(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111709056 A
(43)申请公布日 2020.09.25

(21)申请号 202010853970.1

(22)申请日 2020.08.24

(71)申请人 北京邮电大学
地址 100088 北京市海淀区西土城路10号
申请人 北京腾信光大科技有限公司

(72)发明人 马兆丰 王小畅 杨娟 王凌云 赵伟哲

(74)专利代理机构 北京金咨知识产权代理有限公司 11612
代理人 秦景芳

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

权利要求书4页 说明书19页 附图6页

(54)发明名称

基于区块链的数据共享方法及系统

(57)摘要

本发明提供了一种基于区块链的数据共享方法及系统，其中，该方法包括：在资源拥有者端接收资源上传请求；对资源数据进行加密，并存储密钥；通过区块链上的智能合约将资源访问策略发布至区块链并获取合约调用信息；通过智能合约将资源数据存储至资源存储系统中并获取返回的资源存储地址；在资源请求者端提交资源数据下载请求；通过智能合约根据请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略；通过智能合约进行访问控制决策；通过智能合约在允许访问时根据资源存储地址从资源存储系统读取的加密的资源数据；对加密的资源数据进行解密。通过上述方案能够实现基于区块链的可信数据安全共享和受控访问。

CN 111709056 A

1.一种基于区块链的数据共享方法,其特征在于,包括:

在资源拥有者端上传资源数据;

在资源请求者端请求资源数据;

其中:

在资源拥有者端上传资源数据,包括:

在资源拥有者端接收资源上传请求,其中,所述资源上传请求包括资源数据和资源访问策略;

使用对称加密算法对所述资源数据进行加密;存储加密所述资源数据的密钥;

通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息;

通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址;

在资源请求者端请求资源数据,包括:

在资源请求者端提交资源数据下载请求,其中,所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息;

通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略;

通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策;

通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求;

接收从所述资源存储系统读取的加密的资源数据;

对加密的资源数据进行解密;

通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息,包括:

通过区块链上的策略管理智能合约根据所述资源上传请求中的资源访问策略发送属性添加指令至属性管理智能合约;

通过区块链上的属性管理智能合约根据所述属性添加指令将所述资源访问策略发布至所述区块链,并返回的所述资源访问策略的合约调用信息;

通过策略管理智能合约获取返回的所述资源访问策略的合约调用信息;

通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址,包括:

通过所述区块链上的策略管理智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

2.如权利要求1所述的基于区块链的数据共享方法,其特征在于,

在资源拥有者端上传资源数据,还包括:

使用密文-策略加密算法根据所述资源访问策略对加密所述资源数据所用的密钥进行加密,形成加密密钥;

在资源请求者端请求资源数据,还包括:

对所述加密密钥进行解密,得到明文密钥;

对加密的资源数据进行解密,包括:

利用所述明文密钥对加密的资源数据进行解密。

3.如权利要求1所述的基于区块链的数据共享方法,其特征在于,

通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略,包括:

通过区块链上的策略执行智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息发送属性获取指令至属性管理智能合约;

通过区块链上的属性管理智能合约根据属性获取指令获取请求下载的资源数据对应的资源访问策略;

通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策,包括:

通过区块链上的策略决策智能合约从属性管理智能合约获取请求下载的资源数据对应的资源访问策略,根据获取的请求下载的资源数据对应的资源访问策略和所述资源数据下载请求中的资源请求者的当前访问信息进行访问控制决策,以及返回访问控制决策的结果;

通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求,包括:

通过区块链上的策略执行智能合约获取访问控制决策的结果,在访问控制决策的结果为允许访问的情况下,根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

4.如权利要求1至3任一项所述的基于区块链的数据共享方法,其特征在于,所述资源存储系统为IPFS系统。

5.如权利要求1至3任一项所述的基于区块链的数据共享方法,其特征在于,资源访问策略包括访问主体属性、访问环境属性及访问资源属性;资源请求者的当前访问信息包括资源请求者的主体信息和访问资源信息。

6.如权利要求3所述的基于区块链的数据共享方法,其特征在于,策略管理智能合约、属性管理智能合约、策略执行智能合约及策略决策智能合约符合XACML规范。

7.如权利要求1所述的基于区块链的数据共享方法,其特征在于,

存储加密所述资源数据的密钥,包括:

对加密所述资源数据的密钥进行加密,形成加密密钥,并对所述加密密钥进行中心化存储;并建立加密密钥与所述资源数据的信息的对应关系;

通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息,包括:

通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息,并建立所述资源访问策略的合约调用信息与所述资源数据的信息的对应关系;

通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，包括：

通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，并建立返回的资源存储地址的存储信息与所述资源数据的信息的对应关系。

8.一种基于区块链的数据共享系统，其特征在于，包括：

资源拥有者客户端，用于在资源拥有者端上传资源数据；

资源请求者客户端，用于在资源请求者端请求资源数据；

其中：

资源拥有者客户端，包括：

资源上传请求获取模块，用于在资源拥有者端接收资源上传请求，其中，所述资源上传请求包括资源数据和资源访问策略；

资源加密模块，用于使用对称加密算法对所述资源数据进行加密；存储加密所述资源数据的密钥；

策略创建模块，用于通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息；

资源上传模块，用于通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址；

资源请求者客户端，包括：

下载请求获取模块，用于在资源请求者端提交资源数据下载请求，其中，所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息；

策略获取模块，用于通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略；

访问决策模块，用于通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策；

资源下载请求模块，用于通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求；

资源读取模块，用于接收从所述资源存储系统读取的加密的资源数据；

资源解密模块，用于对加密的资源数据进行解密；

策略创建模块，包括：

策略创建指令发送模块，用于通过区块链上的策略管理智能合约根据所述资源上传请求中的资源访问策略发送属性添加指令至属性管理智能合约；

策略属性发布模块，用于通过区块链上的属性管理智能合约根据所述属性添加指令将所述资源访问策略发布至所述区块链，并返回的所述资源访问策略的合约调用信息；

调用信息返回模块，用于通过策略管理智能合约获取返回的所述资源访问策略的合约调用信息；

资源上传模块，具体用于通过所述区块链上的策略管理智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

9.一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7任一项所述方法的步骤。

基于区块链的数据共享方法及系统

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于区块链的数据共享方法及系统。

背景技术

[0002] 如今社会信息汇聚，使得大量的资源、资源加工的产物同时深入生产生活，为社会带来巨大变革。例如，医疗大数据、金融大数据、能源大数据等，各行各业都在利用大数据创造巨大的社会和经济价值。然而，大数据带来发展机遇的同时，也带来了数据安全等问题，例如，数据管理的安全边界、资源窃取等安全事故频发。另外，因为数据安全、隐私问题、商业因素等形成“资源壁垒”，这样的“数据孤岛”问题使得数据的价值难以被挖掘，各类数据交叉引用所带来的经济效益没有发挥到其所包含的全部潜能。大数据的可信共享和访问权限控制方法是大数据发展过程中亟需解决的关键科学问题。

[0003] 目前使用访问控制系统对用户进行授权及权限管理，禁止非授权访问的操作仍是保障数据安全的主要方式。这虽然在一定程度上解决了大数据可控共享的需求，但是在数据量不断增加的背景下，访问模型的可拓展性、访问策略制定不透明和管理难度增加等问题都在对现有的访问控制方式和数据共享模型进行挑战。

[0004] 为了保证数据安全性，传统的数据共享大多采用线下传输的办法，这种方式的实时性不强，而且人员疏忽造成的数据丢失、出错等后果难以追踪等问题十分明显。随着互联网的普及，线上的数据共享成为数据传输的主要方式，比线下传输的方式在时效性上有很明显的优势。但是近年来互联网数据大爆发，给数据监管、隐私保护、大容量数据存储、数据快传等安全、高效的数据共享手段提出了更高的要求。在技术层面，大数据时代的数据存储在适应高效数据共享需求，面临如下几个问题。

[0005] 首先是存储问题，海量的数据存储不仅需要强大的数据规模，还需要一定的扩展能力以及可以应对庞大的文件数量。传统中心化存储的“中心化”决定了其存储的集中特点，也出现成本高的问题。为了降低成本，中心化存储中心一般选在偏远地区，数据传输速度一定程度上会受到影响。同样的集中化存储也会存在一定的安全隐患，一旦发生停电等故障，可能会导致大量相关业务瘫痪。分布式存储相对于集中存储，物理空间及副本配置使得分布式存储具有更高的可靠性，同时设备价格及维护成本较低，数据失效问题也得以解决。

[0006] 其次是数据传输的安全问题，涉及跨网的数据传输容易出现行为审批流程不规范导致的数据违规访问等问题。解决数据访问权限管理问题，传统的访问控制系统是由访问策略机制制定和策略管理人员进行中心化控制，闭塞的共享策略、僵化的策略执行模式以及单点故障所带来的系统停滞问题在分布式的环境下难以满足大数据安全共享需求。

[0007] 在数据共享的整个过程中，数据来源去向难以追踪是资源请求者以及拥有者对于资源安全性最重要的考量。做到对数据分享、上传、请求、下载等行为可控，且对所有资源的操作进行记录也是数据共享的重要一环。传统的中心化系统一般通过中心操作节点借助数据库或访问日志完成操作记录，可能会发生系统内部人员进行违规修改操作记录导致记录

与实际情况不匹配的现象。同时，中心化系统也可能会出现单点故障问题造成记录结果不完全。

[0008] 另外，区块链是由密码学、网络、分布式存储等技术结合的一种技术，其本身的去中心化、链上信息不可篡改等特点可以原生地解决传统中心化访问的问题，同时在区块链与数据共享技术相结合也可以为数据共享提供底层数据构建能力。但是，目前基于区块链的数据共享尚得不到访问控制。

发明内容

[0009] 有鉴于此，本发明提供了一种基于区块链的数据共享方法及系统，以实现基于区块链的可信数据安全共享和受控访问。

[0010] 为了达到上述目的，本发明采用以下方案实现：

根据本发明实施例的一个方面，提供了一种基于区块链的数据共享方法，包括：在资源拥有者端上传资源数据；在资源请求者端请求资源数据。其中：在资源拥有者端上传资源数据，包括：在资源拥有者端接收资源上传请求，其中，所述资源上传请求包括资源数据和资源访问策略；使用对称加密算法对所述资源数据进行加密；存储加密所述资源数据的密钥；通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息；通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。在资源请求者端请求资源数据，包括：在资源请求者端提交资源数据下载请求，其中，所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息；通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略；通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策；通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求；接收从所述资源存储系统读取的加密的资源数据；对加密的资源数据进行解密。

[0011] 在一些实施例中，在资源拥有者端上传资源数据，还包括：使用密文-策略加密算法根据所述资源访问策略对加密所述资源数据所用的密钥进行加密。在资源请求者端请求资源数据，还包括：对加密的资源数据的加密密钥进行解密，得到加密的资源数据的明文密钥。对加密的资源数据进行解密，包括：利用加密的资源数据的明文密钥对加密的资源数据进行解密。

[0012] 在一些实施例中，通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息，包括：通过区块链上的策略管理智能合约根据所述资源上传请求中的资源访问策略发送属性添加指令至属性管理智能合约；通过区块链上的属性管理智能合约根据所述属性添加指令将所述资源访问策略发布至所述区块链，并返回的所述资源访问策略的合约调用信息；通过策略管理智能合约获取返回的所述资源访问策略的合约调用信息。通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，包括：通过所述区块链上的策略管理智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

[0013] 在一些实施例中，通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略，包括：通过区块链上的策略执行智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息发送属性获取指令至属性管理智能合约；通过区块链上的属性管理智能合约根据属性获取指令获取请求下载的资源数据对应的资源访问策略。通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策，包括：通过区块链上的策略决策智能合约从属性管理智能合约获取请求下载的资源数据对应的资源访问策略，根据获取的请求下载的资源数据对应的资源访问策略和所述资源数据下载请求中的资源请求者的当前访问信息进行访问控制决策，以及返回访问控制决策的结果。通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求，包括：通过区块链上的策略执行智能合约获取访问控制决策的结果，在访问控制决策的结果为允许访问的情况下，根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

[0014] 在一些实施例中，所述资源存储系统为IPFS系统。

[0015] 在一些实施例中，资源访问策略包括访问主体属性、访问环境属性及访问资源属性；资源请求者的当前访问信息包括资源请求者的主体信息和访问资源信息。

[0016] 在一些实施例中，策略管理智能合约、属性管理智能合约、策略执行智能合约及策略决策智能合约符合XACML规范。

[0017] 在一些实施例中，存储加密所述资源数据的密钥，包括：将加密所述资源数据的加密密钥进行中心化存储，并建立加密密钥与所述资源数据的信息的对应关系。通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息，包括：通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息，并建立所述资源访问策略的合约调用信息与所述资源数据的信息的对应关系。通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，包括：通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，并建立返回的资源存储地址的存储信息与所述资源数据的信息的对应关系。

[0018] 根据本发明实施例的一个方面，提供了一种基于区块链的数据共享系统，包括：

资源拥有者客户端，用于在资源拥有者端上传资源数据；

资源请求者客户端，用于在资源请求者端请求资源数据；

其中：

资源拥有者客户端，包括：

资源上传请求获取模块，用于在资源拥有者端接收资源上传请求，其中，所述资源上传请求包括资源数据和资源访问策略；

资源加密模块，用于使用对称加密算法对所述资源数据进行加密；存储加密所述资源数据的密钥；

策略创建模块，用于通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息；

资源上传模块，用于通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址；

资源请求者客户端，包括：

下载请求获取模块，用于在资源请求者端提交资源数据下载请求，其中，所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息；

策略获取模块，用于通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略；

访问决策模块，用于通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策；

资源下载请求模块，用于通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求；

资源读取模块，用于接收从所述资源存储系统读取的加密的资源数据；

资源解密模块，用于对加密的资源数据进行解密。

[0019] 根据本发明实施例的一个方面，提供了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任一实施例所述方法的步骤。

[0020] 本发明实施例的基于区块链的数据共享方法、基于区块链的数据共享系统及计算机可读存储介质，实现了区块链和访问控制的结合，从而不仅能够基于区块链技术实现数据的可信安全共享，而且能够同时实现数据的受控访问。

附图说明

[0021] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。在附图中：

图1是本发明一实施例的基于区块链的数据共享方法的流程示意图；

图2是本发明一实施例的基于区块链的数据共享系统的结构示意图；

图3是本发明一实施例的基于区块链的数据共享架构示意图；

图4是本发明一具体实施例中资源拥有者上传资源的流程示意图；

图5是本发明一具体实施例中资源请求者下载资源的流程示意图；

图6是本发明一具体实施例中区块链上合约间调用关系示意图。

具体实施方式

[0022] 为使本发明实施例的目的、技术方案和优点更加清楚明白，下面结合附图对本发明实施例做进一步详细说明。在此，本发明的示意性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。

[0023] 需要预先说明的是，下述实施例或示例的描述或其中所提及的特征可以以相同或类似的方式，与其他实施例或示例中的特征组合，或替换其他实施例或示例中的特征，以形成可能的实施方式。另外，本文所使用的术语“包括/包含”是指特征、要素、步骤或组件的存

在,但并不排除还存在一个或多个其他特征、要素、步骤或组件。

[0024] 针对现有的线下数据共享实时性不强等问题、传统线上数据共享的存储及安全问题,本发明实施例提出了一种基于区块链的数据共享方法,能够不仅基于区块链技术实现数据的可信安全共享,而且同时实现数据的受控访问。

[0025] 图1是本发明一实施例的基于区块链的数据共享方法的流程示意图,如图1所示,该些实施例的基于区块链的数据共享方法,可包括:

步骤S100:在资源拥有者端上传资源数据;

步骤S200:在资源请求者端请求资源数据。

[0026] 其中,上述步骤S100可以在资源拥有者客户端的设备上执行,同时可涉及与区块链的交易,以及与资源存储系统的数据交互。上述步骤S200可以在资源申请者客户端的设备上执行,同时可涉及与区块链的交易,以及与资源存储系统的数据交互。

[0027] 再参见图1,上述步骤S100,即,在资源拥有者端上传资源数据,具体可包括以下步骤S110~步骤S140。

[0028] 下面将对步骤S110至步骤S140的具体实施方式进行详细说明。

[0029] 步骤S110:在资源拥有者端接收资源上传请求,其中,所述资源上传请求包括资源数据和资源访问策略。

[0030] 上述步骤S110中,作为资源拥有者的主体用户可以输入资源上传请求至其客户端。资源访问策略可包括访问主体属性、访问环境属性及访问资源属性。其中,访问资源属性可称为客体属性。资源访问策略还可包括这些属性间的关系。例如,访问主体属性可以为访问主体的身份或角色(如允许管理员访问),访问环境属性可以为访问特定时间,访问资源属性可以为特定范围的文件。

[0031] 步骤S120:使用对称加密算法对所述资源数据进行加密;存储加密所述资源数据的密钥。

[0032] 该步骤S120中,加密所述资源数据的密钥可以随机生成。加密所述资源数据的密钥可以存储到区块链上,如通过属性管理合约发布到区块链上,或者,可以存到区块链外部任意存储空间,如资源拥有者和各资源请求者均可访问的中心化存储位置,例如,可使密钥更安全。

[0033] 示例性地,该步骤S120中,存储加密所述资源数据的密钥,具体可包括步骤:将加密所述资源数据的加密密钥进行中心化存储,并建立加密密钥与所述资源数据的信息的对应关系。其中,该资源数据的信息可以为资源数据的名称。该对应关系可以存在智能合约中,或存储在智能合约能够访问的位置。

[0034] 步骤S130:通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息。

[0035] 该步骤S130中,可以以智能合约形式将资源访问策略发布至区块链。该合约调用信息可包括通过智能合约获取资源访问策略的相关信息,如资源访问策略的存储位置相关信息。

[0036] 该步骤S130,具体可包括步骤:通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息,并建立所述资源访问策略的合约调用信息与所述资源数据的信息的对应关系。该对应关系可以存在智能合约中,

或存储在智能合约能够访问的位置。

[0037] 步骤S140:通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

[0038] 上述步骤S140中,可以通过执行智能合约,实现将资源数据存储至资源存储系统中,且该资源存储系统可以返回存储地址。所述资源存储系统可以为分布式存储系统,例如,可以为IPFS系统(The InterPlanetary File System,星际文件系统)。IPFS存储具有内容寻址、分布式存储、数据安全、减少数据冗余等优点,而且还可以很好地与区块链相结合。另外,获取返回的资源存储地址后,可以进一步将资源存储地址返回给资源拥有者用户,或可以对应存储起来。

[0039] 该步骤S140,具体可包括步骤:通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址,并建立返回的资源存储地址的存储信息与所述资源数据的信息的对应关系。该对应关系可以存在智能合约中,或存储在智能合约能够访问的位置。

[0040] 另外,再参见图1,上述步骤S200,即,在资源请求者端请求资源数据,具体可包括以下步骤S210~步骤S260。

[0041] 下面将对步骤S210至步骤S260的具体实施方式进行详细说明。

[0042] 步骤S210:在资源请求者端提交资源数据下载请求,其中,所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息。

[0043] 上述步骤S210中,与资源访问策略相对应,资源请求者的当前访问信息可包括资源请求者的主体信息(主体属性)和访问资源信息(客体属性)。例如,访问主体属性信息可以为访问主体的身份或角色(如允许管理员访问),访问资源属性信息可以为特定范围的文件。另外,若需访问环境属性,可以从资源请求者端(如资源请求者客户端)直接获得。

[0044] 步骤S220:通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略。

[0045] 该步骤S220,可以通过智能合约中找到存储资源数据的信息对应的合约调用信息。根据合约调用信息执行智能合约可以找到相应的资源访问策略,其中,资源访问策略可以存在各种可能位置,只要能使智能合约能够调取到即可。

[0046] 步骤S230:通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策。

[0047] 该步骤S230中,资源访问策略可以包含各种所需访问条件,如资源请求者信息、资源数据信息、环境信息等,资源请求者的当前访问信息可以包含资源请求者相关的各种信息,如资源请求者信息,所需的资源数据信息等,主要可以通过比对资源访问策略和资源请求者的当前访问信息中的相应信息进行访问控制决策。若资源访问策略包含资源请求者的当前访问信息之外的信息,可以从资源请求者的当前访问信息之外获取所需信息,如环境信息,一并进行比对。

[0048] 步骤S240:通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

[0049] 步骤S250:接收从所述资源存储系统读取的加密的资源数据。

[0050] 步骤S260:对加密的资源数据进行解密。

[0051] 上述步骤S240中,若允许访问,可以通过智能合约请求从资源存储系统读取所需资源数据。另外,若访问控制决策的结果为拒绝,可以直接驳回请求,具体可以返回驳回的信息至用户。上述步骤S250中,资源存储系统返回的资源数据可以直接返回至资源请求者客户端,此时得到的资源数据是加密的数据。上述步骤S260中,可以根据资源数据的信息(如名称、摘要信息)找到密钥的存储位置,得到密钥,并可利用得到的密钥解密资源数据。得到明文的资源数据可以进一步返回给该资源请求者用户。

[0052] 上述实施例中,上传资源数据时,通过上述步骤S130和步骤S140,以区块链作为连接,通过智能合约执行发布资源访问策略和上传资源数据到资源存储系统,下载资源数据时,通过上述步骤S220~步骤S240,以区块链作为连接,通过智能合约执行获取资源访问策略、访问控制决策及请求从资源存储系统下载资源数据。如此一来,由于智能合约具有不可篡改、公开等特点,所以能够实现安全、实时的数据共享。另外,通过智能合约执行发布资源访问策略,能够实现区块链和访问控制的结合,以此能够实现策略透明、执行公证、过程记录等访问控制效果。在现有技术中,缺乏对于区块链和资源管理、分布式访问控制、操作管理、认证管理适配的模式,而本实施例成功实现了一种基于区块链的可信数据安全共享和受控访问方法。

[0053] 进一步的实施例中,可以对密钥进行加密。例如,图1所示的方法,还可包括步骤:S150,使用密文-策略加密算法对加密所述资源数据所用的密钥进行加密。其中,该密文-策略加密算法可以是现有的可以用来对密钥进行加密的算法。

[0054] 更进一步的实施例中,可以基于访问策略中的信息对密钥进行加密,以此可使密钥的加密结果包含资源拥有者要求的信息。

[0055] 示例性地,图1所示的方法中,步骤S100,即,在资源拥有者端上传资源数据,还可包括步骤:S151,使用密文-策略加密算法根据所述资源访问策略对加密所述资源数据所用的密钥进行加密。或者,可以说是,上述步骤S150具体可以包括该步骤S151。其中,资源访问策略中可以包含客体信息、主体信息、环境信息等,这些信息都可以由资源拥有者在上传资源数据时设置,所以,通过根据这些属性信息加密所述资源数据所用的密钥,可以使密钥考虑了资源拥有的要求。

[0056] 另外,在对密钥加密的情况下,步骤S200,即,在资源请求者端请求资源数据,还可包括步骤:S270,对加密的资源数据的加密密钥进行解密,得到加密的资源数据的明文密钥。在此情况下,上述步骤S260,即,对加密的资源数据进行解密,具体可包括步骤:S261,利用加密的资源数据的明文密钥对加密的资源数据进行解密。

[0057] 为了降低调用智能合约所需的计算资源,上述步骤S100和步骤S200的具体实施方式中所涉及的智能合约可以分成多个智能合约。例如,可以使得每个智能合约执行一个功能,如此一来,可以使得智能合约的执行变得轻量化,避免每执行一次操作就要调用包含很多功能的重量级的智能合约,从而避免花费不必要的计算资源。

[0058] 示例性地,上述步骤S100中涉及的智能合约可以通过资源管理智能合约(或称为资源管理合约、PAC)和属性管理智能合约(或称为属性管理合约、AMC)来实现。

[0059] 在此情况下,上述步骤S130,即,通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息,具体可包括以下步骤:

S131,通过区块链上的策略管理智能合约根据所述资源上传请求中的资源访问策略发送属性添加指令至属性管理智能合约;S132,通过区块链上的属性管理智能合约根据所述属性添加指令将所述资源访问策略发布至所述区块链,并返回的所述资源访问策略的合约调用信息;S133,通过策略管理智能合约获取返回的所述资源访问策略的合约调用信息。其中,属性添加指令中可以包含资源访问策略中各种属性信息。合约调用信息可以返回至策略管理智能合约,策略管理智能合约接收到合约调用信息后,可以准备上传资源数据至资源存储系统。

[0060] 本实施例中,在上传资源过程中,可以通过资源管理智能合约收发创建策略、属性添加、上传资源等指令,可以通过属性管理智能合约进行访问策略、属性等的收集、管理。

[0061] 上述步骤S140,即,通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址,具体可包括步骤:S141,通过所述区块链上的策略管理智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

[0062] 再示例性地,上述步骤S200中涉及的智能合约可以通过资源执行智能合约(或称为资源执行合约、PEC)、属性管理智能合约(或称为属性管理合约、AMC)及策略决策智能合约(或称为策略决策合约、PDC)来实现。

[0063] 在此情况下,上述步骤S220,即,通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略,具体可包括步骤:S221,通过区块链上的策略执行智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息发送属性获取指令至属性管理智能合约;S222,通过区块链上的属性管理智能合约根据属性获取指令获取请求下载的资源数据对应的资源访问策略。

[0064] 上述步骤S230,即,通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策,具体可包括步骤:S231,通过区块链上的策略决策智能合约从属性管理智能合约获取请求下载的资源数据对应的资源访问策略,根据获取的请求下载的资源数据对应的资源访问策略和所述资源数据下载请求中的资源请求者的当前访问信息进行访问控制决策,以及返回访问控制决策的结果。

[0065] 上述步骤S240,即,通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求,具体可包括步骤:S241,通过区块链上的策略执行智能合约获取访问控制决策的结果,在访问控制决策的结果为允许访问的情况下,根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

[0066] 本实施例中,在下载资源过程中,可以通过策略执行智能合约收发下载请求指令、下载资源数据指令等,可以通过属性管理智能合约收集当前属性信息,可以通过策略执行智能合约进行决策判断。

[0067] 进一步地,策略管理智能合约、属性管理智能合约、策略执行智能合约及策略决策智能合约可以是符合XACML(可扩展访问控制标记语言)规范的。在此情况下,策略管理智能合约、属性管理智能合约、策略执行智能合约及策略决策智能合约可以依次对应XACML规范中的策略管理点PAP、属性管理器AMs、策略执行点PEP及策略决策点PDP。当然,本发明各实施例的智能合约还可以包含其他合约,实现其他功能,可以对应XACML规范中的其他组件。

[0068] 在一具体实施例中，基于区块链的数据共享方法主要在两方面进行了创新：(1)提供了基于区块链的数据安全共享架构；(2)提供了基于区块链可审计的访问控制方法。

[0069] 在本实例的第一方面，提供了基于区块链的数据安全共享架构。

[0070] 以区块链作为整体架构的连接，底层可以采用IPFS分布式存储，IPFS存储具有内容寻址、分布式存储、数据安全、减少数据冗余等优点，不仅价格低，还可以便于和区块链相结合；智能合约作为区块链内部调度和其他设备的“路由”，智能合约具有不可篡改、公开、执行成本低等特点，能够保证其为区块链框架提供计算能力；上层访问控制可以采用区块链和访问控制模型ABAC结合并优化的BBAAC模型，通过选用ABAC模型作为基础，能够提升访问控制的力度，采取区块链和访问控制结合的方式能够实现策略透明、执行公证、过程记录等效果。

[0071] 根据数据共享异步性特点，通过整合区块链与其上下游服务实现数据的安全共享。数据共享主要流程包括：资源拥有者注册资源及资源访问策略；资源请求者发现资源；资源请求者申请获取资源；资源请求者获得申请结果，成功则可获取。流程涉及资源存储、访问控制、访问审计问题(其中，访问控制部分在本实施例提供的第二方面进行说明)。将资源存储、访问控制和访问审计模块与区块链技术进行适配，实现存储、访问控制和审计，去中心化，过程透明的效果。

[0072] 基于区块链的数据安全共享架构的实施流程可包括以下步骤：

S1. 注册资源：资源拥有者通过本实施例的系统注册资源，并注册访问资源策略。可资源摘要信息保存至系统的数据库(存储部分)，资源数据可经对称密钥加密后保存至IPFS(The InterPlanetary File System，星际文件系统)。返回资源数据的存储地址、基于属性加密密钥及访问策略，生成智能合约发布至区块链。

[0073] S2. 发现资源：用户访问步骤S1中保存在本实施例的系统发数据库的资源摘要信息列表，可发现需要的资源，并可进行资源访问申请。

[0074] S3. 申请访问：用户发起申请对应资源，区块链可通过策略执行合约对资源数据的访问操作进行拦截，并可以通过策略决策合约判决是否允许访问，并可以返回相应判决结果。如果判决结果为“允许”，则系统可自动进行至下一步骤；否则可“禁止”，对资源请求者驳回并终止请求。

[0075] S4. 获取资源：智能合约可根据保存的IPFS地址进行资源获取，并可通过智能合约对资源密钥获取(加密密钥可中心化存储，所以可以不通过合约进行获取)并进行解密，获得资源明文信息。

[0076] 在本实例的第二方面，提供了基于区块链可审计的访问控制方法(可称为BBAAC，即，Blockchain Based Auditable Access Control)。

[0077] 本实施例的BBAAC的基本思想可以是利用区块链来存储访问控制策略和管理属性，以及执行访问决策过程，即，每次由资源请求者发出访问控制请求时，就利用所需属性评估相关策略。通过区块链来存储访问控制策略和执行访问控制策略。由于区块链是仅可追加的分布式账本，智能合约一旦上传将永远存储在区块链上。但是可以通过在逻辑上简单地上传一个新的逻辑(区块)进行替换或通过交易实现禁用。通过智能合约来表示访问控制策略。智能合约由资源所有者创建，并以交易的形式存储在区块链上，且访问决策过程的执行也可利用区块链执行。实际上，每次资源请求者发出访问请求时，都会在区块链上向其

发出交易以触发智能合约的执行。该消息导致对请求的评估以及相关访问结果的产生(许可或拒绝)。

[0078] 可以基于XACML标准定义ABAC策略、请求和响应。请求用于以与策略相同的格式表示主体必须提供的代表访问上下文的属性值。XACML不仅提供表达策略和请求或响应的标准,而且还提供评估体系结构的标准。XACML架构主要包括以下组件:策略执行点(Policy Enforcement Point,PEP)、策略管理点(Policy Administration Point,PAP)、属性管理器(Attribute Managers,AMs)、策略评估点(Policy Information Points,PIPs)、策略决策点(Policy Decision Point,PDP)。本实施例基于XACML 标准提出基于区块链的访问控制系统主要以智能合约和线下控制结合的方式实现XACML标准的组建,并将本实施例的访问控制部分可分为两个主要模块:策略管理和策略执行。其中,策略管理主要可包括用户、资源、环境的属性管理,还可包括访问策略的管理。策略执行主要可包括策略执行的触发,还可以指示策略的决策。另外,本实施例所涉及的智能合约(或称为策略合约PC)可包括策略管理合约(Policy Administration Contract,PAC)、属性管理合约(Attribute Managers Contract,AMC)、策略执行合约(Policy Enforcement Contract,PEC)、策略决策合约(PolicyDecisionContract,PDC)等。

[0079] 本实施例主要步骤包含在上述第一方面步骤S1~S4中,以下描述为第二方面对第一方面的步骤补充。

[0080] 在上述步骤S1中,资源拥有者首先可以以与区块链交易的形式更新属性管理合约AMC,对资源属性进行预先收集。可通过策略管理合约PAC发布访问PC(Policy Contract,策略合约),智能合约中可包括属性间关系、资源访问控制描述及资源加密密钥信息(不同具体智能合约根据其功能不同可包含不同信息)。

[0081] 在上述步骤S2中,无第二方面的补充部分。

[0082] 在上述步骤S3中,用户访问资源时,可以通过策略执行合约PEC(内嵌在策略合约PC中)拦截并挂起用户的资源请求,可以通过收集属性的属性管理合约AMC触发策略决策合约PDC。可通过策略决策合约PDC计算并返回控制判决结果。

[0083] 在上述步骤S4中,策略合约PC执行IPFS访问,返回加密的资源数据,并对加密的资源数据进行解密操作。

[0084] 访问控制设计模式可以采用ACL(Access Control List,访问控制列表)和RBAC(Role-Based Access Control,基于角色的访问控制)模式。ACL模式是通过记录用户及相应资源的访问权限到列表文件中。ACL模式的缺点在于当用户、资源、操作增长,维护表代价非常大,扩展能力较差,同时,ACL模式将具体用户和具体资源通过权限建立联系,灵活度较差。RBAC采取了个体和权限分离的方法,根据用户属性特点进行用户角色抽象,再为角色分配资源权限。RBAC解决了一部分灵活性的问题,但是其维护成本和权限控制的粒度控制表现依然没有很好的表现。

[0085] 而本实施例的BBAAC通过XACML规范化的、基于属性的访问控制模式实现了标准化、细粒度的访问控制,结合区块链实现了策略可审计(交易)、规则透明、过程去中心化的访问控制策略。

[0086] 基于与图1所示的基于区块链的数据共享方法相同的发明构思,本发明实施例还提供了一种基于区块链的数据共享装置,如下面实施例所述。由于该基于区块链的数据共

享装置解决问题的原理与基于区块链的数据共享方法相似，因此该基于区块链的数据共享装置的实施可以参见基于区块链的数据共享方法的实施，重复之处不再赘述。

[0087] 图2是本发明一实施例的基于区块链的数据共享系统的结构示意图，如图2所示，该些实施例的基于区块链的数据共享系统，可包括：资源拥有者客户端300和资源请求者客户端400。

[0088] 资源拥有者客户端300用于在资源拥有者端上传资源数据。

[0089] 资源请求者客户端400用于在资源请求者端请求资源数据。

[0090] 其中，资源拥有者客户端300，包括：资源上传请求获取模块310、资源加密模块320、策略创建模块330及资源上传模块340。

[0091] 资源上传请求获取模块310用于在资源拥有者端接收资源上传请求，其中，所述资源上传请求包括资源数据和资源访问策略。

[0092] 资源加密模块320用于使用对称加密算法对所述资源数据进行加密；存储加密所述资源数据的密钥。

[0093] 策略创建模块330用于通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息。

[0094] 资源上传模块340用于通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

[0095] 资源请求者客户端400包括：下载请求获取模块410、策略获取模块420、访问决策模块430、资源下载请求模块440、资源读取模块450及资源解密模块460。

[0096] 下载请求获取模块410用于在资源请求者端提交资源数据下载请求，其中，所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息。

[0097] 策略获取模块420用于通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略。

[0098] 访问决策模块430用于通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策。

[0099] 资源下载请求模块440用于通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

[0100] 资源读取模块450用于接收从所述资源存储系统读取的加密的资源数据。

[0101] 资源解密模块460用于对加密的资源数据进行解密。

[0102] 在一些实施例中，资源拥有者客户端300还可包括：密钥加密模块，用于使用密文-策略加密算法根据所述资源访问策略对加密所述资源数据所用的密钥进行加密。

[0103] 资源请求者客户端400还可包括：密钥解密模块，用于对加密的资源数据的加密密钥进行解密，得到加密的资源数据的明文密钥。资源解密模块460具体用于利用加密的资源数据的明文密钥对加密的资源数据进行解密。

[0104] 在一些实施例中，策略创建模块330，包括：

策略创建指令发送模块，用于通过区块链上的策略管理智能合约根据所述资源上传请求中的资源访问策略发送属性添加指令至属性管理智能合约；

策略属性发布模块，用于通过区块链上的属性管理智能合约根据所述属性添加指令将

所述资源访问策略发布至所述区块链，并返回的所述资源访问策略的合约调用信息；

调用信息返回模块，用于通过策略管理智能合约获取返回的所述资源访问策略的合约调用信息。

[0105] 在一些实施例中，资源上传模块340具体用于通过所述区块链上的策略管理智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址。

[0106] 在一些实施例中，策略获取模块420，包括：

属性获取指令发送模块，用于通过区块链上的策略执行智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息发送属性获取指令至属性管理智能合约；

资源访问策略获取模块，用于通过区块链上的属性管理智能合约根据属性获取指令获取请求下载的资源数据对应的资源访问策略。

[0107] 在一些实施例中，访问决策模块430，包括：策略决策模块，用于通过区块链上的策略决策智能合约从属性管理智能合约获取请求下载的资源数据对应的资源访问策略，根据获取的请求下载的资源数据对应的资源访问策略和所述资源数据下载请求中的资源请求者的当前访问信息进行访问控制决策，以及返回访问控制决策的结果。

[0108] 在一些实施例中，资源下载请求模块440，具体用于：通过区块链上的策略执行智能合约获取访问控制决策的结果，在访问控制决策的结果为允许访问的情况下，根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求。

[0109] 在一些实施例中，所述资源存储系统为IPFS系统。

[0110] 在一些实施例中，资源访问策略包括访问主体属性、访问环境属性及访问资源属性；资源请求者的当前访问信息包括资源请求者的主体信息和访问资源信息。

[0111] 在一些实施例中，策略管理智能合约、属性管理智能合约、策略执行智能合约及策略决策智能合约符合XACML规范。

[0112] 在一些实施例中，资源加密模块320具体还用于：将加密所述资源数据的加密密钥进行中心化存储，并建立加密密钥与所述资源数据的信息的对应关系。

[0113] 在一些实施例中，策略创建模块330具体还用于：通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息，并建立所述资源访问策略的合约调用信息与所述资源数据的信息的对应关系。

[0114] 在一些实施例中，资源上传模块340具体还用于：通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址，并建立返回的资源存储地址的存储信息与所述资源数据的信息的对应关系。

[0115] 另外，本发明实施例还提供了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任一实施例所述方法的步骤。

[0116] 为使本领域技术人员更好地了解本发明，下面将以具体实施例说明本发明的实施方式。

[0117] 为了解决大数据安全共享的问题，本实施例提出了区块链作为数据共享流程的基础设施，解决传统中心化数据的共享壁垒等传输问题，具体提供了完整的数据安全共享框架及安全高效的访问控制方法，该方法将区块链与访问控制相结合，并对访问控制方法进行相应的适配，以达到以下目的：可信公开策略、多元交互的分布式访问控制方法；记录数

据操作及访问，系统管理操作的记账服务；访问人员的可靠认证及管理功能。

[0118] 区块链是由密码学、网络、分布式存储等技术结合的一种技术，随着加密货币的盛行逐渐兴起的一种无中心化数据库。区块链本身的去中心化、链上信息不可篡改等特点可以原生地解决传统中心化访问控制的问题，同时在整个共享框架中也可以为其他功能提供有效的底层构建能力。但是在目前已有的相关方案中，缺乏对于区块链和资源管理、分布式访问控制、操作管理、认证管理适配的模式，所以亟需一种基于区块链的可信数据安全共享和受控访问方法。

[0119] 图3是本发明一实施例的基于区块链的数据共享架构示意图。参见图3，参与数据共享的主体用户包括：资源拥有者(DP)和数据请求者(DR)；实现数据共享安全的设备及验证环节可包括：DP客户端、DR客户端、IPFS存储、区块链及智能合约；另外，数据共享客体为数据资源。数据安全共享整体流程的两个重要环节为：资源拥有者上传资源以及资源请求者请求资源。

[0120] 图4是本发明一具体实施例中资源拥有者上传资源的流程示意图，图5是本发明一具体实施例中资源请求者下载资源的流程示意图。图6是本发明一具体实施例中区块链上合约间调用关系示意图。参见图4至图6，资源的流向为资源拥有者到资源请求者，可包括以下过程：

① 资源请求者通过DP-客户端发布资源，加密模块对文件进行加密处理；

② DP-客户端调用合约进行加密文件存储，上传文件加密密钥并使用密文-策略加密算法加密；同时区块链对此操作进行审计(即，交易)，并上传相关的访问策略合约；

③ 合约调用IPFS，将加密文件存储至IPFS节点中；

④ 资源请求者通过DR-客户端请求资源；

⑤ DR-客户端调用合约，获取加密文件和文件解密密钥；区块链对此操作进行审计(即，交易)，并验证资源请求者是否具备资源的访问权限；

⑥ 合约调用IPFS并获取加密文件；

⑦ 合约返回加密文件，并通过密文-策略模块对加密密钥解密，返回解密密钥；

⑧ DR-客户端利用解密密钥解密文件，并返回给解密后的文件给资源请求者。

[0121] 再参见图4，参与数据共享的主体用户中，资源拥有者(DP)实现数据上传所用设备或组件可包括：DP-客户端、智能合约(如策略管理合约、属性管理合约)、IPFS存储。具体的资源上传流程可包括以下过程：

① 资源拥有者通过DP-客户端发送文件上传请求；

② DP-客户端使用对称加密算法对文件进行加密，并使用密文-策略算法根据文件访问策略对密钥进行加密；

③ DP-客户端调用策略管理合约创建策略(上传访问策略)，并存储加密密钥(可存储至区块链或外存)；

④ 策略管理合约调用属性管理合约添加文件属性，并得到合约调用信息；

⑤ 策略管理合约调用IPFS上传加密文件，并将文件地址嵌入策略合约中；

⑥ 策略管理合约添加策略，并返回添加信息；

⑦ 客户端向用户返回资源上传结果。

[0122] 再参见图5，参与数据共享的主体用户中，资源请求者(DR)实现数据下载所用设备

或组件可包括:DR-客户端、智能合约(如策略执行合约、属性管理合约、策略决策合约)、IPFS存储。具体的资源下载流程可包括以下过程:

① 资源请求者通过DR-客户端发送文件下载请求;

② DP-客户端提交文件获取请求,策略执行合约拦截请求;

③ 策略执行合约调用属性管理合约,获取资源请求者属性、环境属性及资源对应访问策略;

④ 策略决策合约根据资源策略对资源请求者属性、环境属性进行决策,并根据决策结果进行返回;

⑤ 策略执行合约根据结果判决执行操作,如果判决结果为允许访问,则向IPFS提交资源请求;

⑥ IPFS返回加密资源,DR-客户端根据加密资源及相应密钥进行资源解密;

⑦ 客户端向用户返回解密资源。

[0123] 在资源拥有者上传资源的过程中,涉及数据加密的步骤,对应地,在资源请求者下载资源的过程中,涉及数据解密的步骤。上述实施例中,可以使用对称密钥对资源数据进行加密,并可采用将加密密钥写入合约的方式,并可将加密密钥存至区块链外部。密文-策略算法是基于属性(如访问策略中的属性)、运用密码机制进行加密保护数据,以此可由资源拥有者规定访问密文的属性策略,将属性集合与访问资源(对称密钥)相关联,资源接收方(资源请求者)可以根据自己的授权属性访问对称密钥。下面对密钥加密算法进行描述,具体加密方法可包括如下过程:

(1)加密初始化

可信密钥分发中心执行随机初始化算法,通过输入($Setup$)隐藏的安全参数产生公开的系统公钥Key_{pub}和系统主密钥Key_{main},可表示为:

$$Setup(\lambda)=\{Key_{pub},Key_{main}\};$$

(2)密钥生成

可信密钥分发中心执行随机化算法,根据系统公钥Key_{pub}、系统主密钥Key_{main}和资源请求者的请求属性集合$ATTR_u$,为资源请求者生成($Generate$)与属性集合相关联的用户密钥Key_u,可表示为:

$$Key_u=Generate(Key_{pub},Key_{main},ATTR_u);$$

(3)加密

资源拥有者执行加密算法,根据系统公钥Key_{pub}、待加密数据D和访问控制结构A_C,产生($Encrypt$)基于属性加密的密文文件CD,可表示为:

$$CD = Encrypt(Key_{pub}, D, A_C)$$；

(4)解密

数据请求者执行解密算法，解密算法为确定性算法；对于系统公钥Key_{pub}、用户密钥Key_u和密文*CD*，判断用户请求的属性集合$ATTR_{u'}$是否满足访问策略，如果满足，则解密（$Decrypt$）密文*CD*并获得对应的明文数据 *D*，可表示为：

$$D = Decrypt(Key_{pub}, Key_u, CD)$$。

[0124] 上述实施例中，属性涉及主体、客体及环境，智能合约包括策略管理合约、策略执行合约、策略决策合约、属性管理合约等。在此，对基于区块链的可信数据安全共享所用的合约具体说明。

[0125] 对于主体、客体、环境属性说明如下：

① *S*(Subject，主体)、*O*(Object，客体)和*E*(environment，环境)的属性分别表示为AS_k(attributeof subject，主体属性，$1 \le k \le K$)、AO_k(attributeofObject，客体属性，$1 \le k \le K$)、AE_k(attributeofenvironment，环境属性，1≤k≤K)，具体可表示为：

$$AS = \{AS_1 \times AS_2 \times \ldots \times AS_k, 1 \le k \le K\}$$

$$AO = \{AO_1 \times AO_2 \times \ldots \times AO_k, 1 \le k \le K\}$$

$$AE = \{AE_1 \times AE_2 \times \ldots \times AE_k, 1 \le k \le K\}$$

② 主体、客体、环境的属性关系集合分别表示为$ATTR_s$(attribute assignment relations for subject，主体属性集)，$ATTR_o$(attribute assignment relations for Object，客体属性集)，$ATTR_e$(attribute assignment relations for environment，环境属性集)，属性关系具体可表示为：

$$ATTR_s \subseteq AS_1 \times AS_2 \times \ldots \times AS_k$$

$$ATTR_o \subseteq AO_1 \times AO_2 \times \ldots \times AO_k$$

$$ATTR_e \subseteq AE_1 \times AE_2 \times \ldots \times AE_k$$。

对于合约说明如下：

(1)策略管理合约PAC

策略管理合约可以是负责管理访问控制策略的智能合约。PAC的主要功能可以是充当用于和存储策略的组件进行交互的合约,以便在资源拥有者对资源上传策略时进行策略存储。PAC的另一个相关功能可涉及策略编写,从而帮助资源拥有者(即决策者)创建和修改策略。PAC还可以支持与政策制定和管理有关的更复杂的功能。

[0126] PAC添加策略:

① 用户添加策略,输入策略规则。其中,规则可包含主体S、客体O及环境E的属性关系集(主体属性$ATTR_s$,客体属性$ATTR_o$,环境属性$ATTR_e$)及三个关系集间的关系($func$)。规则可表示如下:

$$Rule = func(ATTR_s, ATTR_o, ATTR_e)$$;

② 根据用户输入资源发布者属性(attribute of Provider,AP)及客体属性AS生成($Hash$)访问策略Id,保证系统内每个资源对应唯一的访问策略(可由资源发布者制定、更新、删除)。

[0127] $$Id = Hash(AS + AP)$$;

③ 产生资源(客体O)的访问策略Id及相应规则$Rule$,资源提供者签名($sign$)并发布访问策略$Policy_{Id}$。

[0128] $$Policy_{Id} = (Rule)_{sign}$$;

④ 策略将以合约的形式发布在区块链上,发布成功则生成该策略区块,否则返回错误信息。

[0129] PAC删除策略:

① 根据资源提供者和客体属性计算资源策略Id,并根据Id进行策略查找。如果查找失败,则返回错误信息;否则继续进行删除策略操作,可表示为:

$$Id = Hash(AS + AP)$$;

② 验证操作请求签名$Sign'$是否为要求的签名$Sign$,成功则调用($Invoke$)链上合约废除命令DEL,完成策略合约删除操作,可表示为:

$$Sign' = Sign \rightarrow Invoke(DEL)$$。

[0130] PAC更新策略:

① 策略更新操作首先进行策略删除操作,以保证系统内资源策略的唯一性,可表示为:

$$Id = Hash(AS + AP)$$

$$Sign' = Sign \rightarrow Invoke(DEL)$$

② 签名验证及删除操作完成后，资源提供者重新发布新策略 $Rule'$，可表示为：

$Policy_{Id} = (Rule')_{sign}$。

[0131] (2)策略执行合约PEC

策略执行合约是与要保护的资源配对的组件，该组件能够拦截和挂起访问请求以执行策略评估。PEP收集访问请求和一组可用属性，它触发决策过程，并通过实际允许或拒绝执行访问来强制执行相关结果。

[0132] 上述实施例中，将策略评估任务的代码嵌入到策略合约本身的代码中。将策略评估操作作为策略合约所有功能的第一个调用合约操作，以强制执行对访问控制策略的评估，进而执行与用户请求资源的策略合约其他部分。

[0133] (3)策略决策合约PDC

策略决策合约是一种评估合约，它将策略、访问请求和属性值作为输入，评估策略并返回相关的访问决策(允许或拒绝)。PDC的决策过程是通过执行合约的评估功能来执行的，属性值的检索则可通过合同的功能调用直接对同一链上的AMC(对应AMs)实现。所有通信都可以是通过区块链协议隐式管理的智能合约功能调用和事件触发来实现的。

[0134] (4)策略决策合约PDC

① 通过AMC(对应AMs)获取资源请求者属性集(AS_R)、资源属性集(AO_R)及当前环境属性集(AE_R)，请求 $Request$ 和收集属性 $getAttributes$ 可分别表示为：

$$Request = \{AS_R \wedge AO_R \wedge AE_R\}$$

$$getAttributes(Request) \rightarrow \{AS_R, AO_R, AE_R\}$$

② 根据访问策略对资源请求者、资源及环境进行属性判决 can_access（策略决策 $decidePolicy$），可表示为：

$$can\_access = decidePolicy(AS_R, AO_R, AE_R)$$

$$can\_access = \begin{cases} 1, & 允许 \\ 0, & 拒绝 \end{cases}$$

③ 根据访属性判决结果决定资源请求者是否有权限访问资源，

$$can\_access=\begin{cases}1 \rightarrow \text{读取数据}\\ 0 \rightarrow \text{报错}\end{cases}$$ 。

本实施例，提供了区块链与基于属性的访问控制结合的方法，并基于该方法设计了可信数据安全共享架构。区块链可信数据安全共享架构中，区块链作为整体架构的连接，底层采用IPFS分布式存储；智能合约作为区块链内部调度和其他设备的“路由”，为区块链框架提供了计算能力；上层访问控制采用区块链和访问控制模型ABAC结合并优化的方式，选用ABAC模型作为基础。因此，通过区块链与基于属性的访问控制结合，解决了传统访问控制中心化控制造成的信任问题，解决了中心化存储单点失效等问题，使策略发布、策略执行去中心化，过程安全透明。IPFS分布式存储和区块链结合，相对于其他分布式存储，IPFS的存储基于内容寻址、filecoin激励等同区块链有很好的结合，实现了存储减少冗余，价格降低。密钥加密模块为可信数据安全共享提供了有一层的安全保护，能够防止数据存储地址泄露导致文件泄露。基于区块链的数据安全共享方法，解决了传统中心化数据共享问题的共享壁垒，通过实现资源拥有者数据上传、策略变更，用户数据请求、数据传输过程可审计，极大程度地保护用户数据的安全，流程的可追踪。以ABAC模型作为基础，提升了访问控制力度。如此一来通过采取区块链和访问控制结合的方式实现了访问控制力度实现策略透明、执行公证、过程记录等效果。

[0135] 综上所述，本发明实施例的基于区块链的数据共享方法、基于区块链的数据共享系统及计算机可读存储介质，实现了区块链和访问控制的结合，从而不仅能够基于区块链技术实现数据的可信安全共享，而且能够同时实现数据的受控访问。

[0136] 在本说明书的描述中，参考术语“一个实施例”、“一个具体实施例”、“一些实施例”、“例如”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。各实施例中涉及的步骤顺序用于示意性说明本发明的实施，其中的步骤顺序不作限定，可根据需要作适当调整。

[0137] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0138] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0139] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特

定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0140] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0141] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

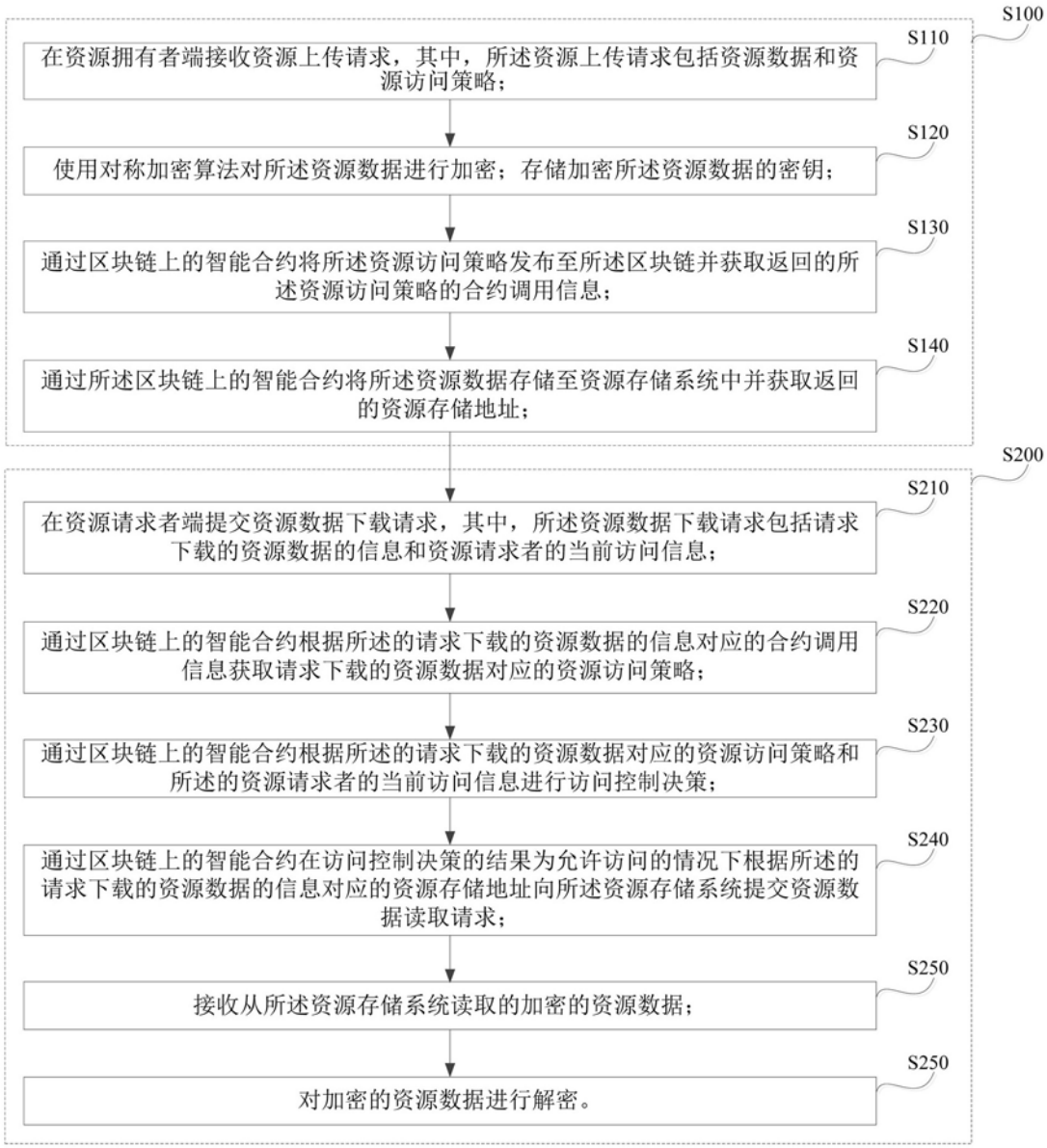
S100
S110
在资源拥有者端接收资源上传请求，其中，所述资源上传请求包括资源数据和资源访问策略；
S120
使用对称加密算法对所述资源数据进行加密；存储加密所述资源数据的密钥；
S130
通过区块链上的智能合约将所述资源访问策略发布至所述区块链并获取返回的所述资源访问策略的合约调用信息；
S140
通过所述区块链上的智能合约将所述资源数据存储至资源存储系统中并获取返回的资源存储地址；
S200
S210
在资源请求者端提交资源数据下载请求，其中，所述资源数据下载请求包括请求下载的资源数据的信息和资源请求者的当前访问信息；
S220
通过区块链上的智能合约根据所述的请求下载的资源数据的信息对应的合约调用信息获取请求下载的资源数据对应的资源访问策略；
S230
通过区块链上的智能合约根据所述的请求下载的资源数据对应的资源访问策略和所述的资源请求者的当前访问信息进行访问控制决策；
S240
通过区块链上的智能合约在访问控制决策的结果为允许访问的情况下根据所述的请求下载的资源数据的信息对应的资源存储地址向所述资源存储系统提交资源数据读取请求；
S250
接收从所述资源存储系统读取的加密的资源数据；
S250
对加密的资源数据进行解密。

图1

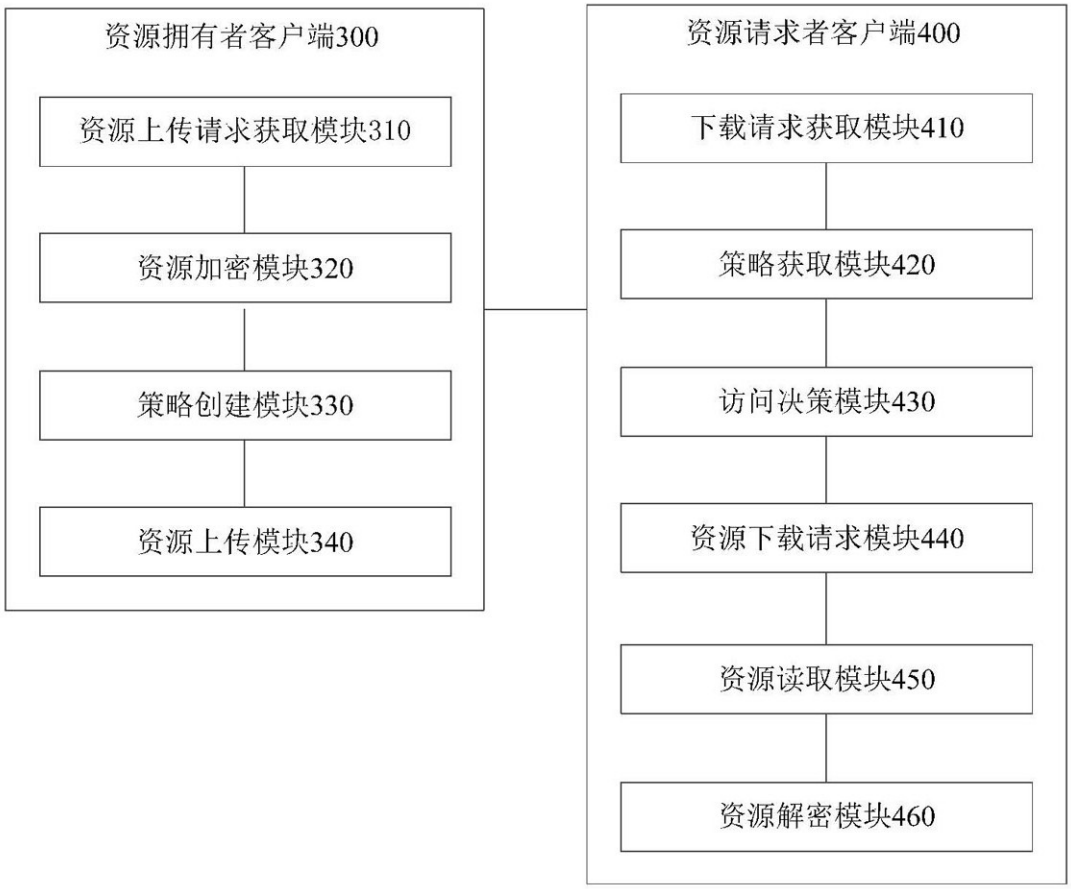
资源拥有者客户端300
资源上传请求获取模块310
资源加密模块320
策略创建模块330
资源上传模块340
资源请求者客户端400
下载请求获取模块410
策略获取模块420
访问决策模块430
资源下载请求模块440
资源读取模块450
资源解密模块460

图2

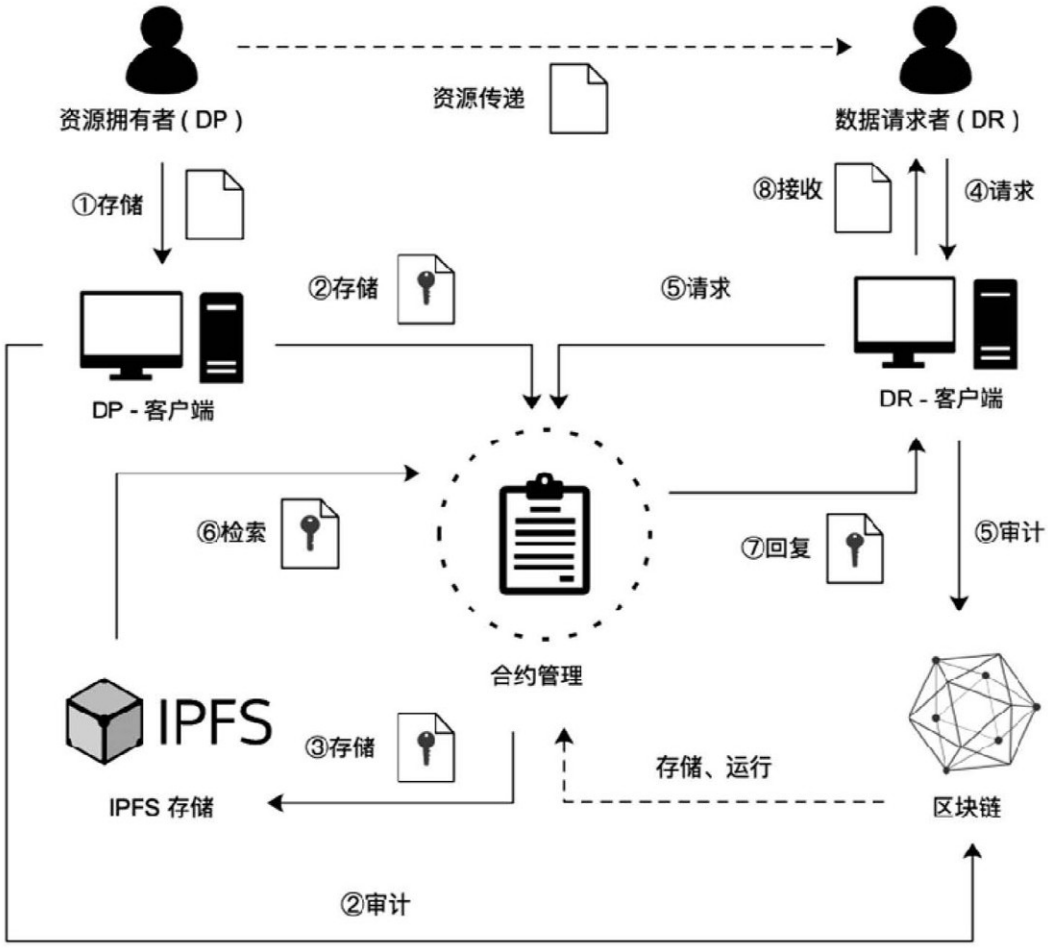
资源拥有者(DP)
资源传递
数据请求者(DR)
①存储
⑧接收
④请求
②存储
⑤请求
DP - 客户端
DR - 客户端
⑥检索
⑦回复
⑤审计
合约管理
IPFS
③存储
存储、运行
IPFS 存储
区块链
②审计

图3

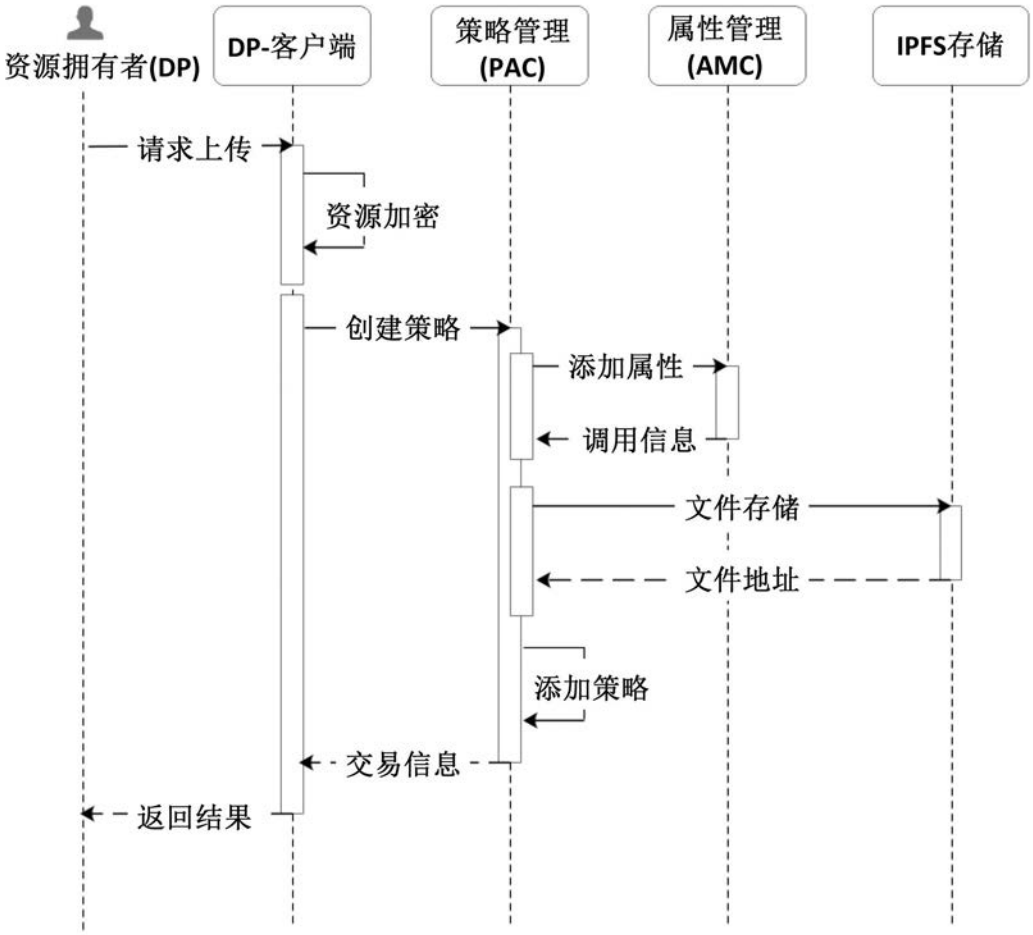
资源拥有者(DP)
DP-客户端
策略管理
(PAC)
属性管理
(AMC)
IPFS存储
请求上传
资源加密
创建策略
添加属性
调用信息
文件存储
文件地址
添加策略
交易信息
返回结果

图4

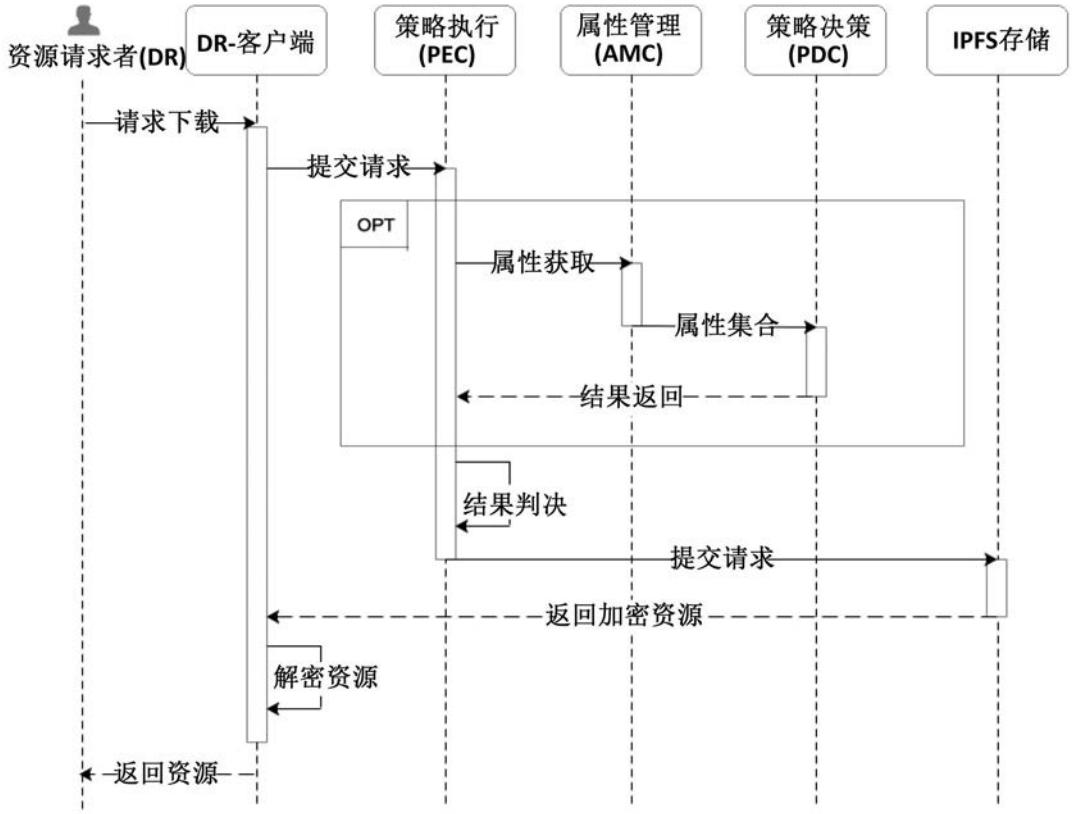
资源请求者(DR)
DR-客户端
策略执行 (PEC)
属性管理 (AMC)
策略决策 (PDC)
IPFS存储
请求下载
提交请求
OPT
属性获取
属性集合
结果返回
结果判决
提交请求
返回加密资源
解密资源
返回资源

图5

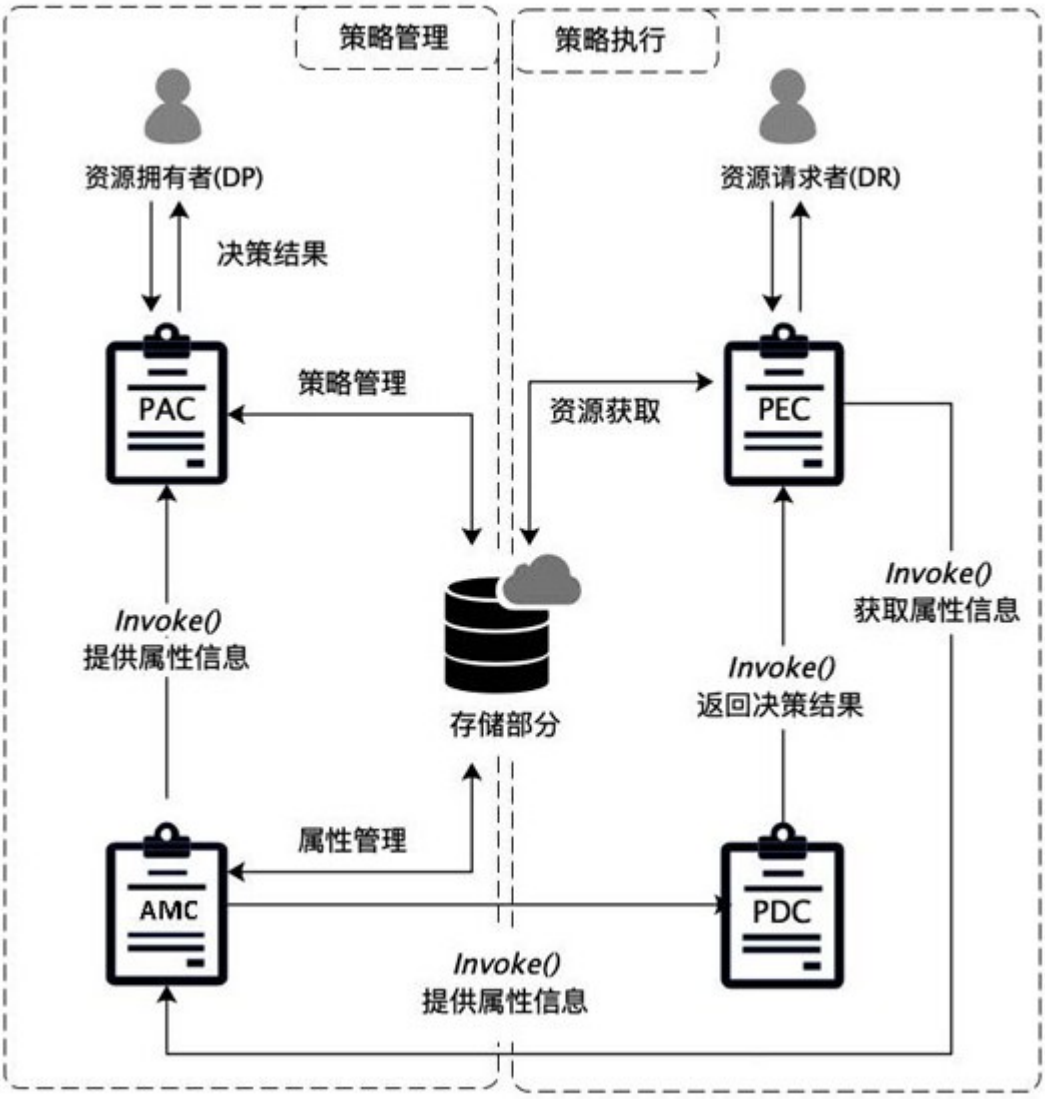
策略管理
策略执行
资源拥有者(DP)
资源请求者(DR)
决策结果
PAC
策略管理
资源获取
PEC
Invoke()
获取属性信息
Invoke()
提供属性信息
存储部分
Invoke()
返回决策结果
属性管理
AMC
PDC
Invoke()
提供属性信息

图6