额，ICS

**ICS** 03.080.99

**A** 20

团体标准

T/CFIS 00XX—202X

**基于区块链的数据资产确权与交易规范**

**Specification of blockchain-based data asset right confirmation and transaction**

202X-0X-XX 发布 202X-0X-XX实施

**发 布**

中国网络社会组织联合会

 版权保护文件

版权所有归属于该标准的发布机构。除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

目 次

[前 言 III](#_Toc141779290)

[引 言 IV](#_Toc141779291)

[1 范围 1](#_Toc141779292)

[2 规范性引用文件 1](#_Toc141779293)

[3 术语和定义 1](#_Toc141779294)

[4 数据资产确权与交易框架 3](#_Toc141779295)

[5 主体要求 5](#_Toc141779296)

[6 区块链系统要求 5](#_Toc141779297)

[7 数据资产确权过程 6](#_Toc141779298)

[8 数据资产确权类型 9](#_Toc141779299)

[9 数据资产交易过程 11](#_Toc141779300)

[附　录　A （资料性） 数据资产登记证书 13](#_Toc141779301)

[附　录　B （资料性） 资产登记申请表 14](#_Toc141779302)

[附　录　C （资料性） 交易安全评价指标体系 15](#_Toc141779303)

[参 考 文 献 18](#_Toc141779304)

前 言

本文件按照GB/T1.1—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》给出的规则起草。

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。

本文件由中国网络社会组织联合会提出并归口。

本文件起草单位：

本文件主要起草人：

引 言

数据已经成为驱动经济发展、社会治理和技术创新的宝贵资源。2022年6月22 日，中央全面深化改革委员会第二十六次会议审议通过《关于构建数据基础制度更好发挥数据要素作用的意见》，承认和保护数据要素各参与方的合法权益，合理界定数据要素市场各参与方的权利和义务，通过权利分割的方法实现数据分类确权与授权，充分凝聚当前共识，要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。数据作为生产要素的前提是数据的资产化，但目前，国际国内、信息技术以及信息技术应用领域对数据资产的理解还未形成共识，数据资产的管理和应用仍然面临着诸多挑战。

编制基于区块链的数据资产确权与交易规范是数据基础制度建设的重要内容。基于区块链技术，针对在数据资产价值实现过程中处于基础性地位的确权和交易环节提出规范性要求，同时构建指标评价指标体系以规范交易安全。本团体标准的制定和实施将对数据资产相关产业的发展形成助力，加快培育统一的数据市场，也为未来国家立法机关出台数据产权的相关法律制度开辟道路、打下社会基础。

基于区块链的数据资产确权与交易规范

1. 范围

本文件规定了基于区块链技术的数据资产确权与交易的术语定义、主体要求、区块链系统要求，数据资产确权过程、确权类型及交易过程等内容。

本文件适用于：

——基于区块链技术的数据资产确权与交易过程；

——指导组织和机构建立、实施、保护和改进数据资产权利认证体系；

——为计划使用区块链进行数据资产确权和交易的组织和机构提供参考；

——为采用区块链进行数据资产确权和交易的行业监管提供参考。

1. 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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010　信息安全技术　术语

GB/T 32905-2016 信息安全技术 SM3密码杂凑算法

GB/T 32918.2-2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32907-2016 信息安全技术 SM4分组密码算法

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37550-2019 电子商务数据资产评价指标体系

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 42460-2023 信息安全技术 个人信息去标识化效果评估指南

GB/T 42570-2023 信息安全技术 区块链技术安全框架

DB15/T 2199-2021 数据交易安全技术要求

1. 术语和定义

GB/T 25069、GB/T 37550、GB/T 37932、GB/T 42570界定的以及下列术语和定义适用于本文件。

区块**block**

一种由一系列信息单元组成的基本数据结构。

[来源：GB/T 42570-2023，3.1]

区块链  **blockchain**

将区块顺序相连，通过共识协议、数字签名、杂凑函数等密码学方式保证的不可伪造、不可篡改和可追溯的分布式数据结构。

[来源：GB/T 42570-2023，3.2]

数字签名  **digital signature**

是一种附加在数据上的信息，它通过对原始数据进行摘要、加密等处理得到。这种信息能够允许数据的接受者确认数据的完整性和来源真实性，并防止数据被伪造或抵赖。

[来源：GB/T 25069-2010，2.1.2，有修改]

摘要算法  **digest algorithm**

使用Hash函数等摘要函数，通过将任意长度的消息输入变成固定长度的短消息输出来保障数据的完整性的算法。

[来源：CBD-Forum-001-2017，2.2.4]

数据**data**

任何以电子或者其他方式对信息的记录。

[来源：中华人民共和国数据安全法第三条]

数据资产**data assets**

以数据为载体和表现形式，能够持续发挥作用并且带来经济利益的数字化资源。

注1：数据资产能够为组织带来有潜在商业价值或实际商业价值。

注2：数据资产能够估值、交易，并以货币计量。

注3：数据资产包含资源性数据资产和经营性数据资产。

[来源：GB/T 37550-2019，2.4]

资源性数据资产 **resource-oriented data assets**

作为数据产品加工原料的数据资产，也称为数据要素。这些数据要素是自然人、法人或非法人组织在依法履职或经营活动中制作或获取的，以电子或其他方式记录、保存的原始数据集合。

经营性数据资产**profit-oriented data assets**

对资源性数据资产进行实质性加工、处理与产品化后形成的数据资产，也称为数据产品，包括但不限于数据集、数据报告、数据可视化产品、数据指数、数据接口、数据应用、加密数据等数据内容或服务。

区块链平台服务机构 **blockchain platform service provider**

具备区块链技术，搭建、管理与维护数据资产确权与交易所需区块链系统，并提供数据上链等相关服务的机构主体。

数据权益人  **data interests holder**

有权对数据资产持有、使用、经营，并可据此申请确认权益的人员主体。

数据资产权利审查机构 **data asset rights reviewer**

对数据资产权利进行审查并颁发权利证书的第三方机构。

数据资产供给方  **data asset provider**

提供数据资产并对其有权利的交易方。

数据资产需求方  **data asset demander**

请求获取数据资产交易方。

数据资产存证 **data asset proof of existence**

数据权益人就数据来源、权属、安全、合规等事项进行声明，并将声明及证明文件经过审查平台审核后上链存证的过程。这些声明和证明文件经过审查平台的审核后，将被记录在区块链上，形成不可篡改的存证信息。这些存证信息可以证明数据的来源、权属、安全、合规等事项。

[来源：T/TJIFA 003-2022，3.11，有修改]

数据资产确权 **data asset right confirmation**

根据数据权益人的申请，经过数据资产存证，数据资产权利审查机构将数据资产权利状态上链，并出具确认其指定数据资产权利的证明文件的过程。

[来源：T/TJIFA 003-2022，3.12]

数据交易  **data transaction**

数据资产供给方和数据资产需求方之间以数据资产作为交易标的，进行的以货币或货币等价物交换数据资产的行为。

[来源：GB/T 37932-2019，3.1]

数据交易过程 **data transaction process**

数据资产双方针对具体的数据交易标的，进行的一次完整和具体的数据交易行为。

注：数据交易过程一般分为交易申请、交易磋商、交易实施和交易结束等环节。

[来源：GB/T 37932-2019，3.10]

1. 数据资产确权与交易框架

数据资产确权与交易过程可分为确权阶段、交易安全评估阶段及交易阶段。三个阶段及所涉主体如图1所示。在确权阶段，数据资产权利审查机构对数据资产进行确权并经区块链平台服务机构对确权信息上链后，向数据权益人颁发确权证书，数据资产确权信息将被公示并可查询；在交易安全评估阶段，数据资产权利审查机构根据交易安全评价指标体系对交易安全进行分类评定并依据相应规则作出交易处理；在交易阶段，数据资产供给方与需求方经数据资产确权审查机构审查后进行数据资产交易，区块链平台服务机构对交易记录、确权变更等信息进行上链。

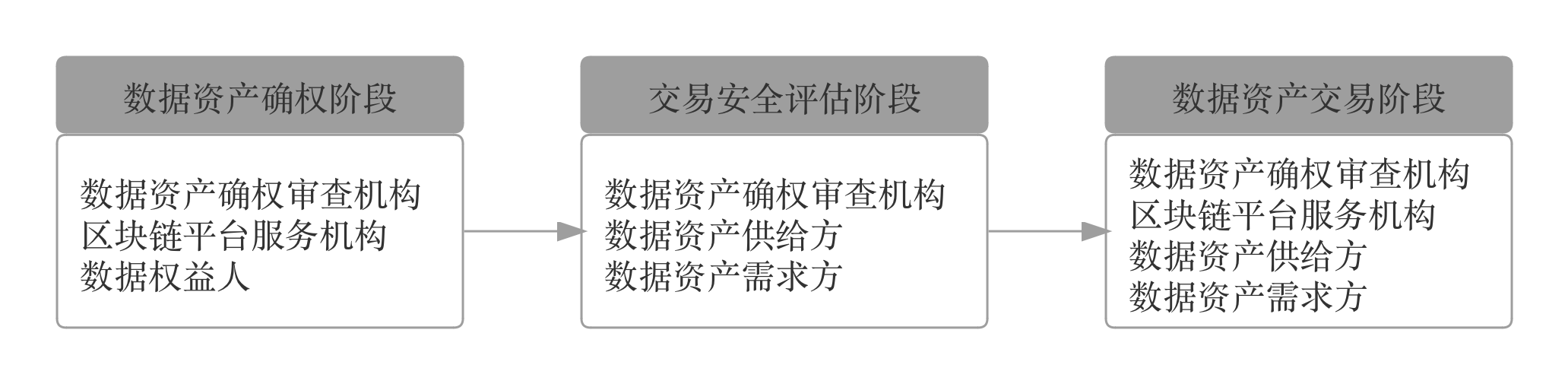


图1 数据资产确权与交易的不同阶段及所涉主体

在数据资产确权流程中，各主体间的交互如图2所示。



图2 数据资产确权主体交互流程

在数据资产交易流程中，各主体间的交互如图3所示。

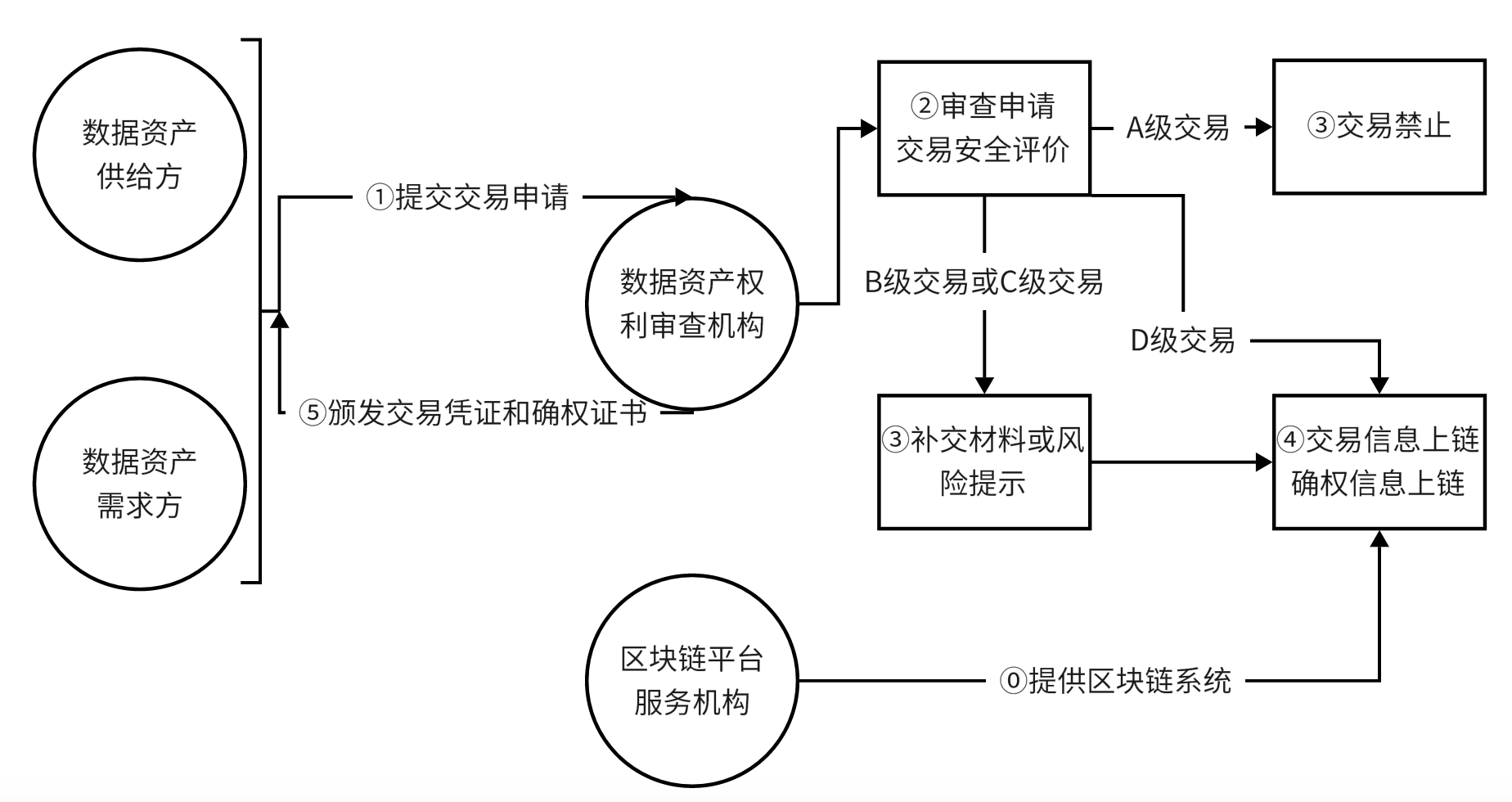


图3 数据资产交易主体交互流程

1. 主体要求
   1. 区块链平台服务机构要求

应至少：

——使用安全、可靠的算法搭建区块链系统；

——具备良好的区块链服务治理及维护能力；

——具备承担数据确权服务相对应的安全保障能力；

——具备完善的数据上链功能，可记录完整的数据上链信息，可提供上链信息查询功能；

——使用保证链上数据完整性、机密性的技术机制，如运用哈希校验、电子签名、加密算法等技术手段防止数据被篡改，确保数据在存储、传输过程中的安全；

——将提供数据确权、数据交易的区块链系统部署在我国境内；

——对违法违规、违反机构服务要求的使用者采取合理的处理措施；

——满足GB/T 37988-2019中的三级要求。

* 1. 数据权益人要求

应至少：

——具有合法合规的数据来源；

——依法依规实现权益。

* 1. 数据资产权利审查机构要求

应至少：

——确保审查过程的中立、严谨及审慎；

——严格保密确权业务使用方提供的数据及其他信息；

——具备对数据权益人提交的数据资产权利申请与证明材料进行审查的能力；

——具备对数据交易双方提交的交易申请材料进行审查的能力，能够使用技术手段提高审查效率。

注：数据资产权利审查机构由相应主管部门确定；若未确定，则由具有公信力、能够独立承担责任的法人组织担任。

* 1. 数据资产供给方

应至少：

——是数据资产的数据权益人；

——保证交易数据与已确权的数据资产的一致性；

——采取必要措施保障交易过程中的数据安全。

* 1. 数据资产需求方

应至少：

——在获取数据资产后，在约定范围内处理数据；

——采取必要措施保障交易过程中的数据安全。

1. 区块链系统要求

区块链系统的基础架构可以分为数据层、网络层、共识层、合约层和应用层，应满足GB/T 22239-2019中的第三级安全保护能力。

* 1. 数据层要求

区块链系统的数据层要求如下：

——应采用较为安全的哈希算法，保障交易数据的完整性等特征，应满足GB/T 32905-2016第5章关于SM3密码杂凑算法的要求；

——应提供可靠的数据加密算法，保障交易数据的保密性、安全性等特征，应满足GB/T 32907-2016关于SM4分组密码算法的要求；

——应对数据资产进行数字签名，保障交易数据的完整性、真实性、交易过程的不可抵赖性，应满足GB/T 32918.2-2016第6章、第7章关于数字签名算法生成与验证的要求。

* 1. 网络层要求

区块链系统的网络层要求如下：

——应支持动态/静态方式增加或删除节点、支持升级或回滚节点，且不影响业务正常运行；

——应能够检测防范恶意节点，能够抵御DDoS攻击、日式攻击、BGP劫持等常见攻击方式；

——应保证区块链系统能够承受一定交易业务压力，避免因资源不足导致节点故障、消息错误等问题；

——应采取安全通信协议（如TSL、IPSec等协议），保障传输数据的保密性、完整性和真实性。

* 1. 共识层要求

区块链系统的共识层要求如下：

——应确保共识机制的安全性，能够抵御重放攻击、51%攻击、恶意代理攻击等常见的共识攻击；

——应确保共识机制的可用性、鲁棒性，使系统具备节点容错功能、保障节点记录的一致性；

——宜提供调整共识机制规模的功能，能够根据确权场景、数据资产交易参与方、交易量、网络规模等调整共识算法。

* 1. 合约层要求

智能合约用于数据资产确权和交易过程，区块链系统的合约层要求如下：

——应确保智能合约代码的正确性，采用最新稳定的智能合约编程语言，编写代码符合代码书写规范、逻辑要求，确保合约按照预期路径执行；

——应确保智能合约执行环境的安全性，采用部署控制、密码技术等防止智能合约被篡改，同时能够抵御重入、交易顺序依赖等攻击；

——应提供智能合约多方控制机制，由区块链系统参与方通过多签、投票等方式共同控制智能合约的发布、修改、销毁等操作。

* 1. 应用层要求

区块链系统的应用层要求如下：

——应具备身份验证功能，通过口令、登录码或手机动态码等方式对用户身份进行验证；同时，应限制非法试图登录次数、登录后可定时自动退出；

——应具备访问控制功能，控制不同主体使用区块链平台进行数据资产确权、数据资产交易、交易溯源等功能；

——应具备异议变更功能，当数据资产信息存在错误或因权利变更等情形需要修改时，区块链平台应接受异议申请、提供信息变更功能；

——应具备安全审计功能，提供行业监管接口，对数据资产确权记录和交易记录进行审计。

1. 数据资产确权过程

为了对数据资产确权，数据权益人应先对数据资产进行预检查，再向数据资产权利审查机构提出权利确认审查、变更审查或注销审查的申请；对于通过数据资产权利审查机构的权利确认审查的数据资产，数据资产权利审查机构应将其上传至区块链平台服务机构提供的区块链系统；最后，数据资产权利审查机构向数据权益人颁发确权证书并做出公示。

数据资产确权的流程如图4所示。

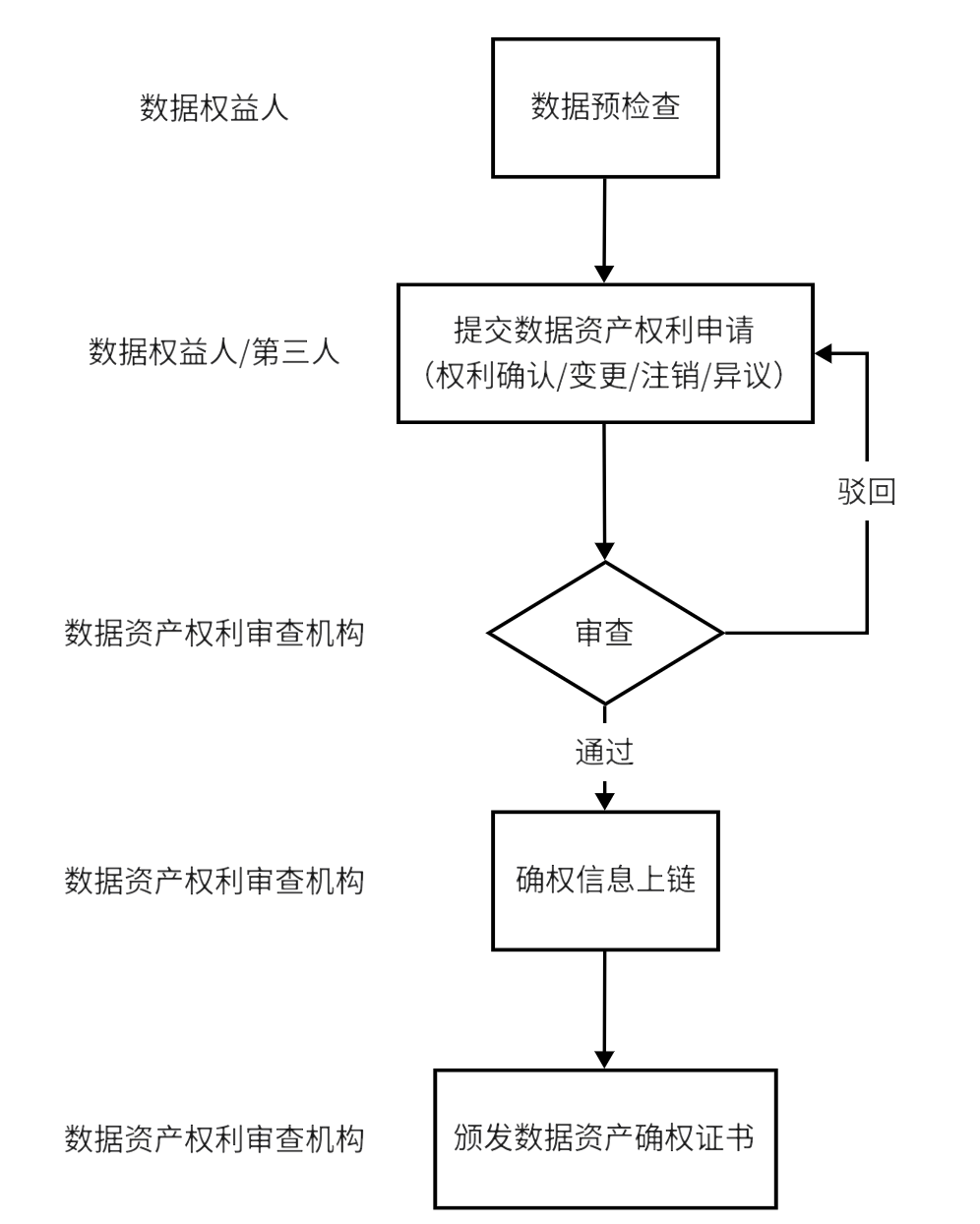


图4 数据资产确权流程

* 1. 搭建区块链系统

区块链平台服务机构按照数据层、网络层、共识层、合约层和应用层要求搭建区块链系统。

* 1. 数据预检查

数据权益人申请数据资产确权前，应进行数据预检查，包括：

——检查数据收集、存储、使用、加工、传输、提供、公开等环节是否符合核心数据、重要数据或一般数据的具体防护要求和操作规程；

——检查数据完整性；

——检查数据传输、存储等环境是否安全、可靠。

* 1. 数据资产权利审查
     1. 数据资产权利的确认审查

确认审查包括：

a）数据权益人向数据资产权利审查机构申请权利确认审查的，应根据不同数据资产确权类型的申请要求，向数据资产权利审查机构提供申请材料，宜包括（详见8 数据资产确权类型）：

——申请人基本信息；

——数据资产必要信息，分为数据要素必要信息和数据产品必要信息。

b）数据资产权利审查机构应对申请材料进行形式审查。

c）申请人需要对申请材料的客观性、真实性、准确性和完整性负责。

* + 1. 数据资产权利的变更审查

变更审查包括：

a）数据权益人对数据持有权进行下列处分后应向数据资产权利审查机构申请变更审查，包括：

——数据权益人通过拍卖、转让等方式，可将已确权的数据资产转移或复制至其他数据权益人名下。数据资产转移指将数据资产的持有权排他性转让给他人，同时自身不再保留持有权。数据资产复制指将数据资产的持有权转移给他人，同时自身保留持有权；

——数据权益人通过设立质押等方式，在已确权的数据资产上设立他项权益。

b）数据权益人申请权利变更审查的，应提交以下材料：

——变更权利审查申请书；

——数据权益人有关身份证明文件；

——数据资产确权证书原件；

——交易或非交易双方签署的合同文本；

——数据资产权利审查机构要求提供的其他材料。

c）变更权利的，应由交易或非交易双方共同申请。

d）数据资产权利审查机构应参照数据资产权利审查要求审核办理变更登记，并出具新的确权登记证书。

* + 1. 数据资产权利的注销审查

注销审查包括：

a）数据权益人向数据资产权利审查机构提出申请注销登记的，应提供以下材料：

——注销权利审查申请书；

——数据权益人有关身份证明文件；

——数据资产确权证书原件；

——数据资产权利审查机构要求提供的其他材料。

b） 因人民法院、仲裁委员会的生效法律文书等情形导致原数据权益人的数据资产相关权利灭失的，由新数据权益人进行注销登记；如无新数据权益人，可由数据资产权利审查机构进行注销。

c）数据资产权利审查机构应参照数据资产确权登记要求审查办理注销，删除已登记内容。

* + 1. 数据资产权利的异议审查

异议审查包括：

a）第三人对数据资产权利存在质疑的，可向数据资产权利审查机构提出数据资产异议申请。异议申请应提供以下材料：

——数据资产异议申请书；

——异议申请人有关身份证明文件；

——申请异议证明材料；

——数据资产权利审查机构要求提供的其他材料。

b）数据资产权利审查机构应通知数据权益人，经综合审查认为异议成立的，应撤销数据权益人数据资产确权证书。

* 1. 数据资产确权信息上链

数据资产通过数据资产权利审查机构的权利审查后，数据资产权利审查机构应以节点形式接入区块链平台服务机构提供的网站、应用程序或编程接口，将信息形成区块上传至区块链中；区块链对该区块进行广播、验证，达成共识后更新。

上链的信息应至少包括：

——数据权益人的名称及公钥信息；

——数据权益人在确权数据资产上使用私钥签名后的信息；

——数据资产的识别性信息，如哈希值；

——数据资产的描述性信息，包括数据资产的名称、类型、数据规模、取得方式等。

* 1. 数据资产确权证书颁发

数据资产确权证书颁发包括：

a）数据资产完成审查并上链后，数据资产权利审查机构应向数据权益人颁发数据资产确权证书。

b）确权证书应至少包含下列信息：

——证书名称；

——统一证书编号；

——数据权益人信息；

——数据资产的描述性信息（名称/类型/数据规模等）；

——数据资产的识别性信息（哈希值等）；

——数据证书的数字签名；

——数据权益人对数据资产的权属关系（数据资源持有权/数据产品持有权）；

——数据资产取得方式（原始取得/收集/交易/其他）、证书发放日期。

* 1. 数据资产公示和查询

经数据资产权利审查机构确认审查、变更审查或注销审查的数据资产应能以便捷、公开的方式进行公示，公示并可被查询得到的数据资产信息应包括：

——数据权益人的名称及公钥信息；

——被电子签名后的数据资产信息；

——数据资产的描述性信息，包括数据资产的名称、类型、数据规模、取得方式等；

——可信时间戳；

——数据资产权利审查机构授予证书的编号。

1. 数据资产确权类型
   1. 概述

可申请确权的数据资产共包括两类：数据资源持有类、数据产品经营类。前一类数据资产为数据要素，确权标的为资源性数据资产。后一类数据资产为数据产品，确权标的为经营性数据资产。

数据权益人根据自身确权需求选定确权类型，向数据资产权利审查机构提交相应申请材料。

* 1. 数据资源持有类
     1. 概述

申请数据资源持有类权利确定审查，表示数据权益人申请确定对相应资源性数据资产具有持有权，能够对资源性数据资产实施持有、加工、使用、转让、复制、许可、收益（融资抵押等）、处分等权能。

数据权益人向数据资产权利审查机构申请数据资源持有类权利确定审查的，应当提交权益申请人基本信息和数据要素必要信息。

* + 1. 申请人基本信息

申请人基本信息应包括：

——权益申请人名称；

——统一社会信用代码；

——公司类型；

——注册资本；

——注册地址；

——经营范围；

——营业期限；

——开户行；

——对公账号；

——营业执照；

——法人代表；

——法人代表身份证正、反面。

* + 1. 数据要素必要信息

数据要素必要信息应包括：

——数据要素的名称、类型；

——数据要素的原始存储介质；

——数据要素的原始取得方式，直接获得的数据要素须提交相关流程并说明源数据的产生过程，间接获得的数据资产须提交收集方案与收集合同、协议等材料，且收集合同、协议应溯及原始取得方；

——数据要素的描述性信息，包括规模、收集时间区间、覆盖范围等；

——数据要素的标识性信息，如哈希值等；

——数据要素的应用场景及禁用场景描述，包括条件、范围等。

* 1. 数据产品经营类
     1. 概述

申请数据产品经营类权利确定审查，表示数据权益人申请确定对相应经营性数据资产具有持有权，能够对经营性数据资产实施持有、转让、许可、授权他人经营、收益（融资抵押、质押等）、处分等权能。

数据权益人向数据资产权利审查机构申请数据产品经营类权利确定审查的，应当提交权益申请人基本信息和数据产品必要信息。

* + 1. 申请人基本信息

申请人基本信息应包括：

——权益申请人名称；

——统一社会信用代码；

——公司类型；

——注册资本；

——注册地址；

——经营范围；

——营业期限；

——开户行；

——对公账号；

——营业执照；

——法人代表；

——法人代表身份证正、反面。

* + 1. 数据产品必要信息

数据产品必要信息应包括：

a）通用信息及材料：

——数据产品的名称、类型；

——数据产品的原始存储介质；

——数据产品数据来源的取得方式，直接获得的数据须提交相关流程并说明源数据的产生过程，间接获得的数据须提交收集方案与收集合同、协议等材料，且收集合同、协议应溯及原始取得方；若数据来源涉及个人信息，须提供相应个人信息主体的授权材料及相关匿名化处理说明；若数据来源是已经过数据资源持有类认证的数据资产，须提供相应数据资源持有类证书及允许持有、加工使用的授权文件；

——数据产品的描述性信息，包括规模、收集时间区间、覆盖范围、生成算法等；

——数据产品的应用场景及禁用场景描述，包括条件、范围等。

b）对于数据集还需要包括以下额外的必要信息：

——文件格式；

——采集时间；

——字段列表；

——数据集的标识信息；

——数据集的相关详细信息，包括可描述数据样例等；

——数据集的相关附件，包括截图、样例文件等。

c）对于数据接口还需要包括以下额外的必要信息：

——接口地址；

——请求方式、请求参数；

——返回类型、返回参数；

——数据接口的标识信息；

——数据接口的相关详细信息，包括可描述接口功能、接口参数、请求示例等；

——数据接口的相关附件，包括相关指导文档等。

d）对于数据报告还需要包括以下额外的必要信息：

——报告更新周期；报告形成日期；

——数据报告的标识信息；

——数据报告的相关详细信息，包括可描述报告的摘要等；

——数据报告的相关附件，包括报告目录、内容节选截图等。

e）对于数据应用还需要包括以下额外的必要信息：

——应用版本号；

——试用链接；

——数据应用的标识信息；

——数据应用的相关详细信息，包括可描述使用说明、应用案例等；

——数据应用的相关附件。

f）对于其他数据产品类型还需要包括以下额外的必要信息：

——数据产品的相关详细信息；

——数据产品的标识信息；

——数据产品的相关附件。

1. 数据资产交易过程
   1. 交易标的

交易标的是经数据资产权利审查机构确权的数据资产，数据资产需求方可以在区块链平台服务机构选择已确权的数据资产进行交易；也可事先与数据资产供给方磋商，请求将约定的数据资产上链确权后进行交易。

* 1. 交易过程
     1. 交易申请

数据资产供给方与数据资产需求方应在区块链平台服务机构对已经确权的数据资产发起交易申请。交易申请的必要事项包括：

——交易双方名称、资质；

——经确权的数据资产信息；

——数据资产需求方的使用目的；

——数据资产需求方的使用范围；

——数据资产需求方的使用期限等。

* + 1. 交易合规性审查及交易安全类别评定

数据资产权利审查机构受理交易申请后，应对交易必要事项进行形式审查，确保交易要件的完备性、交易过程的规范性；并根据数据资产交易安全评价指标（参见附录C）评定该交易的类别，按照处理规则做出相应处理。

* + 1. 数据资产传输

数据资产传输采用链外实现方式，传输范围限于中国境内。交易双方应采用安全可靠的数据传输方式，防止数据丢失、篡改、泄露等事件发生。

* + 1. 数据资产验证

数据传输后，数据资产需求方应对数据资产进行形式验证和实质验证：

a）形式验证：验证交付的数据资产是否为经过区块链确权的数据资产。具体验证方式为：

数据资产需求方根据交易标的在区块链系统中的确权信息对接收的数据资产进行验证，如数据资产识别性信息是否一致、描述性信息是否符合等。

b）实质验证：验证数据资产质量、数量是否满足确权登记中的数据资产描述或双方约定。

* + 1. 交易结束

验证结果经双方确认后交易完成，区块链平台服务机构应对交易记录进行上链。交易记录包括交易主体、交易标的标识信息、交易申请情况、交易必要事项、验证结果等内容。

* + 1. 确权变更

交易结束后，数据资产权利审查机构应根据交易内容进行确权变更，经确权后在区块链平台变更相应确权信息，应满足7.3.2要求。

* 1. 纠纷解决

数据交易双方或第三人就交易内容产生纠纷时，可按照约定或法定的争议解决方式进行处理，或可依据7.3.4向数据资产权利审查机构提出异议审查。依据当事人请求或争议解决机关要求，区块链平台服务机构、数据资产权利审查机构应积极配合，提供确权信息、确权记录、交易记录等材料。

2. （资料性）  
   数据资产登记证书

下面给出了数据资产权利审查机构颁发的数据资产登记证书示例。

示例见表A.1：

* 1. 数据资产登记证书示例

|  |  |  |  |
| --- | --- | --- | --- |
| **数据资产登记证书** | | | |
| 证书名称 |  | | |
| 统一证书编号 |  | | |
| 数据权益人 |  | | |
| 数据资产名称 |  | 数据资产类型 |  |
| 数据资产规模 |  | 数据权益对数据资产的权属关系 | □ 数据资源持有权  □ 数据产品持有权 |
| 数据资产取得方式 |  | | |
| 登记时间 |  | | |
| 上链时间 |  | | |
| 有效期 |  | | |
| Hash值 |  | | |
| 数字签名 |  | | |

1. （资料性）  
   资产登记申请表

下面给出了数据权益人向数据资产权利审查机构提交申请所需填写的表格示例。

示例见表B.1：

* 1. 数据资产申请登记表示例

|  |  |  |
| --- | --- | --- |
| **数据资产登记申请表** | | |
| 一、数据权益人基本信息 | | |
| 权益申请人名称 |  | |
| 统一社会信用代码 |  | |
| 法人代表姓名 |  | |
| 经营范围 |  | |
| 其他已提交的材料及其说明 |  | |
| 二、数据资产必要信息 | | |
| 序号 | 数据资产相关信息 | 具体内容 |
| 1 | 数据资产名称 |  |
| 2 | 类型 | □ 资源性  □ 数据集  □ 数据接口  □ 数据报告  □ 数据应用  □ 其他数据产品类型： |
| 3 | 数据原始存储介质 |  |
| 4 | 数据原始取得方式 |  |
| 5 | 数据资产描述性信息 |  |
| 6 | 数据资产标识性信息 |  |
| 7 | 应用场景及禁用场景 |  |
| 8 | 其他已提交的材料及其说明 |  |
| 三、数据权益人申请声明 | | |
| 本单位保证填报信息及提交材料真实有效，如与事实不符，所产生的一切不良影响及法律后果均由本单位自行承担。  法定代表人签字：  公司盖章                       年    月    日 | | |

1. （资料性）  
   交易安全评价指标体系
   1. 交易安全评价指标体系的构成

交易安全风险评价指标体系如表C.1所示通过交易安全风险评价指标体系，数据资产权利审查机构将一个数据资产交易分为A类（禁止类）、B类（限制类）、C类（警示类）、D类（自治类）四种等级，各自对应不同的交易处理规则。A类交易的风险最高，D类交易的风险最低。

* 1. 交易安全评价指标体系

|  |  |  |  |
| --- | --- | --- | --- |
| **指标代号** | **一级指标** | **二级指标** | **评价内容** |
|  | 数据资产风险 | 数据来源角度 | 数据是否获得权利人授权或主管部门批准、获得授权或批准路径及有效性等。数据来源越清晰，则数据资产风险越低。 |
|  | 数据内容角度 | 数据是否涉及个人信息、商业秘密或涉及国家安全、公共利益、是否符合所属具体行业的数据处理要求等。数据资产对国家安全、公共利益或个人、组织合法权益的危害可能性越高，则数据资产风险越高。 |
|  | 数据规模角度 | 数据规模如何。数据规模越大，则数据资产风险越高。 |
|  | 数据交易主体风险 | 数据安全能力角度 | 数据交易双方的数据安全管理能力、数据安全技术能力、人员管理及安全教育能力。主体数据安全能力越高，则数据交易主体风险越低。 |
|  | 数据安全信用角度 | 近年内是否受到过与数据安全/个人信息保护相关的行政处罚、发生过数据泄露等数据安全事件等。主体数据安全信用越高，则数据交易主体风险越低。 |
|  | 数据处理资质角度 | 是否具有根据法律规定收集、处理特定数据的特定资质或行政许可、是否属于特殊监管行业或承担特殊数据合规义务等。主体数据处理资质越完备，则数据交易主体风险越低。 |
|  | 数据交易习惯角度 | 数据交易主体是否存在不当的交易习惯，主体的不当交易行为越多，则其数据交易习惯越差，数据交易主体风险越高。 |
|  | 数据交易过程风险 | 数据交易场景角度 | 数据交易的场景与目的是否具有危险性。交易场景风险越高，则数据交易过程风险越高。 |
|  | 数据交易合同角度 | 数据交易合同是否完备。数据交易合同越完备，交易合同风险越低，则数据交易过程风险越低。 |
|  | 数据传输风险角度 | 数据传输方式是否安全。数据传输方式越安全，数据传输风险越低，则数据交易过程风险越低。 |

* + 1. 数据资产风险

作为交易标的的数据资产风险将会影响到交易风险，两者呈正相关关系。数据资产风险从以下角度进行评价：

——数据来源角度：包括数据是否获得权利人授权或主管部门批准、获得授权或批准路径及有效性等；数据来源越清晰，则数据资产风险越低。如数据资产包含未依法取得授权的个人数据（宜参见GB/T 35273-2020 5.4、GB/T 41479-2022 5.2等要求开展评价），或数据资产包含未经依法开放的公共数据，或数据资产包括根据合同约定禁止交易的数据，则相关交易为A级交易。

——数据内容角度：包括是否涉及个人信息、商业秘密或涉及国家安全、公共利益、是否符合所属具体行业的数据处理要求等；数据资产对国家安全、公共利益或个人、组织合法权益的危害可能性越高，则数据资产风险越高。核心数据风险最高，不允许确权，且相关交易为A级交易。重要数据风险较高。个人数据风险较高，数据中个人信息的去标识化程度越高则数据资产风险越低（宜参见GB/T 42460-2023开展评价），含有敏感个人信息的数据比仅含有一般个人信息的数据的数据资产风险更高。公开数据风险较低。

——数据规模角度：数据规模越大，则数据资产风险越高。

* + 1. 数据交易主体风险

作为交易双方的数据交易主体风险将会影响到交易风险，两者呈正相关关系。数据交易主体风险从以下角度进行评价：

——数据安全能力角度：包括数据交易双方的数据安全管理能力、数据安全技术能力、人员管理及安全教育能力（宜参见GB/T 36073-2018、GB/T 37988-2019等模型开展评价）。主体数据安全能力越高，则数据交易主体风险越低。

——数据安全信用角度：包括近年内是否受到过与数据安全/个人信息保护相关的行政处罚、发生过数据泄露等数据安全事件等。主体数据安全信用越高，则数据交易主体风险越低。

——数据处理资质角度：包括是否具有根据法律规定收集、处理特定数据的特定资质或行政许可、是否属于特殊监管行业或承担特殊数据合规义务等。主体数据处理资质越完备，则数据交易主体风险越低。

——数据交易习惯角度：包含数据交易主体是否存在不当的交易习惯，主体的不当交易行为越多，则其数据交易习惯越差，数据交易主体风险越高。不当交易行为包括：可能对数据安全产生重大影响的交易行为；以自己为交易对象，多次进行自买自卖的行为；频繁下单并撤单的交易行为；巨额下单，且订单价格明显高于或低于同类数据（产品）的成交价格；针对某一数据（产品），一段时间内进行大量且连续的交易等。

* + 1. 数据交易过程风险

作为交易渠道的数据交易过程风险将会影响到交易风险，两者呈正相关关系。数据交易过程风险从以下角度进行评价：

——交易场景风险角度：包括数据交易的场景与目的是否具有危险性。交易场景风险越高，则数据交易过程风险越高。风险较高的交易场景包括：为关键信息基础设施提供服务、通过算法应用于自动化决策、数据跨境使用。

——交易合同风险角度：包括数据交易合同是否完备。数据交易合同越完备，交易合同风险越低，则数据交易过程风险越低。数据交易合同内容可能包括交易数据资产标的、设定交易双方的权利义务、数据资产的交易价格、数据权属条款、数据安全突发状况的应急处置条款、违约责任条款等。

——数据传输风险角度：包括数据传输方式是否安全。数据传输方式越安全，数据传输风险越低，则数据交易过程风险越低（宜参见GB/T 37932-2019中7.3、DB15/T 2199-2021中6.5等要求开展评价）。如离线数据传输安全性较高，加密在线数据传输安全性较高，明文在线数据传输安全性较低，跨境数据传输安全性较低。

* 1. 交易安全评价指标体系的处理规则

交易安全评价指标体系的处理规则如表C.2所示。

* 1. 交易安全评价指标体系处理规则

|  |  |  |
| --- | --- | --- |
| **交易安全评价等级** | **交易类型** | **处理规则** |
| A类 | 禁止类 | 禁止交易。 |
| B类 | 限制类 | 限制交易，要求数据资产供给方在提供相应材料后才能开展交易。 |
| C类 | 警示类 | 对交易风险进行提示，监督数据资产供给方与需求方在自愿平等的基础上开展交易。 |
| D类 | 自治类 | 自由开展交易。 |

* + 1. A类（禁止类）交易处理规则

数据资产权利审查机构应禁止被评估为A类的数据资产交易。

* + 1. B类（限制类）交易处理规定

数据资产权利审查机构应限制被评估为B类的数据资产交易，并要求数据资产供给方在提供相应材料后才能开展交易。

数据资产供给方需要提供的材料包括但不限于：

——法律法规规定的特殊交易信息及特殊交易场景下所需提交的附加文件，例如针对敏感个人信息规定的个人信息影响评估报告等。

* + 1. C类（警示类）交易处理规则

数据资产权利审查机构应对被评估为C类的数据资产交易作出风险点提示，监督数据资产供给方与需求方在自愿平等的基础上开展交易。

* + 1. D类（自治类）交易处理规则

数据资产权利审查机构应允许被评估为D类的数据资产交易的自由开展。

参 考 文 献

1. DB50/T 1049-2020 基于区块链的电子商务价值行为数据存证规范
2. DB31/T 1331-2021 区块链技术安全通用要求
3. GM/T 0111-2021 区块链密码应用技术要求
4. T/CESA 1048-2018  区块链 存证应用指南
5. T/SHSFJD  0001-2020  基于区块链技术的电子数据存证规范
6. T/TJIFA 003-2022  数据资产登记、存证、确权业务标准
7. T/SDME 01-2022  数据产品登记信息描述规范
8. T\_NSSQ 025-2022 资产管理数据资产确权登记导则
9. T/SSIA 0002-2018 区块链技术安全通用规范
10. TC260-PG-20212A 网络安全标准实践指南—网络数据分类分级指引
11. 山东数据交易有限公司《数据（产品）登记规则》2022
12. 上海数据交易所有限公司《全国统一数据资产登记体系建设白皮书》2022
13. 工业和信息化部《工业和信息化领域数据安全管理办法（试行）》2022
14. 深圳市发展和改革委员会《深圳市数据产权登记管理暂行办法》2023

