(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115242555 A
(43)申请公布日 2022.10.25

(21)申请号 202211152951.1

(22)申请日 2022.09.21

(71)申请人 北京邮电大学
地址 100876 北京市海淀区西土城路10号

(72)发明人 马兆丰 段鹏飞 王晶宇 张宇青

(74)专利代理机构 北京金咨知识产权代理有限公司 11612
专利代理师 薛海波

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/14(2006.01)
H04L 67/1042(2022.01)
H04L 67/1074(2022.01)
H04L 67/1097(2022.01)

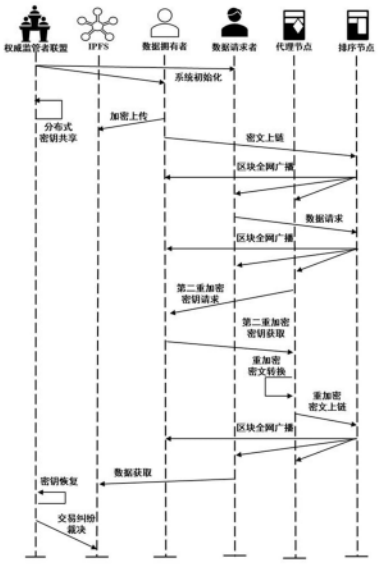
权利要求书2页 说明书14页 附图2页

(54)发明名称

一种可监管的跨链隐私数据共享方法及装置

(57)摘要

本发明提供一种可监管的跨链隐私数据共享方法及装置,数据拥有者通过对称加密的方式对隐私数据加密后上传至独立的预设分布式存储系统并获得访问地址,引入代理重加密的机制,数据拥有者将对称加密密钥和访问地址加密后的密文交由监管链存储,数据请求者在查询请求交易后,数据拥有者利用转换密钥将数据请求者公私密钥中公钥加密的密文转换为数据请求者公私密钥中公钥加密的密文,由数据请求者利用数据请求者公私密钥中私钥解密得到隐私数据在预设分布式存储系统中的访问地址和对称加密密钥,最终得到需要跨链分享的隐私数据。本发明能够在保证可信度的基础上高效分享大文件的隐私数据,速度快、保密性好、完整度高且可用性强。



CN 115242555 A

1.一种可监管的跨链隐私数据共享方法，其特征在于，所述方法在由多个应用链和至少一个监管链的区块链网络上运行，所述方法的执行涉及数据拥有着、数据请求者、代理者和权威监管者联盟，所述数据拥有者和所述数据请求者分别为不同应用链上的节点，所述代理者和所述权威监管者联盟为监管链上的多个节点，该方法包括以下步骤：

根据代理重加密算法的第一重加密密钥生成算法，由所述数据拥有者生成数据拥有者公私密钥，由所述数据请求者生成数据请求者公私密钥；

由所述数据拥有者随机生成对称加密密钥，并利用所述对称加密密钥将隐私数据加密后上传至预设分布式存储系统，并获得对应的访问地址；

由所述数据拥有者利用所述数据拥有者公私密钥中的第一公钥加密所述对称加密密钥和所述访问地址，得到加密隐私数据关键信息并发送至所述监管链进行上链存储；

由所述数据请求者对所述监管链打包的区块链进行检索，查找所述加密隐私数据关键信息，并向所述监管链发送所述数据请求者公私密钥中的第二公钥以及自身属性信息，以发起交易请求；

由所述代理者获取所述交易请求中的所述第二公钥和所述数据请求者的自身属性信息，在对所述自身属性信息审核通过的情况下发送至所述数据拥有者；

根据所述代理重加密算法的第二重加密密钥生成算法，由所述数据拥有者利用所述数据拥有者公私密钥和所述第二公钥生成数据请求者第二重加密密钥，将所述数据请求者第二重加密密钥发送至所述监管链；

根据密文重加密算法，由所述代理者利用所述数据请求者第二重加密密钥对所述加密隐私数据关键信息得到所述数据请求者能够解密的第一转换密文，并在所述监管链做上链存储；

由所述数据请求者在所述监管链上获取所述第一转换密文，并通过所述数据请求者公私密钥中的私钥解密得到所述隐私数据对应的所述对称加密密钥和所述访问地址，根据所述访问地址查询所述预设分布式存储系统，并利用所述对称加密密钥解密得到所述隐私数据。

2.根据权利要求1所述的可监管的跨链隐私数据共享方法，其特征在于，所述方法还包括：

由所述权威监管者联盟生成监管者公私密钥；

所述代理者获取所述交易请求中的所述第二公钥和所述数据请求者的自身属性信息之后，还将所述监管者公私密钥中的第三公钥发送至所述数据拥有者；

根据所述代理重加密算法的第二重加密密钥生成算法，由所述数据拥有者利用所述数据拥有者公私密钥和所述第三公钥生成监管者第二重加密密钥，并发送至所述监管链；

由所述代理者利用所述监管者第二重加密密钥对所述加密隐私数据关键信息得到所述监管者能够解密的第二转换密文，并在所述监管链做上链存储；

在所述隐私数据的共享行为涉嫌非法或发生纠纷时，由所述权威监管者联盟恢复出所述监管者公私密钥的私钥，对所述第二转换密文进行解密，得到所述隐私数据对应的所述对称加密密钥和所述访问地址，根据所述访问地址查询所述预设分布式存储系统，并利用所述对称加密密钥解密得到所述隐私数据，以对涉嫌非法或发生纠纷共享行为进行裁决。

3.根据权利要求2所述的可监管的跨链隐私数据共享方法，其特征在于，由所述权威监

管者联盟生成监管者公私密钥之后，还包括：

基于Shanmir门限秘密共享方案，由所述权威监管者联盟通过秘密多项式将所述监管者公私密钥中的私钥分为第一设定数量个秘密分片，并派发给所述权威监管者联盟中的多个节点，当拥有任意不少于第二设定数量个秘密分片时，恢复所述监管者公私密钥中的私钥。

4.根据权利要求3所述的可监管的跨链隐私数据共享方法，其特征在于，所述方法包括：

对于要分享的所述监管者公私密钥中的私钥sk_{Auth}，创建素数P的有限域GF(p)并从中任意选择(t-1)个元素a_i(i=1,2,…,t-1)构成(t-1)阶多项式 $f(x)=a_0+\sum_{i=1}^{t-1}a_i x^i \bmod p$，其中，$sk_{Auth}=c=f(0)=a_0$；

由所述权威监管者联盟中的各节点在GF(p)内随机选择x_r，代入多项式内得到相应的秘密分片s_r，即 $s_r=f(x_r)=a_0+\sum_{i=1}^{t-1}a_i {x_r}^i \bmod p$，(r=1,2,…,n)；

销毁私钥sk_{Auth}。

5.根据权利要求4所述的可监管的跨链隐私数据共享方法，其特征在于，当拥有任意不少于第二设定数量个秘密分片时，恢复所述监管者公私密钥中的私钥，包括：

将各秘密分片代入拉格朗日插值公式，恢复所述监管者公私密钥中的私钥sk_{Auth}，计算式为：

$$sk_{Auth}=c=f(0)=\sum_{i=1}^{t}f(x_l)\prod_{v=1,v\neq l}^{t}\frac{-x_v}{x_l-x_v} \bmod p$$；

其中，t为所述第二设定数量；c表示x为0时的函数值，x_v表示第v个秘密分片的随机输入值，x_l表示第l个秘密分片的随机输入值。

6.根据权利要求1所述的可监管的跨链隐私数据共享方法，其特征在于，所述预设分布式存储系统为IPFS分布式存储系统。

7.根据权利要求1所述的可监管的跨链隐私数据共享方法，其特征在于，由所述数据拥有者随机生成对称加密密钥，包括：

有所述数据拥有者根据AES对称加密算法随机生成对称加密密钥。

8.根据权利要求1所述的可监管的跨链隐私数据共享方法，其特征在于，得到加密隐私数据关键信息并发送至所述监管链进行上链存储，包括：

将所述加密隐私数据关键信息连同数据哈希值、数据关键词和数据访问规则一起上链存储。

9.一种可监管的跨链隐私数据共享装置，包括处理器和存储器，其特征在于，所述存储器中存储有计算机指令，所述处理器用于执行所述存储器中存储的计算机指令，当所述计算机指令被处理器执行时该装置实现如权利要求1至8中任一项所述方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1至8中任一项所述方法的步骤。

一种可监管的跨链隐私数据共享方法及装置

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种可监管的跨链隐私数据共享方法及装置。

背景技术

[0002] 区块链的概念自诞生以来逐渐开始引起人们的关注，其作为一种分布式账本技术，本质是利用分布式结构、去中心化的理念，将数据存储、分布式算法、点对点网络、加密签名等技术相结合，以摆脱目前互联网服务器中心化的架构，使得所有相关数据都被存证记录在同一条区块链上，链上数据公开透明可验证，被认为是信息互联网转型成为价值互联网的核心技术。当前区块链技术架构的设计理念已被广泛应用于不仅限于金融的各个领域当中。随着区块链底层技术的快速突破和发展，越来越多的企业积极结合其业务需求，加速融入区块链生态，并逐步在跨境支付、供应链金融、电子医疗、物联网、防伪溯源等场景展开落地与应用。在产业变革需求、技术创新发展以及政策红利的共同驱动下，链间互信管理、数据和业务跨链交互的需求也日益增长。在此背景下，跨链通信技术应运而生。

[0003] 跨链指的是通过连接相对独立的区块链系统，实现不同账本的可信互操作。现有的主流跨链机制包括公证人机制、哈希锁、以及侧链/中继模式。在跨链系统中，不同应用链之间会进行频繁的的业务数据往来。由于各应用链由不同主体控制，数据共享难以协调管理，且在跨链共享过程中数据的保密性、完整性和可用性不能保证，可信性存疑。并且对于大文件隐私数据无法有效进行共享。

发明内容

[0004] 鉴于此，本发明实施例提供了一种可监管的跨链隐私数据共享方法及装置，以消除或改善现有技术中存在的一个或更多个缺陷，解决区块链跨链交易过程无法在保证可信度的前提下进行大文件隐私数据共享的问题。

[0005] 本发明的一个方面提供了一种可监管的跨链隐私数据共享方法，所述方法在由多个应用链和至少一个监管链的区块链网络上运行，所述方法的执行涉及数据拥有着、数据请求者、代理者和权威监管者联盟，所述数据拥有者和所述数据请求者分别为不同应用链上的节点，所述代理者和所述权威监管者联盟为监管链上的多个节点，该方法包括以下步骤：

根据代理重加密算法的第一重加密密钥生成算法，由所述数据拥有者生成数据拥有者公私密钥，由所述数据请求者生成数据请求者公私密钥；

由所述数据拥有者随机生成对称加密密钥，并利用所述对称加密密钥将隐私数据加密后上传至预设分布式存储系统，并获得对应的访问地址；

由所述数据拥有者利用所述数据拥有者公私密钥中的第一公钥加密所述对称加密密钥和所述访问地址，得到加密隐私数据关键信息并发送至所述监管链进行上链存储；

由所述数据请求者对所述监管链打包的区块链进行检索，查找所述加密隐私数据

关键信息，并向所述监管链发送所述数据请求者公私密钥中的第二公钥以及自身属性信息，以发起交易请求；

由所述代理者获取所述交易请求中的所述第二公钥和所述数据请求者的自身属性信息，在对所述自身属性信息审核通过的情况下发送至所述数据拥有者；

根据所述代理重加密算法的第二重加密密钥生成算法，由所述数据拥有者利用所述数据拥有者公私密钥和所述第二公钥生成数据请求者第二重加密密钥，将所述数据请求者第二重加密密钥发送至所述监管链；

根据密文重加密算法，由所述代理者利用所述数据请求者第二重加密密钥对所述加密隐私数据关键信息得到所述数据请求者能够解密的第一转换密文，并在所述监管链做上链存储；

由所述数据请求者在所述监管链上获取所述第一转换密文，并通过所述数据请求者公私密钥中的私钥解密得到所述隐私数据对应的所述对称加密密钥和所述访问地址，根据所述访问地址查询所述预设分布式存储系统，并利用所述对称加密密钥解密得到所述隐私数据。

[0006] 在一些实施例中，所述方法还包括：

由所述权威监管者联盟生成监管者公私密钥；

所述代理者获取所述交易请求中的所述第二公钥和所述数据请求者的自身属性信息之后，还将所述监管者公私密钥中的第三公钥发送至所述数据拥有者；

根据所述代理重加密算法的第二重加密密钥生成算法，由所述数据拥有者利用所述数据拥有者公私密钥和所述第三公钥生成监管者第二重加密密钥，并发送至所述监管链；

由所述代理者利用所述监管者第二重加密密钥对所述加密隐私数据关键信息得到所述监管者能够解密的第二转换密文，并在所述监管链做上链存储；

在所述隐私数据的共享行为涉嫌非法或发生纠纷时，由所述权威监管者联盟恢复出所述监管者公私密钥的私钥，对所述第二转换密文进行解密，得到所述隐私数据对应的所述对称加密密钥和所述访问地址，根据所述访问地址查询所述预设分布式存储系统，并利用所述对称加密密钥解密得到所述隐私数据，以对涉嫌非法或发生纠纷共享行为进行裁决。

[0007] 在一些实施例中，由所述权威监管者联盟生成监管者公私密钥之后，还包括：

基于Shanmir门限秘密共享方案，由所述权威监管者联盟通过秘密多项式将所述监管者公私密钥中的私钥分为第一设定数量个秘密分片，并派发给所述权威监管者联盟中的多个节点，当拥有任意不少于第二设定数量个秘密分片时，恢复所述监管者公私密钥中的私钥。

[0008] 在一些实施例中，所述方法包括：

对于要分享的所述监管者公私密钥中的私钥sk_{Auth}，创建素数P的有限域GF(p)并从中任意选择（t-1）个元素a_i（i=1，2，…，t-1）构成（t-1）阶多项式$f(x)=a_0+\sum_{i=1}^{t-1}a_i x^i \bmod p$，其中，p是一个大素数，$sk_{Auth}=c=f(0)=a_0$；由所述权威监管者联盟中的各节点在GF(p)内随机选择x_r，代入多项式内得到相应的秘密分片s_r，即

$s_r = f(x_r) = a_0 + \sum_{i=1}^{t-1} a_i x_r^{\,i} \bmod p$，(r=1,2,…,n)；销毁私钥$sk_{Auth}$。

[0009] 在一些实施例中，当拥有任意不少于第二设定数量个秘密分片时，恢复所述监管者公私密钥中的私钥，包括：

将各秘密分片代入拉格朗日插值公式，恢复所述监管者公私密钥中的私钥sk_{Auth}，计算式为：

$$sk_{Auth} = c = f(0) = \sum_{l=1}^{t} f(x_l) \prod_{v=1, v\neq l}^{t} \frac{-x_v}{x_l - x_v} \bmod p;$$

其中，t为所述第二设定数量；c表示x为0时的函数值，x_v表示第v个秘密分片的随机输入值，x_1表示第1个秘密分片的随机输入值。

[0010] 在一些实施例中，所述预设分布式存储系统为IPFS分布式存储系统。

[0011] 在一些实施例中，由所述数据拥有者随机生成对称加密密钥，包括：有所述数据拥有者根据AES对称加密算法随机生成对称加密密钥。

[0012] 在一些实施例中，得到加密隐私数据关键信息并发送至所述监管链进行上链存储，包括：

将所述加密隐私数据关键信息连同数据哈希值、数据关键词和数据访问规则一起上链存储。

[0013] 另一方面，本发明还提供一种可监管的跨链隐私数据共享装置，包括处理器和存储器，所述存储器中存储有计算机指令，所述处理器用于执行所述存储器中存储的计算机指令，当所述计算机指令被处理器执行时该装置实现上述方法的步骤。

[0014] 另一方面，本发明还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0015] 本发明的有益效果至少是：

本发明所述可监管的跨链隐私数据共享方法及装置中，数据拥有者通过对称加密的方式对隐私数据加密后上传至独立的预设分布式存储系统并获得访问地址，引入代理重加密的机制，数据拥有者将对称加密密钥和访问地址加密后的密文交由监管链存储，数据请求者在查询请求交易后，数据拥有者利用转换密钥将数据请求者公私密钥中公钥加密的密文转换为数据请求者公私密钥中公钥加密的密文，由数据请求者利用数据请求者公私密钥中私钥解密得到隐私数据在预设分布式存储系统中的访问地址和对称加密密钥，最终得到需要跨链分享的隐私数据。本发明能够在保证可信度的基础上高效分享大文件的隐私数据，速度快、保密性好、完整度高且可用性强。

[0016] 本发明的附加优点、目的，以及特征将在下面的描述中将部分地加以阐述，且将对于本领域普通技术人员在研究下文后部分地变得明显，或者可以根据本发明的实践而获知。本发明的目的和其它优点可以通过在说明书以及附图中具体指出的结构实现到并获得。

[0017] 本领域技术人员将会理解的是，能够用本发明实现的目的和优点不限于以上具体所述，并且根据以下详细说明将更清楚地理解本发明能够实现的上述和其他目的。

附图说明

[0018] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，并不构成对本发明的限定。在附图中：

图1为本发明一实施例所述可监管的跨链隐私数据共享方法的流程示意图。

[0019] 图2为本发明另一实施例所述可监管的跨链隐私数据共享方法的时序示意图。

具体实施方式

[0020] 为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施方式和附图，对本发明做进一步详细说明。在此，本发明的示意性实施方式及其说明用于解释本发明，但并不作为对本发明的限定。

[0021] 在此，还需要说明的是，为了避免因不必要的细节而模糊了本发明，在附图中仅仅示出了与根据本发明的方案密切相关的结构和/或处理步骤，而省略了与本发明关系不大的其他细节。

[0022] 应该强调，术语“包括/包含”在本文使用时指特征、要素、步骤或组件的存在，但并不排除一个或更多个其它特征、要素、步骤或组件的存在或附加。

[0023] 在此，还需要说明的是，如果没有特殊说明，术语“连接”在本文不仅可以指直接连接，也可以表示存在中间物的间接连接。

[0024] 现有的主流跨链机制包括公证人机制、哈希锁、以及侧链/中继模式。公证人机制是一种相对容易实现的跨链机制，它通过引入可信的第三方进行跨链消息的验证与转发。当在不同的区块链系统中进行资产兑换和转移时，选举一个或者多个组织作为公证人来自动或者请求式监听不同链上的事件，并通过特定共识算法对事件是否发生达成共识，最后及时做出响应。哈希锁定全称为哈希时间锁定合约(hash timelock contract)，是在无需可信公证人的情况下，通过哈希锁和时间锁共同完成链间资产兑换的一种跨链技术方案。侧链/中继(sidechains/relays)则是一种能够自行检验交易数据且具有可扩展性的跨链技术。当主链上需要处理较多的事务或者出现性能瓶颈时，可以将主链上的资产转移到侧链上处理，进而减轻主链上的压力，达到扩展主链功能和性能的目的。

[0025] 数据资产是指由企业拥有或控制的、能为企业带来未来利益的，以物理或者电子的方式记录的数据资源，如文件资料、电子资料等。作为宝贵的资源，企业可以根据收集的数据预测行业未来趋势，优化决策过程，为用户提供个性化服务。近年来，用户或企业隐私数据安全受威胁事件频发，尤其是在数据共享过程中，用户隐私信息遭受频繁泄露，隐私数据的安全共享已然成为社会和大众关注的热点问题。

[0026] 所以，本发明提供一种可监管的跨链隐私数据共享方法及装置。从系统架构角度来看，本方案中的监管链由五种类型的节点组成：监管节点、跨链节点、代理节点、排序节点和记账节点。其中，隶属于各监管部门的监管节点负责对跨链交易进行监管；隶属于各应用链的跨链节点负责发起与监听跨链交易；位于监管链的代理节点能够使用代理重加密密钥对链上密文进行密文转换；排序节点负责对跨链交易进行排序并打包成块，然后进行全网广播。记账节点负责验证排序节点发布的区块中的交易，并记录在本地的账本副本；从成员角色角度看，本发明考虑了四类实体：数据请求者、数据拥有者、代理者和权威监管者联盟。其中，数据请求者与数据拥有者均位于应用链，属于隐私数据跨链共享的参与双方；代理者

由监管链中的代理节点担任,可对数据拥有者发布的加密隐私数据关键信息进行重加密密文转换,使得数据请求者与权威监管者联盟均能够对密文进行解密;权威监管者联盟由各监管节点组成,参与第一重加密密钥的生成与分发,能够在需要对共享内容及交易纠纷进行裁决时,对第一重加密密钥进行恢复。

[0027] 具体的,所述方法包括以下步骤S101~S108:

步骤S101:根据代理重加密算法的第一重加密密钥生成算法,由数据拥有者生成数据拥有者公私密钥,由数据请求者生成数据请求者公私密钥。

[0028] 步骤S102:由数据拥有者随机生成对称加密密钥,并利用对称加密密钥将隐私数据加密后上传至预设分布式存储系统,并获得对应的访问地址。

[0029] 步骤S103:由数据拥有者利用数据拥有者公私密钥中的第一公钥加密对称加密密钥和访问地址,得到加密隐私数据关键信息并发送至监管链进行上链存储。

[0030] 步骤S104:由数据请求者对监管链打包的区块链进行检索,查找加密隐私数据关键信息,并向监管链发送数据请求者公私密钥中的第二公钥以及自身属性信息,以发起交易请求。

[0031] 步骤S105:由代理者获取交易请求中的第二公钥和数据请求者的自身属性信息,在对自身属性信息审核通过的情况下发送至数据拥有者。

[0032] 步骤S106:根据代理重加密算法的第二重加密密钥生成算法,由数据拥有者利用数据拥有者公私密钥和第二公钥生成数据请求者第二重加密密钥,将数据请求者第二重加密密钥发送至监管链。

[0033] 步骤S107:根据密文重加密算法,由代理者利用数据请求者第二重加密密钥对加密隐私数据关键信息得到数据请求者能够解密的第一转换密文,并在监管链做上链存储。

[0034] 步骤S108:由数据请求者在监管链上获取第一转换密文,并通过数据请求者公私密钥中的私钥解密得到隐私数据对应的对称加密密钥和访问地址,根据访问地址查询预设分布式存储系统,并利用对称加密密钥解密得到隐私数据。

[0035] 步骤S101~S108限定了隐私数据的分享方法,这个过程引入了代重加密(proxyre-encryption ,PRE)技术,代理重加密是一种密文间的转换机制。在PRE中,一个半可信代理方通过代理授权人A产生的转换密钥RK把用授权人A的公钥PKA加密的密文转化为用被授权人B的公钥PKB加密的密文,在这个过程中,代理方得不到数据的明文信息,从而降低了数据泄露风险。本发明中,对于数据拥有者加密后的隐私数据,通过独立的预设分布式存储系统进行存储,而不直接对数据请求者进行分享,所以能够实现对大文件的高效传输。在代理者对数据请求者主体资格审查合格的情况下,利用代理重加密的技术,结合数据请求方提供的公私密钥,数据拥有者将加密隐私数据所用的对称加密秘钥与访问地址的加密文件转换为数据请求方可以利用其私钥直接解密的密文,完成对数据请求者的密文转达,这个过程中,数据拥有者不需要向代理者披露对称加密秘钥与访问地址的明文,也不需要转达加密秘钥,所以极大提高了保密性能。

[0036] 在一些实施例中,步骤S102中,预设分布式存储系统为IPFS分布式存储系统。

[0037] 在一些实施例中,步骤S102中,由数据拥有者随机生成对称加密密钥,包括:有数据拥有者根据AES对称加密算法随机生成对称加密密钥。

[0038] 在一些实施例中,步骤S103中,得到加密隐私数据关键信息并发送至监管链进行

上链存储，包括：将加密隐私数据关键信息连同数据哈希值、数据关键词和数据访问规则一起上链存储。

[0039] 在一些实施例中，所述方法还包括步骤S201~S205：

步骤S201：由权威监管者联盟生成监管者公私密钥。

[0040] 步骤S202：代理者获取交易请求中的第二公钥和数据请求者的自身属性信息之后，还将监管者公私密钥中的第三公钥发送至数据拥有者。

[0041] 步骤S203：根据代理重加密算法的第二重加密密钥生成算法，由数据拥有者利用数据拥有者公私密钥和第三公钥生成监管者第二重加密密钥，并发送至监管链。

[0042] 步骤S204：由代理者利用监管者第二重加密密钥对加密隐私数据关键信息得到监管者能够解密的第二转换密文，并在监管链做上链存储。

[0043] 步骤S205：在隐私数据的共享行为涉嫌非法或发生纠纷时，由权威监管者联盟恢复出监管者公私密钥的私钥，对第二转换密文进行解密，得到隐私数据对应的对称加密密钥和访问地址，根据访问地址查询预设分布式存储系统，并利用对称加密密钥解密得到隐私数据，以对涉嫌非法或发生纠纷共享行为进行裁决。

[0044] 在步骤S101~S108的执行期间，同步执行步骤S201~S205，设置了发生共享行为非法或发生纠纷时的处置流程，数据拥有者将加密隐私数据所用的对称加密秘钥与访问地址的加密文件同步转换为权威监管者能够利用其私钥直接解密的密文，以供在行为非法或发生纠纷的情况下读取相关数据进行裁决。

[0045] 在一些实施例中，步骤S201之后，即由权威监管者联盟生成监管者公私密钥之后，还包括：基于Shanmir门限秘密共享方案，由权威监管者联盟通过秘密多项式将监管者公私密钥中的私钥分为第一设定数量个秘密分片，并派发给权威监管者联盟中的多个节点，当拥有任意不少于第二设定数量个秘密分片时，恢复监管者公私密钥中的私钥。

[0046] 在一些实施例中，所述方法利用Shanmir门限秘密共享方案，对监管者公私密钥中的私钥进行分片，包括步骤S301~步骤S303：

步骤S301：对于要分享的监管者公私密钥中的私钥sk_{Auth}，创建素数P的有限域GF(p)并从中任意选择(t-1)个元素a_i (i=1,2,…,t-1)构成(t-1)阶多项式$f(x)=a_0+\sum_{i=1}^{t-1}a_i x^i \bmod p$，其中，p是一个大素数，$sk_{Auth}=c=f(0)=a_0$。

[0047] 步骤S302：由权威监管者联盟中的各节点在GF(p)内随机选择x_r，代入多项式内得到相应的秘密分片s_r，即$s_r=f(x_r)=a_0+\sum_{i=1}^{t-1}a_i x_r^{\,i} \bmod p$，(r=1,2,…,n)。

[0048] 步骤S303：销毁私钥sk_{Auth}。

[0049] 在一些实施例中，当拥有任意不少于第二设定数量个秘密分片时，恢复监管者公私密钥中的私钥，包括：

将各秘密分片代入拉格朗日插值公式，恢复监管者公私密钥中的私钥sk_{Auth}，计算式为：

$$sk_{Auth}=c=f(0)=\sum_{i=1}^{t}f(x_l)\prod_{v=1,v\neq l}^{t}\frac{-x_v}{x_l-x_v} \bmod p;$$

其中，t为所述第二设定数量；c表示x为0时的函数值，x_v表示第v个秘密分片的随

机输入值，x_1表示第1个秘密分片的随机输入值。

[0050] 具体的，上述步骤S101~S108，步骤S201~S205以及步骤S301~S303可以综合为以下步骤：

步骤1．初始化阶段。

[0051] A.数据请求者DR、数据拥有者DO与权威监管者联盟Auth通过代理重加密算法的第一重加密密钥生成算法生成各自的公私钥对：

$$(pp, sk_{dr}, pk_{dr}, sk_{do}, pk_{do}, sk_{Auth}, pk_{Auth}) \leftarrow \mathcal{PRE}.KeyGen(\lambda)$$

其中，该算法的输入是安全参数 λ ，输出为公共参数pp，数据请求者DR的公私钥对(pk_{dr}， sk_{dr})、数据拥有者DO的公私钥对(pk_{do}， sk_{do})与权威监管者联盟Auth的公私钥对(pk_{Auth}， sk_{Auth})；

B.权威监管者联盟Auth由n个监管节点组成，即Auth={auth1,…,authn}，对联盟第一重加密密钥私钥sk_{Auth}进行秘密分享，并将秘密分片分发至各监管节点，随后销毁sk_{Auth}并公开pk_{Auth}。

[0052] 步骤2．数据拥有者DO随机生成对称加密密钥key，用于将隐私数据data加密为$data_{Enc}$并上传至IPFS分布式存储系统，获得IPFS文件访问地址loc。

[0053] 步骤3．数据拥有者DO将对称加密密钥key与IPFS文件访问地址loc使用其第一重加密密钥公钥pk_{do}加密后得到加密隐私数据关键信息C_{do}：

$$C_{do} \leftarrow \mathcal{PRE}.Encrypt(pk_{do}, key, loc)$$

随后，通过跨链节点向部署于监管链上的隐私数据跨链共享智能合约DSSC发起加密隐私数据关键信息上链交易，实现加密隐私数据关键信息C_{do}上链。此外，该交易内容还包括数据哈希，数据关键词以及数据访问规则等辅助信息。

[0054] 步骤4．监管链上排序节点收集加密隐私数据关键信息上链交易，随后打包成块并进行全网广播。

[0055] 步骤5．数据请求者DR通过跨链节点对监管链区块中的加密隐私数据关键信息上链交易内容进行检索，随后向部署于监管链上的隐私数据跨链共享智能合约DSSC发起数据请求交易，其中包含数据请求者DR的第一重加密密钥公钥pk_{dr}以及自身属性$Attr_{dr}$用以表明自身是否符合该数据的访问规则。

[0056] 步骤6．代理节点从数据请求交易中获得数据请求者的第一重加密密钥公钥pk_{dr}及其自身属性$Attr_{dr}$，随后连同权威监管者联盟第一重加密密钥公钥pk_{Auth}一并发送给数据拥有者DO，后者在本地执行代理重加密的第二重加密密钥生成算法，分别生成第二重加密密钥$rk_{do\text{-}dr}$与$rk_{do\text{-}Auth}$：

$$rk_{do-dr} \leftarrow \mathcal{PRE}.ReKeyGen(sk_{do}, pk_{do}, pk_{dr})$$

$$rk_{do-Auth} \leftarrow \mathcal{PRE}.ReKeyGen(sk_{do}, pk_{do}, pk_{Auth})$$

随后，将其发送至监管链中的代理节点。

[0057] 步骤7．代理节点在本地执行代理重加密的密文重加密算法，将加密隐私数据关键信息进行密文转换，获得数据请求者DR与权威监管者联盟能解密的密文C_{dr}与C_{Auth}：

$$C_{dr} \leftarrow \mathcal{PRE}.ReEnc(C_{do}, rk_{do-dr})$$

$$C_{Auth} \leftarrow \mathcal{PRE}.ReEnc(C_{do}, rk_{do-Auth})$$

随后，向隐私数据跨链共享智能合约DSSC发起重加密密文上链交易，实现重加密密文的上链。

[0058] 步骤8．数据请求者DR通过跨链节点从重加密密文上链交易中获取其能进行解密的密文C_{dr}，使用自己的第一重加密密钥私钥sk_{dr}进行解密，获得对称加密密钥key与IPFS文件访问地址loc：

$$(key, loc) \leftarrow \mathcal{PRE}.Decrypt(C_{dr}, sk_{dr})$$

随后，数据请求者根据IPFS文件访问地址loc从IPFS分布式存储系统中获取$data_{Enc}$并使用对称加密密钥key进行解密，得到隐私数据data。

[0059] 步骤9．当收发双方就隐私数据共享过程发生纠纷或共享隐私数据内容涉嫌非法时，监管链中的各监管节点组成权威监管者联盟，共同恢复出联盟第一重加密密钥私钥sk_{Auth}，对密文C_{Auth}进行解密：

$$(key, loc) \leftarrow \mathcal{PRE}.Decrypt(C_{Auth}, sk_{Auth})$$

根据IPFS文件访问地址loc从IPFS分布式存储系统中获取$data_{Enc}$并使用对称加密密钥key进行解密，得到隐私数据data，从而对上述情况做出裁决。

[0060] 另一方面，本发明还提供一种可监管的跨链隐私数据共享装置，包括处理器和存储器，所述存储器中存储有计算机指令，所述处理器用于执行所述存储器中存储的计算机指令，当所述计算机指令被处理器执行时该装置实现上述方法的步骤。

[0061] 另一方面，本发明还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。

[0062] 下面结合一具体实施例对本发明进行说明：

图1是基于代理重加密的可监管跨链隐私数据共享方法流程示意图，图2是基于代理重加密的可监管跨链隐私数据共享方法时序示意图。在此，本实施例及其说明用于解释本发明，但并不作为对本发明的限定。

[0063] 本实施例所涉及的角色主要包括以下四类：数据拥有者、数据请求者、代理者、权威监管者联盟，其中，每个角色承担如下任务：

数据拥有者：位于各应用链系统中，与数据请求者是相对的概念。当其拥有共享价值的隐私数据时，会将其加密上传至IPFS分布式存储系统中，同时将隐私数据的关键信息加密上链，供数据请求者检索。

[0064] 数据请求者：位于各应用链系统中，与数据拥有者是相对的概念。当需要进行跨链访问其余应用链中的数据拥有者所持有的的隐私数据时，会通过隶属于本应用链的跨链节点发起数据请求，由其来通过调用部署于监管链上的隐私数据跨链共享智能合约DSSC实现数据获取。

[0065] 代理者：位于监管链系统中，由代理节点担任。当有数据请求者发布数据请求交易时，代理者将数据请求者的第一重加密密钥公钥pk_{dr}，连同权威监管者联盟的第一重加密密

钥公钥pkAuth一并发送至数据拥有者。待数据拥有者在本地执行重加密密钥生成算法，分别生成第二重加密密钥$rk_{do\text{-}dr}$与$rk_{do\text{-}Auth}$，随后由代理节点执行重加密算法，将密文数据进行密文转换，使得数据请求者与权威监管者联盟均能对重加密后的密文进行解密。

[0066] 权威监管者联盟由各隶属于监管部门的监管节点组成。在初始化阶段，联盟对其第一重加密密钥私钥sk_{Auth}进行秘密分享，由各监管节点持有秘密分片，随后销毁该私钥。在交易纠纷处理或交易内容监管阶段，权威监管者联盟对第一重加密密钥私钥sk_{Auth}进行秘密恢复，实现对加密隐私数据的解密，从而对上述情况做出裁决。

[0067] 如图1和图2所示，本实施例包括如下步骤：

步骤1)初始化阶段。

[0068] A．数据请求者DR、数据拥有者DO与权威监管者联盟Auth通过代理重加密的第一重加密密钥生成算法生成各自的公私钥对：

$$(pp, sk_{dr}, pk_{dr}, sk_{do}, pk_{do}, sk_{Auth}, pk_{Auth}) \leftarrow \mathcal{PRE}.KeyGen(\lambda)$$；

其中，该算法的输入是安全参数 λ ，输出为公共参数pp，数据请求者DR的公私钥对(pk_{dr}，sk_{dr})、数据拥有者DO的公私钥对(pk_{do}，sk_{do})与权威监管者联盟Auth的公私钥对(pk_{Auth}，sk_{Auth})。

[0069] 为实例化描述该步骤，本发明给出其具体算法描述。选择两个阶为素数q的乘法循环群G_1和G_2，g_1和g_2分别为G_1、G_2的两个生成元，设置双线性映射：$\hat{e}: G_1 \times G_1 \rightarrow G_2$，定义哈希函数组$H_i$ (i=1,2,3,4)，函数组具体定义如下：$H_1: \{0,1\}^* \rightarrow G_1$，$H_2: \{0,1\}^* \rightarrow Z_p^*$，$H_3: G_2 \rightarrow \{0,1\}^l$，$H_4: \{0,1\}^* \rightarrow G_1$，得公共参数

$pp = (q, g_1, g_2, G_1, G_2, H_1, H_2, H_3, H_4)$。随机选择 $a,b,c \in \mathbb{Z}^*_q$，设置数据请求者DR的公私钥对 $(sk_{dr}, pk_{dr}) := (a, g_1^a)$ 、数据拥有者DO的公私钥对 $(sk_{do}, pk_{do}) := (b, g_1^b)$ 与权威监管者联盟Auth的公私钥对 $(sk_{Auth}, pk_{Auth}) := (c, g_1^c)$。

[0070] B．权威监管者联盟Auth由n个监管节点组成，即Auth={$auth_1$,…,$auth_n$}。对联盟第一重加密私钥sk_{Auth}进行秘密分享，并将秘密分片分发至各监管节点，随后销毁sk_{Auth}并公开pk_{Auth}；为实例化描述该步骤，本实施例使用Shamir门限秘密共享方案作为秘密分享方案，该方案是基于Lagrange插值公式构造的。其基本思想是权威监管者联盟通过秘密多项式f(x)将联盟第一重加密私钥sk_{Auth}分为n个秘密分片并分发给各监管节点。当拥有任意不少于t个秘密分片时，均能成功恢复联盟第一重加密私钥sk_{Auth}；少于t个秘密分片时则得不到联盟私钥的任何信息。

[0071] 在本实施例中，权威监管者联盟要共享的秘密为sk_{Auth}，即 $sk_{Auth} = c \in \mathbb{Z}_q^*$，其中q为大素数。创建素数P的有限域GF(p)并从中任意选择(t-1)个元素a_i (i=1,2,…,t-1)构成(t-1)阶多项式 $f(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i \bmod p$ ，其中，p是一个大素数，秘密

$sk_{Auth}=c=f(0)=a_0$。各监管节点$auth_r$在GF(p)内随机选择x_r，代入多项式内得到其秘密分片s_r，即 $s_r=f(x_r)=a_0+\sum_{i=1}^{t-1}a_i x_r^{\,i} \bmod p$，(r=1,2,…,n)，随后销毁$sk_{Auth}$并公开$pk_{Auth}$。

[0072] 步骤2)数据拥有者DO随机生成对称加密密钥key，用于将隐私数据data加密为$data_{Enc}$并上传至IPFS分布式存储系统，获得隐私数据IPFS访问地址loc；此处使用的加密方法为AES对称加密算法。AES 的全称是 Advanced Encryption Standard，其加解密都是采用同一个密钥。

[0073] 步骤3)数据拥有者DO将对称加密密钥key与隐私数据IPFS访问地址loc使用其第一重加密密钥公钥pk_{do}加密后得到加密隐私数据关键信息C_{do}：

$$C_{do}\leftarrow \mathcal{PRE}.Encrypt(pk_{do},key,loc)$$；

为实例化描述该步骤，本实施例给出其具体算法描述。具体地，数据拥有者DO使用其第一重加密密钥公钥pk_{do}加密明文信息m=(key||loc)，选取，计算：

$$r=H_2(m\|k)$$，

$$c_1=g_1^{r}$$，

$$c_2=k\cdot e(pk_{do},H_1(pk_{do}))^{r}$$，

$$c_3=m\oplus H_3(k)$$，

$$c_4=H_1(pk_{do})$$，

$$c_5=H_4(c_1\|c_2\|c_3\|c_4)^{r}$$，

得到隐私数据关键信息的密文$C_{do}=(c_1,c_2,c_3,c_4,c_5)$。随后，通过跨链节点向部署于监管链上的隐私数据跨链共享智能合约DSSC发起加密隐私数据关键信息上链交易，实现隐私数据关键信息的密文C_{do}上链。此外，该交易内容还包括数据哈希，数据关键词以及隐私数据访问规则等辅助信息；部署于监管链上的隐私数据跨链共享智能合约DSSC包括：加密隐私数据关键信息上链接口、隐私数据请求接口、重加密密文上链接口。

[0074] 步骤4)排序节点收集监管链中的加密隐私数据关键信息上链交易，随后打包成块并进行全网广播。

[0075] 步骤5)数据请求者DR通过跨链节点对监管链区块中的加密隐私数据关键信息上链交易内容进行检索，随后向监管链上的隐私数据跨链共享智能合约DSSC发起数据请求交易，其中包含数据请求者DR的第一重加密密钥公钥pk_{dr}以及自身属性$Attr_{dr}$用以向数据拥有者表明其是否符合隐私数据的访问规则。

[0076] 步骤6)代理节点从隐私数据请求交易中获得数据请求者的第一重加密密钥公钥pk_{dr}及其自身属性$Attr_{dr}$，随后连同权威监管者联盟第一重加密密钥公钥pk_{Auth}一并发送给数据拥有者DO，后者在本地执行代理重加密的第二重加密密钥生成算法，分别生成第二重加密密钥$rk_{do\text{-}dr}$与$rk_{do\text{-}Auth}$：

$$rk_{do-dr} \leftarrow \mathcal{PRE}.ReKeyGen(sk_{do}, pk_{do}, pk_{dr})$$；

$$rk_{do-Auth} \leftarrow \mathcal{PRE}.ReKeyGen(sk_{do}, pk_{do}, pk_{Auth})$$；

为实例化描述该步骤，本实施例给出其具体算法描述。

[0077] 具体地，数据拥有者在本地计算数据拥有者DO与数据请求者DR之间的第二重加密密钥rk_{do-dr}：

$$rk_{do-dr} = (r, H_1(pk_{do})^{sk_{do}})$$；

以及数据拥有者DO与权威监管者联盟Auth之间的第二重加密密钥$rk_{do-Auth}$：

$$rk_{do-Auth} = (r, H_1(pk_{do})^{sk_{do}})$$；

随后，将rk_{do-dr}与$rk_{do-Auth}$发送至监管链中的代理节点。

[0078] 步骤7)代理节点在本地执行代理重加密的密文重加密算法，将隐私数据关键信息的密文C_{do}进行密文转换，分别得到数据请求者DR与权威监管者联盟能进行解密的密文C_{dr}与C_{Auth}：

$$C_{dr} \leftarrow \mathcal{PRE}.ReEnc(C_{do}, rk_{do-dr})$$；

$$C_{Auth} \leftarrow \mathcal{PRE}.ReEnc(C_{do}, rk_{do-Auth})$$；

为实例化描述该步骤，本实施例给出其具体算法描述。

[0079] 为得到密文C_{dr}，代理节点使用第二重加密密钥rk_{do-dr}对密文C_{do}进行密文转换，首先检查 $e(c_1, H_4(c_1 \| c_2 \| c_3 \| c_4)) \stackrel{?}{=} e(g, c_5)$，若成立则进行如下计算：

$$c_1' = c_1$$；

$$c_2' = c_2 \cdot e(pk_{dr}^r g^{-r}, H_1(pk_{do})^{-sk_{do}}) \cdot e(pk_{dr}^r, H_1(pk_{dr}) \cdot H_1(pk_{do})^{-sk_{do}})$$

$$= k \cdot e(pk_{dr}^r, H_1(pk_{dr}))$$；

$$c_3' = c_3$$；

$$c_4' = H_1(pk_{dr})$$；

$$c_5' = H_4(c_1' \| c_2' \| c_3' \| c_4')^r$$；

得到可以被数据请求者所解密的密文$C_{dr} = (c_1', c_2', c_3', c_4', c_5')$。

[0080] 为得到密文C_{Auth}，代理节点使用第二重加密密钥$rk_{do-Auth}$对密文C_{do}进行密文转换，首先检查 $e(c_1, H_4(c_1 \| c_2 \| c_3 \| c_4)) \stackrel{?}{=} e(g, c_5)$，若成立则进行如下计算：

$$c_1^* = c_1$$；

$$c_2^* = c_2 \cdot e(pk_{Auth}^r g^{-r}, H_1(pk_{do})^{-sk_{do}}) \cdot e(pk_{Auth}^r, H_1(pk_{Auth}) \cdot H_1(pk_{do})^{-sk_{do}})$$

$=k\cdot e(pk_{Auth}^{r},H_1(pk_{Auth}))$；

$c_3^{*}=c_3$；

$c_4^{*}=H_1(pk_{Auth})$；

$c_5^{*}=H_4(c_1^{*}\|c_2^{*}\|c_3^{*}\|c_4^{*})^{r}$；

得到可以被权威监管者联盟所解密的密文$C_{dr}=(c_1^{*},c_2^{*},c_3^{*},c_4^{*},c_5^{*})$。

[0081] 随后，向监管链上的隐私数据跨链共享智能合约DSSC发起重加密密文上链交易，实现重加密密文的上链。

[0082] 步骤8)数据请求者DR通过跨链节点从重加密密文上链交易中获取其能解密的密文C_{dr}，随后使用自己的第一重加密密钥私钥skdr进行解密，获得对称加密密钥key与IPFS访问地址loc：

$$(key,loc)\leftarrow \mathcal{PRE}.Decrypt(C_{dr},sk_{dr})$$；

为实例化描述该步骤，本实施例给出其具体算法描述。

[0083] 首先检查$e(c_1',H_4(c_1'\|c_2'\|c_3'\|c_4'))\overset{?}{=}e(g,c_5')$，若成立则进行如下计算：

$k=c_2'/e(c_1',H_1(pk_{dr}))^{sk_{dr}}$；

$m=c_3'\oplus H_3(k)$；

计算$r=H_2(m\|k)$，若$c_1'=g_1^{r}$且$c_2'=k\cdot e(pk_{dr}^{r},H_1(pk_{dr}))$，则输出明文m，即获得对称加密密钥key与隐私数据IPFS访问地址loc。

[0084] 随后，数据请求者根据IPFS文件访问地址loc从IPFS分布式存储系统中获取dataEnc并使用对称加密密钥key进行解密，得到隐私数据data。

[0085] 步骤9)当收发双方就隐私数据共享过程发生纠纷或共享隐私数据内容涉嫌非法时，监管链中的各监管节点组成权威监管者联盟，共同恢复出联盟第一重加密密钥私钥sk_{Auth}，对密文C_{Auth}进行解密：

$$(key,loc)\leftarrow \mathcal{PRE}.Decrypt(C_{Auth},sk_{Auth})$$；

为实例化描述该步骤，本实施例给出其具体算法描述。

[0086] 首先，权威监管者联盟进行联盟第一重加密密钥私钥sk_{Auth}恢复，任何t个秘密分片持有者$\{auth_1,\cdots,auth_t\}$将其秘密分片带入下述拉格朗日插值公式：

$$f(x)=\sum_{i=1}^{t}f(x_l)\prod_{v=1,v\neq l}^{t}\frac{x-x_v}{x_l-x_v}\bmod p$$；

其中，t为所述第二设定数量；x为取值范围为GF(p)的自变量，x_v表示第v个秘密分片的随机输入值，x_1表示第1个秘密分片的随机输入值。

[0087] 由：

$$sk_{Auth}=c=f(0)=\sum_{i=1}^{t}f(x_i)\prod_{v=1,v\neq i}^{t}\frac{-x_v}{x_i-x_v}\bmod p;$$

即可恢复出监管者联盟的私钥sk_{Auth}，其中，t为所述第二设定数量；c表示x为0时的函数值，x_v表示第v个秘密分片的随机输入值，x_1表示第1个秘密分片的随机输入值。

[0088] 其次，权威监管者联盟从重加密密文上链交易中获取其能解密的密文C_{Auth}，并使用联盟私钥sk_{Auth}对其进行解密。首先检查$e(c_1^*,H_4(c_1^*\|c_2^*\|c_3^*\|c_4^*))\stackrel{?}{=}e(g,c_5^*)$，若成立则进行如下计算：

$$k=c_2^*/e(c_1^*,H_1(pk_{Auth}))^{sk_{Auth}};$$

$$m=c_3^*\oplus H_3(k);$$

计算$r=H_2(m\|k)$，若$c_1^*=g_1^r$且$c_2^*=k\cdot e(pk_{Auth}^r,H_1(pk_{Auth}))$，则输出明文m，即获得第二加密密钥key与隐私数据IPFS访问地址loc。

[0089] 根据IPFS文件访问地址loc从IPFS分布式存储系统中获取$data_{Enc}$并使用对称加密密钥key进行解密，得到隐私数据data，从而对上述情况做出裁决。

[0090] 本实施例使用代理重加密实现在侧链/中继模式的跨链系统中，应用链间隐私数据的安全跨链共享，能够避免隐私数据的明文传输，保障隐私数据安全。为解决大文件隐私数据无法有效共享的问题，本实施例通过对大文件隐私数据进行对称加密存储，随后将加密密钥与IPFS访问地址进行上链存储，实现大文件隐私数据的高效共享。同时，由于本发明的隐私数据共享过程是通过部署于中继链上的隐私数据跨链共享智能合约完成的，数据共享参与双方的操作记录是可查询可追溯的。最后，本实施例采用秘密共享方案将联盟第一重加密密钥进行秘密分发，可在监管方需要对共享隐私数据内容进行监管及对交易纠纷进行裁决时，通过重组权威监管者联盟的方式对联盟第一重加密密钥进行秘密恢复，实现了在进行跨链隐私数据安全共享的同时，兼顾权威监管机构对数据共享过程的监管需求。

[0091] 综上所述，本发明所述可监管的跨链隐私数据共享方法及装置中，数据拥有者通过对称加密的方式对隐私数据加密后上传至独立的预设分布式存储系统并获得访问地址，引入代理重加密的机制，数据拥有者将对称加密密钥和访问地址加密后的密文交由监管链存储，数据请求者在查询请求交易后，数据拥有者利用转换密钥将数据请求者公私密钥中公钥加密的密文转换为数据请求者公私密钥中公钥加密的密文，由数据请求者利用数据请求者公私密钥中私钥解密得到隐私数据在预设分布式存储系统中的访问地址和对称加密密钥，最终得到需要跨链分享的隐私数据。本发明能够在保证可信度的基础上高效分享大文件的隐私数据，速度快、保密性好、完整度高且可用性强。

[0092] 与上述方法相应地，本发明还提供了一种可监管的跨链隐私数据共享装置，该装置包括计算机设备，所述计算机设备包括处理器和存储器，所述存储器中存储有计算机指令，所述处理器用于执行所述存储器中存储的计算机指令，当所述计算机指令被处理器执行时该装置实现如前所述方法的步骤。

[0093] 本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该计算

机程序被处理器执行时以实现前述边缘计算服务器部署方法的步骤。该计算机可读存储介质可以是有形存储介质，诸如随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、软盘、硬盘、可移动存储盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质。

[0094] 本领域普通技术人员应该可以明白，结合本文中所公开的实施方式描述的各示例性的组成部分、系统和方法，能够以硬件、软件或者二者的结合来实现。具体究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。当以硬件方式实现时，其可以例如是电子电路、专用集成电路(ASIC)、适当的固件、插件、功能卡等等。当以软件方式实现时，本发明的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。

[0095] 需要明确的是，本发明并不局限于上文所描述并在图中示出的特定配置和处理。为了简明起见，这里省略了对已知方法的详细描述。在上述实施例中，描述和示出了若干具体的步骤作为示例。但是，本发明的方法过程并不限于所描述和示出的具体步骤，本领域的技术人员可以在领会本发明的精神后，作出各种改变、修改和添加，或者改变步骤之间的顺序。

[0096] 本发明中，针对一个实施方式描述和/或例示的特征，可以在一个或更多个其它实施方式中以相同方式或以类似方式使用，和/或与其他实施方式的特征相结合或代替其他实施方式的特征。

[0097] 以上所述仅为本发明的优选实施例，并不用于限制本发明，对于本领域的技术人员来说，本发明实施例可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

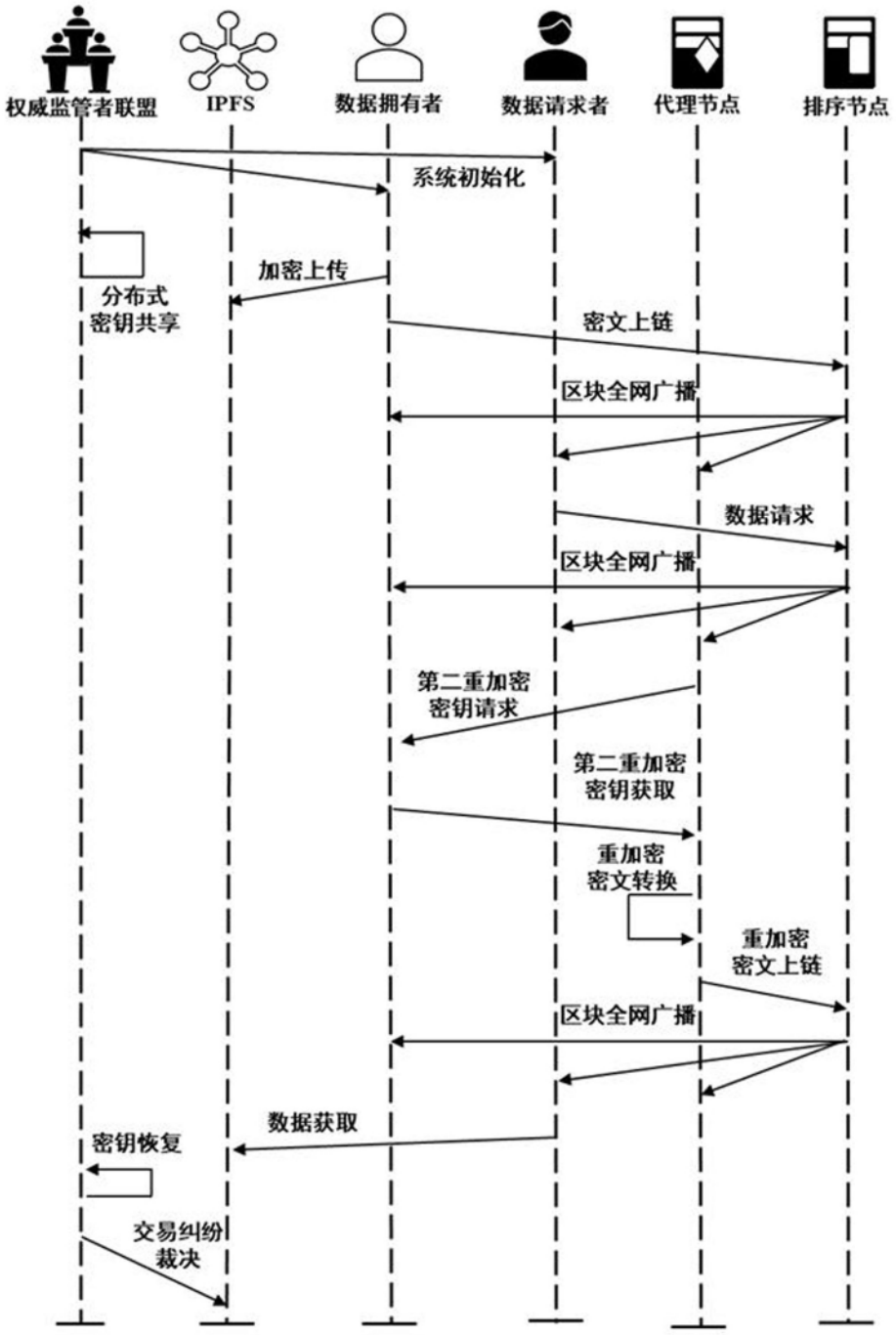

权威监管者联盟
IPFS
数据拥有者
数据请求者
代理节点
排序节点
系统初始化
分布式
密钥共享
加密上传
密文上链
区块全网广播
数据请求
区块全网广播
第二重加密
密钥请求
第二重加密
密钥获取
重加密
密文转换
重加密
密文上链
区块全网广播
数据获取
密钥恢复
交易纠纷
裁决

图1

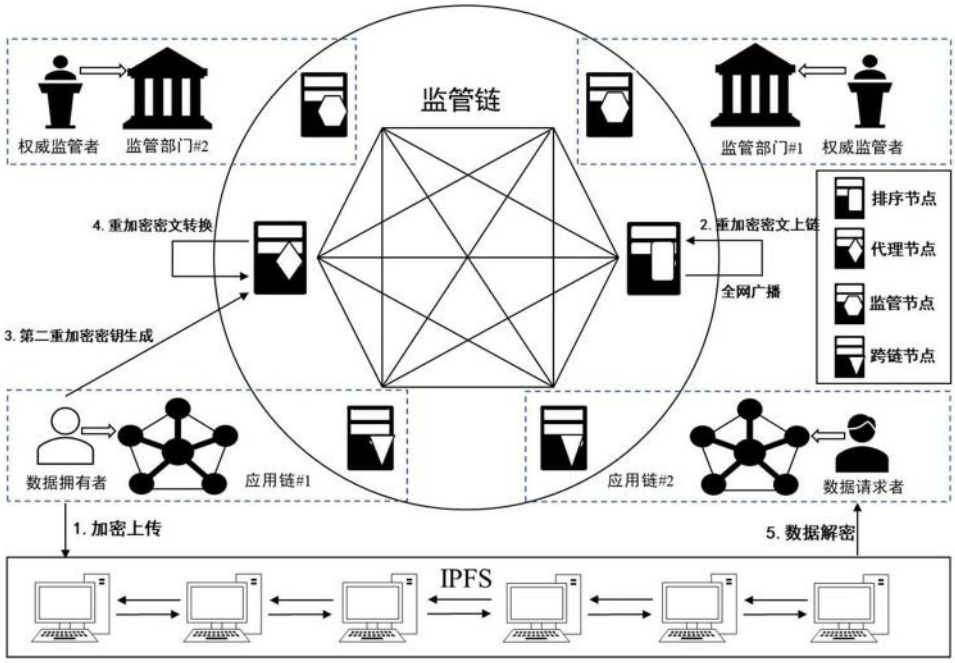

监管链
权威监管者
监管部门#2
监管部门#1
权威监管者
排序节点
代理节点
监管节点
跨链节点
4. 重加密密文转换
2. 重加密密文上链
全网广播
3. 第二重加密密钥生成
数据拥有者
应用链#1
应用链#2
数据请求者
1. 加密上传
5. 数据解密
IPFS

图2