ICS 35.060
CCS L 74

中　国　电　子　学　会　标　准

JH/CIE 195—2021

区块链　数据要素流通授权管理规范

Blockchain — authorization specification for the circulation of data elements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电子学会 发布

目　次

前　　言 1
引　　言 2
1 范围 3
2 规范性引用文件 3
3 术语和定义 3
3.1 基本术语 3
3.2 参与方 4
3.3 数据授权通证 5
3.4 加密通证 6
3.5 数据使用通证 6
4 缩略语 6
5 概述 6
6 密钥管理机制 8
6.1 通则 8
6.2 基于 SM2 椭圆曲线公钥密码算法的密钥对生成 9
6.3 基于属性加密的密钥生成 9
6.3.1 初始化算法 9
6.3.2 使用方认证节点初始化算法 9
6.3.3 用户密钥产生算法 9
7 授权方授权与撤销 9
7.1 授权通证生成 9
7.2 授权通证加密 10
7.2.1 对称加密 10
7.2.2 生成授权策略 10
7.2.3 基于属性的加密 10
7.2.4 加密通证数据结构 10
7.3 加密通证上链 11
7.4 授权撤销 11

8 使用方申请 11
8.1 授权通证获取 11
8.2 数据使用通证生成 11
8.3 数据使用通证发送 12
8.3.1 单一数据使用通证发送 12
8.3.2 批量数据使用通证发送 12
9 数据源验证 13
9.1 数据使用通证合法性验证 13
9.2 数据使用通证存证验证 13
9.2.1 单一数据使用通证存证验证 13
9.2.2 批量数据使用通证存证验证 13
附录 A（资料性） 授权方授权示例 14
附录 B（资料性） 使用方申请示例 16
附录 C（资料性） 数据源验证示例 18

前　言

本文件依据 GB/T 1.1-2020《标准化工业导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件由清华大学提出。

本文件由中国电子学会区块链分会归口。

本文件起草单位：清华大学、工业互联网研究院、中国传媒大学、湖南省卫健委信息统计中心、湖南网数科技有限公司、岳麓山数据科学与技术研究院、北京科技大学。

本文件主要起草人：

引　言

2020 年 4 月 9 日，中共中央、国务院颁布了《关于构建更加完善的要素市场化配置体制机制的意见》，提出“加快培育数据要素市场”，进一步强化了数据作为生产要素的重要性。促进数据要素合法、合规地流通，是激发数据要素市场活力的着力点。

如图 1 所示，数据要素流通的主要流程包括：原始数据经过数据清洗和脱敏，并经过数据注册登记，形成便于流通的数据要素。数据要素经过数据授权后由数据使用方获得数据使用权，最后进行相应数据应用。其中，数据授权是构建数据要素市场，保护个人信息和推动数据要素安全应用的前提条件。

本文件所规范的数据要素授权主要由授权方将数据要素的使用权按照一定规则通过授权系统授予经过认证的数据使用方，并由数据源进行使用权的验证。授权过程中监管方实时监控授权系统和数据源。

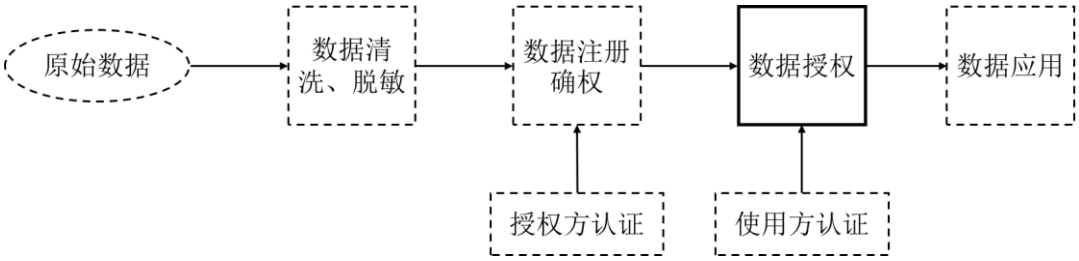

图 1 本文件所覆盖流程与数据流通上下游流程关联图

本文件的发布机构提请注意，声明符合本文件时，可能涉及到第7-10章与数据授权相关的专利的使用。本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利：《基于区块链和属性加密的医疗数据授权机制》

专利持有人姓名：清华大学

地址：北京市海淀区蓝旗营双清路30号

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

区块链 数据要素流通授权管理规范

1 范围

本文件规定了数据要素流通过程中的用户授权流程要求，包括密钥管理、授权方授权与撤销、使用方申请和数据源验证，描述了对应的监测方法，界定了有关术语和定义，并给出了示例。

本文件适用于不同实体间数据要素流通过程中用户授权的场景。

[示例：用户授权场景如医疗数据共享中的授权、金融数据流通中的授权]

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是未注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32918.1-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则

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/T32905-2016 信息安全技术 SM3 密码杂凑算法

ISO 22739:2020 区块链和分布式账本技术—词汇(Blockchain and distributed ledger technologies — Vocabulary)

3 术语和定义

下列术语和定义适用于本文件。

3.1 基本术语

3.1.1

数据要素 data element

经过数据治理和注册登记后，便于流通的数据单元。

3.1.2

实体 entity

独立并可被识别的对象。

[示例：实体如医院、银行、保险公司]

3.1.3

授权策略 authorization policy

数据授权方定义的包含访问控制条件的规则集。

3.1.4

通证 token

以数字形式存在的权益证明，代表系统中数据使用权的授予。

3.1.5

属性 attribute

由使用方认证节点负责定义和分配的，供数据授权方进行授权策略制定的数据使用方的特征。

3.2 参与方

3.2.1

数据授权方 data authorizer

数据授权过程中可对数据使用权进行分配的实体。

3.2.2

数据使用方 data user

数据授权过程中接受数据使用权转移的实体。

3.2.3

数据源 data source

负责数据存储和数据授权过程中数据使用权鉴定的实体。

3.2.4

监管方 supervisor

数据授权过程中负责实时监控授权行为是否违规的实体。
[示例：行政机关]

3.2.5

使用方认证节点 user authentication node

用于鉴别数据使用方身份并给其分配相应基于属性加密密钥的管理节点。

3.3 数据授权通证

3.3.1

数据哈希 data hash

流通数据通过 SM3 计算得到的哈希值，作为数据授权过程中数据的主键并可用于验证流通数据的完整性。

3.3.2

授权方账号 data authorizer account

数据授权方所拥有的基于 SM2 椭圆曲线公钥密码算法的公钥。主要用于标记数据授权方身份和验证其签名。

3.3.3

截止时间 authorization deadline

对应授权失效时间的字段。

3.3.4

数据源 ID data source ID

数据源在系统中的唯一标识符。

3.3.5

撤销信息 revocation information

数据授权方生成并进行授权撤销验证的字段。

3.3.6

授权方签名 authorizer signature

数据授权方生成用于证明其行使权利的字段。

3.4

加密通证 encrypted token

将数据授权通证中可能泄露隐私部分加密后生成的通证。

3.5

数据使用通证 data usage token

由数据使用方编辑，用于向数据源申请数据使用权限的通证。

4 缩略语

下列缩略语适用于本文件。
DO：数据授权方（data authorizer）
DU：数据使用方（data user）
DSC：数据源（data source）
ABE：基于属性的加密（attribute-based encryption）
DAT：数据授权通证（data authorization token）
ET：加密通证（encrypted token）
DUT：数据使用通证（data usage token）

5 概述

本文件描述了数据要素流通过程中的授权管理。授权管理主要由授权方将数据要素的使用权按照一定规则通过授权系统授予经过认证的数据使用方，并由数据源进行使用权的验证。授权过程中监管方实时监控授权系统和数据源。

授权过程中参与方间的关系见图 2。其中，使用方认证节点负责鉴别和认证数据使用方，给经过认证的数据使用方分配对应属性的密钥。数据授权方拥有分配数据要素使用权的权力。数据使用方通过授权系统获得数据授权方分配的数据使用权，并向数据源发起数据使用申请。数据源负责存储和管理数据，并验证数据访问请求的合法性。监管方宜由政府机构等可信第三方承担，负责实时监控授权系统和数据源，避免出现数据滥用等情况。

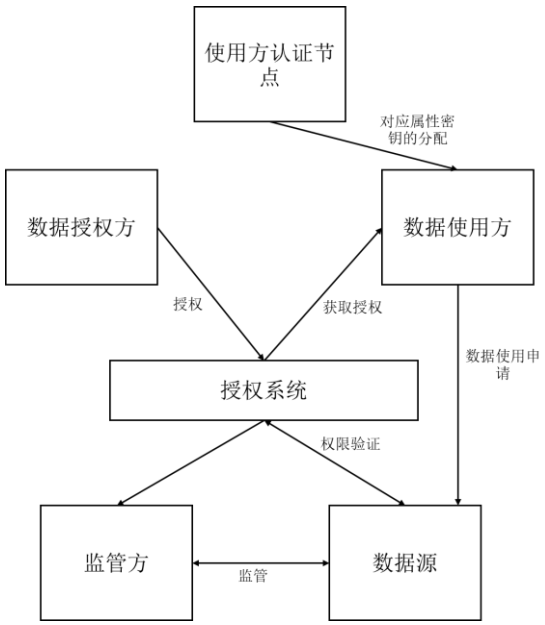

图 2 参与方关系图

数据授权管理流程应包括密钥管理、授权方授权与撤销、使用方申请和数据源验证四部分。其中，密钥管理应包括基于 SM2 椭圆曲线公钥密码算法的密钥对生成和基于属性加密的密钥生成。见图 3，授权方授权与撤销应包括生成数据授权通证、授权通证加密、加密通证上链和授权撤销 4 部分，示例见附录 A。使用方申请应包括授权获取、数据使用通证生成和数据使用通证发送 3 部分，示例见附录 B。数据源验证应包括数据使用通证合法性验证和数据使用通证存证验证 2 部分，示例见附录 C。

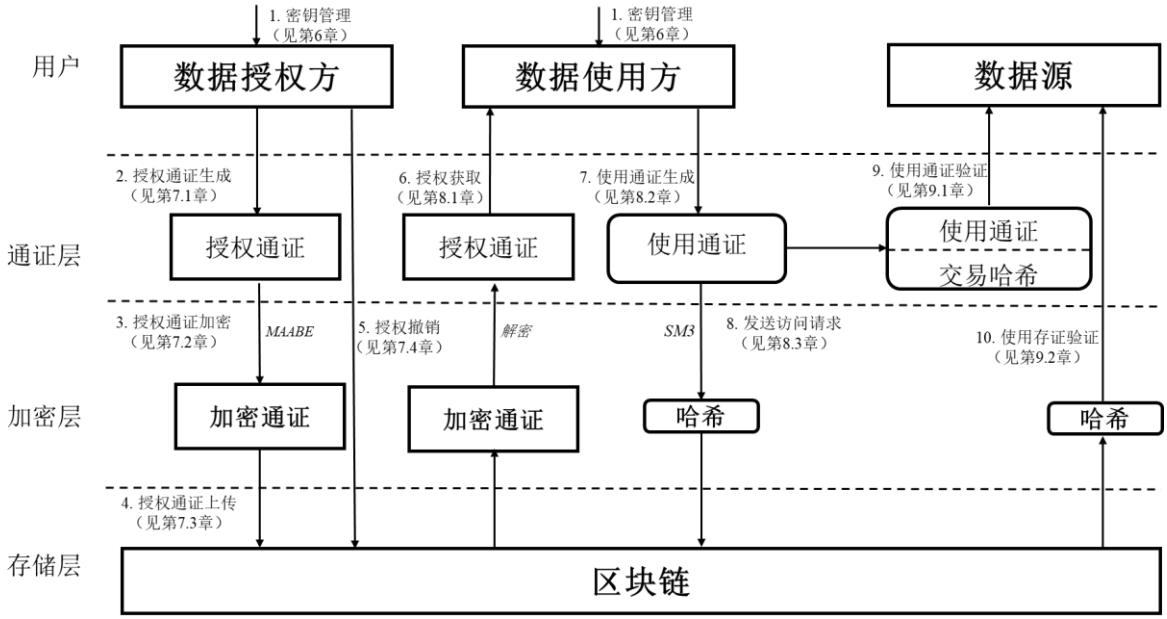

图 3 数据授权管理构成要素

a) 密钥管理：指数据授权方和数据使用方所拥有的密钥类型及其生成方式。

b) 授权通证生成：指数据授权方根据授权的数据、授权截止时间等构建具有授权功能的通证。

c) 授权通证加密：指数据授权方根据授权目标的属性加密授权通证生成加密通证。

d) 加密通证上链：指数据授权方将加密通证通过智能合约存储上区块链。

e) 授权撤销：指数据授权方主动发起使已上链加密通证失效的过程。

f) 授权获取：指数据使用方从区块链获取加密通证，并依靠自己基于属性的密钥进行解密进而获得完整授权通证的过程。

g) 使用通证生成：指数据使用方根据自身需求和获得的授权通证，签名并生成数据使用通证的过程。

h) 使用通证发送：指数据使用方将使用通证的哈希通过智能合约存证到区块链上并向数据源发送使用通证和存证的交易哈希。

i) 使用通证合法性验证：指数据源获得使用通证后验证使用通证合法性的过程。

j) 使用通证存证验证：指数据源在验证通证合法性后，通过区块链验证该使用通证的哈希有无被存证的过程。

授权系统结构见图 4，共分为通证层、加密层和存储层三层。其中通证层包括授权通证、使用通证等通证;加密层包含基于属性加密等多种加密工具;存储层包括区块链及链上的智能合约。

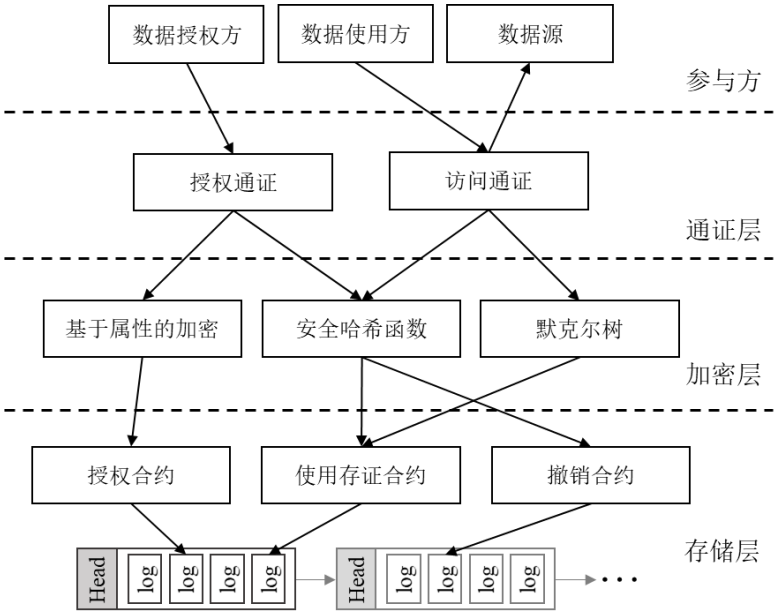

图 4 授权系统结构图

6 密钥管理机制

6.1 通则

密钥管理机制描述了数据授权方和数据使用方所拥有的密钥类型及其生成方式。数据授权方应拥有基于 SM2 椭圆曲线公钥密码算法的密钥对；数据使用方应拥有基于 SM2 椭圆曲线公钥密码算法的密钥对和基于属性加密的密钥。

6.2 基于 SM2 椭圆曲线公钥密码算法的密钥对生成

该密钥对的生成算法和公钥验证算法应符合 GB/T 32918.1-2016 第 6 章的规定。

6.3 基于属性加密的密钥生成

6.3.1 初始化算法

使用方认证节点生成随机参数 λ 为安全参数，输出系统公开参数为 Params。Params 作为后续每步操作的输入参数。方案中有 N 个使用方认证节点$\{A_1,A_2,...,A_N\}$，每个管理节点 A_i 管理一类属性集合并拥有唯一 ID。每个数据使用方拥有一个根据 uuid4[2]生成的唯一标识符 GID，并拥有一个经过参与者认证后得到的属性集合 SID。

6.3.2 使用方认证节点初始化算法

使用方认证节点应输入公开参数 Params 和认证节点的 ID_i，输出每个认证节点 A_i 的公私钥对$\{PK_i,SK_i\}$。

6.3.3 用户密钥产生算法

数据授权方应输入用户标识符 GID、用户属性集合 $SID \cap A_i$ 及授权机构的私钥 SK_i，输出每个用户的私钥 SK^i_{GID}。

7 授权方授权与撤销

7.1 授权通证生成

数据授权通证应由数据授权方生成，包含数据哈希、授权方账号、数据源 ID、截止时间、撤销信息和对上述信息的签名。通证结构应符合图 5 规定，采用 JSON 格式表示。

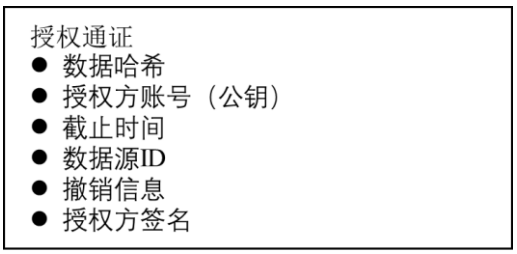

图 5 授权通证结构

图 5 中，数据哈希应由进行授权的数据通过哈希函数计算得到，哈希函数应符合 GB/T32905-2016 的规定；授权方账号应为数据授权方基于 SM2 椭圆曲线公钥密码算法生成的公钥；数据源 ID 应是提前定义的数据源在系统中的唯一标识符；截止时间应是本授权通证失效时间，应采用 64 位 Unix 时间格式；授权方签名方法应符合 GB/T 32918.2-2016 的规定。

撤销信息生成方式应符合图 6 规定。数据授权方将数据哈希、授权方帐户、数据源 ID、授权期限进行基于属性的加密，具体加密方式见 7.2 节。随后，数据授权方将加密后的数据与生成的 256 位随机数拼接，并计算哈希函数结果，该计算的哈希函数结果作为撤销信息。过程中使用的哈希函数应符合 GB/T32905-2016 的规定。

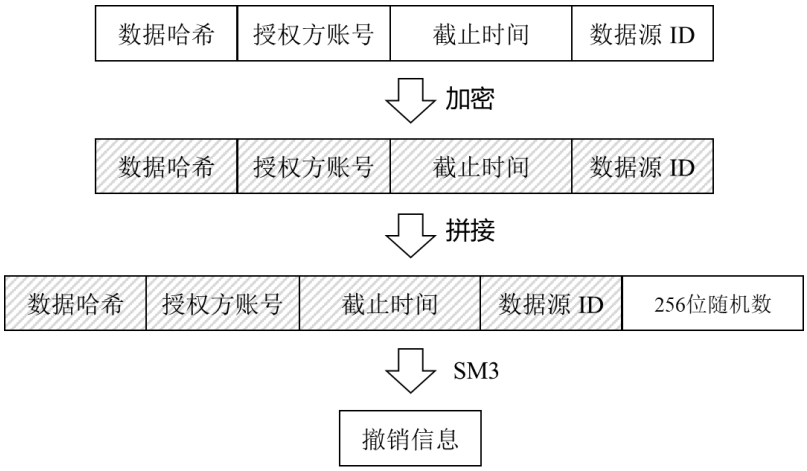

图 6 撤销信息生成

7.2 授权通证加密

7.2.1 对称加密

数据使用方应生成 128 位随机数，根据该随机数利用 AES 算法加密数据哈希、授权方账号、截止时间和数据源 ID 4 个字段。

7.2.2 生成授权策略

数据授权方应按需选择解密加密通证的属性，生成授权策略。

7.2.3 基于属性的加密

数据授权方应输入 AES 密钥、授权策略和使用方认证节点公钥 PK_i，输出密文。

7.2.4 加密通证数据结构

加密通证结构应符合图 7 规定，使用 JSON 格式表示，应包括通证头数据、通证验证数据和访问密钥三部分。其中通证头数据应包含数据哈希、授权方账号、截止时间和数据源 ID 共 4 个字段，使用 AES 加密；通证验证数据应包含撤销信息和签名共 2 个字段，为明文；访问密钥应包含 AES 密钥，使用基于属性的加密。

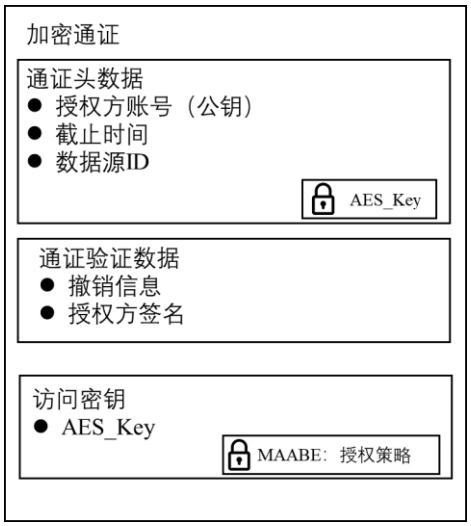

图 7 加密通证

7.3 加密通证上链

数据授权方应将加密通证通过智能合约写入事件中进行持久化存储。智能合约和区块链关系应符合 ISO 22739:2020 界定的条件。

7.4 授权撤销

授权撤销应由授权方提交申请主动授权撤销。

当数据授权方想要撤销授权时，应通过区块链的智能合约接口提交加密通证上链的交易哈希和用于授权撤销 256 位随机数。然后，区块链各共识节点可以通过再次计算撤销信息来验证撤销是否有效。由于 SM3 的抗碰撞性，随机数很难被别人伪造。如果新计算的撤销信息与链上的相同，则证明授权被数据授权方撤销。验证无误后，区块链共识节点将撤销信息和随机数作为映射结构写入区块链，供用户和数据源验证。

在整个撤销过程中，数据授权方只需要提供随机数。授权方的账户和其他私人信息不会被泄露。

8 使用方申请

8.1 授权通证获取

数据使用方从区块链上下载加密通证后，利用基于属性加密的用户私钥组 SK^{i}_{GID} 解密访问密钥得到 AES 密钥，进而通过 AES 密钥解密通证头数据中的全部字段，得到完整的授权通证。不符合访问结构的数据使用方无法解密加密后的访问密钥。

8.2 数据使用通证生成

数据使用方应对授权通证和自己的账号进行签名，将数据授权通证、使用方账号和签名拼接后得到数据使用通证，并使用 JSON 格式表示。其中，使用方账号为数据使用方基于 SM2 椭圆曲线公钥密码算法的公钥，签名应符合 GB/T 32918.2-2016 的规定。

生成的数据使用通证格式应符合图 8 规定。

图 8 数据使用通证

8.3 数据使用通证发送

8.3.1 单一数据使用通证发送

数据使用方应利用 SM3 计算数据使用通证的哈希值，并将其通过智能合约写入区块链中进行持久化存储，用于数据使用过程的留痕并便于未来审计。随后，数据使用方将数据使用通证和合约交易的哈希值传输给对应的数据源。

8.3.2 批量数据使用通证发送

数据使用方经常需要同时使用多个数据。本文件允许将多个数据使用通证的哈希聚合为一个进行链上存证。

数据使用方应将自己的多个数据使用通证的哈希值通过默克尔树聚合成一个哈希值。见图 9，A-F 代表一条数据使用通知，其中 A-D 属于数据源 A，E 和 F 属于数据源 B。为了便于数据源进行验证，数据使用方先将同一家数据源的数据通过 Merkel 树进行聚合，比如数据源 A 内的数据 A-D 聚合成该云的根哈希 Hash(A|B|C|D)，再将不同数据源的根哈希聚合成本次数据申请最终的根哈希，并将该根哈希通过智能合约对应接口写入区块链。随后，数据使用方将数据使用通证、合约交易的哈希值和计算根哈希对应路径上的哈希传输给对应的数据源。

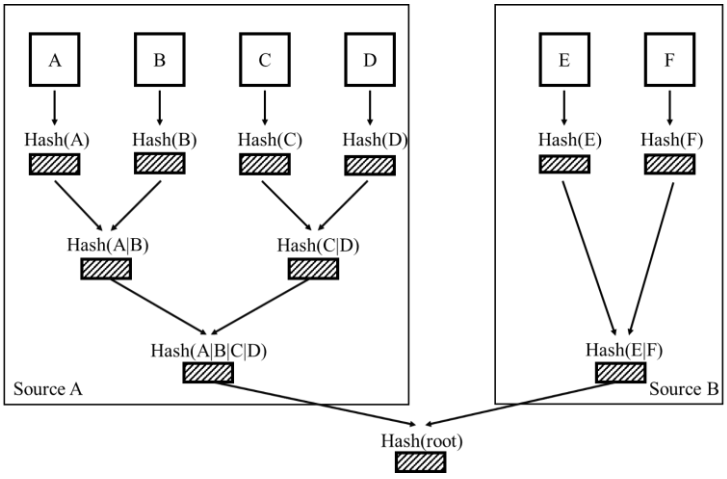

图 9 批量数据使用通证哈希聚合

9 数据源验证

9.1 数据使用通证合法性验证

数据源应依次验证数据使用通证中数据哈希是否在数据源存储系统内存在，通证中数据授权方账号是否与数据源信息系统中对应数据记录的授权方账号相同，当前时间是否超过截至时间，授权是否被授权方撤销，授权方签名和使用方签名是否符合，使用方是否符合监管方要求。若上述验证均通过，则数据使用通证合法。

9.2 数据使用通证存证验证

9.2.1 单一数据使用通证存证验证

数据源应利用 SM3 计算数据使用通证的哈希，然后根据数据使用方发送的交易哈希验证该交易是否在区块链中存在；若存在则判断通过交易哈希在链上找到的使用通证哈希与数据源计算得到的使用通证哈希是否相同，若相同则说明数据使用通证存证验证通过。

9.2.2 批量数据使用通证存证验证

数据使用方应在给数据源发送批量数据申请时，应发送该数据到根哈希对应路径上的哈希以进行验证。见图 9 中，数据源 A 进行存证验证时，需要数据使用方发送完整的数据使用通证 A-D，对应哈希 Hash(E|F)，存证信息的交易哈希。数据源 A 计算得到根哈希，再将此哈希和区块链中存储的对应哈希值进行比对，如果相同则验证通过，否则验证不通过。

附录 A

（资料性）

授权方授权示例

A.1 背景

本附录描述了一个医疗数据流通授权中授权方授权的示例。患者（数据授权方 A）的医疗数据经过治理后形成数据要素（数据 D）。该数据要素存储在某医院（数据源 S）中。患者希望将数据授权给从事肿瘤方向医学研究的三甲医院医生，故授权对象的属性应包括**三甲医院医生**和**从事肿瘤方向医学研究**。其中，属性三甲医院医生的通过某省卫健委信息科（使用方认证节点 AM1）认证；属性从事肿瘤方向医学研究通过某医科大学（使用方认证节点 AM2）认证。

数据授权方 A 针对数据 D 生成相应的授权通证，并根据需求（肿瘤方向医学研究和三甲医院）进行属性加密。患者将加密通证存储到区块链上。

A.2 授权系统初始化与密钥管理

A.2.1 初始数据

数据源 S 中存储的数据 D 哈希值为：’0ba928304d78f6a9d83e066e3a5f87e3157315d5c800723b8560840047de876e’

数据源 S 的 ID：’HN132’

数据授权方 A 的 SM2 密钥对(base64)：{"pk": "99eiRa1NnQEp3RqlSeFwqBRJe4hg+85Qx6e2lo3U/fXroj3xOUjIKBvFDW/7tXI17YLSBvtAglmqxRBgxJJV1Q==", "sk": "ZCAh0MnU10Gbar9i9UzuLuyIvPjV/PAK67jyp/dwf9k="}

A.2.2 基于属性加密密钥的生成

基于属性加密的公共参数：{'g1': [80102601856999629943396397899070816650911674141786731315016484272205239701555609285401047298817774160184621243070357871208505581298052465247715691414166692, 866489475245383361136197480529284018199347569547024156656062557143275735976012292648769701518502292855066868972763372905840651262205365139717956289359854 2], 'g2': [79208247711853767705463735158105953568040052908490415720202453100313788003682914179852391110929542347753514180340340821432066838502838330348144602824933 96, 78912349110945172836996707331960867994268424111026399823929884037232899495751613615319887630839155504297176159569481456791512170949676837932214756793263 01], 'egg': [21287448335711470812111687919607971397452268660946785495391203504859356203640917528338317855564147499044933896802376404890105887395571171874726688684915 9, 60215951651157115706947226024669266641926923351444448311884531206142794951086016987356988440726753005965693417985000772199226926865817586209667961681262 47]}

使用方认证节点 AM1 的公私钥对为：{'egga': [55431332526446726717564760073955482861164625653610313711391854210845601171430326913958050525120873688699266125803122466608342305824817501096505411130874205316533323715270133944505982496953143038613304042195300897109338177586481156995967520642057417820129346895921842314245988718434194957428589704811939379674], 'gy': [19157141461120727276759414937038706705313544042897408343055512936133734923069803568060348826907411865032056776522532850067105092375444303314774751266569155666394398048453251703079508320474009333314963167145943365271376643557300105830016571

722235035387985585002388443384151192709827554020911760054920704715331 8]}

使用方认证节点 AM2 的公私钥对为：{'egga':
[722016293678725992845746571298556364583142395401680019545159326660023485035993494079498799103815098683792788903571370327789365630878104463833649503563000,
361017163625419676513733619300933938749750174661821127628078230869968655191937022340860096104358282481011503024632436933135497578857090458071950789286469 7], 'gy':
[602379010152612185424576599282410271272629234241612761486879114717590226165470136252423075872286940700993571153390921900260084279596322461538750372556 25,
421535139081436846057639906150787111676424934132474752822346400928213116594018972635151507507820091136002765529361343892978957086830512322374041910884125 7]}

A.3 数据授权通证生成

数据授权方 A 生成关于数据 D 的授权通证，该授权通证的失效时间为北京时间 2022 年 12 月 31 日 12 点。生成的授权通证如下所示：

{"Data Hash": "0ba928304d78f6a9d83e066e3a5f87e3157315d5c800723b8560840047de876e",
"Authorizer Account":
"99eiRa1NnQEp3RqlSeFwqBRJe4hg+85Qx6e2lo3U/fXroj3xOUjIKBvFDW/7tXI17YLSBvtAglmqxRBgxJJV1Q==", "End Time": "1672459200", "Source ID": "HN132", "Revocation Information": "",
"SignatureA":
"SPKE+auAdo/6p8CnpoLozUOczyMMHvj80nwnFJShCA1vKJ2HngWilJKD0JB73zrm/f4ZoMFl9nUnMcHANH3bzg=="}

A.4 加密通证生成

数据授权方 A 根据“从事肿瘤方向医学研究”和“三甲医院医生”2 项属性，对上一步生成的授权通证进行加密，生成的加密通证如下：

{“Token Headers”:
[244390291215946417381821074274832973108412171505936851812730581442473803875827862518035283953948986672478497923388185502787143096758432996829802178059876,
533757252761625490009078981900548896684534896320649419281939140809993478626464861565248655997549437907661861976804445847115238228329056905717583320071119 2]; “Token Verification Data”: {"Revocation Information": "";"SignatureA":
"SPKE+auAdo/6p8CnpoLozUOczyMMHvj80nwnFJShCA1vKJ2HngWilJKD0JB73zrm/f4ZoMFl9nUnMcHANH3bzg=="}; “Access Key”:
28dfa28f4b16e74b95774a1236ec5d7f464dcc26c756c94b0919d7d4913cc23e}

A.5 加密通证上链

数据授权方 A 通过智能合约将加密通证记录在区块链上。

附录 B

（资料性）

使用方申请示例

B.1 背景

本附录描述了一个医疗数据流通授权中使用方申请的示例。三甲医院从事肿瘤方向医学研究的医生（数据使用方 B）试图通过授权系统获得相关数据的授权。数据使用方 B 进行通过某省卫健委信息科（使用方认证节点 AM1）认证其三甲医院医生的身份，通过某医科大学（使用方认证节点 AM2）认证其从事肿瘤方向医学研究，并获得相应的属性密钥。

医生从区块链上获取加密通证并解密，生成相应的使用通证，将使用通证的哈希值存证在区块链上，并向数据源 S 发起数据使用申请。

B.2 授权系统初始化

B.2.1 初始数据

数据使用方 B 的 GID 为：’945da329-1d77-4e4d-9242-b1db42e5cb14’

数据使用方 B 的 SM2 密钥对(base64)为：{"pk": "bHyE/HAj+Y68lVlF1225H/m/SKcUyH8li/6ltiJ0Dy3Oc8nhmAdSBXqmTochXe4fG+NfvuBJGq3tkPoJaOslUA==", "sk": "fxJTqu6GOhUGI9kOAD7fpbLLdPqqi/pBubDQbJ7QukU="}

B.2.2 基于属性加密密钥的生成

公共参数、使用方认证节点 AM1、AM2 公私钥同附录 A。

数据使用方 B 分别去使用方认证节点 AM1、AM2 认证身份，并获得属性密钥如下所示：

{'keys': {'PHD@AM1': {'K':
[852420535411363076970633918197590235256939453610428273719530895830106258370038407295473918743544175797835706397385040328955718473949294259995699591972901 5,
27491342496999133178702367127905303006384629829986965934046682214622597303448393733799896588266428781987840405812425300488688675602034267800391597636343 13], 'KP':
[418818153001842345201204648292722005139563016561245996036847950507590065220204664581840217076421390678681773834447624663532102631283852529806113513092481 5,
661172080161726868906006581324518720894673259208626293426490536538255337308707823950594191429802082966468848588860664996373859492933500286962633057838707 0]},
'Hospital@AM2': {'K':
[766892115690590244329475391864310115384851126620549055487892231529978936268632538190771116977442129247584642189532002358066089010701142936432033792955753 0,
777420471219371423798527378573956453441967152018180616713322557345712284101683642196924550144934625256350148373252443056084297785616371218598146255920571 5], 'KP':
[469080915090255326677472660792346258713081915223402773935121788481878419476326393279305773401041326472807869411185675634395610192056145757103318519994705 4,
502273329055759529934430675777044262605539207485056468103658895946015452956320765431473259334888435674998200302609137033137135695144616653866394440599140 6]}}}

B.3 授权获取

数据使用方 B 从区块链获取相应的加密通证，解密后得到完整的授权通证如下：

{"Data Hash": "0ba928304d78f6a9d83e066e3a5f87e3157315d5c800723b8560840047de876e", "Authorizer Account": "99eiRa1NnQEp3RqlSeFwqBRJe4hg+85Qx6e2lo3U/fXroj3xOUjIKBvFDW/7tXI17YLSBvtAglmqxRBgxJJV1Q==", "End Time": "1672459200", "Source ID": "HN132", "Revocation Information": "", "SignatureA": "SPKE+auAdo/6p8CnpoLozUOczyMMHvj80nwnFJShCA1vKJ2HngWilJKD0JB73zrm/f4ZoMFl9nUnMcHANH3bzg=="}

B.4 数据使用通证生成

数据使用方 B 根据授权通证生成使用通证，内容如下：

{"Authorization Token": {"Data Hash": "0ba928304d78f6a9d83e066e3a5f87e3157315d5c800723b8560840047de876e", "Authorizer Account": "99eiRa1NnQEp3RqlSeFwqBRJe4hg+85Qx6e2lo3U/fXroj3xOUjIKBvFDW/7tXI17YLSBvtAglmqxRBgxJJV1Q==", "End Time": "1672459200", "Source ID": "HN132", "Revocation Information": "", "SignatureA": "SPKE+auAdo/6p8CnpoLozUOczyMMHvj80nwnFJShCA1vKJ2HngWilJKD0JB73zrm/f4ZoMFl9nUnMcHANH3bzg=="}, "User Account": "zlATZLYi7Pe5iUoVe6mcDMYZuOvzNgYp6k6iLN0CvamCHkVcH8uhxaQlYvk57x7udKidQejRwc1483wYifXBTw==", "SignatureU": "bHyE/HAj+Y68lVlF1225H/m/SKcUyH8li/6ltiJ0Dy3Oc8nhmAdSBXqmTochXe4fG+NfvuBJGq3tkPoJaOslUA=="}

B.5 使用通证发送

数据使用方 B 计算使用通证的哈希值，结果如下：

877fb6649cec5870e5e63e0c5180de1a8182b33d5022cf3103290cb7608ff688

将哈希值通过智能合约存证到区块链上并得到相应的交易哈希。智能合约执行完毕后，数据使用方 B 将使用通证和交易哈希发送给数据源 S。

在批量数据申请使用时，通过 8.3.2 节的方式将多个使用通证的哈希值聚合为一个根哈希，并将该根哈希存证到区块链上。之后将数据使用通证、合约交易的哈希值和计算根哈希对应路径上的哈希传输给对应的数据源 S。

附录 C

（资料性）

数据源验证示例

C.1 背景

本附录描述了一个医疗数据流通授权中数据源验证的场景。某医院（数据源 S）接受数据使用方发起的数据使用申请，并进行相关验证。某省卫健委综合监督处（监管方）实时监控数据源 S 和区块链上的相关信息。

数据源 S 在接受到数据使用方 B 的使用申请（使用通证和交易哈希）后，进行使用通证的验证，并向监管方验证该数据使用申请是否符合监管要求。

C.2 数据使用通证验证

数据源 S 在接受到数据使用方 B 的使用申请后，分别验证如下 6 步的正确性。若验证均通过则说明使用通证验证合法。

a) 验证数据哈希是否在数据源存储系统内存在

b) 验证数据授权方账号是否与数据源信息系统中对应数据记录的授权方账号一致

c) 验证当前时间是否在截止时间范围内

d) 验证授权是否被数据授权方撤销

e) 验证数据使用方和授权方签名是否正确

f) 验证使用方是否符合监管方要求

C.3 数据使用通证存证验证

数据源 S 计算接收到的数据使用方 B 的使用通证的哈希，随后通过交易哈希从区块链获得数据使用方 B 存证的使用通证哈希。

数据源 S 判断使用通证的哈希值与区块链上存证的哈希值是否一致，若一致则证明使用通证存证验证通过，若不一致则说明验证不通过。

参 考 文 献

[1] Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption[C]. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015: 315-332.

[2] Leach P, Mealling M, Salz R. A universally unique identifier (uuid) urn namespace[J]. 2005.