ICS
CCS
备案号：

团　　体　　标　　准

T/××× ×××—20××

基于区块链和隐私计算的数据安全流通技术规范

Technical Specifications for Secure Flow of Data Based on Blockchain and Privacy Computation

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

××××－××－××发布　　××××－××－××实施

标准发布单位　　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。

本文件由广东省通信产业服务有限公司、广东省电信规划设计院有限公司提出。

本文件由广东省云计算应用协会归口。

本文件起草单位：广东省通信产业服务有限公司、广东省电信规划设计院有限公司、广东省电子商务认证有限公司、中数通信息有限公司、天讯瑞达通信技术有限公司、广州赛西标准检测研究院有限公司、广州民航信息技术有限公司、布比（北京）网络技术有限公司、移动通信国家工程研究中心、华南理工大学、中山大学、华南师范大学、暨南大学、广州大学、广州番禺职业技术学院、广东邮电职业技术学院、工业和信息化部电子第五研究所、广州软件技术研究院、中国电信广东公司、中国移动广东公司、中国联通广东公司、×××、×××。

本文件主要起草人：×××、×××、×××。

本文件为首次发布。

引　言

数据作为新型生产要素，对传统生产方式变革具有重大影响。随着市场主体和市场环境不断完善，数据要素质量得到大幅提升，但是制约数据要素市场化配置的流通规则、流通技术等关键性难题仍有待破解。数据要素要实现安全高效流通，需要通过一系列规则设计和技术手段，建立起数据要素安全流通技术规范。当前保障提供方数据安全、防止数据价值稀释的数据流通技术蓬勃发展，以区块链、隐私计算为代表的数据流通技术提供了“数据可信可追溯”“数据可用不可见”的流通新范式，为需求方实现安全可信地获取和分析外部获取的数据提供了技术可能。本文件旨在规定基于区块链和隐私计算的数据安全流通技术要求，以确保数据流通的安全性和稳定性。

基于区块链和隐私计算的数据安全流通技术规范

1 范围

本文件规定了基于区块链和隐私计算的数据流通安全的技术要求，包括需使用的区块链和隐私计算相关技术，以及在数据资产化和流通过程中必要的技术要求。

本文件适用于基于区块链和隐私计算的数据安全流通产品的研发、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 20518-2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

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 20518-2018、GB/T 42752-2023、T/CCSA 410—2022界定的以及下列术语和定义适用于本文件。

3.1

数字证书 digital certificate

由个国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。

【源自GB/T 20518-2018 中3.7】

3.2

主体身份 subject identity

对参与主体的身份信息进行处理，形成的可查询、识别和验证的数字代码。

3.3

数据凭证 data credential

基于数据本身和其属性信息，经过一系列加工后形成的能够证明该数据对象的标识。

3.4

数据授权 data authorization

授予特定参与主体使用、访问和处理数据的权限和权利的过程。

3.5

数据定价 data pricing

为数据产品或服务确定合理的价格或费用的过程。

3.6

数据交付 data delivery

将数据按照特定的格式、方式和时间交付给需求方，以便其使用、分析或进一步处理。

3.7

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。

【源自GB/T 42752-2023 中3.12、3.6和3.10】

3.8

上链 record on chain

将信息写入区块链的过程。

【源自GB/T 42752-2023 中3.13】

3.9

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”。

【源自T/CCSA 410—2022 中3.1，有改动】

4 缩略语

下列缩略语适用于本文件：

P2P：点对点（Peer to Peer）

CA：认证机构（Certificate Authority）

RSA：非对称加密算法（Ron Rivest, Adi Shamir, Leonard Adleman）

SM2：商用密码之椭圆曲线公钥密码算法（ShangMi2）

ECDSA：椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm）

SHA256：256位安全散列算法（Secure Hash Algorithm 256）

SM3：商用密码之杂凑算法（ShangMi3）

API：应用程序接口（Application Programming Interface）

5 技术架构

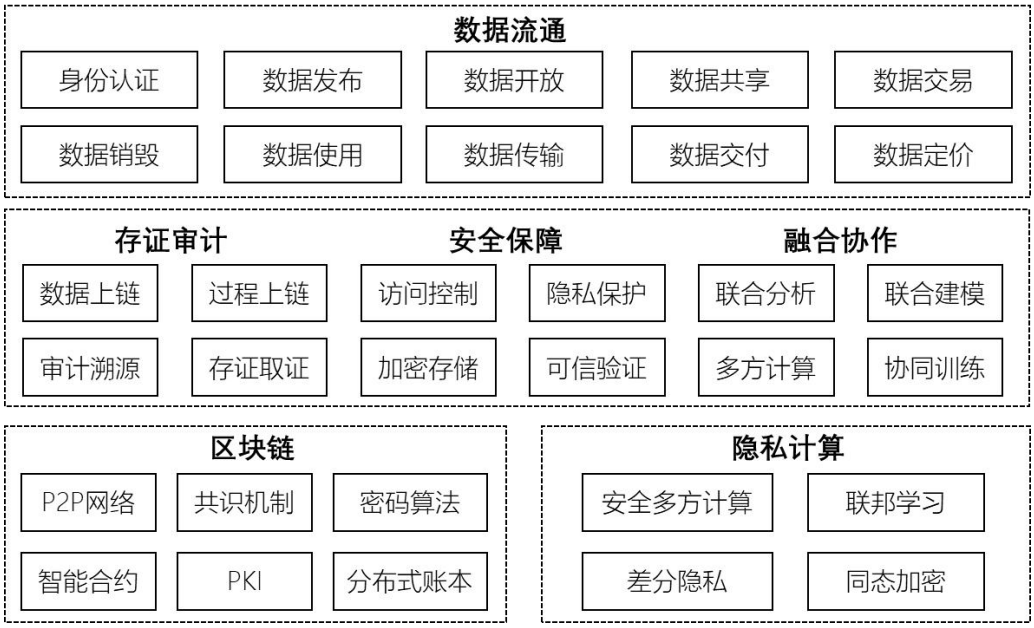

图 1　技术架构

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，为数据流通场景下的身份认证，以及数据开放、共享和交易等业务模式下，数据的发布、定价、交付、传输、使用和销毁等环节提供存证审计、融合协作和安全保障的服务。

6　网络结构

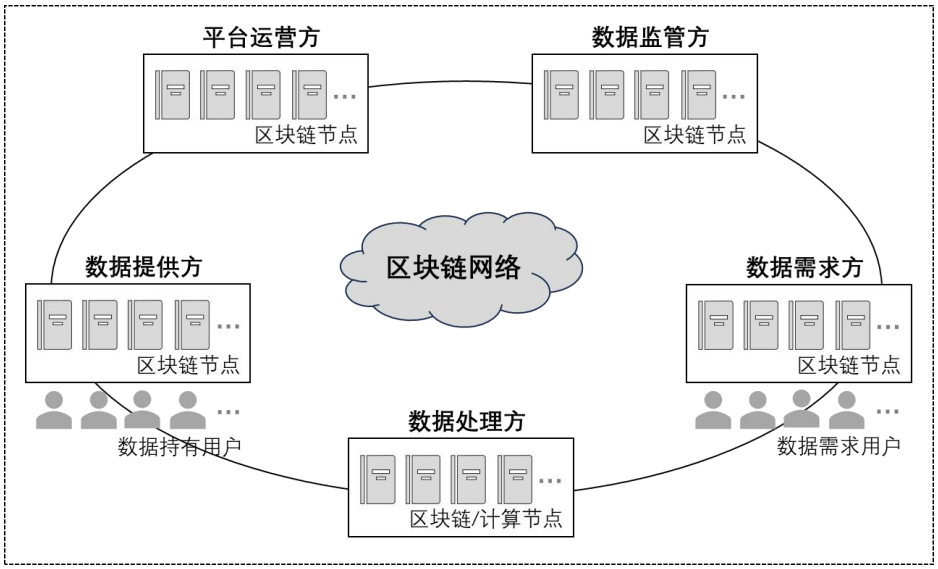

图 2　网络结构

平台运营方和数据监管方应作为核心节点组成区块链网络，数据处理方兼具区块链节点和计算节点身份，数据提供方和数据需求方可以节点形式的加入区块链网络，也可以用户的形式参与。相关参与节点应满足以下要求：

a) 具备足够的计算、存储和资源，以处理事务和维护网络；
b) 支持区块链网络所要求的操作系统，如 Linux、Windows 等；
c) 能够保持稳定的网络连接，同其他节点进行通信和同步数据；
d) 具备身份验证机制和访问控制措施，防止非法参与方加入网络。

7 技术要求

7.1 主体身份要求

7.1.1 主体身份认证

7.1.1.1 总体要求

参与节点或用户的身份信息认证，宜支持数字证书方式实现，包括证书申请，身份验证、证书生成和颁发。具体应满足以下要求：

a) 选择适合场景且安全系数高的证书类型，见 7.1.1.2；
b) 选择使用范围广且可信度高的 CA 用于颁发和管理数字证书，见 7.1.1.3。

7.1.1.2 数字证书

参与主体在加入区块链网络，以及进行身份登记前，应向第三方证书注册机构申请数字证书以进行身份验证。申请的数字证书应满足以下要求：

a) 证书类型应符合实际的数据流通场景和需求，包括以下：
   1) 服务器证书：授予参与流通的节点，用于验证节点的身份和真实性；
   2) 用户证书：授予参与流通的用户，用于验证用户的身份，确保操作可信；
   3) CA根证书：节点需安装和信任与所用CA相关的根证书信任链。
b) 证书所包含的参与主体信息应完整和明确，具备身份验证效力，应包括但不限以下：
   1) 发布组织：证书注册机构名称和相关信息；
   2) 参与方身份信息：证书授权实体的名称、单位或自然人、国家/地区、角色类型；
   3) 序列号、有效期、公钥信息、签名算法等。
c) 证书所使用的密码算法和密钥长度应满足国际或国家标准，确保安全性足够强；
   1) 加密算法：使用非对称公钥密码算法，如RSA、ECDSA或国密SM2；
   2) 数字签名和验签算法：使用RSA、ECDSA或国密SM2；
   3) 哈希算法：使用SHA256或国密SM3。
d) 证书有效期应根据数据流通业务流程需求制定，在减少证书更新频率的同时提高安全性。

7.1.1.3 证书注册机构 CA

为确保数字证书的安全和可靠，应选择可信度高、使用范围广的第三方数字证书注册机构，应从以下方面进行筛选：

a) 是否受到主流操作系统、浏览器和应用程序，以及业界广泛的认可和信任；
b) 是否支持数据流通场景下所需的证书类型和功能；
c) 是否在证书签发、密钥管理、身份验证等流程采取适当的安全措施；
d) 是否在证书到期或发生安全问题时能够及时更新或吊销。

7.1.2 主体身份登记

7.1.2.1 总体要求

参与节点或用户的身份信息应在区块链上进行登记，需经过平台运营方、数据监管方，以及数据提供或需求方的一致性共识，确保在数据流通过程中各参与方的可信，明确权益和责任归属。

7.1.2.2 链上身份信息

区块链上保存的主体身份信息，应包括以下属性：

a) 基本信息：主体名称、类型、组别；
b) 登记信息：登记时间、有效期限；
c) 数字证书标识：数字证书哈希值；
d) 数字签名：核验通过后节点的数字签名；
e) 身份标识：由其余项拼接后取哈希值得到。

7.2 数据发布要求

7.2.1 数据定价

在数据交易业务模式中，确定拟发布数据的市场流通价格，价格制定应满足以下要求：

a) 应在预估价值的基础上合理制定市场流通价格；
b) 应支持成本法、收益法和市场法进行价值评估：
    1) 在数据流通市场价格相对缺失以及预期收益不定的情况下，应使用成本法；
    2) 在数据流通市场价格可获得以及预期收益相对稳定的情况下，应使用收益法；
    3) 在具有相对完善的数据流通市场的情况下，应使用市场法。

7.2.2 凭证发布

区块链发布和存证的数据凭证信息应包括：

a) 凭证标识：由其余项拼接取哈希值得到；
b) 登记时间；
c) 登记主体；
d) 数据信息：数据基本信息；
e) 签名信息：参与背书的节点签名集合。

7.3 数据存储要求

7.3.1 通用要求

数据提供方将数据进行链上和链下组合存储：

a) 链下存储对象为数据本身，加密存储于数据库中；
b) 链上存储对象为数据身份信息，以事务的形式加密存储于分布式账本中。

7.3.2 链下存储

a) 存储对象应为数据本身；
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。

7.3.3 链上存储

a) 存储对象应为数据身份信息；
b) 宜通过智能合约的方式设置访问权限。

7.4 数据流通要求

7.4.1 数据授权

数据需求方通过区块链检索查阅意向的开放/共享/交易类型的数据，提交数据授权请求。平台运营方审核数据授权请求，审核通过后，平台运营方对授权信息进行签名，发布至区块链网络。授权信息应包括：

a) 数据凭证标识；
b) 授权主体，数据提供方；
c) 授予主体，数据需求/处理方；
d) 授予权限，使用权、管理权、收益权等；
e) 授予日期；
f) 有效期限。

7.4.2 交付形式

应支持以下交付数据的方式：

a) 原始数据交付：数据提供方直接将原始数据发送给数据需求方；
b) API 接口交付：数据提供方开放外部 API 接口供数据需求方使用；
c) 隐私计算交付，可采用以下方式：
   1) 安全多方计算：数据处理方按照数据需求方的计算要求，进行多方协同计算，交付计算结果；
   2) 联邦学习：数据处理方按照数据需求方的训练要求，进行多方联合学习，交付模型参数；
   3) 脱敏数据：使用差分技术对原数据进行扰动处理，添加噪声，交付扰动数据；或对原数据进行同态加密，交付加密数据。

7.4.3 传输方式

应支持以下传输数据的方式：

a) 原始数据：数据提供方和需求方间建立安全的连接通道，以密文的形式传输；
b) API 接口：数据提供方提供安全的外部接口，数据以密文形式交互；
c) 隐私计算，可采用以下方式：
   1) 安全多方计算：数据处理方宜将计算结果上传至区块链完成计算结果整合，数据需求方自行下载。
   2) 联邦学习：数据处理方宜将训练结果上传至区块链完成模型整合，数据需求方自行下载。
   3) 脱敏数据：传输添加扰动或加密后的数据。

7.5 数据使用要求

应支持以下使用数据的方式：

a) 原始数据：对数据完全掌控，可根据自身需求进行再分析处理，形成个性化的产品和服务，实现数据价值转换；
b) API 接口：不完全掌控数据，可通过调用已有产品和服务的接口获取数据本身或价值。

c） 隐私计算，可采用以下方式：

1） 安全多方计算：数据需求方提出计算要求，交予多个数据处理方计算，由区块链整合后，得到目标结果。

2） 联邦学习：数据需求方给出模型训练要求，交予多个数据处理方训练，由区块链整合后，得到目标模型参数。

3） 脱敏数据：数据需求/处理方在扰动或加密数据的基础上完成计算得到结果，将结果交予数据提供方进行解密，得到目标结果。

7.6 数据销毁要求

破坏数据需求方存储介质中原始数据的完整性，或限制使用方式，撤销相关数据权限，应满足以下要求：

a） 原始数据或脱敏数据：结合多种方式进行删除，可采用专业数据销毁工具、文件复写和消磁等方式；

b） API 接口：撤销数据需求方对于相关数据产品或服务调用的接口权限；

c） 隐私计算：安全多方计算或联邦学习，拒绝响应计算或训练请求。

完成数据销毁操作后，应在区块链上进行权限撤销、更新、备案。

7.7 存证审计要求

在数据流通过程中，数据监管方应对关键信息和流程操作进行审计，相关信息上链存证。审计和存证的内容包括：

a） 主体身份：身份认证、申请、审核、登记操作，主体身份信息；

b） 数据发布：数据登记、审核、凭证授予操作，数据身份信息；

c） 数据存储：数据存储信息；

d） 数据流通：数据授权、交付、传输操作，数据流向信息；

e） 数据使用：数据使用信息；

f） 数据销毁：数据销毁操作。

附 录 A

（规范性）
技术要素

A.1 区块链技术

根据具体需求，应选择适宜的区块链平台或协议实现数据可信存证，保证链上数据的不可篡改、可溯源。具体要求如下：

a) 共识算法：应选择适宜的共识机制实现多节点共识，以具备一定的容错能力；
b) 去中心化：存证数据应以去中心化的方式存储，以防止单点故障和数据篡改；
c) 密码算法：应支持主流加密算法或国密算法，密钥长度要符合加密算法和实际应用场景的要求；
d) 访问控制和权限管理：一般宜基于密码学安全机制，建立访问控制和权限管理体系，确保只有授权用户可以访问存证数据，以维护数据的隐私和安全性；
e) 智能合约：宜支持智能合约和全生命周期管理，包括编写、检测、编译、部署和调试；
f) 可信存储：应具有链上存储，并可组成链上和链下存储的组合，以支持隐私监管要求。

A.2 隐私计算技术

A.2.1 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.2.2 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.2.3 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。