



(12)发明专利申请

(10)申请公布号 CN 108449336 A

(43)申请公布日 2018.08.24

(21)申请号 201810220660.9

(22)申请日 2018.03.16

(71)申请人 浙江创邻科技有限公司

地址 310030 浙江省杭州市西湖区三墩镇
紫宣路158号1幢801室

(72)发明人 张晨

(74)专利代理机构 北京酷爱智慧知识产权代理
有限公司 11514

代理人 高江玲

(51)Int.Cl.

H04L 29/06(2006.01)

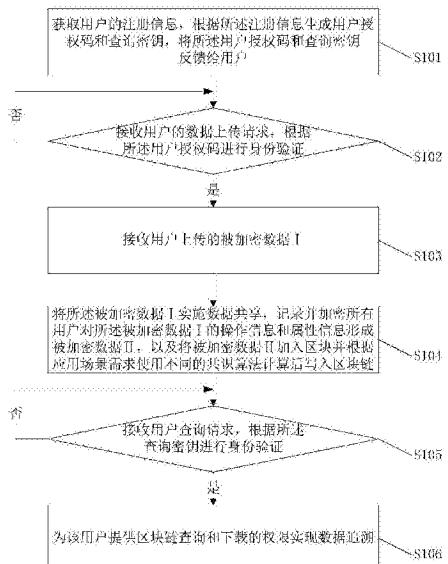
权利要求书1页 说明书9页 附图3页

(54)发明名称

基于区块链的数据追溯与强加密方法、装置、介质及系统

(57)摘要

本发明涉及区块链技术应用领域，基于区块链的数据追溯与强加密方法、装置、介质及系统；其方法包括获取用户的注册信息，根据注册信息生成用户授权码和查询密钥，并将其反馈给用户；接收用户的数据上传请求，然后再接收验证通过的用户所上传的被加密数据I；将被加密数据I实施数据共享，记录并加密所有用户对被加密数据I的操作信息和属性信息形成被加密数据II，将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链；接收用户查询请求，根据查询密钥进行身份验证，为验证通过的用户提供区块链查询和下载的权限实现数据追溯。本发明让用户能够受益于共享数据带来的加成价值，又享有完全的数据隐私和数据安全。



1. 基于区块链的数据追溯与强加密方法，其特征在于，包括如下步骤：

获取用户的注册信息，根据所述注册信息生成用户授权码和查询密钥，以及将所述用户授权码和查询密钥反馈给用户；

接收用户的数据上传请求，根据所述用户授权码进行身份验证，若验证通过，则接收用户上传的被加密数据I；

将所述被加密数据I实施数据共享，记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II，以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链；

接收用户查询请求，根据所述查询密钥进行身份验证，若验证通过，则为该用户提供区块链查询和下载的权限实现数据追溯。

2. 根据权利要求1所述的基于区块链的数据追溯与强加密方法，其特征在于，所述接收用户上传的被加密数据I包括：

接收用户通过可加密客户端上传的被加密数据I。

3. 根据权利要求1或2任意一项所述的基于区块链的数据追溯与强加密方法，其特征在于，所述接收用户上传的被加密数据I包括：

接收用户通过加密通道上传的数据，并将所述数据通过处理模块强加密，形成被加密数据I。

4. 根据权利要求1所述的基于区块链的数据追溯与强加密方法，其特征在于：

所述操作信息包括：添加操作信息、修改操作信息、删除操作信息和/或访问操作信息。

5. 根据权利要求4所述的基于区块链的数据追溯与强加密方法，其特征在于：

所述属性信息包括时间、IP、用户名和/或操作类型。

6. 根据权利要求1所述的基于区块链的数据追溯与强加密方法，其特征在于，所述基于区块链的数据追溯与强加密方法还包括：

将使用共享信息进行的算法迭代的结果反馈给所有用户。

7. 根据权利要求6所述的基于区块链的数据追溯与强加密方法，其特征在于：

所述使用共享信息进行的算法迭代中涉及的算法是根据上层应用和共享目的决定。

8. 一种基于区块链的数据追溯与强加密装置，其特征在于：所述基于区块链的数据追溯与强加密装置包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的程序，所述存储器和处理器电连，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器被配置用于调用所述程序指令，执行如权利要求1-7任意一项所述的基于区块链的数据追溯与强加密方法的步骤。

9. 一种计算机可读存储介质，其特征在于：所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如权利要求1-7任意一项所述的基于区块链的数据追溯与强加密方法的步骤。

10. 一种基于区块链的数据追溯与强加密系统，其特征在于：所述基于区块链的数据追溯与强加密系统包括基于区块链的数据追溯与强加密装置和客户端，所述基于区块链的数据追溯与强加密装置与客户端通信连接，所述基于区块链的数据追溯与强加密装置执行如权利要求1-7任意一项所述的基于区块链的数据追溯与强加密方法的步骤。

基于区块链的数据追溯与强加密方法、装置、介质及系统

技术领域

[0001] 本发明涉及区块链技术应用领域,尤其是基于区块链的数据追溯与强加密方法、装置、介质及系统。

背景技术

[0002] 区块链技术是一项颠覆性的技术,目前无论是底层技术还是上层应用都是最前沿的科研方向。以金融数据为例,当前的痛点是很多金融公司都有自己的数据,但是大家都不愿意共享出来,尽管所有人都知道基于一个共享的大数据池可以得到单个数据孤岛无法产生的价值。现在不存在一种方法或者系统,可以保证数据的可追溯以及绝对的数据安全,以至于只有授权的计算机才能打开数据,即使硬盘被拿走,数据在其他任何未授权环境打开也是加密的乱码,同时任何共享数据的一方都只能看到和追溯自己的数据在何时何地被何人授权打开,而不能看到任何他人的共享数据信息,只能看到一个由所有参与者共享的链条来保证记录的不可篡改以及可追溯。

发明内容

[0003] 针对现有技术中的缺陷,本发明提供一种基于区块链的数据追溯与强加密方法、装置、介质及系统实现了既共享数据,能够受益于共享数据带来的加成价值,又享有完全的数据隐私和数据安全。

[0004] 为了实现上述目的,第一方面,本发明提供的基于区块链的数据追溯与强加密方法,包括如下步骤:

[0005] 获取用户的注册信息,根据所述注册信息生成用户授权码和查询密钥,以及将所述用户授权码和查询密钥反馈给用户;

[0006] 接收用户的数据上传请求,根据所述用户授权码进行身份验证,若验证通过,则接收用户上传的被加密数据I;

[0007] 将所述被加密数据I实施数据共享,记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II,以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链;

[0008] 接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则为该用户提供区块链查询和下载的权限实现数据追溯。

[0009] 作为本申请一种优选的实施方式,所述接收用户上传的被加密数据I包括:

[0010] 接收用户通过可加密客户端上传的被加密数据I。

[0011] 作为本申请一种优选的实施方式,所述接收用户上传的被加密数据I包括:

[0012] 接收用户通过加密通道上传的数据,并将所述数据通过处理模块强加密,形成被加密数据I。

[0013] 作为本申请一种优选的实施方式,所述操作信息包括:添加操作信息、修改操作信息、删除操作信息和/或访问操作信息。

- [0014] 作为本申请一种优选的实施方式,所述属性信息包括时间、IP、用户名和/或操作类型。
- [0015] 作为本申请一种优选的实施方式,所述基于区块链的数据追溯与强加密方法还包括:
- [0016] 将使用共享信息进行的算法迭代的结果反馈给所有用户。
- [0017] 作为本申请一种优选的实施方式,所述使用共享信息进行的算法迭代中涉及的算法是根据上层应用和共享目的决定。
- [0018] 第二方面,本发明提供的一种基于区块链的数据追溯与强加密装置,所述基于区块链的数据追溯与强加密装置包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的程序,所述存储器和处理器电连,其中,所述存储器用于存储计算机程序,所述计算机程序包括程序指令,所述处理器被配置用于调用所述程序指令,执行如所述的基于区块链的数据追溯与强加密方法的步骤。
- [0019] 第三方面,本发明提供的一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序包括程序指令,所述程序指令当被处理器执行时使所述处理器执行如所述的基于区块链的数据追溯与强加密方法的步骤。
- [0020] 第四方面,本发明提供的一种基于区块链的数据追溯与强加密系统,所述基于区块链的数据追溯与强加密系统包括基于区块链的数据追溯与强加密装置和客户端,所述基于区块链的数据追溯与强加密装置与客户端通信连接,所述基于区块链的数据追溯与强加密装置执行如所述的基于区块链的数据追溯与强加密方法的步骤。
- [0021] 本发明的有益效果是:本发明提供的基于区块链的数据追溯与强加密方法、装置、介质及系统实现了既共享数据,能够受益于共享数据带来的加成价值,又享有完全的数据隐私和数据安全,以至于任何其他参与共享的第三方在未授权的计算机都无法看到数据,甚至是把数据硬盘直接拿走也无法看到解密数据。即使是参与共享的用户自己下载了自己共享后的数据,也无法打开,因为任何参与共享的用户都没有也无法访问系统授权的计算机。实现了对参与共享的所有用户的数据的强加密,以保障数据隐私和安全。

附图说明

- [0022] 图1为本发明基于区块链的数据追溯与强加密方法第一实施例的流程图;
- [0023] 图2为本发明基于区块链的数据追溯与强加密方法第二实施例的流程图;
- [0024] 图3为本发明基于区块链的数据追溯与强加密装置第一实施例的框图;
- [0025] 图4为本发明基于区块链的数据追溯与强加密系统第一实施例的框图。

具体实施方式

- [0026] 下面将详细描述本发明的具体实施例,应当注意,这里描述的实施例只用于举例说明,并不用于限制本发明。在以下描述中,为了提供对本发明的透彻理解,阐述了大量特定细节。然而,对于本领域普通技术人员显而易见的是:不必采用这些特定细节来实行本发明。在其他实例中,为了避免混淆本发明,未具体描述公知的电路,软件或方法。
- [0027] 在整个说明书中,对“一个实施例”、“实施例”、“一个示例”或“示例”的提及意味着:结合该实施例或示例描述的特定特征、结构或特性被包含在本发明至少一个实施例中。

因此,在整个说明书的各个地方出现的短语“在一个实施例中”、“在实施例中”、“一个示例”或“示例”不一定都指同一实施例或示例。此外,可以以任何适当的组合和、或子组合将特定的特征、结构或特性组合在一个或多个实施例或示例中。此外,本领域普通技术人员应当理解,在此提供的示图都是为了说明的目的,并且示图不一定是按比例绘制的。

[0028] 基于区块链的数据追溯与强加密方法的第一实施例:

[0029] 如图1所示,所述基于区块链的数据追溯与强加密方法,包括如下步骤:

[0030] S101,获取用户的注册信息,根据所述注册信息生成用户授权码和查询密钥,将所述用户授权和查询密钥反馈给用户。

[0031] S102,接收用户的数据上传请求,根据所述用户授权码进行身份验证,若验证通过,则执行步骤S103;若验证失败,则重复步骤S102。

[0032] S103,接收用户上传的被加密数据I。

[0033] S104,将所述被加密数据I实施数据共享,记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II,以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链。

[0034] S105,接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则执行步骤S106;若验证失败,则重复步骤S105。

[0035] S106,为该用户提供区块链查询和下载的权限实现数据追溯。

[0036] 具体的,本发明能够受益于共享数据带来的加成价值,又享有完全的数据隐私和数据安全,以至于任何其他参与共享的第三方在未授权的计算机都无法看到数据,甚至是把数据硬盘直接拿走也无法看到解密数据。即使是参与共享的用户自己下载了自己共享后的数据,也无法打开,因为任何参与共享的用户都没有也无法访问系统授权的计算机。实现了对参与共享的所有用户的数据的强加密,以保障数据隐私和安全。

[0037] 基于区块链的数据追溯与强加密方法的第二实施例:

[0038] 如图2所示,所述基于区块链的数据追溯与强加密方法,包括如下步骤:

[0039] S201,获取用户的注册信息,根据所述注册信息生成用户授权码和查询密钥,将所述用户授权和查询密钥反馈给用户。

[0040] 具体的,用户的注册信息可以包括但不限于用户的姓名和地址信息,所述地址信息可以包括:邮件地址,或者与邮件地址唯一对应的编号,也可以是移动通信终端号码,只要是对应了可以收发消息的地址信息都应在本发明的保护范围之内。

[0041] S202,接收用户的数据上传请求,根据所述用户授权码进行身份验证,若验证通过,则执行步骤S203;若验证失败,则重复步骤S202。

[0042] 具体的,本发明中可以通过前端API接收用户的数据上传请求,并利用所述授权码验证其身份,提高了上传数据的安全系数,能够实现限制客户上传恶意数据等目的。

[0043] S203,接收用户上传的被加密数据I。

[0044] 具体的,所述接收用户上传的被加密数据I包括以下两种方式:

[0045] 1、接收用户通过可加密客户端上传的被加密数据I;所述可加密客户端是指特定的安全系数较高的可加密客户端,使得用户通过该客户端上传的数据已经是完全的加密数据,即被加密数据I,这样可以全面的保证数据隐私和安全。

[0046] 2、接收用户通过加密通道上传的数据,并将所述数据通过处理模块强加密,形成

被加密数据I;用户可以通过普通的客户端实现数据上传,数据通过加密通道进行传输给后台的处理模块,所述处理模块可以根据实际情况选择不同的加密算法对用户上传的数据进行加密,进而形成密文。

[0047] S204,将所述被加密数据I实施数据共享,记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II,以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链。

[0048] 具体的,通过将被加密数据I放入共享数据池中实现了数据共享,后台记录并加密所有用户对加密数据I的操作信息和属性信息形成被加密数据II;所述操作信息包括但不限于添加操作信息、修改操作信息、删除操作信息和访问操作信息;所述属性信息包括但不限于时间、IP、用户名和操作类型。再将所述加密数据II以payload加入区块,并根据应用场景需求使用包括但不限于POW、POS、DPOS、dBFT、PBFT、Paxos和Raft的一种算法进行计算,广播达成共识后写入区块链。需要进行说明的是,后台的综合计算结果纯粹是基于加密数据接口,不会暴露任何隐私数据或原始数据。

[0049] S205,将使用共享信息进行的算法迭代的结果反馈给所有用户

[0050] 具体的,所述使用共享信息进行的算法迭代的具体算法是根据上层应用和共享目的而定。譬如,可以计算共享信息的数量加和、平均、对共享信息进行线性变换等的一种或多种。

[0051] S206,接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则执行步骤S207;若验证失败,则重复步骤S206。

[0052] 具体的,当数据的原拥有者需要进行想要进行查询的时候,可以利用反馈得到的查询密钥进行身份信息验证,保证了数据隐私和数据安全。

[0053] S207,为该用户提供区块链查询和下载的权限实现数据追溯。

[0054] 具体的,在验证通过之后用户获得了区块链查询和下载的权限,用户可以通过web管理界面查看区块链,查看并追溯其余所有用户对自己已经共享的数据的操作信息以及操作的属性信息,查询并下载自己共享的数据的加密版本。需要进行说明的是,下载的加密数据即使是原数据拥有者也无法打开,因为任何参与共享的用户都不拥有被授权的计算机。

[0055] 基于区块链的数据追溯与强加密装置的第一实施例:

[0056] 如图3所示,所述基于区块链的数据追溯与强加密装置包括:处理器40,存储器41,总线42、通信接口43以及存储在所述存储器中并可在所述处理器40上运行的程序。

[0057] 具体的,存储器41可能包含高速随机存取存储器(RAM:Random Access Memory),也可能还包括非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。通过至少一个通信接口43(可以是有线或者无线)实现该系统网元与至少一个其他网元之间的通信连接,可以使用互联网,广域网,本地网,城域网等。

[0058] 总线42可以是ISA总线、PCI总线或EISA总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图3中仅用一个双向箭头表示,但并不表示仅有的一根总线或一种类型的总线。

[0059] 具体的,存储器41用于存储程序401,所述处理器40在接收到执行指令后,执行所述程序401,前述本发明实施例任一实施例揭示的流过程定义的装置所执行的方法可以应用于处理器40中,或者由处理器40实现。

[0060] 处理器40可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器40中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器40可以是通用处理器，包括中央处理器(Central Processing Unit，简称CPU)、网络处理器(Network Processor，简称NP)等；还可以是数字信号处理器(DSP)、专用集成电路(ASIC)、现成可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器41，处理器40读取存储器41中的信息，结合其硬件完成基于区块链的数据追溯与强加密方法的步骤。

[0061] 本实施例中，所述基于区块链的数据追溯与强加密方法在被执行时包括如下步骤：

[0062] S301，获取用户的注册信息，根据所述注册信息生成用户授权码和查询密钥，将所述用户授权和查询密钥反馈给用户。

[0063] 具体的，用户的注册信息可以包括但不限于用户的姓名和地址信息，所述地址信息可以包括：邮件地址，或者与邮件地址唯一对应的编号，也可以是移动通信终端号码，只要是对应了可以收发消息的地址信息都应在本发明的保护范围之内。

[0064] S302，接收用户的数据上传请求，根据所述用户授权码进行身份验证，若验证通过，则执行步骤S303；若验证失败，则重复步骤S302。

[0065] 具体的，本发明中可以通过前端API接收用户的数据上传请求，并利用所述授权码验证其身份，提高了上传数据的安全系数，能够实现限制客户上传恶意数据等目的。

[0066] S303，接收用户上传的被加密数据I。

[0067] 具体的，所述接收用户上传的被加密数据I包括以下两种方式：

[0068] 1、接收用户通过可加密客户端上传的被加密数据I；所述可加密客户端是指特定的安全系数较高的可加密客户端，使得用户通过该客户端上传的数据已经是完全的加密数据，即被加密数据I，这样可以全面的保证数据隐私和安全。

[0069] 2、接收用户通过加密通道上传的数据，并将所述数据通过处理模块强加密，形成被加密数据I；用户可以通过普通的客户端实现数据上传，数据通过加密通道进行传输给后台的处理模块，所述处理模块可以根据实际情况选择不同的加密算法对用户上传的数据进行加密，进而形成密文。

[0070] S304，将所述被加密数据I实施数据共享，记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II，以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链。

[0071] 具体的，通过将被加密数据I放入共享数据池中实现了数据共享，后台记录并加密所有用户对加密数据I的操作信息和属性信息形成被加密数据II；所述操作信息包括但不限于添加操作信息、修改操作信息、删除操作信息和访问操作信息；所述属性信息包括但不限于时间、IP、用户名和操作类型。再将所述加密数据II以payload加入区块，并根据应用场

景需求使用包括但不限于POW、POS、DPOS、dBFT、PBFT、Paxos和Raft的一种算法进行计算，广播达成共识后写入区块链。需要进行说明的是，后台的综合计算结果纯粹是基于加密数据接口，不会暴露任何隐私数据或原始数据。

[0072] S305,将使用共享信息进行的算法迭代的结果反馈给所有用户

[0073] 具体的，所述使用共享信息进行的算法迭代的具体算法是根据上层应用和共享目的而定。譬如，可以计算共享信息的数量加和、平均、对共享信息进行线性变换等的一种或多种。

[0074] S306,接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则执行步骤S307;若验证失败,则重复步骤S306。

[0075] 具体的，当数据的原拥有者需要进行想要进行查询的时候，可以利用反馈得到的查询密钥进行身份信息验证，保证了数据隐私和数据安全。

[0076] S307,为该用户提供区块链查询和下载的权限实现数据追溯。

[0077] 具体的，在验证通过之后用户获得了区块链查询和下载的权限，用户可以通过web管理界面查看区块链，查看并追溯其余所有用户对自己已经共享的数据的操作信息以及操作的属性信息，查询并下载自己共享的数据的加密版本。需要进行说明的是，下载的加密数据即使是原数据拥有着也无法打开，因为任何参与共享的用户都不拥有被授权的计算机。

[0078] 计算机可读存储介质的第一实施例：

[0079] 所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如所述的基于区块链的数据追溯与强加密方法的步骤。

[0080] 具体的，所述计算机可读存储介质可包括缓存(Cache)、高速随机存取存储器(RAM)，例如常见的双倍数据率同步动态随机存取内存(DDR SDRAM)，并且还可包括非易失性存储器(NVRAM)，诸如一个或多个只读存储器(ROM)、磁盘存储设备、闪存(Flash)存储器设备、或其他非易失性固态存储器设备例如光盘(CD-ROM, DVD-ROM)，软盘或数据磁带等。

[0081] 本实施例中，所述程序指令当被处理器执行时使所述处理器执行如基于区块链的数据追溯与强加密方法的步骤具体包括：

[0082] S401,获取用户的注册信息,根据所述注册信息生成用户授权码和查询密钥,将所述用户授权和查询密钥反馈给用户。

[0083] 具体的，用户的注册信息可以包括但不限于用户的姓名和地址信息，所述地址信息可以包括：邮件地址，或者与邮件地址唯一对应的编号，也可以是移动通信终端号码，只要是对应了可以收发消息的地址信息都应在本发明的保护范围之内。

[0084] S402,接收用户的数据上传请求,根据所述用户授权码进行身份验证,若验证通过,则执行步骤S403;若验证失败,则重复步骤S402。

[0085] 具体的，本发明中可以通过前端API接收用户的数据上传请求，并利用所述授权码验证其身份，提高了上传数据的安全系数，能够实现限制客户上传恶意数据等目的。

[0086] S403,接收用户上传的被加密数据I。

[0087] 具体的，所述接收用户上传的被加密数据I包括以下两种方式：

[0088] 1、接收用户通过可加密客户端上传的被加密数据I；所述可加密客户端是指特定的安全系数较高的可加密客户端，使得用户通过该客户端上传的数据已经是完全的加密数

据,即被加密数据I,这样可以全面的保证数据隐私和安全。

[0089] 2、接收用户通过加密通道上传的数据,并将所述数据通过处理模块强加密,形成被加密数据I;用户可以通过普通的客户端实现数据上传,数据通过加密通道进行传输给后台的处理模块,所述处理模块可以根据实际情况选择不同的加密算法对用户上传的数据进行加密,进而形成密文。

[0090] S404,将所述被加密数据I实施数据共享,记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II,以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链。

[0091] 具体的,通过将被加密数据I放入共享数据池中实现了数据共享,后台记录并加密所有用户对加密数据I的操作信息和属性信息形成被加密数据II;所述操作信息包括但不限于添加操作信息、修改操作信息、删除操作信息和访问操作信息;所述属性信息包括但不限于时间、IP、用户名和操作类型。再将所述加密数据II以payload加入区块,并根据应用场景需求使用包括但不限于POW、POS、DPOS、dBFT、PBFT、Paxos和Raft的一种算法进行计算,广播达成共识后写入区块链。需要进行说明的是,后台的综合计算结果纯粹是基于加密数据接口,不会暴露任何隐私数据或原始数据。

[0092] S405,将使用共享信息进行的算法迭代的结果反馈给所有用户

[0093] 具体的,所述使用共享信息进行的算法迭代的具体算法是根据上层应用和共享目的而定。譬如,可以计算共享信息的数量加和、平均、对共享信息进行线性变换等的一种或多种。

[0094] S406,接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则执行步骤S407;若验证失败,则重复步骤S406。

[0095] 具体的,当数据的原拥有者需要进行想要进行查询的时候,可以利用反馈得到的查询密钥进行身份信息验证,保证了数据隐私和数据安全。

[0096] S407,为该用户提供区块链查询和下载的权限实现数据追溯。

[0097] 具体的,在验证通过之后用户获得了区块链查询和下载的权限,用户可以通过web管理界面查看区块链,查看并追溯其余所有用户对自己已经共享的数据的操作信息以及操作的属性信息,查询并下载自己共享的数据的加密版本。需要进行说明的是,下载的加密数据即使是原数据拥有者也无法打开,因为任何参与共享的用户都不拥有被授权的计算机。

[0098] 基于区块链的数据追溯与强加密系统的第一实施例:

[0099] 如图4所示,所述基于区块链的数据追溯与强加密系统包括基于区块链的数据追溯与强加密装置和多个客户端,所述基于区块链的数据追溯与强加密装置与客户端通信连接,所述基于区块链的数据追溯与强加密装置执行如所述的基于区块链的数据追溯与强加密方法的步骤。

[0100] 本实施例中,所述基于区块链的数据追溯与强加密方法在被执行时包括如下步骤:

[0101] S501,获取用户的注册信息,根据所述注册信息生成用户授权码和查询密钥,将所述用户授权和查询密钥反馈给用户。

[0102] 具体的,用户的注册信息可以包括但不限于用户的姓名和地址信息,所述地址信息可以包括:邮件地址,或者与邮件地址唯一对应的编号,也可以是移动通信终端号码,只

要是对应了可以收发消息的地址信息都应在本发明的保护范围之内。

[0103] S502,接收用户的数据上传请求,根据所述用户授权码进行身份验证,若验证通过,则执行步骤S503;若验证失败,则重复步骤S502。

[0104] 具体的,本发明中可以通过前端API接收用户的数据上传请求,并利用所述授权码验证其身份,提高了上传数据的安全系数,能够实现限制客户上传恶意数据等目的。

[0105] S503,接收用户上传的被加密数据I。

[0106] 具体的,所述接收用户上传的被加密数据I包括以下两种方式:

[0107] 1、接收用户通过可加密客户端上传的被加密数据I;所述可加密客户端是指特定的安全系数较高的可加密客户端,使得用户通过该客户端上传的数据已经是完全的加密数据,即被加密数据I,这样可以全面的保证数据隐私和安全。

[0108] 2、接收用户通过加密通道上传的数据,并将所述数据通过处理模块强加密,形成被加密数据I;用户可以通过普通的客户端实现数据上传,数据通过加密通道进行传输给后台的处理模块,所述处理模块可以根据实际情况选择不同的加密算法对用户上传的数据进行加密,进而形成密文。

[0109] S504,将所述被加密数据I实施数据共享,记录并加密所有用户对所述被加密数据I的操作信息和属性信息形成被加密数据II,以及将被加密数据II加入区块并根据应用场景需求使用不同的共识算法计算后写入区块链。

[0110] 具体的,通过将被加密数据I放入共享数据池中实现了数据共享,后台记录并加密所有用户对加密数据I的操作信息和属性信息形成被加密数据II;所述操作信息包括但不限于添加操作信息、修改操作信息、删除操作信息和访问操作信息;所述属性信息包括但不限于时间、IP、用户名和操作类型。再将所述加密数据II以payload加入区块,并根据应用场景需求使用包括但不限于POW、POS、DPOS、dBFT、PBFT、Paxos和Raft的一种算法进行计算,广播达成共识后写入区块链。需要进行说明的是,后台的综合计算结果纯粹是基于加密数据接口,不会暴露任何隐私数据或原始数据。

[0111] S505,将使用共享信息进行的算法迭代的结果反馈给所有用户

[0112] 具体的,所述使用共享信息进行的算法迭代的具体算法是根据上层应用和共享目的而定。譬如,可以计算共享信息的数量加和、平均、对共享信息进行线性变换等的一种或多种。

[0113] S506,接收用户查询请求,根据所述查询密钥进行身份验证,若验证通过,则执行步骤S507;若验证失败,则重复步骤S506。

[0114] 具体的,当数据的原拥有者需要进行想要进行查询的时候,可以利用反馈得到的查询密钥进行身份信息验证,保证了数据隐私和数据安全。

[0115] S507,为该用户提供区块链查询和下载的权限实现数据追溯。

[0116] 具体的,在验证通过之后用户获得了区块链查询和下载的权限,用户可以通过web管理界面查看区块链,查看并追溯其余所有用户对自己已经共享的数据的操作信息以及操作的属性信息,查询并下载自己共享的数据的加密版本。需要进行说明的是,下载的加密数据即使是原数据拥有者也无法打开,因为任何参与共享的用户都不拥有被授权的计算机。

[0117] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依

然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的范围,其均应涵盖在本发明的权利要求和说明书的范围当中。

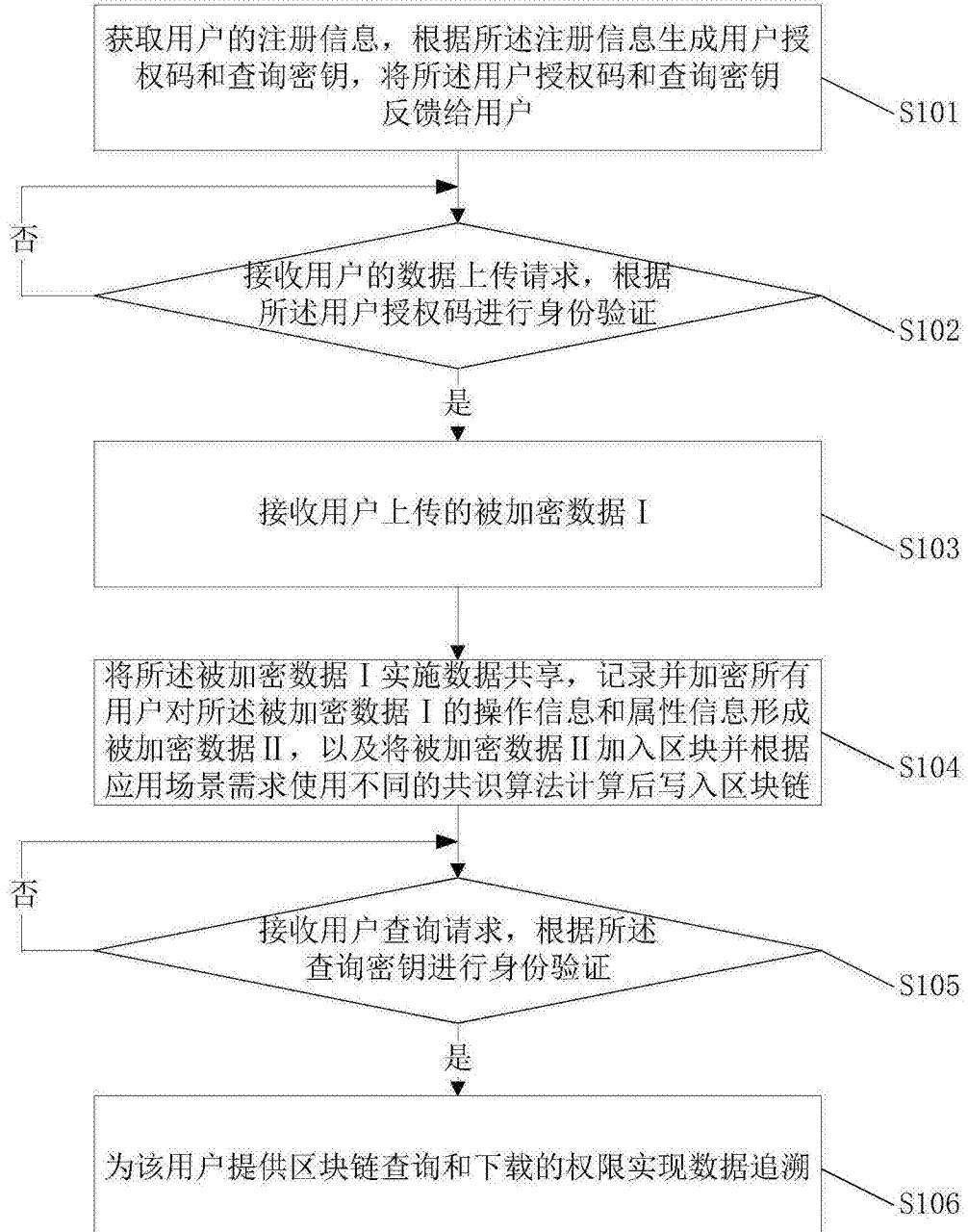


图1

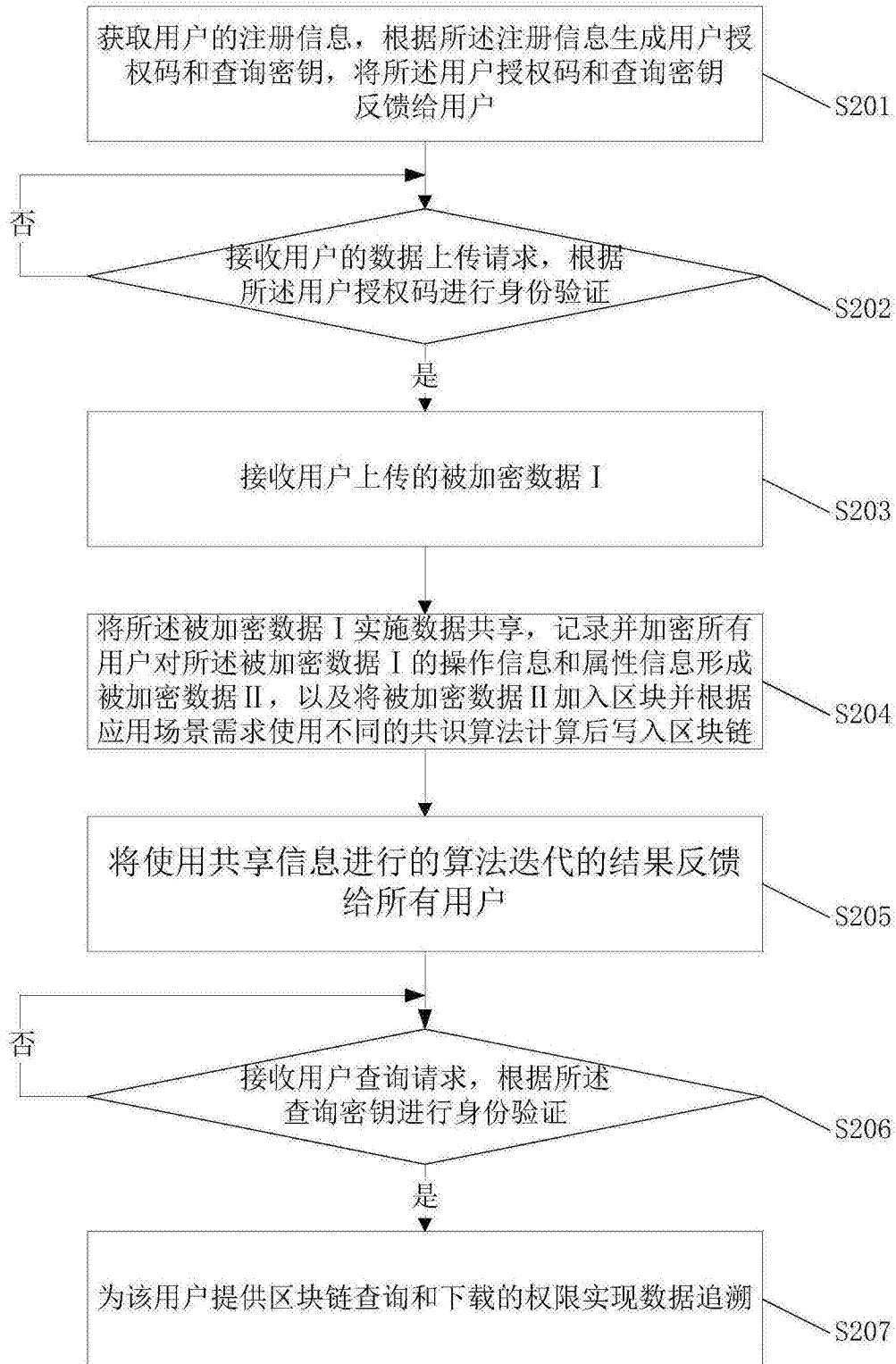


图2

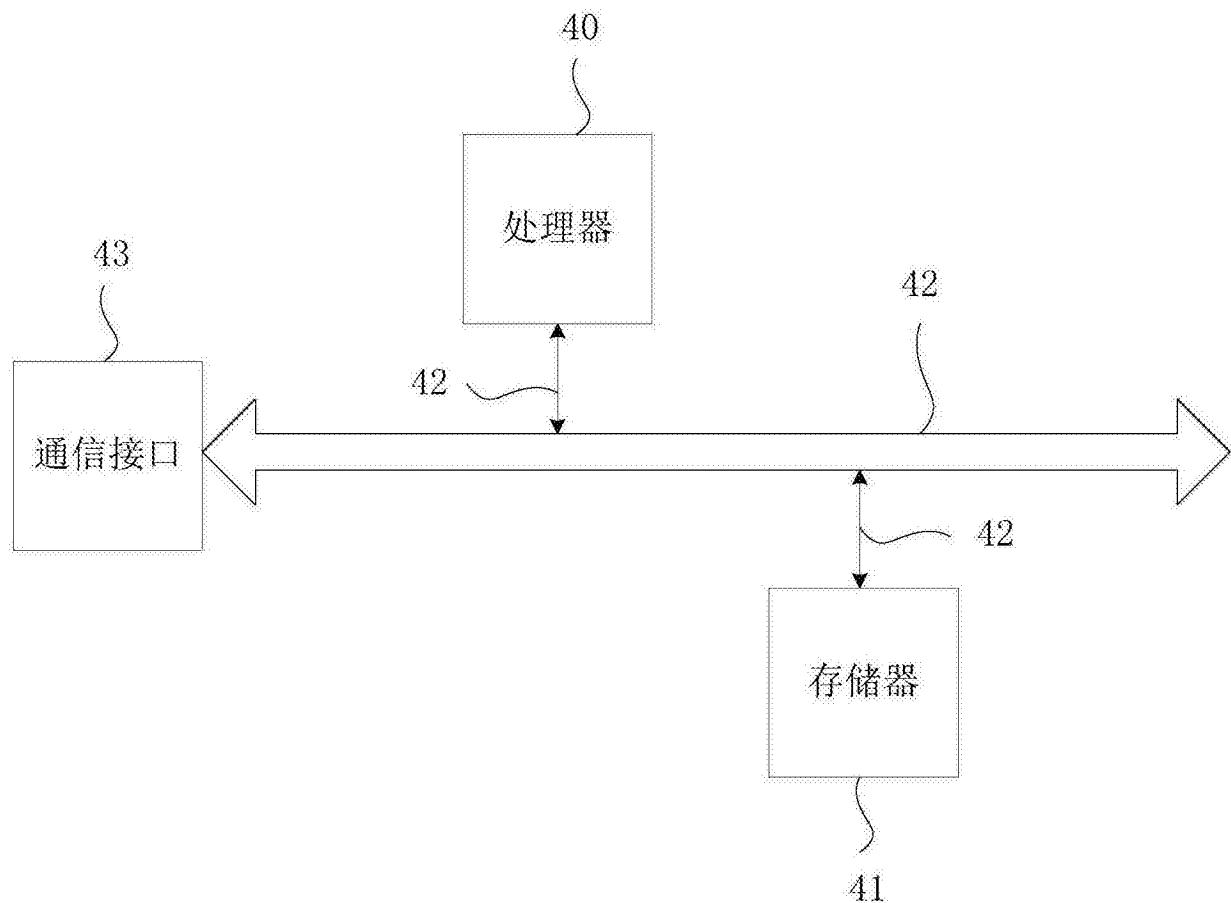


图3

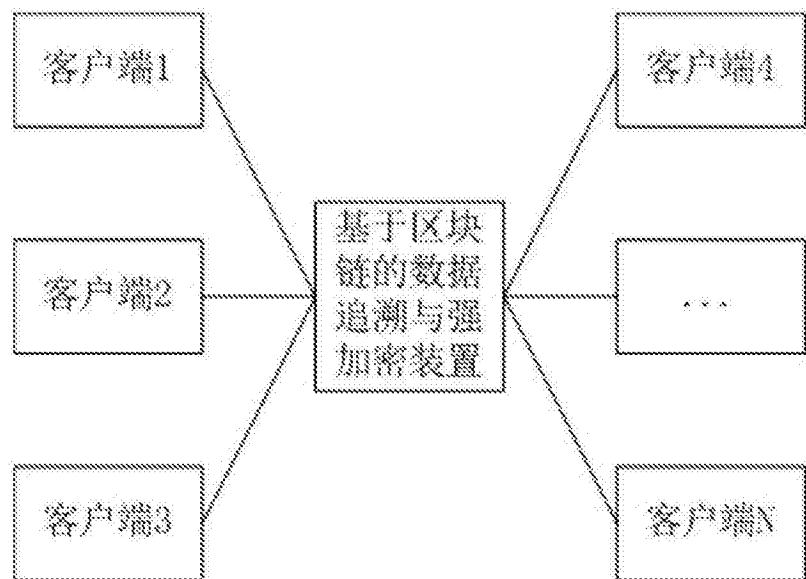


图4