

一种数据访问权限的控制方法和装置

本申请要求于 2018 年 3 月 19 日提交中国国家知识产权局、申请号为 201810224356.1, 发明名称为“一种数据访问权限的控制方法和装置”的中国专利申请的优先权, 其全部内容通过引用结合在本申请中。

技术领域

本申请涉及区块链领域, 尤其涉及一种数据访问权限的控制方法和装置。
背景技术

区块链(Block Chain)又称作分布式账本, 就是交易记账由分布在不同地方的多个节点共同完成, 并且每一个节点都记录完整的账目。狭义来说, 所述区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 并以密码学方式保证的不可篡改和不可伪造的一种分布式账本。

对于区块链技术而言, 区块链具有去中心化和去信任的特征。所述去中心化是指, 整个区块链网络没有中心化的硬件或管理机制, 任意节点之间的权利和义务都是均等的, 且任一个节点的损坏或者丢失都不会影响整个网络系统的运作, 因此, 保证区块链网络具有良好的健壮性。所述去信任是指, 参与整个网络中的每个节点之间进行数据交换是无需互相信任的, 整个区块链网络系统的运作规则是公开透明的, 所有区块链节点上的数据内容也是公开的, 因此, 在系统指定的规则或时间范围内, 各个节点之间是不能也无法相互欺骗。

客户端向区块链中的一个节点请求访问数据, 该区块链节点向该客户端提供加密数据和解密密钥, 然后客户端再利用解密密钥对该加密数据进行解密得到访问数据, 并将其记账在区块链上。在这一过程中, 由于对区块链节点的账本的历史交易数据无法做修改或删除操作, 并且区块链上数据都是公开的无法取消, 所以一旦授予某一用户访问权限, 分发解密密钥后, 就无法撤销, 进而导致当需要禁止该用户访问权限时, 无法阻止该用户对数据进行访问, 使得对数据访问存在一定风险和不安安全性。

发明内容

本申请提供了一种数据访问权限的控制方法和装置, 以解决在用户的访问权限发生变化时, 能够控制对用户请求的数据或密文的发放。

具体地, 为了解决上述技术问题, 本申请公开了如下技术方案:

第一方面, 本申请提供了一种数据访问权限的控制方法, 所述方法包括步骤如下: 第一代理节点接收来自请求节点的第一请求消息, 所述第一请求消息中包括请求节点的身份标识和待访问的数据标识; 所述第一代理节点根据所述待访问的数据标识在区块链网络中确定第一加密密文, 根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文; 如果是, 则向至少一个第二代理节点发起对所述请求节点的权限验证请求, 并根据所述至少一个第二代理节点的反馈结果, 确定所述第一加密密文的发放。

可选的, 所述第一代理节点根据所述请求节点的身份标识判断所述请求节点如果无

权读取所述第一加密密文，则拒绝所述请求节点的第一请求。

本方面提供的方法，通过在区块链网络中加入代理节点，实现了数据源节点在不修改密文的情况下也能够自由地授予或撤销请求节点的权限，即通过代理节点在区块链上对请求节点最新权限的读取来确定是否授权或拒绝访问请求，如果最新权限是拒绝访问，则可以阻止该用户对数据继续进行访问，从而保证了网络中信息的安全。

另外，利用至少一个第二代理节点对请求方的身份进一步验证，可以防止只利用一个第一代理节点验证时发生作弊的可能，进一步地提高了验证的准确性，进而保证了信息传输的安全性。

结合第一方面，在第一方面的一种实现方式中，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文，包括：根据所述请求节点的身份标识，在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息，所述授权信息包括允许或不允许。

本实现方式中，通过读取最接近区块链链式存储结构末端的请求节点的授权信息可以获取到请求方的最近访问权限，从而为验证请求节点是否可以获取加密密文和密钥做准备。

结合第一方面，在第一方面的另一种实现方式中，所述向至少一个第二代理节点发起对所述请求节点的权限验证请求，包括：所述第一代理节点确定 m 个第二代理节点， m 为大于等于 1 的正整数；生成所述权限验证请求，所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；将所述权限验证请求分别发送给所述 m 个第二代理节点。

结合第一方面，在第一方面的又一种实现方式中，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放，包括：

所述第一代理节点接收来自至少 k 个第二代理节点发送的部分密钥，所述部分密钥是所述第二代理节点，根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的，且 $k \leq m$ ；对所述至少 k 个部分密钥进行还原，生成转换密钥；利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文，所述第二加密密文由所述请求节点的公钥加密后生成；将所述第二加密密文发送给所述请求节点。

本实现方式中，第一代理节点将权限验证请求发送给多个第二代理节点，并在获取到足够数量的第二代理节点发送的部分密钥后才能还原出转换密钥，即需要通过多个第二代理节点共同参与和联合解密才能生成转换密钥，单一的节点或者密钥参与者无法获取转换密钥或密文，从而有效地防止少数节点通过作弊方式绕过权限控制获取密文，本方法增加了解密的复杂度，进而有效地保证密文传输和读取的安全性，防止非授权用户读取密文或数据。

结合第一方面，在第一方面的又一种实现方式中，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放，包括：如果所述第一代理节点接收小于 k 个第二代理节点发送的部分密钥，或者，接收至少一个所述第二代理节点反馈的拒绝消息，则向所述请求节点发送拒绝访问的消息。

结合第一方面，在第一方面的又一种实现方式中，所述第一代理节点接收来自请求节点的第一请求消息，包括：所述第一代理节点接收通过所述区块链网络中的任一区块链节点转发的所述第一请求消息。

第二方面，本申请还提供了一种数据传输方法，该方法可以应用于数据源节点或数据所有方，本方面中以第一节点为例，所述方法包括如下步骤：

第一节点获得第二节点的身份标识，所述身份标识用于确定所述第二节点的授权信息，所述授权信息包括允许和不允许，所述第二节点为请求节点或数据请求方；如果所述授权信息为允许，则所述第一节点利用第一节点的私钥、第二节点的公钥和加密算法生成转换密钥；所述第一节点利用区块链网络中的代理节点的公钥对所述转换密钥进行加密，生成加密后的部分密钥；所述第一节点生成第一交易信息，并将所述第一交易信息记录在所述区块链网络上，所述第一交易信息包括：第二节点的身份标识、第二节点的授权信息和加密后的部分密钥。

结合第二方面，在第二方面的一种实现方式中，所述第一节点利用区块链网络中的代理节点的公钥对所述转换密钥进行加密，生成加密后的部分密钥，包括：所述第一节点利用秘密分享算法将所述转换密钥分解成 n 个部分密钥， n 为大于等于 1 的正整数；所述第一节点在所述区块链网络中选取 m 个代理节点，并使用所述 m 个代理节点的公钥对所述 n 个部分密钥进行加密，生成 n 个加密后的部分密钥， $m \leq n$ 。

结合第二方面，在第二方面的另一种实现方式中，所述第一交易信息中还包括： m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥的数量 k ，当获取的部分密钥的数量小于 k 个时，则不能还原出所需的转换密钥，进而可以防止少数或部分代理节点作弊，从而提高验证的安全性和可靠性。

结合第二方面，在第二方面的又一种实现方式中，将所述第一交易信息记录在所述区块链网络上，包括：所述第一节点将所述第一交易信息发送给区块链网络中的区块链节点，并通过所述区块链节点在全网广播和共识，保存所述第一交易信息。

结合第二方面，在第二方面的又一种实现方式中，所述方法还包括：如果所述授权信息为不允许，则取消所述第二节点的授权信息；生成第二交易信息，所述第二交易信息包括第二节点的身份标识和第二节点的授权信息；将所述第二交易信息记录在所述区块链网络上。

结合第二方面，在第二方面的又一种实现方式中，在第一节点获得第二节点的身份标识之前，所述方法还包括：所述第一节点使用第一节点的公钥通过代理重加密算法对待访问数据进行加密，生成第一加密密文；所述第一节点将所述第一加密密文作为一个交易保存在所述区块链网络中。

第三方面，本申请还提供了一种数据传输方法，该方法可以应用于第二代理节点，所述第二代理节点也可以是一种第一代理节点或主代理节点，所述方法包括如下步骤：

第二代理节点接收来自第一代理节点的权限验证请求，所述权限验证请求中包括请求节点的身份标识和第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；所述第二代理节点根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果是，则生成部分密钥，并将所述部分密钥发送给所述第一代理节点。

本方面中，第二代理节点在第一代理节点验证允许请求节点访问的情况下，对请求节点的权限进一步验证，并在验证是允许访问时，将生成的部分密钥发送给第一代理节点，以使得第一代理节点收集并合成最终的转换密钥，从而可以有效地防止第一代理节点作弊，提高了验证的安全性。

结合第三方面，在第三方面的一种实现方式中，所述生成部分密钥，包括：所述第二代理节点在区块链网络中获得加密后的部分密钥，所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的；所述第二代理节点利用自己的私钥对所述加密后的部分密钥进行解密，生成所述部分密钥。

结合第三方面，在第三方面的另一种实现方式中，所述方法还包括：所述第二代理节点根据所述请求节点的身份标识判断所述请求节点如果无权读取所述第一加密密文，则拒绝所述第一代理节点的第一请求。

第四方面，本申请还提供了一种数据访问权限的控制装置，例如所述装置可以是一种网络节点，或配置在所述网络节点上，其中，所述装置或网络节点可以是以上方面所述的第一代理节点、第一节点或第二代理节点，所述装置中包括用于执行上述第一方面至第三方面，以及各方面的各种实现方式中方法步骤的单元。

具体地，所述装置包括接收单元、处理单元和发送单元，此外，还可以还包括存储单元等其他单元或模块等，本申请不予限制。

第五方面，本申请还提供了一种网络节点，所述网络节点包括处理器，收发器和存储器，其中，在所述网络节点为第一代理节点的情况下，

所述收发器，用于接收来自请求节点的第一请求消息，所述第一请求消息中包括请求节点的身份标识和待访问的数据标识；

所述处理器，用于根据所述待访问的数据标识在区块链网络中确定第一加密密文，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果否，则拒绝所述请求节点的第一请求；如果是，则向至少一个第二代理节点发起对所述请求节点的权限验证请求，并根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放。

结合第五方面，在第五方面的一种实现方式中，所述处理器，具体用于根据所述请求节点的身份标识，在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息，所述授权信息包括允许和不允许。

结合第五方面，在第五方面的另一种实现方式中，所述处理器，具体用于确定 m 个第二代理节点， m 为大于等于 1 的正整数；生成所述权限验证请求，所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；利用所述收发器将所述权限验证请求分别发送给所述 m 个第二代理节点。

结合第五方面，在第五方面的又一种实现方式中，所述收发器，具体用于接收来自至少 k 个第二代理节点发送的部分密钥，所述部分密钥是所述第二代理节点，根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的，且 $k \leq m$ ；

所述处理器，具体用于对所述至少 k 个部分密钥进行还原，生成转换密钥；利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文，所述第二加密密文由所述请求节点的公钥加密后生成；

所述收发器，具体用于将所述第二加密密文发送给所述请求节点。

结合第五方面，在第五方面的又一种实现方式中，所述处理器，具体用于如果所述第一代理节点接收小于 k 个第二代理节点发送的部分密钥，或者，接收至少一个所述第二代理节点反馈的拒绝消息，则利用所述收发器向所述请求节点发送拒绝访问的消息。

结合第五方面，在第五方面的又一种实现方式中，所述收发器，具体用于接收通过所述区块链网络中的任一区块链节点转发的所述第一请求消息。

此外，在所述网络节点为第一代理节点的情况下，所述收发器，用于接收来自第一代理节点的权限验证请求，所述权限验证请求中包括请求节点的身份标识和第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；

所述处理器，用于根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果否，则拒绝所述第一代理节点的第一请求；如果是，则生成部分密钥；

所述收发器，还用于将所述部分密钥发送给所述第一代理节点。

可选的，所述处理器，具体用于在区块链网络中获得加密后的部分密钥，所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的；利用自己的私钥对所述加密后的部分密钥进行解密，生成所述部分密钥。

第六方面，本申请还提供了一种网络节点，所述网络节点包括处理器，收发器和存储器，其中，在所述网络节点为数据源节点或数据所有方，例如第一节点的情况下，

所述收发器，用于获得第二节点的身份标识，所述身份标识用于确定所述第二节点的授权信息，所述授权信息包括允许和不允许；

所述处理器，用于在所述授权信息为允许的情况下，利用所述网络节点的私钥、第二节点的公钥和加密算法生成转换密钥；利用区块链网络中的代理节点的公钥对所述转换密钥进行加密，生成加密后的部分密钥；以及，生成第一交易信息，并将所述第一交易信息记录在所述区块链网络上；

其中，所述第一交易信息包括：第二节点的身份标识、第二节点的授权信息和加密后的部分密钥。

结合第五方面，在第五方面的一种实现方式中，所述处理器，具体用于利用秘密分享算法将所述转换密钥分解成 n 个部分密钥， n 为大于等于 1 的正整数；在所述区块链网络中选取 m 个代理节点，并使用所述 m 个代理节点的公钥对所述 n 个部分密钥进行加密，生成 n 个加密后的部分密钥， $m \leq n$ 。

结合第五方面，在第五方面的另一种实现方式中，所述第一交易信息中还包括： m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥的数量 k 。

结合第五方面，在第五方面的又一种实现方式中，所述处理器，具体用于利用发送单元将所述第一交易信息发送给区块链网络中的区块链节点，并通过所述区块链节点在全网广播和共识，保存所述第一交易信息。

结合第五方面，在第五方面的又一种实现方式中，所述处理器，还用于在所述授权信息为不允许的情况下，取消所述第二节点的授权信息；生成第二交易信息，并将所述第二交易信息记录在所述区块链网络上，所述第二交易信息包括第二节点的身份标识和第二节点的授权信息。

结合第五方面，在第五方面的又一种实现方式中，所述处理器，还用于在获得第二节点的身份标识之前，使用公钥通过代理重加密算法对待访问数据进行加密，生成第一加密密文；以及，将所述第一加密密文作为一个交易保存在所述区块链网络中。

第七方面，本申请还提供了一种计算机存储介质，该计算机存储介质可存储有指令，该指令执行时可实现本申请提供的第一方面至第三方面，以及第一方面至第三方面中的

各种实现方式中的数据访问权限的控制方法的部分或全部步骤。

第八方面，本申请还提供了一种包含指令的计算机程序产品，当所述指令在计算机上运行时，所述计算机执行上述各个方面所述的方法。

附图说明

图 1 为本申请提供的一种 Fabric 架构的示意图；

图 2 为本申请提供的一种在门限密码系统中解密的流程图；

图 3 为本申请提供的一种客户端在区块链网络中请求访问数据的流程图；

图 4a 为本申请提供的一种区块链系统的结构示意图；

图 4b 为本申请提供的一种数据访问权限的控制方法的流程图；

图 5 为本申请提供的另一种数据访问权限的控制方法的流程图；

图 6 为本申请提供的另一种数据访问权限的控制方法的流程图；

图 7 为本申请提供的一种代理重加密体系的角色流程图；

图 8 为本申请提供的又一种数据访问权限的控制方法的流程图；

图 9 为本申请提供的一种网络节点的结构示意图；

图 10 为本申请提供的一种网络节点的装置示意图。

具体实施方式

为了使本技术领域的人员更好地理解本申请实施例中的技术方案，并使本申请实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本申请实施例中的技术方案作进一步详细的说明。

首先，对本申请涉及到的基本概念进行详细地介绍和说明。

本申请的技术方案涉及区块链，所述区块链（Block Chain）是一种分布式数据库，起源自比特币，是比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块（block）。

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链是一个分布式的账本，通过多个独立的分布式节点保存相同的记录。

区块链技术是一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。每当有新的数据需要写入区块链时，这些数据会汇总到一个区块中，添加在已有区块链的末端，通过共识算法保证每个节点新添加的区块是完全相同的。

其中，每个区块内记录了若干条交易记录，同时包含了前一个区块的哈希值（hash），所有区块就是通过这样保存前一个块中的信息，按顺序相连，组成了区块链，难以被篡改。基于区块链技术，可以达成一致的双方直接交易（Transaction, Tx），从而不需要可信赖的第三方中心化中介机构的参与。

智能合约（smart contract）是由事件驱动、具有状态的、运行在一个分布式区块链账本之上的、且能够管理账本上数据的程序。智能合约可以看作是一段普通的计算机执行程序，满足可准确自动执行即可。智能合约的代码内容规定了交易的规则和逻辑，使用者签署调用智能合约就意味着合约内容会被执行并写入区块链账本。

区块链的核心技术之一就是共识算法，例如比特币中所使用的工作量证明（Proof of

Work, PoW) 算法。区块链中的共识算法, 要解决的是面向拜占庭容错的共识场景, 即区块链网络中的节点相互之间并不信任, 有可能存在恶意说谎节点。区块链网络中的每个节点都有可能是“说谎”的节点, 但是众多的节点聚到一个网络中, 它们共识的结果就是一个可信的结果。共识算法的主要作用, 就是让区块链中的所有节点记录相同的有效交易区块内容。

另外, 区块链还是一种解决多方之间信任问题的技术机制。多方信任的前提是技术机制本身就是可信的, 因此区块链需要可审计。区块链系统、智能合约和共识算法在多方之间是必须要开源公开。

超级账本 (Hyperledger) 的 Fabric 项目使用了一种机制用于加快共识的达成, 该机制的核心在于多个背书节点 (endorser peer) 运行智能合约并对运行结果 (endorsement) 进行背书, 例如通过对背书节点本身的合约运行结果内容进行签名, 保证是由特定背书节点发出的结果。用户可以根据实际需求设置自己的智能合约要信任的背书节点及对多个结果的验证策略, 例如设置背书策略 (endorse policy)。

如图 1 所示, 客户端可以向 3 个背书节点发送智能合约运行请求 (proposal), 背书策略可以要求 3 个运行结果内容必须一致, 也可以要求至少两个运行结果的内容一致。客户端收集背书节点反馈的运行结果, 通过排序节点 (Orderer peer) 将记录在一个交易上的运行结果广播到区块链网络中, 区块链网络中的节点, 例如背书节点读取该交易, 并检验当满足背书策略的情况下, 才认为该交易是一个有效交易, 并接受该交易中对数据的修改, 并写入到区块链中。

其中, 客户端 (client) 或客户端应用: 使用软件开发工具包 (Software Development Kit, SDK) 和 Fabric 系统进行交互, 构造合法的交易所, 并将所述交易所提供给背书节点; 当收集到足够符合背书策略要求的背书节点支持后可以构造合法的交易所请求, 并发给排序节点或代理节点。

背书节点 (endorser peer): 负责对来自客户端的交易所进行合法性和权限检查, 如果符合要求, 则签名并返回结果给客户端。

排序节点 (orderer peer): 负责为各个交易所做排序, 并将排好序的交易所广播到其它节点。其中, 所述排序节点包括提供共识服务的节点或者集群。

确认节点 (committer peer): 用于将达成一致顺序的批量交易所结果进行状态检查, 验证交易所是否符合背书策略要求并且确保账本的 read 集变量状态不变, 执行合法的交易所, 生成区块, 并写入账本。

为了提高信息传输的安全性和身份验证的准确性, 本申请的技术方案还涉及门限密码系统 (Threshold cryptosystem)。所述门限密码系统, 是将与公钥对应的私钥分享在多个成员中, 只有当指定数目的成员共同协作, 才能完成对公钥加密的密文进行解密的操作。其中, 门限密码系统的基础是秘密共享 (secret sharing)。

具体地, 一种门限密码系统的方案是将密钥分割成若干份额, 比如分割成 n 份, 并将这些份额一对一地发送给 n 个参与者, n 个参与者中任意 t ($t < n$) 个或 t 个以上的参与者可以协作完成解密操作, 如果参与者小于 t 个则不能完成解密操作。

下面对门限密码系统中的各角色的功能和解密过程进行介绍和说明。

图 2 示出了一种在门限密码系统中解密的流程示意图。其中，所述门限密码系统中涉及密钥分发者、密钥参与者和密钥合成者。进一步地，密钥分发者，用于建立门限密码系统的可信实体，负责生成门限密码系统中涉及到的各个参数，以及将这些参数安全地发送给各个密钥共享者。所述密钥参与者为参与门限密码系统解密操作的单个实体；所述密钥合成者，获取多个参与者的解密份额，并对这些解密份额进行验证和解密操作。

例如，图 2 所示，步骤 1：门限初始化设置，密钥分发者输入安全参数，门限密码系统返回一组公共参数（可用 PK 表示），例如 n ， t 和 SK，其中， n 表示密钥参与者的数量， t 表示门限值，SK 表示门限密码系统生成主密钥，可选的， $SK = (SK_1, SK_2, \dots, SK_n)$ ；

步骤 2：加密，利用所述系统的公共参数 PK 和密钥参与者的身份 ID，对明文消息进行加密，并生成和输出加密密文 c ；

步骤 3：密钥份额生成 (Share key Gen)，密钥分发者利用系统公共参数 PK、加密密文 c 和主密钥 SK，计算得到密钥份额 U_i ；

步骤 4：密钥分发者将密钥份额 U_i 发送给若干个密钥参与者；

步骤 5：密钥参与者获取密钥份额 U_i ，每个密钥参与者对密钥份额 U_i 进行解密生成解密份额，例如解密份额 1，...，解密份额 t ；

步骤 6：各个密钥参与者将自己解密后生成的解密份额发送给密钥合成者；

步骤 7：联合解密，密钥合成者获取所述解密份额，例如获取 t 个解密份额，并验证这 t 个解密份额，利用公共参数 PK 将 t 个解密份额进行合成得到所述加密密文 c ，最后再对所述加密密文进行解密获得明文消息。

本申请提供的技术方案用于解决在区块链中的访问权限一旦授权和下发，就无法更改或撤销，导致非授权用户可以对数据进行访问的技术问题。具体地，客户端在区块链网络中请求访问数据和对密钥解密的过程如下：

如图 3 所示，步骤 1：用户 A 利用客户端 1 登记信息生成信息，例如明文信息；

步骤 2：客户端 1 使用对称密钥加密信息；

步骤 3：客户端 1 发送所述加密信息，并将所述加密信息所存为区块链上的一个交易记录在区块链节点 1 上；

步骤 4：区块链节点 1 验证和广播所述交易；

步骤 5：区块链节点 1、2 和 3 对包含该交易的区块进行共识；所述区块链节点 1、2 和 3 是位于同一区块链上的节点。

所述共识可以理解为区块链节点 1、2 和 3 分别对该交易是否符合策略进行验证，生成对应的验证结果，且三个区块链节点生成的验证结果都相同。

步骤 6：区块链节点确认并生成区块，将所述区块添加在本地账本已有区块链的链式结构的末端；

步骤 7：用户 B 使用客户端 2 获取信息，例如明文信息；

步骤 8：客户端 2 向客户端 1 请求获取用户 B 请求访问所述明文信息的访问权限；

步骤 9：客户端 1 将访问权限信息发送给客户端 2，其中，所述访问权限信息中包含对称密钥；

步骤 10：客户端 2 向区块链节点 3 请求获取保存在区块链账本中的加密信息；

步骤 11：客户端 2 使用对称密钥解密信息。

在上述访问权限下发和解密数据的过程中，由于对区块链节点的账本的历史交易数据无法做修改或删除操作，并且区块链上数据都是公开的无法取消，所以一旦授予某一用户访问权限，分发解密密钥后，就无法撤销，进而导致当需要禁止该用户访问权限时，无法阻止该用户对数据进行访问，使得非授权用户对数据访问存在一定风险和不安定性。

为解决上述问题，本申请各实施例的技术方案的主要思想是：在区块链系统中加入多个代理节点，每个代理节点除了具备普通节点的功能外，还用于联合验证用户的访问权限，并执行密文的转换操作。

如图 4 所示，区块链系统中包括数据源节点或数据所有者、至少一个代理节点 (Proxy)、多个普通节点和数据请求节点。其中，所述数据源节点或数据所有者为数据的保存者和访问权限的授权方；所述普通节点可以用于执行区块链上交易的广播、共识和记录保存等功能。所述用户请求节点为请求访问数据的节点或客户端。

本申请提供的技术方案主要包括三部分流程，分别是：数据保存、权限授予和请求数据。概况地，首先，数据源节点 (data source) 或者数据所有者对原始密文进行加密，并记录和保存在区块链上。

然后，当数据源节点或数据所有者进行授权时，在区块链上写入权限信息，并生成与被授权节点对应的一个转换密钥。数据源节点或数据所有者将所述转换密钥分为若干个部分，发送给不同的代理节点。

最后，当数据请求节点请求访问数据时，各个代理节点发起共识，读取数据请求节点最新的访问权限，验证数据请求节点是否有权，若有权，则代理节点收集转换密钥，将原始密文转换为仅能由被授权节点自己能够解密的另一份密文返回给请求节点；若无权，则拒绝访问。

需要说明的是，在本申请的以下各个实施例中，各个网络设备统称为网络节点，所述网络节点可以是发送请求消息的第一节点、第二节点，还可以是区块链上的某一个区块链节点，例如第一区块链节点或第一代理节点，转发的中继节点，任意的普通节点，还可以是数据源节点。

进一步地，所述网络节点包括但不限于站点、基站、用户设备、客户端和终端。另外，本申请各个实施例中的设备和节点这两个概念等同，即所述设备可以指代节点、站点、UE、网元设备、传感器等。

本申请所述的区块链和区块链系统可以应用于各种网络中 (例如物联网中)，所述区块或者区块链节点可以部署在各种网络设备 (例如物联网设备) 上。所述网络设备包括工业物联网设备，例如各类工业传感器、控制模块等等；还可以是可穿戴设备、家用电器、家居传感器、家居控制模块等，或者是基站、增强型基站、或具有调度功能的中继、或具有基站功能的设备等。其中，基站可以是 LTE 系统中的演进型基站 (evolved Node B, eNB)，也可以其他系统中的基站，本申请实施例并不限定。

另外，上述各类设备可以是用户设备 (user equipment, UE)，例如手机、智能终端、多媒体设备、流媒体设备等。所述 UE 还可以是其它无线网络设备，例如基站 (Node B)，具体地该无线网络设备的形式和类型本申请不予限制。

UE 可以经无线接入网 (radio access network, RAN) 与一个或多个核心网进行通信, UE 还可以通过其它方式接入无线网络进行通信, UE 也可以与其它 UE 直接进行无线通信, 本申请实施例对此不作限定。

参见图 4b, 本申请实施例提供了一种数据访问权限的控制方法, 所述方法包括:

步骤 401: 第一代理节点接收来自请求节点的第一请求消息, 所述第一请求消息中包括请求节点的身份标识和待访问的数据标识。

其中, 一种实现方式包括: 第一代理节点接收通过所述区块链网络中的任一区块链节点转发的所述第一请求消息。

步骤 402: 第一代理节点根据所述待访问的数据标识在区块链网络中确定第一加密密文, 根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文。

其中, 步骤 402 中, 根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文, 包括: 根据所述请求节点的身份标识, 在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息, 所述授权信息包括允许或不允许。

步骤 403: 如果有权读取所述第一加密密文, 即所述授权信息为允许, 则向至少一个第二代理节点发起对所述请求节点的权限验证请求, 并根据所述至少一个第二代理节点的反馈结果, 确定所述第一加密密文的发放。

此外, 如果第一代理节点判断无权读取所述第一加密密文, 则拒绝所述请求节点的第一请求。

在步骤 403 中, 第一代理节点所述向至少一个第二代理节点发起对所述请求节点的权限验证请求, 包括:

所述第一代理节点确定 m 个第二代理节点, m 为大于等于 1 的正整数; 生成所述权限验证请求, 所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文, 所述第一加密密文是通过对待访问数据进行加密后生成; 将所述权限验证请求分别发送给所述 m 个第二代理节点。

可选的, 第一代理节点根据所述至少一个第二代理节点的反馈结果, 确定所述第一加密密文的发放, 包括:

所述第一代理节点接收来自至少 k 个第二代理节点发送的部分密钥, 所述部分密钥是所述第二代理节点, 根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的, 且 $k \leq m$; 对所述至少 k 个部分密钥进行还原, 生成转换密钥; 利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文, 所述第二加密密文由所述请求节点的公钥加密后生成; 将所述第二加密密文发送给所述请求节点。

进一步地, 第一代理节点根据所述至少一个第二代理节点的反馈结果, 确定所述第一加密密文的发放, 包括: 如果所述第一代理节点接收小于 k 个第二代理节点发送的部分密钥, 或者, 接收至少一个所述第二代理节点反馈的拒绝消息, 则向所述请求节点发送拒绝访问的消息。

本实施例提供的方法, 通过在区块链网络中加入代理节点, 实现了数据源节点在不修改密文的情况下也能够自由地授予或撤销请求节点的权限, 即通过代理节点在区块链上对请求节点最新权限的读取来确定是否授权或拒绝访问请求, 如果最新权限是拒绝访

问,则可以阻止该用户对数据继续进行访问,从而保证了网络中信息的安全。

另外,利用至少一个第二代理节点对请求方的身份进一步验证,可以防止只利用一个第一代理节点验证时发生作弊的可能,进一步地提高了验证的准确性,进而保证了信息传输的安全性。

其中,第二代理节点接收来自第一代理节点的权限验证请求,所述权限验证请求中包括请求节点的身份标识和第一加密密文,所述第一加密密文是通过对待访问数据进行加密后生成;

所述第二代理节点根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文;如果否,则拒绝所述第一代理节点的第一请求;如果是,则生成部分密钥,并将所述部分密钥发送给所述第一代理节点。

可选的,所述生成部分密钥,包括:所述第二代理节点在区块链网络中获得加密后的部分密钥,所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的;所述第二代理节点利用自己的私钥对所述加密后的部分密钥进行解密,生成所述部分密钥。

在本实施例中,第二代理节点在第一代理节点验证允许请求节点访问的情况下,对请求节点的权限进一步验证,并在验证是允许访问时,将生成的部分密钥发送给第一代理节点,以使得第一代理节点收集并合成最终的转换密钥,从而可以有效地防止第一代理节点作弊,提高了验证的安全性。

在一个具体实施例中,对本申请所公开的技术方案,按照上述三部分流程进行详细地说明。

a. 数据保存流程

在“数据保存流程”中所执行操作的主体可以是数据源节点或者数据所有者,还可以是其它具有保存数据和给予授权功能的节点,本实施例中以“第一节点”来表示执行数据保存流程的主体,可以理解地,还可以采用其它名称,例如数据所有者等,本申请对此不进行限制。

在所述数据保存流程中涉及公开密钥加密技术,具体地,所述公开密钥加密(Public key cryptograph)也可称为非对称加密(asymmetric cryptography),它是密码学的一种算法,主要涉及两个密钥:一个是公开密钥,被称为“公钥”,另一个是私有密钥,被称为“私钥”。

两个密钥的功能不同,一个用作加密,另一个则用作解密。例如,使用其中一个密钥对明文进行加密,得到加密密文后,只能用相对应的另一个密钥才能解密得到原本的明文。即不能利用加密的密钥对密文进行解密和访问数据,由于对明文的加密和解密分别使用了两个不同的密钥,故这一过程又可以被称为非对称加密,相比于利用同一个密钥进行加密和解密的对称加密,采用非对称加密的方式安全性更高,因为即使获取到两个密钥中的一个,也不能对加密密文进行解密,并且也不能通过计算得到另一个密钥,因此,其中的公钥可以公开,向外发布,例如记录在区块链上;私钥则由客户端或 UE 自己单独保管。

在“数据保存流程”中,第一节点主要执行以下方法流程:

第一节点使用第一节点的公钥通过加密算法,例如代理重加密算法对密文进行加

密，生成第一加密密文 Ea ；

第一节点将所述第一加密密文 Ea 作为一个交易 (transaction) 保存在区块链网络中。

可选的，一种保存交易的方式是，第一节点向区块链网络中的任意一个普通节点发送交易请求，所述交易请求中包括第一加密密文 Ea ；接收到所述交易请求的普通节点在区块链网络中进行广播，使得区块链上的各个区块链节点共识和保存所述第一加密密文 Ea 的相关交易。

另外，可选的，另一种保存交易的方式是，第一节点直接将包含所述第一加密密文的交易请求发送给任意一个代理节点，例如第一代理节点，并通过第一代理节点广播和共识该交易到区块链上。

b. 权限授予流程

如图 5 所示，方法包括：

步骤 501：第一节点记录第二节点的身份标识 I ，以及所述第二节点对第一加密密文 Ea 的访问权限信息 R 。

其中，所述第二节点为被授权用户，所述第二节点的身份标识 I 可以是第二节点标识、用户 ID、设备 ID 或设备标识等。所述访问权限信息 R 包括：授予权限和取消授权。

步骤 502：判断所述访问权限信息 R 中是包括授予权限还是取消授权的内容。

步骤 503a：如果所述访问权限信息 R 中携带授予权限的内容，则所述第一节点利用第一节点的私钥、第二节点的公钥和加密算法生成转换密钥 T 。

步骤 503b：如果所述访问权限信息 R 中携带取消权限的内容，则所述第一节点向区块链网络中的任意一个节点发送交易请求，所述交易请求中包括所述访问权限信息 R 和第二节点的身份标识 I 。

步骤 504：继续步骤 503a 的流程，第一节点利用秘密分享算法将所述转换密钥 T 分解成 n 个部分密钥， n 为大于等于 1 的正整数。

可选的，将所述转换密钥 T 分解为 (m, T_n) ，其中， T_n 表示分解后的任意一个部分密钥， m 表示能够还原转换密钥 T 的最小 T_n 数量。

步骤 505：第一节点在所述区块链网络中随机选取 m 个代理节点，并使用所述 m 个代理节点的公钥对所述 n 个部分密钥 T_n 进行加密，生成 n 个加密后的部分密钥 T_{ne} ，且 $m \leq n$ 。

步骤 506：第一节点生成第一交易信息，并将所述第一交易信息发送给任意一个普通节点或区块链节点，所述第一交易信息包括以下至少一项：第二节点的身份标识 I 、第二节点的授权信息（或访问权限信息 R ）和加密后的部分密钥 T_{ne} 。

可选的，所述第一交易信息中还包括： m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥 T_{ne} 的数量 m 。

步骤 507：普通节点或代理节点在所述区块链网络中广播和保存所述第一交易信息 (I, R, T_{ne}, m) ，或者，在上述步骤 503b 的流程基础上，广播和记录所述交易请求 (I, R) 。

c. 请求数据流程

本“请求数据流程”中介绍请求节点向区块链发起数据访问请求，并在满足授权访问的情况下，对加密密文解密和访问的过程，具体地，如图 6 所示，该流程包括以下步骤：

步骤 601: 数据请求节点向任意一个普通节点发送第一请求消息, 所述第一请求消息中包括: 请求节点的身份标识 I 和待访问的数据标识, 或者是所述待访问数据标识所对应的第一加密密文 Ea;

步骤 602: 普通节点接收并转发所述第一请求消息给第一代理节点 Pm;

可选的, 第一代理节点 Pm 可作为本次请求的主节点。

步骤 603: 第一代理节点 Pm 接收所述第一请求消息, 根据第一请求消息中携带的所述待访问的数据标识在区块链网络中确定第一加密密文 Ea, 以及根据所述请求节点的身份标识 I 判断其是否有权读取所述第一加密密文 Ea;

例如, 第一代理节点 Pm 根据所述请求节点的身份标识 I, 在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息, 所述授权信息包括允许和不允许。

可选的, 如果存在多个授权信息, 以授权信息所在区块编号最大的为准;

步骤 604a: 如果无权或者不允许, 则拒绝数据请求节点的本次访问请求;

步骤 604b: 如果有权或者允许访问, 则向至少一个第二代理节点 P 发起对所述请求节点的权限验证请求;

其中, 所述第二代理节点的选择可以是预先在区块链上设置的, 或者系统默认区块链节点是可以相互发现的。

进一步地, 所述默认区块链节点间互相发现是指, 通过在“权限授予流程”中保存在区块链上的交易信息, 例如第一交易信息, 第一代理节点可以知道哪些第二代理节点对部分密钥 Tn 进行了加密, 并生成了加密后的部分密钥 Tne, 然后将所述权限验证请求发送给这些第二代理节点。

其中, 所述权限验证请求中包括: 所述请求节点的身份标识 I 和第一加密密文 Ea。

步骤 605: 第二代理节点 P 接收来自第一代理节点 Pm 的权限验证请求 (I, Ea), 根据所述请求节点的身份标识 I 判断所述数据请求节点是否有权读取第一加密密文 Ea;

其中, 所述第一加密密文 Ea 是通过对待访问数据进行加密后生成。

步骤 606a: 如果否 (无权), 则拒绝数据请求节点的本次访问请求, 例如第二代理节点 P 向第一代理节点 Pm 反馈拒绝访问的消息;

步骤 606b: 如果是 (有权), 则生成部分密钥 Tn, 并将所述部分密钥 Tn 发送给所述第一代理节点 Pm。

具体地, 第二代理节点 P 在区块链上读取加密后的部分密钥 Tne, 利用自己的私钥对所述 Tne 进行解密得到所述部分密钥 Tn。

步骤 607: 第一代理节点 Pm 接收来自至少 k 个第二代理节点 P 发送的部分密钥 Tn, $k \leq m$, m 为第一代理节点 Pm 确定的发送所述权限验证请求的第二代理节点的 m 数量。

步骤 608: 第一代理节点 Pm 对所述至少 k 个部分密钥 Tn 进行还原, 生成转换密钥 T;

步骤 609: 第一代理节点 Pm 利用所述转换密钥 T 和加密算法将所述第一加密密文 Ea 转换为第二加密密文 Eb, 所述第二加密密文 Eb 由所述数据请求节点的公钥加密后生成的。

步骤 610: 第一代理节点 Pm 将所述第二加密密文 Eb 发送给普通节点;

步骤 611: 所述普通节点接收并发送所述第二加密密文 Eb 给数据请求节点, 以使所述数据请求节点利用自己的私钥对所述第二加密密文 Eb 进行解密, 得到所述待访问数

据。

有益效果

本申请实施例提供的方法，通过在区块链网络中加入代理节点，实现了数据源节点在不修改密文的情况下也能够自由地授予或撤销请求节点的权限，即通过代理节点在区块链上对请求节点最新权限的读取来确定是否授权或拒绝访问请求，如果最新权限是拒绝访问，则可以阻止该用户对数据继续进行访问，从而保证了网络中信息的安全。

在“权限授予流程”中数据源节点通过将转换密钥分解成多个部分密钥，并上链给多个代理节点持有，使得在“请求数据流程”中只有在获取足够数量的部分密钥后才能够还原出转换密钥，单一的节点或者密钥参与者无法获取转换密钥或密文，从而有效地防止少数节点通过作弊方式绕过权限控制，获取密文，本方法增加了解密的复杂度，进而有效地保证密文传输和读取的安全性，防止非授权用户读取密文或数据。

另外，在读取数据时非授权方，例如第一代理节点和第二代理节点都无法获取明文，进而也就无法读取明文内容，从而保护了数据的隐私。

需要说明的是，本实施例中的“权限授予流程”和“请求数据流程”中关于转换密钥的分解和还原过程可以参考前述介绍的门限密码系统中各个角色的功能和流程图（图2所示）。

另外，本实施例中的代理节点可以是基于代理重加密体系中的一个代理节点或代理者，所述代理重加密（Proxy re-encryption）是一种具有对密文安全转换功能的新颖公钥加密体系。

参见图7，为本实施例提供的一种代理重加密体系的角色流程图；该体系中包括：委托者（Delegator）、一个半可信代理者（Proxy）和被委托者（Delegatee）。

具体地，步骤701：委托者使用委托者自身的公钥加密明文消息生成加密密文；

步骤702：委托者将所述加密密文发送给一个半可信代理者；

步骤703：委托者获取被委托者的公钥；

步骤704：委托者授权一个针对所述被委托者的密文转换密钥；

步骤705：委托者将所述密文转换密钥发送给所述半可信代理者；

步骤706：半可信代理者获取来自所述委托者的加密密文，和针对被委托者的密文转换密钥，半可信代理者对所述加密密文做转换，具体地，将所述加密密文转换为由所述被委托者的公钥加密后的密文；

步骤707：半可信代理者将转换后的密文发送给被委托者；

步骤708：被委托者获取所述转换后的密文，并使用被委托者自身的私钥对所述转换后的密文进行解密生成所述明文消息。

本实施例中，基于代理重加密体系的角色功能，在代理节点处增加了权限验证过程，进而对不满足授权访问权限的节点，拒绝其访问，进而实现了对区块链中各个权限的控制和变更，进而提高数据传输的安全性和可靠性。

在一个具体的实施例中，以在超级账本 Fabric 区块链中实现 Alice 存储自己的年龄，控制 Bob 可以进行访问为例，对本申请提供的方法进行详细地说明。

本实施例中预先所有参与者已进行过系统建立，并生成了自己的一对密钥（公钥和私钥），且公钥已记录和公开在区块链网络中。

在现有的 Fabric 区块链网络中增加新的代理节点，所述新的代理节点具备执行权限验证和密文转换等功能，通过如下配置文件增加三个代理节点(X,Y,Z)到所述 Fabric 区块链网络中。

具体的流程如图 8 所示，

在数据保存流程中，Alice 可作为数据所有者或数据源节点执行以下方法步骤：

步骤 801: Alice 使用自己的公钥 Pa 将自己的年龄 a，执行代理重加密算法生成第二层密文 Ea。

其中，所述代理重加密算法可以是论文《Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage》所描述代理重加密算法中的第二层加密算法(E2)。

步骤 802: Alice 将 Ea 的打包为一个交易发送给区块链网络中的任意一个普通节点；所述普通节点接收该交易，并进行广播和共识确认该交易。

可选的，

保存数据伪码如下：

```
Func encrypt(data) {  
    Ea = E2(data, Pa) //生成第二层密文  
    Tx = Package(Ea) //打包交易  
    Send(Tx) //发送交易  
}
```

打包的交易如表 1 所示

Tx1Id	Tx2Type (TRANSACTION)	timestamp
Channel	chaincodeName	chaincodeVersion
Invoke Method:	“write Data, Ea, Alice”	
readSet		
writeSet	Data, {Ea, Alice}	
Response	“SUCCESS”	
endorser Identity	Endorser Signature	
Creator Identity	Alice Signature	

表 1

普通节点执行的记录数据的伪码如下：

```
func writeData(data, owner) {  
    id==null:0?id++  
    putState(“Data” , { “id” :id, “data” :data, “owner” :owner }) //保存数据  
    return SUCCESS  
}
```

交易完成后，在 Fabric 区块链上记录的 world state 状态以表 2 的方式显示为：

Key	Value	Version
Data	{id: 1, data: Ea, owner: Alice}	1

表 2

权限授予流程

步骤 803: Alice 使用自己的私钥 Sa, 与 Bob 的公钥 Pb, 执行上述代理重加密算法中的重加密密钥生成算法 (RG), 生成重加密密钥 T 或称转换密钥 T。

步骤 804: Alice 使用所述重加密密钥 T, 设置 $n=3$, $k=2$, 所述 n 表示将重加密密钥 T 分解的份数, k 表示还原所述 T 的最少代理节点的数量; 通过 Shamir 密钥分享算法将重加密密钥 T 分解为三个部分密钥 T1, T2, T3。

步骤 805: Alice 使用代理节点 X, Y, Z 的公钥对所述部分密钥 T1, T2, T3 分别加密生成加密后的部分密钥, 例如分别为 T1x, T2y, T3z。

步骤 806: Alice 记录请求者 Bob 对所述第二层密文 Ea 有权进行访问, 密文处理节点为 X, Y, Z, 且最少需要 2 个节点共同处理。

步骤 807: Alice 将上述信息打包为交易发送给一个普通节点, 该普通节点对该交易的信息进行广播和共识确认该交易。

可选的,

授权伪码如下:

```

Func Authorize(dataid, delegatee, right, threshold, division) {
    T = RG(Sa, delegatee) //生成转换密钥
    Tn = ShamirSplit(T, division, threshold) //将转换密钥分解为 division 份,
    可通过最少 threshold 份还原
    Foreach(t in Tn) { //对于 Tn 中的每一份密钥
        p = Ramdon(proxylist) //随机选取一个 proxy
        Proxies += p //记录选择的 proxy
        Tne += Encrypt(t, p.Pk) //使用 proxy 的公钥对 t 加密
    }
    Tx = Package(Alice, dataid, delegatee, right, Proxies, Tne, threshold)
    Send(Tx)
}

```

打包的交易如表 3 所示

Tx1Id	Tx2 Type (TRANSACTION)	timestamp
Channel	Chain code Name	Chain code Version
InvokeMethod:	“authorize, Alice, 1, Bob, allow, [X, Y, Z], [T1x, T2y, T3z], 2”	
readSet		
writeSet	Auth, {1, Bob, allow, [T1x, T2y, T3z] } Proxy, {[X, Y, Z], 2}	
Response	“SUCCESS”	

endorserIdentity	Endorser Signature
creatorIdentity	Alice Signature

表 3

可选的，所述普通节点执行的记录授权信息的伪码如下：

```
func authorize(delegator, dataid, delegatee, right, keys, proxy, keys,
threshold) {
    if delegator == data.owner{//判断授权者是否是数据所有者
        id==null: 0?id++
        putState("Auth", { "id":id, "data":dataid, "delegatee":delegatee,
"right":right, "kyes":keys})//保存授权信息
        putState("Proxy", { "id":id, "proxy":proxy, "threshold":threshold})
//保存代理信息
        return SUCCESS
    }
    return FAIL
}
```

交易完成后，在 Fabric 区块链上记录的 world state 状态以表 4 的方式显示为：

Key	Value	Version
Auth	{id:1,data:1,delegatee:Bob,right:allow,keys:[T1x, T2y, T3z]}	1
Proxy	{id:1, proxy:[X,Y,Z], threshold:2}	1

表 4

请求数据流程

步骤 808: Bob 向任意一个普通节点发起数据请求，所述数据请求包含自身身份信息 Bob 和访问数据对象 1；

步骤 809: 普通节点将所述数据请求转发给代理节点 X，所述代理节点 X 将作为本次请求的主节点或第一代理节点；

步骤 810: 代理节点 X 读取区块链上 Bob 对数据对象 1 的最新权限，所述读取的结果为 allow；

步骤 811: 代理节点 X 读取数据对象 1 的密钥处理节点为 [X, Y, Z]，代理节点 X 分别向节点 X, Y, Z 发起密钥请求，该密钥请求包含 Bob 身份标识和数据对象 1，并开始等待反馈结果；

步骤 812: 代理节点 X, Y, Z 读取链上 Bob 对数据对象 1 的最新权限，所述读取的结果为 allow；

步骤 813: 在读取结果为 allow 的情况下，代理节点 X, Y, Z 分别读取链上记录的加密后的部分密钥 T1x, T2y, T3z，使用代理节点 X, Y, Z 的私钥解密这些加密后的部分密钥得到部分密钥 T1, T2, T3，然后发送给代理节点 X；

步骤 814: 代理节点 X 收到部分密钥 T1、T2 和 T3 中的任意至少两个，例如 T1 和 T2，使用 Shamir 秘密分享算法将分解的部分密钥还原成转换密钥 T；

步骤 815: 代理节点 X 读取数据对象 1 对应的第二层密文 Ea, 使用所述转换密钥 T, 执行前述代理重加密算法中的重加密方法 (R) 将所述第二层密文 Ea 转换为以 Bob 的公钥 Pb 加密后的第一层密文 Eb;

步骤 816: 代理节点 X 将所述第一层密文 Eb 发送给 Bob;

步骤 817: Bob 接收并根据第一层密文 Eb, 使用自己的私钥 Sb, 执行前述代理重加密算法中的解密方法 (D) 获得 Alice 的年龄 a。

本实施例提供的方法, 在区块链上增加代理节点, 实现了对链上数据传输间任意节点的权限控制, 即可以在发现数据请求节点无权访问数据的情况下, 变更或拒绝数据请求节点的本次请求, 防止其继续访问数据, 从而保证网络中信息的安全。

另外, 基于门限密码系统中各个参与者协同工作, 完成解密的特点, 将转换密钥分解成多个部分密钥, 并上链给多个代理节点持有, 使得在“请求数据流程”中只有在获取足够数量的部分密钥后才能够还原出转换密钥, 单一的节点或者密钥参与者无法获取转换密钥或密文, 从而有效地防止少数节点通过作弊方式绕过权限控制获取密文, 本方法增加了解密的复杂度, 提高了数据传输和读取的安全性。

可选的, 代理节点 X 执行的读取数据伪码如下:

```
Func ReadData(data, delegatee) {
    R = ReadLastestRight(data, delegatee) //读取最新的权限信息
    if (R==allow) { //判断是否已授权
        Proxies, Threshold = ReadProxy(data) //读取持有转换密钥的代理节点
        Foreach(p in Proxies) {
            Keys += requestKey(p, data, delegatee) //申请转换密钥片段
        }
        If (Keys.size >= Threshold) { //收集到的密钥片段数量大于门限时
            T = Shamir.RecoverKey(Keys) //还原密钥
            Ea = ReadEncryptData(data) //读取原始密文
            Eb = R(Ea, T) //将针对 Alice 公钥的第二层密文转换为针对 Bob 公钥的第一层
            密文
            Return Eb
        }
        Return FAIL //未收集到足够的转换密钥片段
    }
    Return UNAUTHORIZED //未授权
}
```

代理节点 X, Y, Z 执行的读取密钥伪码如下:

```
Func ReadKey(data, delegatee) {
    R = ReadLastesRight(data, delegatee) //读取最新的权限信息
    if (R==allow) { //判断是否已授权
        EKey = ReadEncryptedKey(data, delegatee) //读取自己持有的转换密钥片段
```

```

    Key = Decrypt(Ekey, self.Sk) //使用自己的私钥解密
    Return Key
}

Return UNAUTHORIZED //未授权
}

```

撤销授权流程:

在上述实施例中, 如果 Alice 读取 Bob 的最新访问权限为 disallow 时, 则撤销之前对 Bob 的授权, 具体地过程如下:

Alice 在区块链上追加 Bob 的权限为 disallow。

此时, 在 Fabric 区块链上记录的 world state 状态以表 5 的方式显示为:

Key	Value	Version
Auth	{id: 1, data: 1, delegatee: Bob, right: disallow, keys: [T1x, T2y, T3z]}	2
Proxy	{id: 1, proxy: [X, Y, Z], threshold: 2}	1

表 5

当代理节点 X 读取权限信息过程中发现该权限信息指示不允许访问时, 则拒绝请求节点的访问请求。

可以理解地, 所述代理节点 X 也可以是主代理节点, 例如第一代理节点, 还可以是其它代理节点, 例如代理节点 Y 和 Z。

可选的, 本申请上述实施例中的访问权限控制方法还可以防止某个代理节点作弊, 具体地, 以本实施例中将转换密钥分解为 3 份, 且密钥共享参与者的门限数量为 2 为例, 存在以下作弊情况:

情况一: 代理节点 X 作弊, 权限是 disallow 时继续申请部分密钥, 代理节点 Y 和 Z 未作弊, 对发现是 disallow 的权限信息时拒绝请求节点的访问请求, 则代理节点 X 无法获得转换密钥。

情况二: 代理节点 X 和 Y 联合作弊, 虽然可以获取转换密钥, 但是对转换密钥转换后的结果是 Bob 的密文, 代理节点 X 和 Y 没有 Bob 的私钥, 所以不能解密获取明文。

情况三: Bob 作弊, 无法获得转换密钥。

情况四: 代理节点 X、Y 和 Bob 联合作弊:

若 Bob 未获得过授权, 则不会获得转换密钥;

若 Bob 的授权被撤销, 则可以获得转换密钥, 也能由 Bob 解密出明文, 但是, 该作弊成本高于 Bob 在授权期间缓存明文的方式, 所以只会泄漏 Bob 获得过授权的数据, 不会影响其他数据。

参见图 9, 为本申请一实施例提供的一种数据访问权限控制装置的结构示意图, 所述装置包括代理节点, 所述装置可以为前述实施例中的代理节点, 也可以设置在代理节点上, 或应用与第一代理节点, 用于执行图 5 和图 6 所对应的权限控制方法。

如图 9 所示, 该网络节点包括: 接收单元 901、处理单元 902 和发送单元 903, 此外, 还可以包括其它单元和模块, 例如存储单元等。

具体地，接收单元 901，用于接收来自请求节点的第一请求消息，所述第一请求消息中包括请求节点的身份标识和待访问的数据标识；

处理单元 902，用于根据所述待访问的数据标识在区块链网络中确定第一加密密文，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；

发送单元 903，用于在无权读取所述第一加密密文的情况下，拒绝所述请求节点的第一请求；在有权的情况下，向至少一个第二代理节点发起对所述请求节点的权限验证请求，

所述处理单元 902，还用于在所述有权的情况下，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放。

可选的，在本实施例的一种可能的实现方式中，发送单元 903，具体用于根据所述请求节点的身份标识，在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息，所述授权信息包括允许和不允许。

可选的，在本实施例的另一种可能的实现方式中，所述处理单元 902，具体用于确定 m 个第二代理节点，生成所述权限验证请求，所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成， m 为大于等于 1 的正整数；

所述发送单元 903，具体用于将所述权限验证请求分别发送给所述 m 个第二代理节点。

可选的，在本实施例的又一种可能的实现方式中，所述接收单元 901，还用于接收来自至少 k 个第二代理节点发送的部分密钥，所述部分密钥是所述第二代理节点，根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的，且 $k \leq m$ ；

所述处理单元 902，具体用于对所述至少 k 个部分密钥进行还原，生成转换密钥；利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文，所述第二加密密文由所述请求节点的公钥加密后生成；

发送单元 903，还用于将所述第二加密密文发送给所述请求节点。

可选的，在本实施例的又一种可能的实现方式中，所述处理单元 902，具体用于通过所述接收单元在接收到小于 k 个第二代理节点发送的部分密钥，或者，接收至少一个所述第二代理节点反馈的拒绝消息的情况下，通过所述发送单元向所述请求节点发送拒绝访问的消息。

可选的，在本实施例的又一种可能的实现方式中，所述接收单元 901，具体用于接收通过所述区块链网络中的任一区块链节点转发的所述第一请求消息。

其中，所述网络节点还可以应用于第二代理节点，用于执行第二代理节点的权限验证和结果反馈等功能。

具体地，接收单元 901，用于接收来自第一代理节点的权限验证请求，所述权限验证请求中包括请求节点的身份标识和第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；

处理单元 902，用于根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果否，则拒绝所述第一代理节点的第一请求；如果是，则生成部分密钥；

发送单元 903，用于将所述部分密钥发送给所述第一代理节点。

另外，可选的，所述处理单元 902，具体用于在区块链网络中获得加密后的部分密钥，所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的；利用自己的私钥对所述加密后的部分密钥进行解密，生成所述部分密钥。

此外，所述网络节点还可以是数据源节点或数据所有者，例如第一节点，且该第一节点的结构与图 9 所示的网络节点的结构相同，但该网络节点中的各个单元还具备以下功能。

具体地，接收单元 901，用于获得第二节点的身份标识，所述身份标识用于确定所述第二节点的授权信息，所述授权信息包括允许或不允许；

处理单元 902，用于在所述授权信息为允许的情况下，利用所述网络节点的私钥、第二节点的公钥和加密算法生成转换密钥；利用区块链网络中的代理节点的公钥对所述转换密钥进行加密，生成加密后的部分密钥；以及，生成第一交易信息，并将所述第一交易信息记录在所述区块链网络上；

所述第一交易信息包括：第二节点的身份标识、第二节点的授权信息和加密后的部分密钥。

可选的，在本实施例的一种可能的实现方式中，所述处理单元 902，具体用于利用秘密分享算法将所述转换密钥分解成 n 个部分密钥， n 为大于等于 1 的正整数；在所述区块链网络中选取 m 个代理节点，并使用所述 m 个代理节点的公钥对所述 n 个部分密钥进行加密，生成 n 个加密后的部分密钥， $m \leq n$ 。

其中，所述第一交易信息中还包括： m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥的数量 k 。

可选的，在本实施例的另一种可能的实现方式中，所述处理单元 902，具体用于利用发送单元将所述第一交易信息发送给区块链网络中的区块链节点，并通过所述区块链节点在全网广播和共识，保存所述第一交易信息。

可选的，在本实施例的又一种可能的实现方式中，所述处理单元 902，还用于在所述授权信息为不允许的情况下，取消所述第二节点的授权信息；生成第二交易信息，并将所述第二交易信息记录在所述区块链网络上，所述第二交易信息包括第二节点的身份标识和第二节点的授权信息。

可选的，在本实施例的又一种可能的实现方式中，所述处理单元 902，还用于在获得第二节点的身份标识之前，使用公钥通过代理重加密算法对待访问数据进行加密，生成第一加密密文；以及，将所述第一加密密文作为一个交易保存在所述区块链网络中。

在具体的硬件实现中，如图 10 所示，上述实施例中的网络节点包括：收发器 1201、处理器 1202 和存储器 1203，所述网络节点还可以包括更多或更少的部件，或者组合某些部件，或者不同的部件布置，本申请对此不进行限定。

所述收发器 1001 用于获取请求消息和反馈信息的收发，并与网络中的其他节点进行数据传输。其中，所述收发器可以包括收发模块，所述收发模块可以包括无线局域网（wireless local area network, WLAN）模块、蓝牙模块、基带（base band）模块等通信模块，以及所述通信模块对应的射频（radio frequency, RF）电路，用于进行无线局域网络通信、蓝牙通信、红外线通信及/或蜂窝式通信系统通信，例如宽带码分多

重接入 (wideband code division multiple access, WCDMA) 及/或高速下行封包存取 (high speed downlink packet access, HSDPA)。所述收发模块用于控制终端设备中的各组件的通信, 并且可以支持直接内存存取 (direct memory access)。

所述处理器 1002 为交换机的控制中心, 利用各种接口和线路连接整个交换机的各个部分, 通过运行或执行存储在存储器 1203 内的软件程序和/或模块, 以及调用存储在存储器 1203 内的数据, 以执行交换机设备的各种功能和/或处理数据。

所述处理器 1202 可以由集成电路 (Integrated Circuit, IC) 组成, 例如可以由单颗封装的 IC 所组成, 也可以由连接多颗相同功能或不同功能的封装 IC 而组成。举例来说, 处理器可以仅包括中央处理器 (Central Processing Unit, CPU), 也可以是 GPU、数字信号处理器 (Digital Signal Processor, DSP)、及收发器中的控制芯片 (例如基带芯片) 的组合。在本申请的各种实施方式中, CPU 可以是单运算核心, 也可以包括多运算核心。

所述存储器 1003 可以包括易失性存储器 (volatile memory), 例如随机存取内存 (Random Access Memory, RAM); 还可以包括非易失性存储器 (non-volatile memory), 例如快闪存储器 (flash memory), 硬盘 (Hard Disk Drive, HDD) 或固态硬盘 (Solid-State Drive, SSD); 存储器还可以包括上述种类的存储器的组合。所述存储器中可以存储有程序或代码, 交换机中的处理器 1002 通过执行所述程序或代码可以实现所述网络节点的功能。

在本实施例中, 所述收发器 1001 所要实现的功能可以由图 9 所示的接收单元 901 和发送单元 903 来实现, 或者由处理器 1002 控制的收发器 1001 实现; 所述处理单元 902 所要实现的功能则可以由处理器 1002 实现。

此外, 本申请还提供一种计算机存储介质, 其中, 该计算机存储介质可存储有程序, 该程序执行时可包括本申请提供的数据访问权限的控制方法、数据传输方法的各实施例中的部分或全部步骤。所述的存储介质可为磁碟、光盘、只读存储记忆体 ROM 或随机存储记忆体 RAM 等。

在上述实施例中, 可以全部或部分通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。

所述计算机程序产品包括一个或多个计算机指令, 例如验证指令。在计算机加载和执行所述计算机程序时, 全部或部分地产生按照本申请上述实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络或者其他可编程装置。

所述计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网络站点、计算机、服务器或数据中心通过有线或无线方式向另一个站点、计算机或服务器进行传输。

所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等存储设备。所述可用介质可以是磁性介质, 例如软盘、硬盘、磁带、光介质 (例如 DVD)、或半导体介质, 例如固态硬盘 SSD 等。

另外, 需要说明的是, 本申请个实施例中所述的网络节点可以是基站, 或者接入点。例如, 基站可以是 GSM 或 CDMA 中的基站 (BTS, Base Transceiver Station), 也可以是 WCDMA 中的基站 (NodeB), 还可以是 LTE 中的演进型基站 (eNB 或 e-NodeB, evolutionary Node B), 本申请不予限定。

另外，所述网络节点还可以是客户端、终端设备，所述终端设备，可以是指向用户提供语音和/或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。

无线终端可以经无线接入网 RAN 与一个或多个节点进行通信，所述无线终端可以是移动终端，如移动电话（或称为“蜂窝”电话）和具有移动终端的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。例如，个人通信业务（PCS，Personal Communication Service）电话、无绳电话、会话发起协议（SIP）话机、无线本地环路（WLL，Wireless Local Loop）站、个人数字助理（PDA，Personal Digital Assistant）等设备。无线终端也可以称为系统、订户单元（Subscriber Unit）、订户站（Subscriber Station）、移动站（Mobile Station）、移动台（Mobile）、远程站（Remote Station）、接入点（Access Point）、远程终端（Remote Terminal）、接入终端（Access Terminal）、用户终端（User Terminal）、用户代理（User Agent）、用户设备（User Device）、或用户装备（User Equipment）。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排除他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

本领域的技术人员可以清楚地了解到本发明实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明实施例中的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本发明各个实施例或者实施例的某些部分所述的方法。

本说明书中各个实施例之间相同相似的部分互相参见即可。尤其，对于网络节点或装置设备而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例中的说明即可。

以上所述的本申请实施方式并不构成对本申请保护范围的限定。

权 利 要 求 书

1、一种数据访问权限的控制方法，其特征在于，所述方法包括：

第一代理节点接收来自请求节点的第一请求消息，所述第一请求消息中包括请求节点的身份标识和待访问的数据标识；

所述第一代理节点根据所述待访问的数据标识在区块链网络中确定第一加密密文，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；

如果是，则向至少一个第二代理节点发起对所述请求节点的权限验证请求，并根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放。

2、根据权利要求 1 所述的方法，其特征在于，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文，包括：

根据所述请求节点的身份标识，在区块链上读取最接近区块链链式存储结构末端的请求节点的授权信息，所述授权信息包括允许或不允许。

3、根据权利要求 1 所述的方法，其特征在于，所述向至少一个第二代理节点发起对所述请求节点的权限验证请求，包括：

所述第一代理节点确定 m 个第二代理节点， m 为大于等于 1 的正整数；

生成所述权限验证请求，所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；

将所述权限验证请求分别发送给所述 m 个第二代理节点。

4、根据权利要求 1-3 任一项所述的方法，其特征在于，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放，包括：

所述第一代理节点接收来自至少 k 个第二代理节点发送的部分密钥，所述部分密钥是所述第二代理节点，根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的，且 $k \leq m$ ；

对所述至少 k 个部分密钥进行还原，生成转换密钥；

利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文，所述第二加密密文由所述请求节点的公钥加密后生成；

将所述第二加密密文发送给所述请求节点。

5、根据权利要求 3 所述的方法，其特征在于，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放，包括：

如果所述第一代理节点接收小于 k 个第二代理节点发送的部分密钥，或者，接收至少一个所述第二代理节点反馈的拒绝消息，则向所述请求节点发送拒绝访问的消息。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述第一代理节点接收来自请求节点的第一请求消息，包括：

所述第一代理节点接收通过所述区块链网络中的任一区块链节点转发的所述第一请求消息。

7、根据权利要求 1-5 任一项所述的方法，其特征在于，所述方法还包括：

所述第一代理节点根据所述请求节点的身份标识判断所述请求节点如果无权读取所述第一加密密文，则拒绝所述请求节点的第一请求。

8、一种数据传输方法，其特征在于，所述方法包括：

第一节点获得第二节点的身份标识,所述身份标识用于确定所述第二节点的授权信息;

如果所述授权信息为允许,则所述第一节点利用第一节点的私钥、第二节点的公钥和加密算法生成转换密钥;

所述第一节点利用区块链网络中的代理节点的公钥对所述转换密钥进行加密,生成加密后的部分密钥;

所述第一节点生成第一交易信息,并将所述第一交易信息记录在所述区块链网络上,所述第一交易信息包括:第二节点的身份标识、第二节点的授权信息和加密后的部分密钥。

9、根据权利要求8所述的方法,其特征在于,所述第一节点利用区块链网络中的代理节点的公钥对所述转换密钥进行加密,生成加密后的部分密钥,包括:

所述第一节点利用秘密分享算法将所述转换密钥分解成 n 个部分密钥, n 为大于等于1的正整数;

所述第一节点在所述区块链网络中选取 m 个代理节点,并使用所述 m 个代理节点的公钥对所述 n 个部分密钥进行加密,生成 n 个加密后的部分密钥, $m \leq n$ 。

10、根据权利要求9所述的方法,其特征在于,

所述第一交易信息中还包括: m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥的数量 k 。

11、根据权利要求8-10任一项所述的方法,其特征在于,将所述第一交易信息记录在所述区块链网络上,包括:

所述第一节点将所述第一交易信息发送给区块链网络中的区块链节点,并通过所述区块链节点在全网广播和共识,保存所述第一交易信息。

12、根据权利要求8所述的方法,其特征在于,所述方法还包括:

如果所述授权信息为不允许,则取消所述第二节点的授权信息;

生成第二交易信息,所述第二交易信息包括第二节点的身份标识和第二节点的授权信息;

将所述第二交易信息记录在所述区块链网络上。

13、根据权利要求8-10任一项所述的方法,其特征在于,在第一节点获得第二节点的身份标识之前,所述方法还包括:

所述第一节点使用第一节点的公钥通过代理重加密算法对待访问数据进行加密,生成第一加密密文;

所述第一节点将所述第一加密密文作为一个交易保存在所述区块链网络中。

14、一种数据传输方法,其特征在于,所述方法包括:

第二代理节点接收来自第一代理节点的权限验证请求,所述权限验证请求中包括请求节点的身份标识和第一加密密文,所述第一加密密文是通过对待访问数据进行加密后生成;

所述第二代理节点根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文;

如果是,则生成部分密钥,并将所述部分密钥发送给所述第一代理节点。

15、根据权利要求 14 所述的方法，其特征在于，所述生成部分密钥，包括：

所述第二代理节点在区块链网络中获得加密后的部分密钥，所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的；

所述第二代理节点利用自己的私钥对所述加密后的部分密钥进行解密，生成所述部分密钥。

16、根据权利要求 14 或 15 所述的方法，其特征在于，所述方法还包括：

所述第二代理节点根据所述请求节点的身份标识判断所述请求节点如果无权读取所述第一加密密文，则拒绝所述第一代理节点的第一请求。

17、一种网络节点，其特征在于，应用于第一代理节点，包括：

接收单元，用于接收来自请求节点的第一请求消息，所述第一请求消息中包括请求节点的身份标识和待访问的数据标识；

处理单元，用于根据所述待访问的数据标识在区块链网络中确定第一加密密文，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；

发送单元，用于在有权读取所述第一加密密文的情况下，向至少一个第二代理节点发起对所述请求节点的权限验证请求；

所述处理单元，还用于在所述有权读取所述第一加密密文的情况下，根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放。

18、根据权利要求 17 所述的网络节点，其特征在于，

发送单元，具体用于根据所述请求节点的身份标识，在区块链上读取最接近区块链式存储结构末端的请求节点的授权信息，所述授权信息包括允许或不允许。

19、根据权利要求 17 所述的网络节点，其特征在于，

所述处理单元，具体用于确定 m 个第二代理节点，生成所述权限验证请求，所述权限验证请求中包括所述请求节点的身份标识和所述第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成， m 为大于等于 1 的正整数；

所述发送单元，具体用于将所述权限验证请求分别发送给所述 m 个第二代理节点。

20、根据权利要求 17-19 任一项所述的网络节点，其特征在于，

所述接收单元，还用于接收来自至少 k 个第二代理节点发送的部分密钥，所述部分密钥是所述第二代理节点，根据所述请求节点的身份标识在验证所述请求节点有权访问数据后生成并发送的，且 $k \leq m$ ；

所述处理单元，具体用于对所述至少 k 个部分密钥进行还原，生成转换密钥；利用所述转换密钥和加密算法将所述第一加密密文转换为第二加密密文，所述第二加密密文由所述请求节点的公钥加密后生成；

发送单元，还用于将所述第二加密密文发送给所述请求节点。

21、根据权利要求 20 所述的网络节点，其特征在于，

所述处理单元，具体用于通过所述接收单元在接收到小于 k 个第二代理节点发送的部分密钥，或者，接收至少一个所述第二代理节点反馈的拒绝消息的情况下，通过所述发送单元向所述请求节点发送拒绝访问的消息。

22、根据权利要求 17-21 任一项所述的网络节点，其特征在于，

所述接收单元，具体用于接收通过所述区块链网络中的任一区块链节点转发的所述

第一请求消息。

23、根据权利要求 17-21 任一项所述的网络节点，其特征在于，

所述处理单元，还用于根据所述请求节点的身份标识判断所述请求节点如果无权读取所述第一加密密文，则拒绝所述请求节点的第一请求。

24、一种网络节点，其特征在于，应用于第一节点，包括：

接收单元，用于获得第二节点的身份标识，所述身份标识用于确定所述第二节点的授权信息；

处理单元，用于在所述授权信息为允许的情况下，利用所述网络节点的私钥、第二节点的公钥和加密算法生成转换密钥；利用区块链网络中的代理节点的公钥对所述转换密钥进行加密，生成加密后的部分密钥；以及，生成第一交易信息，并将所述第一交易信息记录在所述区块链网络上；

所述第一交易信息包括：第二节点的身份标识、第二节点的授权信息和加密后的部分密钥。

25、根据权利要求 24 所述的网络节点，其特征在于，

所述处理单元，具体用于利用秘密分享算法将所述转换密钥分解成 n 个部分密钥， n 为大于等于 1 的正整数；在所述区块链网络中选取 m 个代理节点，并使用所述 m 个代理节点的公钥对所述 n 个部分密钥进行加密，生成 n 个加密后的部分密钥， $m \leq n$ 。

26、根据权利要求 25 所述的网络节点，其特征在于，

所述第一交易信息中还包括： m 个代理节点的身份标识和还原所述转换密钥的最小部分密钥的数量 k 。

27、根据权利要求 24-26 任一项所述的网络节点，其特征在于，

所述处理单元，具体用于利用发送单元将所述第一交易信息发送给区块链网络中的区块链节点，并通过所述区块链节点在全网广播和共识，保存所述第一交易信息。

28、根据权利要求 27 所述的网络节点，其特征在于，

所述处理单元，还用于在所述授权信息为不允许的情况下，取消所述第二节点的授权信息；生成第二交易信息，并将所述第二交易信息记录在所述区块链网络上，所述第二交易信息包括第二节点的身份标识和第二节点的授权信息。

29、根据权利要求 24-26 任一项所述的网络节点，其特征在于，

所述处理单元，还用于在获得第二节点的身份标识之前，使用公钥通过代理重加密算法对待访问数据进行加密，生成第一加密密文；以及，将所述第一加密密文作为一个交易保存在所述区块链网络中。

30、一种网络节点，其特征在于，应用于第二代理节点，包括：

接收单元，用于接收来自第一代理节点的权限验证请求，所述权限验证请求中包括请求节点的身份标识和第一加密密文，所述第一加密密文是通过对待访问数据进行加密后生成；

处理单元，用于根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果是，则生成部分密钥；

发送单元，用于将所述部分密钥发送给所述第一代理节点。

31、根据权利要求 30 所述的网络节点，其特征在于，

所述处理单元，具体用于在区块链网络中获得加密后的部分密钥，所述加密后的部分密钥是利用所述第二代理节点的公钥加密后生成的；利用自己的私钥对所述加密后的部分密钥进行解密，生成所述部分密钥。

32、根据权利要求 30 或 31 所述的网络节点，其特征在于，

所述处理单元，还用于根据所述请求节点的身份标识判断所述请求节点如果无权读取所述第一加密密文，则拒绝所述第一代理节点的第一请求。