(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110071969 B
(45)授权公告日 2021.11.30

(21)申请号 201910307310.0
(22)申请日 2019.04.17
(65)同一申请的已公布的文献号
申请公布号 CN 110071969 A
(43)申请公布日 2019.07.30
(73)专利权人 杭州云象网络技术有限公司
地址 311121 浙江省杭州市余杭区仓前街道海创科技中心2幢301室
(72)发明人 黄步添 刘振广 陈建海 石太彬 闫凤喜 王从礼
(74)专利代理机构 杭州天勤知识产权代理有限公司 33224
代理人 王琛
(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 107241360 A,2017.10.10
CN 109472569 A,2019.03.15
CN 107886388 A,2018.04.06
CN 109410053 A,2019.03.01
CN 108876669 A,2018.11.23
CN 107995120 A,2018.05.04
KR 101893729 B1,2018.10.04

审查员 刘磊

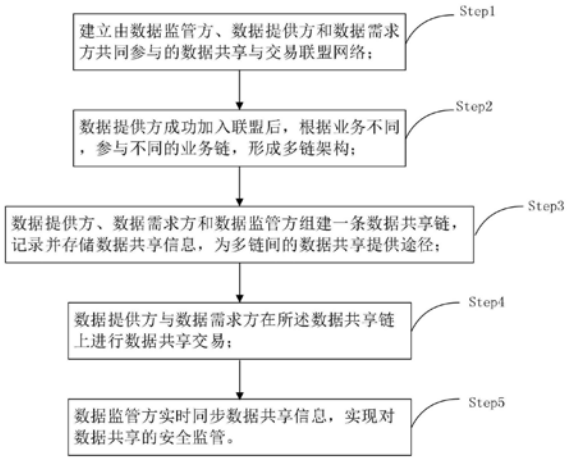
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种基于多链架构的数据安全共享方法

(57)摘要

本发明公开了一种基于多链架构的数据安全共享方法，在多链架构下，完成链与链之间共享数据的自由发布、自主发现、灵活交付，实现数据安全共享与交易。本发明采用多链架构的数据共享联盟链网络，实现不同业务数据的隔离，并创建数据提供方、数据需求方和数据监管方共同参与的数据共享链，实现链与链之间去中心化的数据自主共享与交易，并且赋予数据监管方超级权限，同步链上数据共享和交易记录，规范数据共享交易的安全有序性。



CN 110071969 B

1.一种基于多链架构的数据安全共享方法,包括如下步骤:

(1)建立由数据监管方、数据提供方和数据需求方共同参与的数据共享与交易联盟网络系统;

(2)加入联盟网络后,数据提供方根据不同业务参与不同的业务链,形成多链架构,具体实现过程如下:

2.1加入联盟网络的数据提供方根据业务数据需求,创建不同的业务节点,组建多条业务链,每条业务链包含与本业务链相关的数据账本和合约部署;

2.2任一数据提供方根据所参与的业务类型选择性加入一条或多条业务链,使得数据提供方根据数据业务类型的不同实现数据隔离和扩展;

2.3数据提供方在每条业务链上产生的业务数据经加密后存储在对应链上的数据中心账本中;

(3)由数据提供方、数据需求方和数据监管方组建一条数据共享链记录并存储数据共享信息,为多链间的数据共享提供途径,具体实现过程如下:

3.1数据提供方在每条业务链中提供一个可读取的数据存储节点,该节点存储对应业务链的数据描述信息,由多个数据存储节点加入并组建一条数据共享链;

3.2数据需求方和数据监管方作为节点加入该数据共享链,分别在链上参与数据共享和监管;

3.3为每个加入的节点分配一对秘钥,将各节点的信息写入数据共享链中,各节点利用所拥有公钥对其数据信息加密后进行广播至链上,并利用私钥对其获取的信息进行解密,保证数据信息的安全防篡改;

(4)数据提供方与数据需求方在数据共享链上进行数据共享交易;

(5)数据监管方实时同步数据共享信息,实现对数据共享的安全监管。

2.根据权利要求1所述的数据安全共享方法,其特征在于:所述步骤(1)的具体实现过程如下:

1.1由相关平台运营方负责搭建数据共享与交易联盟网络系统,数据监管方加入该系统并运行联盟网络,系统为数据监管方分配一对秘钥,用于对新加入成员的注册申请进行审核签名,并生成可信证书,作为新加入成员的加入凭证,实现对联盟网络的监管;

1.2数据提供方和数据需求方分别进行系统注册和认证,认证通过后加入联盟网络,认证信息包括身份信息和加入凭证,所述加入凭证为数据监管方颁发的可信证书,即数据提供方和数据需求方分别进行系统注册,提供身份信息,数据监管方获取到新加入成员的注册信息,对其进行审核,审核通过则颁发可信证书,进行注册的数据提供方和数据需求方可凭借获取的可信证书加入联盟网络。

3.根据权利要求1所述的数据安全共享方法,其特征在于:所述步骤(4)的具体实现过程如下:

4.1数据提供方将其在不同业务链上的数据描述信息在数据共享链进行广播并写入数据存储节点;

4.2数据需求方从数据共享链中读取数据提供方发布的数据描述信息,根据自身数据需求选择目标数据,并向该目标数据对应的数据提供方发送数据权限请求;

4.3数据提供方获取数据需求方发送的数据权限请求,按照特定规则对获取的数据权

限请求进行权限批复，将权限批复结果发布到链上；

4.4数据需求方获取权限批复结果，若权限批复通过，则拥有权限并可访问相应数据中心账本的数据；若未通过，则无法访问。

4.根据权利要求3所述的数据安全共享方法，其特征在于：在数据共享链上制定权限批复协议，该协议包括数据提供方对数据需求方的审核要求及数据监管方制定的数据共享规则，步骤4.3中所述的特定规则即根据该权限批复协议进行权限批复。

5.根据权利要求1所述的数据安全共享方法，其特征在于：所述步骤(5)的具体实现过程为：数据监管方参与数据共享链，针对每个业务链的可共享数据均拥有相应的数据中心账本，数据监管方持有公钥，利用公钥对链上数据中心账本中的内容进行加密，并随时调取其中数据共享及交易信息，实现对数据共享与交易的安全监管。

6.根据权利要求1所述的数据安全共享方法，其特征在于：还包括选取代理节点，所述代理节点包括数据提供方的访问代理节点、数据需求方的请求代理节点和数据监管方的监管代理节点；由请求代理节点发送数据权限请求，访问代理节点将数据描述信息在数据共享链上进行广播并根据权限请求进行权限批复，监管代理节点负责颁发可信证书，并同步数据共享和交易记录。

一种基于多链架构的数据安全共享方法

技术领域

[0001] 本发明属于数据共享及区块链技术领域，具体涉及一种基于多链架构的数据安全共享方法。

背景技术

[0002] 随着数据规模和价值的日益提升，通过数据共享挖掘数据的潜在价值变得越来越重要；但如何确保数据拥有者放下猜忌，相互信任，有效地解决“信息孤岛”难题，并在开放共享同时，保护敏感信息、涉密数据等不被非法获取利用，是开放共享的基本共识和需求。

[0003] 目前的数据共享方法，主要包括传统数据共享方案和中心化数据共享方案；传统数据共享方案是使用传统的隐私保护手段实现内部共享，同时为降低暴露隐私数据的风险选择拒绝对外开放共享；中心化数据共享方案是以第三方为数据开放和共享为中枢，各数据拥有者对第三方信任并对第三方开放数据，数据共享过程通过第三方来调度实现。现有的传统共享方案以拒绝对外开放来降低隐私风险，不仅无法挖掘数据的潜在价值，不能最大化其利益，且会导致信息建设滞后；中心化数据共享方案虽然解决了互不信任的问题，但却由于数据集中在第三方而带来的安全问题，第三方无法保证绝对数据安全，一旦发生数据泄漏会造成严重后果。

[0004] 近几年来，当下具备分布式组织架构和去中心化、高保密性特点的区块链技术日益引起人们的关注；特别是联盟链技术，能够建立有别于自上而下监管体制的众多行业机构间相互监督的分布式对等监管体制，由专业的人进行专业的监管，能够有效克服传统监管的弊端。目前区块链技术越来越多的被应用到实体行业内，现有的基于联盟链的信用存证、防伪平台、智能交通以及联盟链政府机构等渐渐出现在大众面前。

[0005] 与云存储不同的是，区块链是去中心化的计算和存储技术，提供存储能力的节点可以分布在不同位置，现有区块链技术在单链架构下存在性能、容量、隐私、隔离性、扩展上的瓶颈。随着的账本数量的增长，交互延迟会呈指数式增长，也就是说区块链网络中的账本越多延迟就会越高。另外，联盟链是个广泛的治理共同体，但依旧允许广泛共同体下存在多个不同的小集体，既是允许机构或行业做更深度的治理收敛，同时多个不同的小集体又共享联盟链的基础设施。如果实际操作中以一个治理收敛为一条链，那多链既是更符合实际的治理场景。

[0006] 区块链是分布式总账的一种，一条区块链就是一个独立的账本，两条不同的链，就是两个不同的独立的账本，两个账本没有关联，本质上价值没有办法在账本间转移。在多链架构的场景下的区块链网络中，不同业务的数据存储在各个区块链的账本中，而链与链之间无法直接进行去中心化的数据共享和交易，无法满足用户的个性化数据共享需求。因此，多链架构下数据共享过程的安全可控、全面监管等技术是目前急切需要突破的。

发明内容

[0007] 鉴于上述，本发明提供了一种基于多链架构的数据安全共享方法，在多链架构下，

完成链与链之间共享数据的自由发布、自主发现、灵活交付，实现数据安全共享与交易。

[0008] 一种基于多链架构的数据安全共享方法，包括如下步骤：

[0009] (1)建立由数据监管方、数据提供方和数据需求方共同参与的数据共享与交易联盟网络系统；

[0010] (2)加入联盟网络后，数据提供方根据不同业务参与不同的业务链，形成多链架构；

[0011] (3)由数据提供方、数据需求方和数据监管方组建一条数据共享链记录并存储数据共享信息，为多链间的数据共享提供途径；

[0012] (4)数据提供方与数据需求方在数据共享链上进行数据共享交易；

[0013] (5)数据监管方实时同步数据共享信息，实现对数据共享的安全监管。

[0014] 进一步地，所述步骤(1)的具体实现过程如下：

[0015] 1.1由相关平台运营方负责搭建数据共享与交易联盟网络系统，数据监管方加入该系统并运行联盟网络，系统为数据监管方分配一对秘钥，用于对新加入成员(数据提供方和数据需求方)的注册申请进行审核签名，并生成可信证书，作为新加入成员的加入凭证，实现对联盟网络的监管；

[0016] 1.2数据提供方和数据需求方分别进行系统注册和认证，认证通过后加入联盟网络，认证信息包括身份信息和加入凭证，所述加入凭证为数据监管方颁发的可信证书，即数据提供方和数据需求方分别进行系统注册，提供身份信息，数据监管方获取到新加入成员(数据提供方和数据需求方)的注册信息，对其进行审核，审核通过则颁发可信证书，进行注册的数据提供方和数据需求方可凭借获取的可信证书加入联盟网络。

[0017] 进一步地，所述步骤(2)的具体实现过程如下：

[0018] 2.1加入联盟网络的数据提供方根据业务数据需求，创建不同的业务节点，组建多条业务链，每条业务链包含与本业务链相关的数据账本和合约部署；

[0019] 2.2任一数据提供方根据所参与的业务类型选择性加入一条或多条业务链，使得数据提供方根据数据业务类型的不同实现数据隔离和扩展；

[0020] 2.3数据提供方在每条业务链上产生的业务数据经加密后存储在对应链上的数据中心账本中。

[0021] 进一步地，所述步骤(3)的具体实现过程如下：

[0022] 3.1数据提供方在每条业务链中提供一个可读取的数据存储节点，该节点存储对应业务链的数据描述信息，由多个数据存储节点加入并组建一条数据共享链；

[0023] 3.2数据需求方和数据监管方作为节点加入该数据共享链，分别在链上参与数据共享和监管；

[0024] 3.3为每个加入的节点分配一对秘钥，将各节点的信息写入数据共享链中，各节点利用所拥有公钥对其数据信息加密后进行广播至链上，并利用私钥对其获取的信息进行解密，保证数据信息的安全防篡改。

[0025] 进一步地，所述步骤(4)的具体实现过程如下：

[0026] 4.1数据提供方将其在不同业务链上的数据描述信息在数据共享链进行广播并写入数据存储节点；

[0027] 4.2数据需求方从数据共享链中读取数据提供方发布的数据描述信息，根据自身

数据需求选择目标数据，并向该目标数据对应的数据提供方发送数据权限请求；

[0028] 4.3数据提供方获取数据需求方发送的数据权限请求，按照特定规则对获取的数据权限请求进行权限批复，将权限批复结果发布到链上；

[0029] 4.4数据需求方获取权限批复结果，若权限批复通过，则拥有权限并可访问相应数据中心账本的数据；若未通过，则无法访问。

[0030] 进一步地，在数据共享链上制定权限批复协议，该协议包括数据提供方对数据需求方的审核要求及数据监管方制定的数据共享规则，步骤4.3中所述的特定规则即根据该权限批复协议进行权限批复。

[0031] 进一步地，所述步骤(5)的具体实现过程为：数据监管方参与数据共享链，针对每个业务链的可共享数据均拥有相应的数据中心账本，数据监管方持有公钥，利用公钥对链上数据中心账本中的内容进行加密，并随时调取其中数据共享及交易信息，实现对数据共享与交易的安全监管。

[0032] 进一步地，所述数据安全共享方法还包括选取代理节点，所述代理节点包括数据提供方的访问代理节点、数据需求方的请求代理节点和数据监管方的监管代理节点；由请求代理节点发送数据权限请求，访问代理节点将数据描述信息在数据共享链上进行广播并根据权限请求进行权限批复，监管代理节点负责颁发可信证书，并同步数据共享和交易记录。

[0033] 本发明采用多链架构的数据共享联盟链网络，实现不同业务数据的隔离，并创建数据提供方、数据需求方和数据监管方共同参与的数据共享链，实现链与链之间去中心化的数据自主共享与交易，并且赋予数据监管方超级权限，同步链上数据共享和交易记录，规范数据共享交易的安全有序性。

附图说明

[0034] 图1为本发明基于多链架构数据安全共享方法的系统架构示意图。

[0035] 图2为本发明基于多链架构数据安全共享方法的流程示意图。

[0036] 图3为数据提供方与数据需求方在数据共享链上进行数据共享交易的流程示意图。

具体实施方式

[0037] 为了更为具体地描述本发明，下面结合附图及具体实施方式对本发明的技术方案进行详细说明。

[0038] 在本实施例中，系统架构如图1所示，该系统架构下的数据安全共享方法包括如下步骤，整体流程如图2所示。

[0039] Step1：建立由数据监管方、数据提供方和数据需求方共同参与的数据共享与交易联盟网络。

[0040] (1)首先由联盟平台运营方负责搭建数据共享与交易联盟系统，数据监管方加入系统并运行联盟链网络，系统为监管机构分配一对秘钥，用于对数据提供方1、2、3和数据需求方注册加入的审核签名，并生成可信证书，作为加入成员的加入凭证，监管机构选取监管代理节点，为后续加入的数据提供方和数据需求方成员颁发可信证书，实现对联盟网络的

监管；

[0041] (2)数据提供方1、2、3和数据需求方分别进行系统注册，在注册界面提交认证信息包括身份信息(机构名称、机构代码、注册时间、资格认证信息、法人姓名以及法人身份信息等)，数据监管方获取到加入成员的注册信息，对其进行审核，审核通过后进行认证签名，生成可信证书，由监管代理节点为加入成员颁发可信证书，进行注册的数据提供方和数据需求方凭借获取的可信证书加入联盟网络。数据提供方1、2、3成功加入联盟网络后分别选取各自的访问代理节点，数据需求方选取请求代理节点。

[0042] 其中数据监管方和数据需求方及数据提供方根据实际联盟情况均可为一个或多个；本实施例中，初始联盟网络是由数据提供方1、数据提供方2、数据提供方3和数据监管方和数据需求方参与组成，后续加入成员均可按照本实施例方法加入该联盟网络。

[0043] Step2：数据提供方成功加入联盟后，根据业务不同，参与不同的业务链，形成多链架构。

[0044] (1)数据提供方1根据业务数据需求，创建2种不同的业务节点，参与组建业务链1和业务链2；数据提供方2参与组建业务链3；数据提供方3参与组建业务链4；每条业务链包含与本业务链相关的数据账本和相关的合约部署。

[0045] (2)联盟网络中的数据提供方可根据自身的业务扩展情况选择性加入一条或多条业务链；数据提供方1在业务链1上产生的业务数据经其加密后存储在业务链1上的数据中心账本中，其在业务链2的业务数据经其加密后存储在业务链2上的数据中心账本中，同样，数据提供方2和3分别在业务链3和业务链4的数据中心账本中存储相应的数据，实现数据提供方根据数据业务类型的不同进行数据隔离和扩展。

[0046] Step3：数据提供方、数据需求方和数据监管方组建一条数据共享链，记录并存储数据共享信息，为多链间的数据共享提供途径。

[0047] (1)数据提供方1在业务链1和业务链2中分别提供一个可读取的数据存储节点，该节点可存储对应业务链1和业务链2的数据描述信息；数据提供方2提供一个可读取其在业务链3的数据存储节点，数据提供方3提供一个可读取其在业务链4的数据存储节点，由这些数据存储节点加入并组建一条数据共享链。

[0048] (2)数据需求方和监管方选取节点加入数据共享链，数据存储节点形成对等网络，分别在链上参与数据共享交易和监管。

[0049] (3)为每个加入的节点分配一对秘钥，将各节点的信息写入数据共享链中，各节点可利用所拥有公钥对其数据信息加密后进行广播至链上，并可利用私钥对其获取的信息进行解密，保证数据信息的安全防篡改。

[0050] Step4：数据提供方与数据需求方在所述数据共享链上进行数据共享交易，具体实现过程如图3所示。

[0051] (1)数据提供方1、2、3分别将其在不同业务链的数据描述信息在数据共享链进行广播并写入相应的存储节点，数据描述信息可根据实际联盟需求选择性地包括数据功能信息、数据共享及交易信息等。

[0052] (2)数据需求方从数据共享链中读取各数据提供方发布的数据描述信息，根据自身数据需求，选择目标数据描述信息，由请求代理向该目标数据描述信息对应的数据提供方2的访问代理发送数据权限请求。

[0053] (3)数据提供方2的访问代理获取请求代理发送的数据权限请求，按照权限批复协议对获取的数据权限请求进行权限批复，将权限批复结果发布到链上。

[0054] (4)请求代理获取权限批复结果，若权限批复通过，该权限批复结果内包含存储需求数据的数据中心账本地址，则该数据需求方获取该数据中心地址，拥有需求数据的访问权限，可以访问相应数据中心账本的数据，若权限批复未通过，则不能访问。

[0055] Step5:数据监管方在共享链中拥有超级权限，针对每个业务链的可共享数据均拥有相应的数据中心账本，并持有公钥，利用所述公钥对链上的数据中心账本中的内容进行加密，并可随时调取其中数据共享及交易信息，实现对数据共享交易的安全监管。

[0056] 上述对实施例的描述是为便于本技术领域的普通技术人员能理解和应用本发明。熟悉本领域技术的人员显然可以容易地对上述实施例做出各种修改，并把在此说明的一般原理应用到其他实施例中而不必经过创造性的劳动。因此，本发明不限于上述实施例，本领域技术人员根据本发明的揭示，对于本发明做出的改进和修改都应该在本发明的保护范围之内。

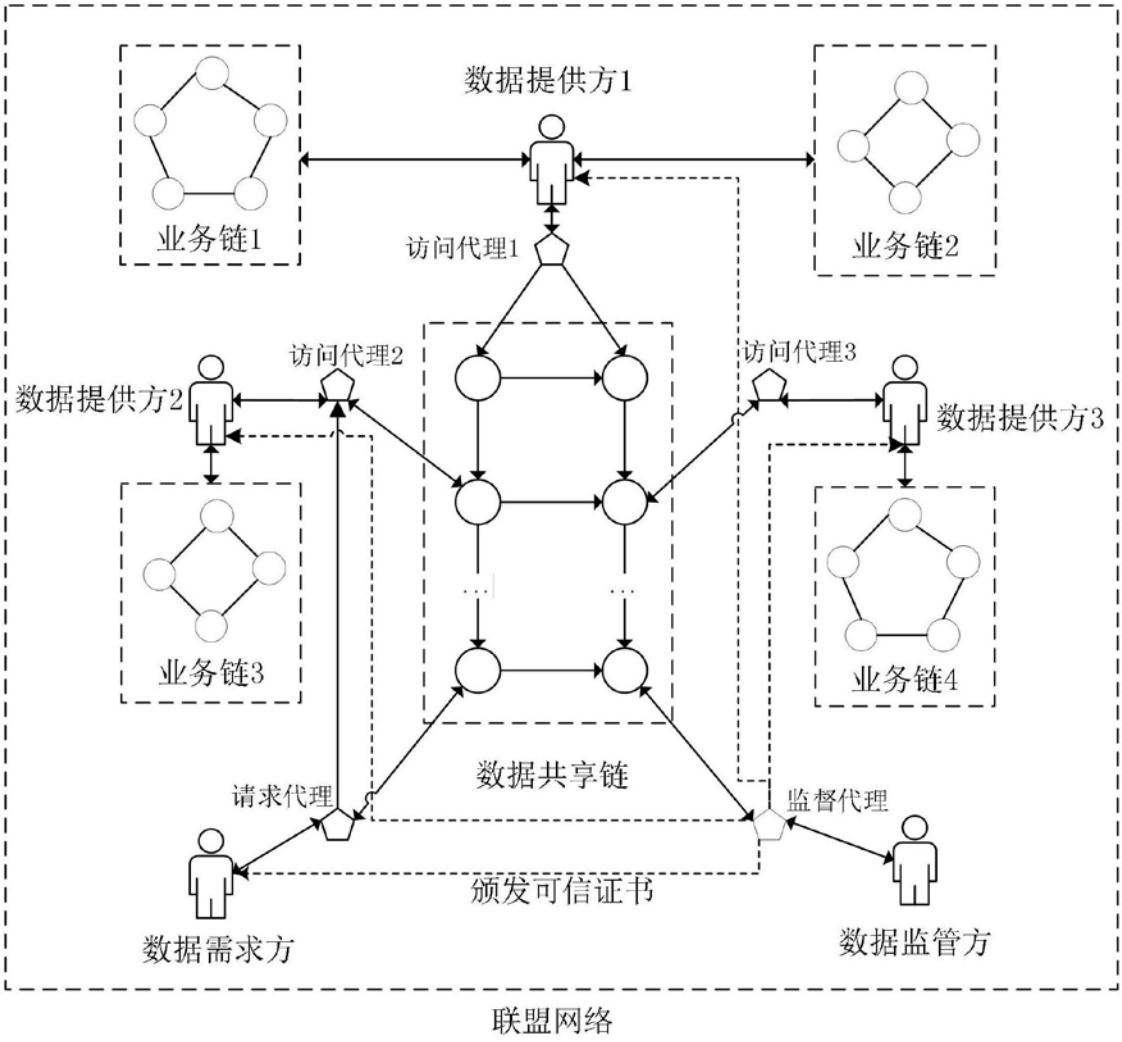

数据提供方1
业务链1
业务链2
访问代理1
访问代理2
访问代理3
数据提供方2
数据提供方3
业务链3
业务链4
数据共享链
请求代理
监督代理
颁发可信证书
数据需求方
数据监管方
联盟网络

图1

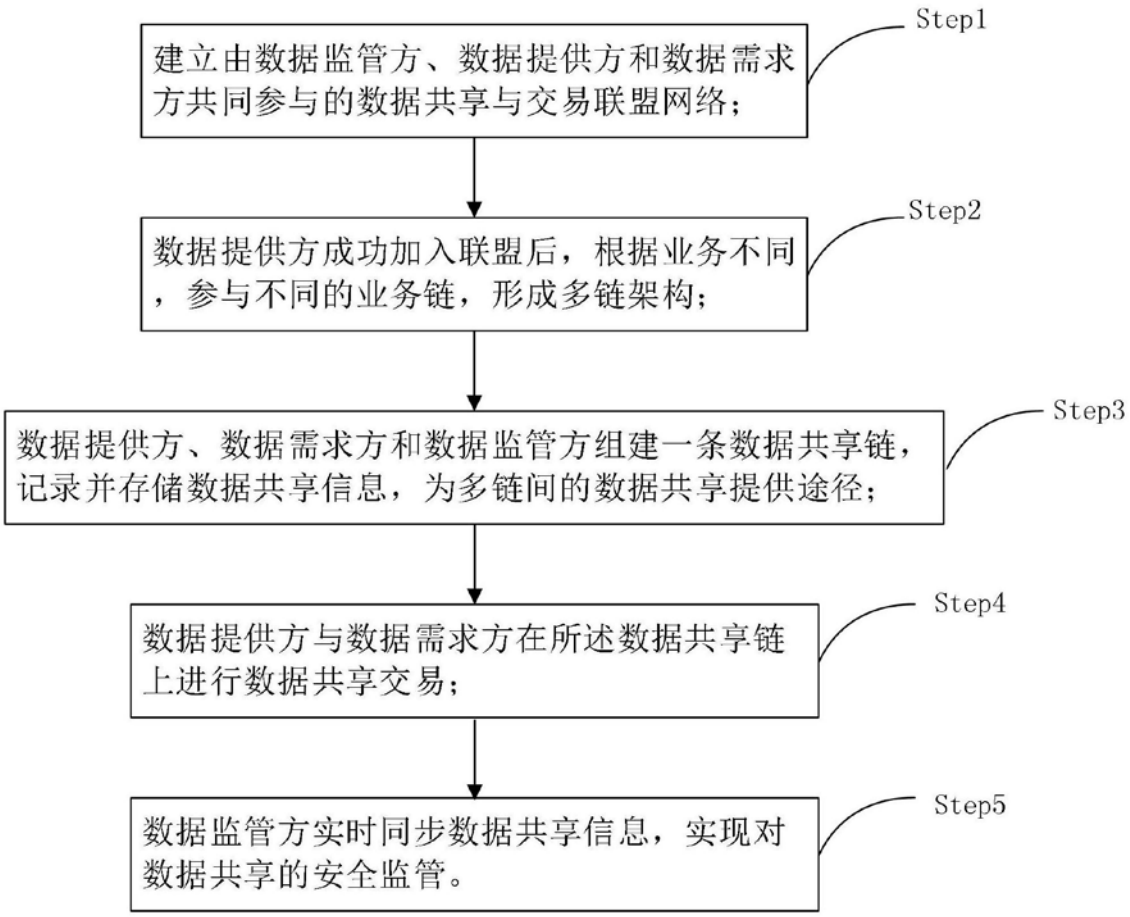

Step1
建立由数据监管方、数据提供方和数据需求方共同参与的数据共享与交易联盟网络；
Step2
数据提供方成功加入联盟后，根据业务不同，参与不同的业务链，形成多链架构；
Step3
数据提供方、数据需求方和数据监管方组建一条数据共享链，记录并存储数据共享信息，为多链间的数据共享提供途径；
Step4
数据提供方与数据需求方在所述数据共享链上进行数据共享交易；
Step5
数据监管方实时同步数据共享信息，实现对数据共享的安全监管。

图2

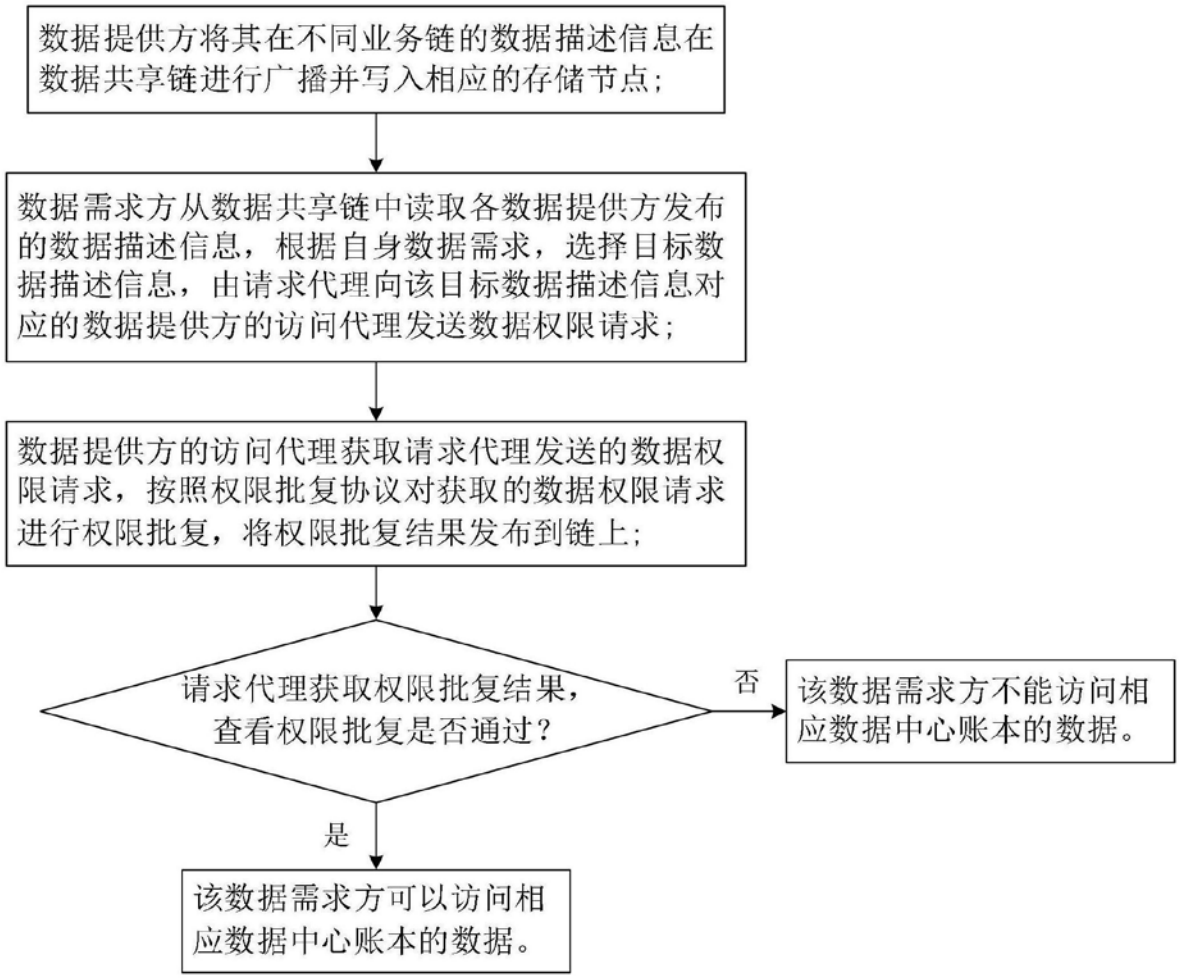

数据提供方将其在不同业务链的数据描述信息在数据共享链进行广播并写入相应的存储节点；
数据需求方从数据共享链中读取各数据提供方发布的数据描述信息，根据自身数据需求，选择目标数据描述信息，由请求代理向该目标数据描述信息对应的数据提供方的访问代理发送数据权限请求；
数据提供方的访问代理获取请求代理发送的数据权限请求，按照权限批复协议对获取的数据权限请求进行权限批复，将权限批复结果发布到链上；
请求代理获取权限批复结果，查看权限批复是否通过？
否
该数据需求方不能访问相应数据中心账本的数据。
是
该数据需求方可以访问相应数据中心账本的数据。

图3