/T 42571-2023，3.5]

3.6

上链 record on chain

将信息写入区块链的过程。

[来源：GB/T 42752-2023，3.13]

3.7

隐私计算 privacy-preserving computation

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类信息技术，保障数据在产生、存储、计算、应用和销毁等信息流程全过程的各个环节中“可用不可见”。

[来源：T/CCSA 410—2022，3.1]

4 技术架构

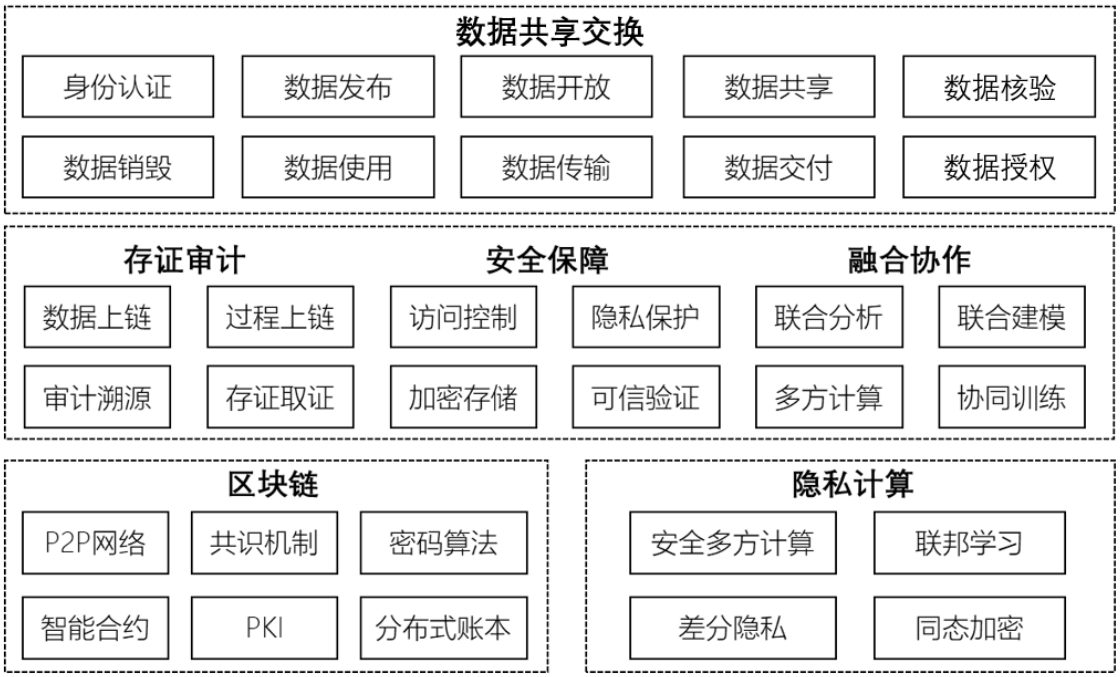

图1 技术架构

区块链依托分布式账本、P2P网络、共识机制等组件，具备数据和过程上链，审计溯源，存证取证等存证审计能力。安全多方计算、联邦学习、差分隐私和同态加密等隐私计算技术在保证数据隐私前提

下，能够促进数据融合和多方协作。两者结合，为数据交换场景下的身份认证，以及数据开放、共享和交易等业务模式下，数据的采集、登记、存储、共享、传输等环节提供存证审计、融合协作和安全保障的服务。

5 技术要求

5.1 数据发布和存储技术要求

5.1.1 数据采集

数据提供方根据自身业务范围和能力，通过合法手段，将相对分散的各原始数据进行收集，形成原始数据集，应上链的内容包括但不限于：

a) 数据的对象、来源、类型，宜采用原始数据上链的方式；
b) 使用的采集技术、采集方法、采集时间，宜采用原始数据上链的方式；
c) 最终的原始数据集，宜采用摘要信息上链的方式。

5.1.2 数据标准化

数据提供方对原始数据集进行清洗、预处理后形成高质量、标准化数据集，应上链的内容包括但不限于：

a) 清洗的对象、操作，预处理的中间操作，宜采用原始数据上链的方式；
b) 清洗和预处理的结果，宜采用原始数据上链的方式；
c) 最终的标准化数据集，宜采用摘要信息上链的方式。

5.1.2.1 数据登记

数据提供方依照规定在政务区块链平台登记和公开所持有数据的控制状况的过程，以维护合法权益的，宜采用摘要信息上链的方式进行存证，应上链的内容包括但不限于：

a) 基本信息：包括登记主体、数据的名称、所属行业类别、数据类型、摘要信息等；
b) 数据来源：如来源于授权应提供凭证或许可编号，如自生产应提供对应的生产环节信息；
c) 权属关系：数据的所属权、使用权等归属；
d) 数据属性：数据的私密级别。

5.1.2.2 数据核验

应利用政务区块链平台对欲登记的数据进行核验，应核验的内容包括但不限于：

a) 登记主体是否已在链上注册；
b) 欲登记数据的名称、行业、数据类型和摘要信息是否与原始数据一致；
c) 授权的凭证或许可是否登记在链且有效，自生产对应的生产环节信息是否与链上存储的数据的历史操作记录相符合；
d) 欲登记的数据的权属关系是否在对应智能合约授权列表内。

5.1.2.3 数据凭证化

核验通过后，应通过政务区块链平台生成对应数据的凭证并存储于链上，以实现数据的可溯源、可核验、防篡改和跨域互认，凭证的内容包括但不限于：

a) 凭证标识；
b) 数据摘要信息；
c) 登记时间；

d) 权属关系；
e) 有效期。

5.1.3 数据存储

数据提供方应采用链上和链下组合的方式进行数据存储。

5.1.3.1 链下存储

a) 存储对象应为原始数据集；
b) 应根据数据类型选择适宜的存储方式，数据库类型；
c) 应加密存储，选择符合标准且安全级别的密码算法；
d) 应设置对应的数据访问权限。

5.1.3.2 链上存储

a) 存储对象应为数据摘要信息；
b) 应以密文的形式存储于分布式账本；
c) 宜通过智能合约的方式设置访问权限。

5.2 数据交换共享技术要求

5.2.1 身份鉴别

a) 在数据交换前，应创建用户身份存储在区块链上，以确保不可篡改；
b) 用户身份信息应使用哈希函数进行加密处理，生成唯一的身份哈希作为用户的数字身份标识，用于与区块链上的用户身份记录相匹配；
c) 将用户身份信息和相应的身份哈希存储在区块链上，确保只有授权的用户可以访问和修改这些信息；
d) 在数据交换开始时，应通过区块链获取数据共享双方的用户身份信息和身份哈希，确认双方的用户身份。

5.2.2 访问控制

a) 在数据共享交换前，应为每份数据创建其权属标签，明确该数据的持有权、使用权的归属方；
b) 数据权属标签应存储在区块链上，以确保不可篡改；
c) 在数据共享交换前，数据需求方应对需要访问的数据提出授权申请，数据提供方根据数据及数据权属信息决定是否为数据需求方提供数据访问授权，并为需求方颁发授权访问令牌；
d) 数据需求方应使用正确的授权访问令牌调用数据；
e) 数据的所有上链、授权、使用都应被记录并存储在区块链上，便于监管方进行监督和管理。

5.2.3 授权管理

a) 应规定数据的交换规则，包括访问权限、访问时间、授权主体等；
b) 可采用智能合约的方式进行授权管理，已部署的智能合约应能被替换、升级和废止，以确保数据权限的更新；
c) 授权管理的所有操作都应被记录并存储在区块链上，便于监管方进行监督和管理，以追溯数据的交换过程。

5.2.4 脱敏保护

如果交换数据属于私密和敏感信息，应进行脱敏处理，以降低数据泄漏的风险，具体要求如下：

a) 宜选择自动触发的方式执行脱敏操作，在敏感数据被访问时实时进行脱敏处理；
b) 宜针对不同角色和不同权限制定多种脱敏方案，能够根据身份自动辨别选择方案执行；
c) 可选择使用智能合约实现脱敏操作的方案选择和自动执行；
d) 应将脱敏处理的操作信息上链，能够根据链上信息对脱敏操作进行审计；
e) 在数据脱敏过程中，可根据数据类型和计算要求选择适宜的隐私计算技术。

5.2.5 数据加密

数据在数据提供方和数据需求方交换的过程中，应根据数据安全级别、数据类型、合规要求、应用场景、业务性能的需求，制定加密传输策略，具体要求如下：

a) 加密算法：应根据数据类型和安全要求级别选择对应符合标准的密码算法；
b) 数字证书：应使用区块链认证的身份数字证书用于传输，保证传输过程中的不可抵赖和篡改；
c) 主体身份鉴别和认证：应对传输双方的身份信息进行认证，见5.2.1。

5.2.6 完整性校验

数据需求方应能够通过区块链上存储的数据摘要信息对接收到的数据进行完整性校验具体，校验内容包括但不限于：

a) 数字证书是否正确；
b) 数据凭证是否登记在链上且处于有效期内；
c) 数据的摘要信息是否同链上存储的摘要信息一致；
d) 登记主体信息是否已在链上注册；
e) 身份信息是否已在权属列表中且正确对应权利。

5.2.7 安全审计

数据在数据提供方和数据需求方交换的过程中，应使用区块链对交换全过程进行记录，以供可信溯源和安全审计，上链的内容包括但不限于：

a) 数据提供方和需求方的身份信息；
b) 交换的数据信息，包括凭证、摘要等；
c) 数据被访问和授权的记录，包括访问的主体、时间、操作，授权的对象、权利等；
d) 脱敏处理所使用的智能合约记录，包括数据的敏感级别，使用的脱敏方案，隐私计算技术；
e) 数据加密传输信息，包括传输路径，使用的加密算法，加密后的数据内容，身份校验结果等；
校验信息，包括完整性校验结果，检验失败的原因等。

附 录 A
（资料性）
技术要素

A.1 多方安全计算

a) 私密性保护：应保证参与方在计算过程中的输入和输出的机密性；
b) 计算正确性：应确保计算结果的正确性，即使在有恶意参与方的情况下也能够得到正确的结果；
c) 安全模型：应明确定义安全模型，阐述受到攻击者可能进行的攻击、攻击者的能力以及计算参与方所要达到的安全属性；
d) 密钥管理：加密算法应有对应的安全密钥管理方案；
e) 通信安全：通信协议应确保消息传输的安全性，以防止攻击者对消息进行窃听或篡改。

A.2 联邦学习

a) 模型聚合性：应确保局部模型能够更新聚合成全局模型；
b) 模型安全性：应确保在训练过程和模型更新中防止中间人攻击、模型窃取和针对性攻击等安全威胁；
c) 隐私保护：宜结合隐私保护技术，如差分隐私、安全多方计算和同态加密等。

A.3 数据脱敏

a) 脱敏规则：应定义数据脱敏处理方式的指导原则和策略；
b) 脱敏级别：应支持不同级别的敏感度和对应的脱敏方案；
c) 访问控制：应确保只有经过授权的用户能够访问脱敏后的数据；
d) 数据可用性：应采用同态加密和差分隐私等技术，在保护隐私的同时保持数据的可用性和有效性。