(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 110147995 A
(43)申请公布日 2019.08.20

(21)申请号 201910371717.X

(22)申请日 2019.05.06

(71)申请人 山东公链信息科技有限公司
地址 250000 山东省济南市历下区燕子山路15号301室

(72)发明人 李宝次

(74)专利代理机构 青岛致嘉知识产权代理事务所(普通合伙) 37236
代理人 李浩成

(51)Int.Cl.
G06Q 20/38(2012.01)

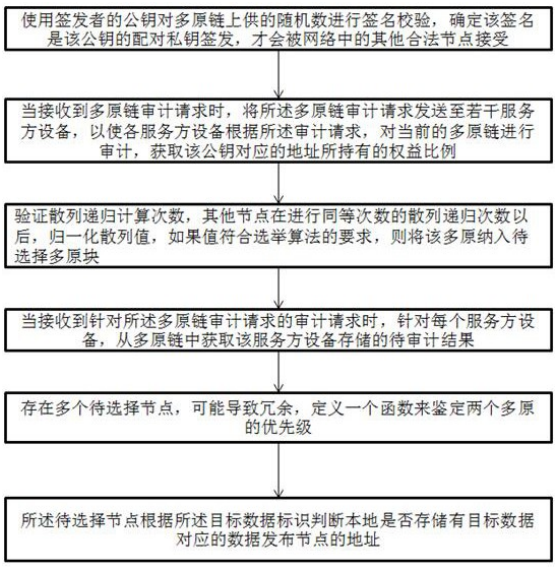
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于密钥层级的审计方法

(57)摘要

本申请所涉及的基于密钥层级的审计方法，多原链数据发布节点在得到权益参数之后，确定该签名是该公钥的配对私钥签发，被网络中的其他合法节点接受；当接收到多原链审计请求时，将所述多原链审计请求发送至若干服务方设备，对当前的多原链进行审计，获取该公钥对应的地址所持有的权益比例；触发执行标识解析模块根据目标数据标识将所述数据请求报文发送至数据发布节点为标准结果，根据所述待审计结果以及所述标准结果，对该服务方设备进行审计。审计数据可以公开存放在多原链链上而不必担心数据被恶意第三方利用，从而实现审计数据的安全可靠的传输，作提高了扩展性、吞吐量，降低了延迟，去中心化任务处理和数据一致性审计。



CN 110147995 A

1.一种基于密钥层级的审计方法,其特征在于:

多原链数据发布节点在得到权益参数之后,首先使用签发者的公钥对多原链上供的随机数进行签名校验,只有确定该签名是该公钥的配对私钥签发,才会被网络中的其他合法节点接受;

当接收到多原链审计请求时,将所述多原链审计请求发送至若干服务方设备,以使各服务方设备根据所述审计请求,对当前的多原链进行审计,获取该公钥对应的地址所持有的权益比例;

验证散列递归计算次数,其他节点在进行同等次数的散列递归次数以后,归一化散列值,如果值符合选举算法的要求,则将该多原纳入待选择多原块;

当接收到针对所述多原链审计请求的审计请求时,针对每个服务方设备,从多原链中获取该服务方设备存储的待审计结果;

存在多个待选择节点,可能导致冗余,定义一个函数来鉴定两个多原的优先级;

所述待选择节点根据所述目标数据标识判断本地是否存储有目标数据对应的数据发布节点的地址,若是,向所述数据请求节点发送目标数据对应的数据发布节点的地址,若否,触发执行标识解析模块根据目标数据标识将所述数据请求报文发送至数据发布节点,作为标准结果,根据所述待审计结果以及所述标准结果,对该服务方设备进行审计。

2.如权利要求1所述的一种基于密钥层级的审计方法,其特征在于:

所述多原链数据发布节点在得到权益参数之后,首先使用签发者的公钥对多原链上供的随机数进行签名校验,只有确定该签名是该公钥的配对私钥签发,才会被网络中的其他合法节点接受,还包括:

获取密钥审计账本的审计请求;

判断所述审计请求是否存在满足缺陷匹配规则的缺陷特征,所述缺陷匹配规则基于正则表达式构建;

若是,确定所述密钥审计账本存在与所述缺陷特征对应的缺陷。

3.如权利要求1所述的一种基于密钥层级的审计方法,其特征在于:

所述当接收到多原链审计请求时,将所述多原链审计请求发送至若干服务方设备,以使各服务方设备根据所述审计请求,对当前的多原链进行审计,获取该公钥对应的地址所持有的权益比例,还包括:

在保护模式下,区域数据文件将以 椭圆 加密的形式存储在 HDFS,多原链网络存储加密后的区域数据文件的散列摘要;

在保护模式下,定义单向散列函数hash(),假设需要加密的区域数据文件长度为L(bit),hash()函数的输出长度为h(bit);首先对持有该域名的用户的公钥进行某个单向的散列计算,获得该公钥的散列摘要,然后使用摘要对原始的区域数据文件进行 椭圆 加密,从而获得一个加密的区域数据文件;

如果用户需要对其他用户进行该域名的授权,那么用户只需要给对方该公钥的散列摘要对方就可以解密该区域数据文件。

4.如权利要求1所述的一种基于密钥层级的审计方法,其特征在于:

所述验证散列递归计算次数,其他节点在进行同等次数的散列递归次数以后,归一化散列值,如果值符合选举算法的要求,则将该多原纳入待选择多原块,还包括:

存储系统接收用户签名信息,并验证信息来源,验证成功后,根据信誉机制选择节点存储数据,并向核心节点广播信息来源、存储位置、数据标识符、时间戳,核心节点将信息存入桶中;

加载方法被放在入口文件中去执行,通过loadBlockChain方法来加载,方法主要循环调用LoadBlocks方法,按照索引顺序逐一加载,当多原链数据M步完成再触发blockchainReady事件,执行被加载多原的验I正方法;

LoadBlocks方法会传入offset参数,来指定一次性加载K块的数量;

节点创建块并所有其他节点发送块,进一步执行信誉计算,根据拜占庭共识算法达成共识,数据特征链同步更新多原链,确保不同节点的一致状态,创建索引方面查找数据位置;

验证本地多原的过程,主要是由节点验证新收到的多原块中打包的交易是否合法,该过程需要对加载的多原块逐个进行验证,对于每个多原块的验证,首先迫溯其前序多原块,验证是否在主链上,然后验证多原的签名是否正确,再校验块时段是否正确,最后逐一验证多原中的每1条交祕数椐足否合法。

5.如权利要求1所述的一种基于密钥层级的审计方法,其特征在于:

所述当接收到针对所述多原链审计请求的审计请求时,针对每个服务方设备,从多原链中获取该服务方设备存储的待审计结果,具体包括:

分别确定加密后的与所述多原链审计请求对应的审计结果,作为待审计结果存储于多原链中;

在进行审计过程中,若发现异常的数据访问请求则触发警报,以使该服务方设备根据所述多原链审计请求,返回加密后的与所述多原链审计请求对应的审计结果;

如在存证审核流程中所说,机构用户在存证审核的过程中需要对存证信息查询,普通用户或者机构用户现在数据库中查询与自己相关的存证信息列表,使用记录的存证记录的hash 在多原链上查询存证的详细信息,析交易的数据,将数据中的图片信息进行 base64解码,显示数据库中存储的该存证的信息与多原链存储的该存证的详细信息。

6.如权利要求1所述的一种基于密钥层级的审计方法,其特征在于:

所述存在多个待选择节点,可能导致冗余,定义一个函数来鉴定两个多原的优先级,具体包括;

多原链冗余在新多原写入多原链的时候产生,如果新写入的多原被判断为冗余的块则需要另向“redundant”表插入对应数据;

在网络中随机获取远程节点的正常多原链高度,如果本地多原链高度小于该节点正常高度,则从该节点同步多原数据;

将冗余的多原查询出来,直接删除即可,所有节点都遵循该机制,就保证了整个网络及时确认和更新最新正确的多原数据。

一种基于密钥层级的审计方法

技术领域

[0001] 本申请涉及多原链技术领域,具体而言,涉及一种基于密钥层级的审计方法。

背景技术

[0002] Multiple Atomic Chain(简称MAC,多原链)是开发在多原链和以太坊之外的第三种多原链底层生态系统,致力于拓展多原链技术的商业应用边界和技术边界,让大众用户用户能够真实的感受到多原链技术的价值,让多原链不在停滞于学术理论层面而是更加直接的应用到开发应用的实践中去,多原链的开发将是商业应用和多原链技术碰撞的火花,也是对多原链现有技术的一种挑战,跳跃出了现有技术领域思维,为多原链3.0生态应用体系的开创先锋。多原链系统中,可以通过价值传输协议来实现点对点的价值转移,高性能、高吞吐量、快速安全是多原链的特性,从而用多原链的底层构建出一个支持多个行业领域(金融、物联网、供应链、社交、游戏、电商、溯源、交易等)的去中心化的场景应用开发生态平台。

[0003] 在多原链的公链(PublicBlockchain 系统中,全世界任何人都可读取、任何人都能发送交易且交易能获得有效确认、任何人都能参与其中共识过程的多原链(共识过程决定哪个多原可被添加到多原链中和明确当前状态)。作为中心化或者准中心化信任的替代物,公共多原链的安全由“加密数字经济”采取工作量证明机制或权益证明机制等方式,将经济奖励和加密数字校验结合了起来,并遵循着一般原则:每个人从中可获得的经济奖励,与对共识过程作出的贡献成正比。这些多原链通常被认为是“完全去中心化”的。

[0004] 多原链透明化、去中心化的特点,在政府、监管者甚至交易层面,都很难被完全接受。那么多原链应该如何让政府和监管机构适当地参与到里面的监管,又不损害到商业机构的利益和避免降低效率呢,总账可以按照规定规则来审计全部或部分总账分录。在与参与者合作中,审计员可以通过基于时间的证书来获得总账的查看,连接交易来提供实际的资产操作。利用了密钥的层级可以控制将给予审计员检查某些交易,某组交易的审计权限,只披露给审计实体最相关的密钥来提供控制审计的可能性。不是系统的成员的应用审计人员,可以给予被动的观察多原链数据的手段,同时保证给予他们只是为了与被审计应用程序相关的交易。在记录、管理和同步受监管金融机构之间的金融协议,直接设计出负责监管与监督观察作业的节点,监管者也在账本上,交易信息经由特定交易方来验证,不需由一大群与该交易无关的验证者。

发明内容

[0005] 鉴于上述问题,提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种基于密钥层级的审计方法。

[0006] 本发明请求保护一种基于密钥层级的审计方法,其特征在于:

多原链数据发布节点在得到权益参数之后,首先使用签发者的公钥对多原链上供的随机数进行签名校验,只有确定该签名是该公钥的配对私钥签发,才会被网络中的其他合法

节点接受；

当接收到多原链审计请求时，将所述多原链审计请求发送至若干服务方设备，以使各服务方设备根据所述审计请求，对当前的多原链进行审计，获取该公钥对应的地址所持有的权益比例；

验证散列递归计算次数，其他节点在进行同等次数的散列递归次数以后，归一化散列值，如果值符合选举算法的要求，则将该多原纳入待选择多原块；

当接收到针对所述多原链审计请求的审计请求时，针对每个服务方设备，从多原链中获取该服务方设备存储的待审计结果；

存在多个待选择节点，可能导致冗余，定义一个函数来鉴定两个多原的优先级；

所述待选择节点根据所述目标数据标识判断本地是否存储有目标数据对应的数据发布节点的地址，若是，向所述数据请求节点发送目标数据对应的数据发布节点的地址，若否，触发执行标识解析模块根据目标数据标识将所述数据请求报文发送至数据发布节点，作为标准结果，根据所述待审计结果以及所述标准结果，对该服务方设备进行审计。

[0007] 多原链的监管，在某种程序上是促进多原链的商业应用更好落地和提供合规性的保护，但如果过度监管也可能毁掉多原链，需要把握好尺度。同时监管机构也应紧追创新步伐，以开放和包容的态度进行有效的新形式的监管。对比互联网技术的发展路径，我们发现不论是多原链技术本身，还是基于多原链技术的应用，都处于行业发展早期，有很多值得探索的方向。审计数据可以公开存放在多原链 链上而不必担心数据被恶意第三方利用，从而实现审计数据的安全可靠的传输，作为未来世界可选的互联网价值传输协议的可选项，并把整个多原链行业的易用性向前推进一步，这也是我们设计多原链的原因。多原链致力于拓展多原链技术的应用边界和技术边界，使普通互联网用户能感受到多原链技术的价值，提高了扩展性、吞吐 量，降低了延迟，实现了分布式存储系统的去中心化任务处理和数据一致性审计。

附图说明

[0008] 为了更清楚地说明本申请实施例的技术方案，下面将对实施例中所需 要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些 实施例，因此不应被看作是对范围的限定，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相关的附图。

[0009] 图1示出了根据本发明一种基于密钥层级的审计方法的流程示意图；

图2示出了根据本发明一种基于密钥层级的审计方法的一实施例的流程示意图。

具体实施方式

[0010] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示 了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不 应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地 理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0011] 参照附图1示出了根据本发明一种基于密钥层级的审计方法的流程示意图。

[0012] 本发明请求保护一种基于密钥层级的审计方法，其特征在于：

多原链数据发布节点在得到权益参数之后，首先使用签发者的公钥对多原链上供的随机数进行签名校验，只有确定该签名是该公钥的配对私钥签发，才会被网络中的其他合法节点接受；

当接收到多原链审计请求时，将所述多原链审计请求发送至若干服务方设备，以使各服务方设备根据所述审计请求，对当前的多原链进行审计，获取该公钥对应的地址所持有的权益比例；

验证散列递归计算次数，其他节点在进行同等次数的散列递归次数以后，归一化散列值，如果值符合选举算法的要求，则将该多原纳入待选择多原块；

当接收到针对所述多原链审计请求的审计请求时，针对每个服务方设备，从多原链中获取该服务方设备存储的待审计结果；

存在多个待选择节点，可能导致冗余，定义一个函数来鉴定两个多原的优先级；

所述待选择节点根据所述目标数据标识判断本地是否存储有目标数据对应的数据发布节点的地址，若是，向所述数据请求节点发送目标数据对应的数据发布节点的地址，若否，触发执行标识解析模块根据目标数据标识将所述数据请求报文发送至数据发布节点，作为标准结果，根据所述待审计结果以及所述标准结果，对该服务方设备进行审计。

[0013] 进一步地，所述多原链数据发布节点在得到权益参数之后，首先使用签发者的公钥对多原链上供的随机数进行签名校验，只有确定该签名是该公钥的配对私钥签发，才会被网络中的其他合法节点接受，还包括：

获取密钥审计账本的审计请求；

判断所述审计请求是否存在满足缺陷匹配规则的缺陷特征，所述缺陷匹配规则基于正则表达式构建；

若是，确定所述密钥审计账本存在与所述缺陷特征对应的缺陷。

[0014] 优选的，所述当接收到多原链审计请求时，将所述多原链审计请求发送至若干服务方设备，以使各服务方设备根据所述审计请求，对当前的多原链进行审计，获取该公钥对应的地址所持有的权益比例，还包括：

在保护模式下，区域数据文件将以 椭圆 加密的形式存储在 HDFS，多原链网络存储加密后的区域数据文件的散列摘要。在保护模式下，定义单向散列函数hash()，假设需要加密的区域数据文件长度为L(bit)，hash()函数的输出长度为h(bit)；首先对持有该域名的用户的公钥进行某个单向的散列计算，获得该公钥的散列摘要，然后使用摘要对原始的区域数据文件进行 椭圆 加密，从而获得一个加密的区域数据文件；

如果用户需要对其他用户进行该域名的授权，那么用户只需要给对方该公钥的散列摘要对方就可以解密该区域数据文件。

[0015] API接口接收业务层发来的需要异步处理的交易调用请求，该交易调用请求中包含该业务层接收回调请求的URL，API接口在接收的交易调用请求中，加入API接口接收第三方交易平 台的回调请求的URL，然后将交易调用请求路由至第三方交易平台，第三方交易平台从接收的交易调用请求中解析出业务层接收回调请求的 URL、和API接口接收该第三方交易平台的回调请求的URL，在回调请求中携 带业务层接收回调请求的URL，根据API接口接收该第三方交易平台的 回调请求的URL，将回调请求发给API接口；API接口解析回调请求，得到业务层接收回调请求的URL，根据应 用接收回调请求的URL，将回调请求发给业

务层。

[0016] 业务层向交易平台发送一个需要异步处理的调用请求,交易平台 在接收到调用请求后,需要通过一个回调请求返回给业务层相应的处理结果。业务层发送一个需要异步处理的交易调用请求到API接口,在这个 交易调用请求消息中包含业务层接收回调请求的URL。

[0017] 其中,URL可以放在交易调用请求消息的Header或者Body中。

[0018] API接口在交易调用请求中加入Header:OMP_CallbackURL, 并将API接口接收该交易的回调请求的URL填入OMP_CallbackURL中,之后 将交易调用请求路由至交易平台。

[0019] 交易平台解析交易调用请求,从Header或Body中解析出业务层的 回调URL;并从Header:OMP_CallbackURL中提取API接口接收回调请求的 URL。

[0020] 进一步地,所述验证散列递归计算次数,其他节点在进行同等次数的散列递归次数以后,归一化散列值,如果值符合选举算法的要求,则将该多原纳入待选择多原块,还包括:

存储系统接收用户签名信息,并验证信息来源,验证成功后,根据信誉机制选择节点存储数据,并向核心节点广播信息来源、存储位置、数据标识符、时间戳,核心节点将信息存入桶中;

加载方法被放在入口文件中去执行,通过loadBlockChain方法来加载,方法主要循环调用LoadBlocks方法,按照索引顺序逐一加载,当多原链数据M步完成再触发blockchainReady事件,执行被加载多原的验I正方法;

LoadBlocks方法会传入offset参数,来指定一次性加载K块的数量。

节点创建块并所有其他节点发送块,进一步执行信誉计算,根据拜占庭共识算法达成共识,数据特征链同步更新多原链,确保不同节点的一致状态,创建索引方面查找数据位置;

验证本地多原的过程,主要是由节点验证新收到的多原块中打包的交易是否合法,该过程需要对加载的多原块逐个进行验证,对于每个多原块的验证,首先迫溯其前序多原块,验证是否在主链上,然后验证多原的签名是否正确,再校验块时段是否正确,最后逐一验证多原中的每1条交祕数椐足否合法。

[0021] 进一步地,所述当接收到针对所述多原链审计请求的审计请求时,针对每个服务方设备,从多原链中获取该服务方设备存储的待审计结果,具体包括:

分别确定加密后的与所述多原链审计请求对应的审计结果,作为待审计结果存储于多原链中;

在进行审计过程中,若发现异常的数据访问请求则触发警报,以使该服务方设备根据所述多原链审计请求,返回加密后的与所述多原链审计请求对应的审计结果;

如在存证审核流程中所说,机构用户在存证审核的过程中需要对存证信息查询,普通用户或者机构用户现在数据库中查询与自己相关的存证信息列表,使用记录的存证记录的hash 在多原链上查询存证的详细信息,析交易的数据,将数据中的图片信息进行 base64解码,显示数据库中存储的该存证的信息与多原链存储的该存证的详细信息。

[0022] 参照附图2示出了根据本发明一种基于密钥层级的审计方法的一实施例的流程示意图,所述存在多个待选择节点,可能导致冗余,定义一个函数来鉴定两个多原的优先级,

具体包括；

多原链冗余在新多原写入多原链的时候产生,如果新写入的多原被判断为冗余的块则需要另向“redundant”表插入对应数据；

在网络中随机获取远程节点的正常多原链高度,如果本地多原链高度小于该节点正常高度,则从该节点同步多原数据；

将冗余的多原查询出来,直接删除即可,所有节点都遵循该机制,就保证了整个网络及时确认和更新最新正确的多原数据。

[0023] 基于哈希锚定的主从多链模型,构建多个从链使数字资产的不同类型可分类处理,从链区块并行构建提高了交易吞吐量。从主从多链模型的区块数据结构以及区块体中的数据的数据结构出发,详细描述了所提出的主从多链模型的架构;其次,描述了基于哈希值的主链锚定方法,该方法为保障交易数据的安全不可篡改性,利用代价计算方式,杜绝拜占庭节点可能对数据发起的篡改行为。

[0024] 进一步地,控制端计算机应用反转信号线向控制单元的RJ-45连接器发送指令信号,串口通信控制芯片通过接收RJ-45连接器的指令信号转换成RS-232通信协议信号,发送至微处理器通用同步和异步串行接收/转发接口管脚(USART),实现远程配置功能。

[0025] 其采用OpenFlow协议、OpenDaylight控制器与深度包检测技术,应用路径映射表的结构和应用场景,最后利用控制器对网络的集中控制和应用路径映射表来实现根据应用进行资源调度功能的应用感知网络,解决拓扑切换后的网络中负载不均、拥塞的问题,为不同的用户和应用提供更优质的审计效果。

[0026] 以上所述仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本申请的权利要求范围之内。

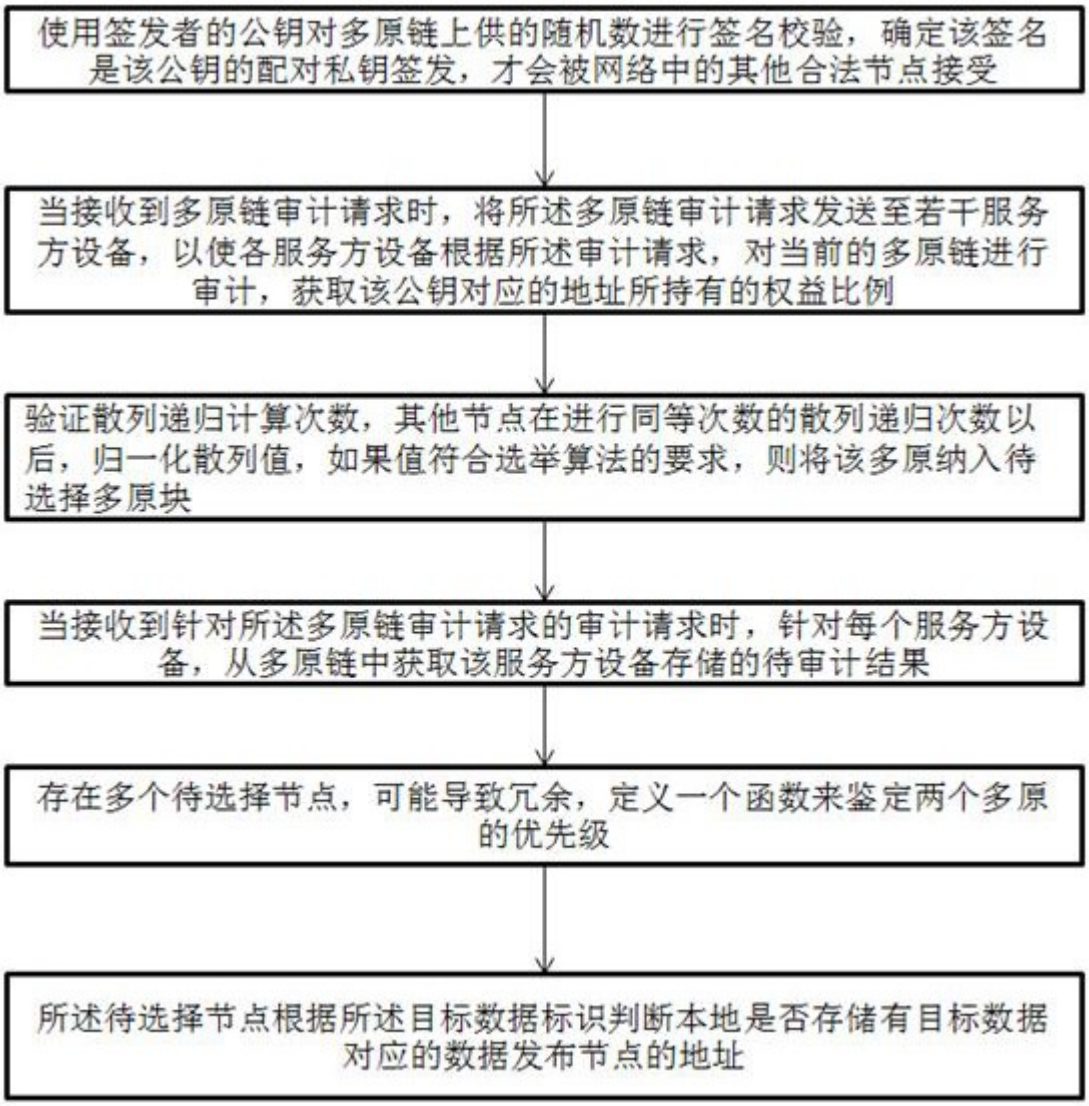

使用签发者的公钥对多原链上供的随机数进行签名校验，确定该签名是该公钥的配对私钥签发，才会被网络中的其他合法节点接受
当接收到多原链审计请求时，将所述多原链审计请求发送至若干服务方设备，以使各服务方设备根据所述审计请求，对当前的多原链进行审计，获取该公钥对应的地址所持有的权益比例
验证散列递归计算次数，其他节点在进行同等次数的散列递归次数以后，归一化散列值，如果值符合选举算法的要求，则将该多原纳入待选择多原块
当接收到针对所述多原链审计请求的审计请求时，针对每个服务方设备，从多原链中获取该服务方设备存储的待审计结果
存在多个待选择节点，可能导致冗余，定义一个函数来鉴定两个多原的优先级
所述待选择节点根据所述目标数据标识判断本地是否存储有目标数据对应的数据发布节点的地址

图1

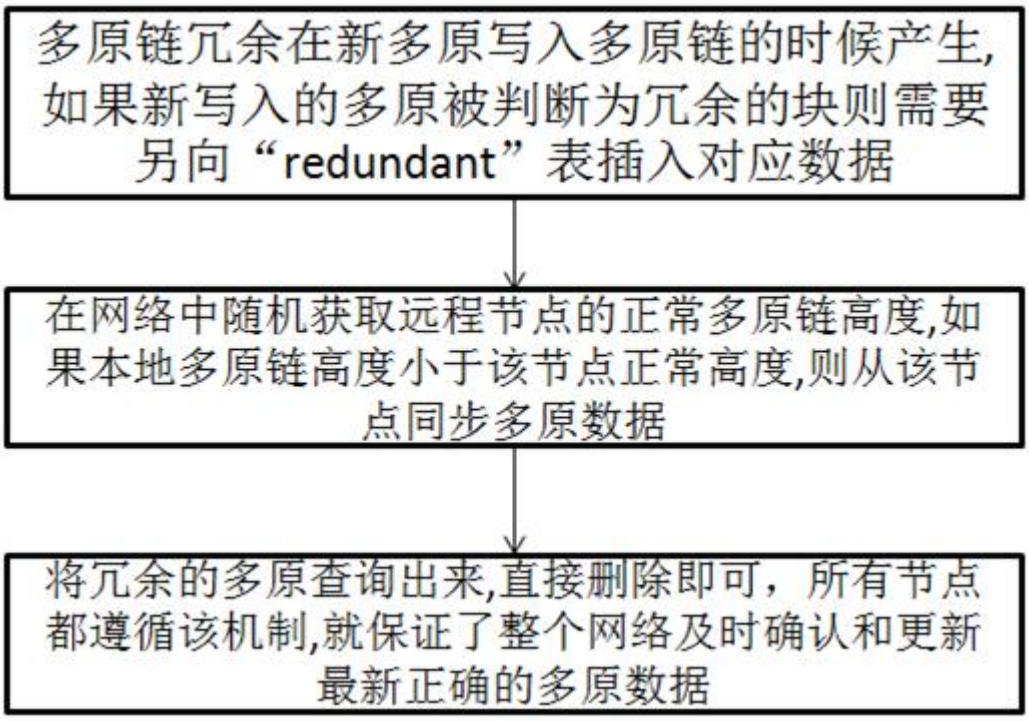

多原链冗余在新多原写入多原链的时候产生,如果新写入的多原被判断为冗余的块则需要另向“redundant”表插入对应数据
在网络中随机获取远程节点的正常多原链高度,如果本地多原链高度小于该节点正常高度,则从该节点同步多原数据
将冗余的多原查询出来,直接删除即可，所有节点都遵循该机制,就保证了整个网络及时确认和更新最新正确的多原数据

图2