(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108876378 B
(45)授权公告日 2022.04.19

(21)申请号 201810760177.X

(22)申请日 2018.07.11

(65)同一申请的已公布的文献号
申请公布号 CN 108876378 A

(43)申请公布日 2018.11.23

(73)专利权人 北京国泰网信科技有限公司
地址 100195 北京市海淀区昆明湖南路51号B座3层303号
专利权人 成都国泰网信科技有限公司

(72)发明人 杨国超

(74)专利代理机构 深圳泛航知识产权代理事务所(普通合伙) 44867
代理人 邓爱军

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/06(2012.01)

(56)对比文件
CN 107657438 A,2018.02.02
CN 106603198 A,2017.04.26
WO 2018115567 A1,2018.06.28
US 2018189753 A1,2018.07.05
CN 106682907 A,2017.05.17
CN 105719185 A,2016.06.29
CN 107786339 A,2018.03.09
CN 107807951 A,2018.03.16
CN 105761146 A,2016.07.13
CN 106815722 A,2017.06.09

审查员 汪杨

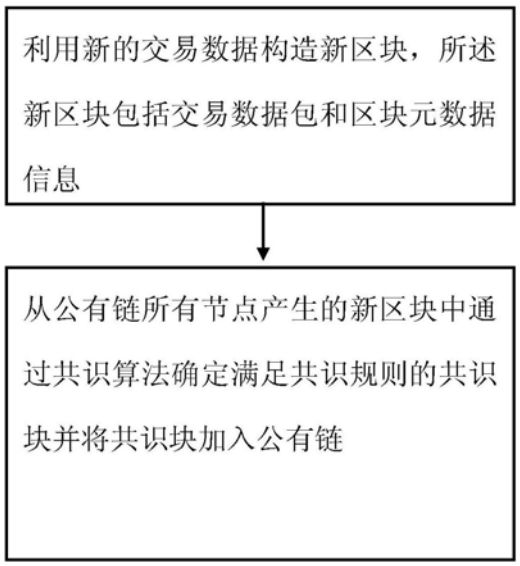
权利要求书2页 说明书6页 附图1页

(54)发明名称

公有链数据加密备份方法

(57)摘要

本发明提供了一种公有链数据加密备份方法,该方法包括:利用新的交易数据构造新区块,所述新区块包括交易数据包和区块元数据信息;所述区块元数据信息中包括节点的公有链中前序区块的区块元数据信息摘要值;从公有链所有节点产生的新区块中通过共识算法确定满足共识规则的共识块并将共识块加入公有链。本发明提出了一种公有链数据加密备份方法,利用公有链自身系统实现了区块间的数据同步验证,并快速校正区块数据存在的错误。



CN 108876378 B

1.一种公有链数据加密备份方法,其特征在于,包括:

利用新的交易数据构造新区块,所述新区块包括交易数据包和区块元数据信息;所述区块元数据信息中包括节点的公有链中前序区块的区块元数据信息摘要值;

从公有链所有节点产生的新区块中通过共识算法确定满足共识规则的共识块并将共识块加入公有链;

所述区块元数据信息中还包括N个新区块数据分别对应的N个摘要信息的元数据摘要值,N为所获取的新区块数据的数量;

在根据N个字节信息分别计算N个新区块数据的摘要信息之后,对N个摘要信息进行划分;

计算每个划分的摘要值,获取N个摘要信息的二级摘要值;

对二级摘要值继续划分,并返回计算每个划分的摘要值,直至获取元数据摘要值;

其中,在计算每个划分的摘要值时,先根据第一散列规则计算划分的中间摘要值,再根据第二散列规则计算中间摘要值的摘要值作为划分后的摘要值;

对于区块元数据,设有交易集合$S_C=\{c_1,c_2,\cdots,c_m\}$,每个交易对应的摘要集合$S_{Abs}=\{abs_1,abs_2,\cdots,abs_m\}$,$SF=\{f_1,f_2,\cdots,f_m\}$为每个交易待存储的数据集合,$S_P=\{p_{abs1},p_{abs2},\cdots,p_{absm}\}$为每个摘要数据存储到公有链系统后的位置信息,通过首节点获取,$SV=\{n^1_v,n^2_v,n^3_v,\cdots,n^s_v\}$为同步验证发起节点;存储元数据的过程包括以下步骤:

(1)对待存储的数据计算摘要,得到数据$SF'=\{\langle f_{abs1},abs_1\rangle,\langle f_{abs2},abs_2\rangle,\cdots,\langle f_{absm},abs_m\rangle\}$保存到公有链,其中$f_{absi}$表示交易$c_i$摘要后的数据,其中$0<i\leqslant m$;

(2)将SF'发送给所有同步验证发起节点SV,同步验证发起节点验证每个交易的摘要信息,验证完所有摘要信息的节点的广播消息bct;其他同步验证发起节点收到bct后终止当前验证过程,等待下一次验证;同时,该同步验证发起节点获得记录权限,记为n'_v;

(3)n'_v向首节点获取SF'中所有数据的位置信息SP,通过元数据$S_M=\{\langle abs_1,p_{abs1}\rangle,\langle abs_2,p_{abs2}\rangle,\cdots,\langle abs_m,p_{absm}\rangle\}$构造一个元数据区块MB,最后将元数据区块写入节点内部公有链中;

(4)n'_v将MB记录到全局公有链;记录成功后,n'_v广播消息bct,通知其他同步验证发起节点同步节点内部公有链状态;

其中,所有同步验证发起节点S_V同时收集给定时间段内所有交易的摘要信息S_{Abs}和数据副本信息,在验证摘要过程中,最先完成所有交易摘要信息验证的节点可以获得记录权限,并广播消息通知其他节点;没有得到记录权限的同步验证发起节点,则终止当前操作,等待下个时间段内的请求。

2.根据权利要求1所述的方法,其特征在于,所述前序区块为公有链的最长链中最新加入的区块。

3.根据权利要求1所述的方法,其特征在于,在每个新区块数据的摘要信息时,先将新区块数据二进制化,得到新区块数据的字节信息,再对字节信息进行散列运算,获得新区块数据的摘要信息。

4.根据权利要求1所述的方法,其特征在于,所述区块元数据信息还包括随机验证码,所述随机验证码用于共识算法中对共识块的确定。

5.根据权利要求4所述的方法,其特征在于,还包括:

所述公有链系统的每一个节点在构建交易数据包以及区块元数据信息中的其它部分后，尝试多个随机验证码，随机验证码的改变直接导致新区块的区块元数据信息摘要值的变化，当任一区块的区块元数据信息摘要值首先满足预设数量的前n个比特位为0时，该节点将其构建的新区块将作为共识块广播至公有链系统中的其它节点；其它节点在接收到共识块广播后，停止构建新区块，并将共识块加入公有链。

公有链数据加密备份方法

技术领域

[0001] 本发明涉及区块链,特别涉及一种公有链数据加密备份方法。

背景技术

[0002] 公有链技术用数据区块取代目前互联网对中心服务器的依赖,使得所有数据的变更或者交易项目都被同时记录在多个账本节点之上。现有的公有链是沿着公有链的延展方向,依次生成新的区块,且区块之间满足同步验证,防止区块中的数据被恶意篡改。当有业务需要进行交易汇总时,那么该业务请求需要公有链节点之外的外部节点投赞成票才能进行;而外部节点的响应可能减慢并且公有链内部节点会暂停。此外,在一些情况下,当公有链上的某个区块中的区块数据确实存在错误,如果强行对该数据进行修改,必然导致公有链的同步验证不通过,造成修改区块数据与公有链同步验证之间的矛盾。

发明内容

[0003] 为解决上述现有技术所存在的问题,本发明提出了一种公有链数据加密备份方法,包括:

[0004] 利用新的交易数据构造新区块,所述新区块包括交易数据包和区块元数据信息;所述区块元数据信息中包括节点的公有链中前序区块的区块元数据信息摘要值;

[0005] 从公有链所有节点产生的新区块中通过共识算法确定满足共识规则的共识块并将共识块加入公有链。

[0006] 优选地,所述区块元数据信息中还包括N个新区块数据分别对应的N个摘要信息的元数据摘要值,N为所获取的新区块数据的数量。

[0007] 优选地,所述前序区块为公有链的最长链中最新加入的区块。

[0008] 优选地,在每个新区块数据的摘要信息时,先将新区块数据二进制化,得到新区块数据的字节信息,再对字节信息进行散列运算,获得新区块数据的摘要信息。

[0009] 优选地,所述区块元数据信息还包括随机验证码,所述随机验证码用于共识算法中对共识块的确定。

[0010] 优选地,所述公有链系统的每一个节点在构建交易数据包以及区块元数据信息中的其它部分后,尝试多个随机验证码,随机验证码的改变直接导致新区块的区块元数据信息摘要值的变化,当任一区块的区块元数据信息摘要值首先满足预设数量的前n个比特位为0时,该节点将其构建的新区块将作为共识块广播至公有链系统中的其它节点;其它节点在接收到共识块广播后,停止构建新区块,并将共识块加入公有链。

[0011] 本发明相比现有技术,具有以下优点:

[0012] 本发明提出了一种公有链数据加密备份方法,利用公有链自身系统实现了区块间的数据同步验证,并快速校正区块数据存在的错误。

附图说明

[0013] 图1是根据本发明实施例的公有链数据加密备份方法的流程图。

具体实施方式

[0014] 下文与图示本发明原理的附图一起提供对本发明一个或者多个实施例的详细描述。结合这样的实施例描述本发明，但是本发明不限于任何实施例。本发明的范围仅由权利要求书限定，并且本发明涵盖诸多替代、修改和等同物。在下文描述中阐述诸多具体细节以便提供对本发明的透彻理解。出于示例的目的而提供这些细节，并且无这些具体细节中的一些或者所有细节也可以根据权利要求书实现本发明。

[0015] 本发明的一方面提供了一种公有链数据加密备份方法。图1是根据本发明实施例的公有链数据加密备份方法流程图。

[0016] 本发明提供的公有链系统包括多个公有链节点，形成一个去中心化的系统。在写入交易数据时，将系统的多个节点(设为T个)中的任一节点作为首节点接收新区块数据；首节点将新区块数据存入首节点的新区块缓存，并向其它T-1个节点发送交易数据更新请求；交易数据更新请求中包括该新区块数据；该交易数据更新请求用于指示其它T-1个节点中任一个节点将新区块数据的摘要信息存入各自的新区块缓存，即对于其它T-1个节点中的任一节点，在收到交易数据更新请求后，获取其中的新区块数据并存入各自的新区块缓存。经过上述过程，系统中的每一个公有链节点都收到了新区块数据。

[0017] 具体地，在新区块数据写入过程中，针对公有链系统的T个节点中的任一节点：

[0018] 1.1：获取N个新区块数据；根据预设的二进制化规则分别二进制化处理N个新区块数据，得到N个新区块数据分别对应的N个字节信息。

[0019] 1.2：构造新区块，新区块包括交易数据包和区块元数据信息；区块元数据信息中包括节点的公有链中前序区块的区块元数据信息摘要值；前序区块为公有链的最长链中最新加入的区块。在本发明的公有链系统中，T个节点各自拥有节点内部的公有链，节点内部公有链中每个区块通过指针即前序区块的区块元数据信息摘要值串接在一起。

[0020] 1.3：从T个节点产生的新区块中通过共识算法确定满足共识规则的共识块并将共识块加入公有链。优选地，在节点的新区块缓存中新区块数据的摘要信息的数量达到预设数量时，执行步骤1.1；优选地，在距上次构造新区块的时间间隔达到预设时间时，执行步骤1.1。

[0021] 所述区块元数据信息中还包括N个新区块数据分别对应的N个摘要信息的元数据摘要值。每个新区块数据都拥有自己的摘要信息，具体计算过程是先将新区块数据二进制化，得到新区块数据的字节信息，再对字节信息进行散列运算，获得新区块数据的摘要信息。元数据摘要值可用于在数据同步验证时，验证区块的交易数据包是否有被篡改。

[0022] 优选地，节点内部公有链中保存着新区块数据的字节信息，区块元数据信息同时将二进制化规则所对应的二进制化类型进行记录，在数据同步验证时，公有链系统的节点根据字节信息和二进制化规则得到区块中数据的原始形式。

[0023] 为了保证系统中公有链的一致，所述区块元数据信息还包括随机验证码，随机验证码用于共识算法中对共识块的确定。T个节点中的每一个节点在构建交易数据包以及区块元数据信息中的其它部分后，尝试多个随机验证码，随机验证码的改变直接导致新区块

的区块元数据信息摘要值的变化，当任一区块的区块元数据信息摘要值首先满足预设数量的前n个比特位为0时，该节点将其构建的新区块将作为共识块广播至公有链系统中的其它节点。其它节点在接收到共识块广播后，停止构建新区块，并将共识块加入公有链。优选地，预设数量n是根据产生新区块的平均耗时周期性动态调整。从T个节点产生的新区块中确定共识块之后，针对T个节点中的任一节点，从节点的新区块缓存中去除共识块中包括的N个字节信息所对应的N个新区块数据，防止重复写入。

[0024] 优选地，从T个节点产生的新区块中确定满足共识算法规则的共识块加入公有链之后，还包括：针对共识块中的每个字节信息，获取与字节信息对应的新区块数据的摘要信息；将新区块数据的摘要信息以及新区块数据对应的寻址信息保存在本地地址库中；寻址信息包括新区块数据所对应的字节信息在区块中的位置ID。公有链系统中的每个节点都将区块中的数据的寻址信息存入本地地址库，用户在进行数据同步验证时，只需提供新交易数据的摘要信息。优选地，在满足共识算法规则的共识块加入公有链之后，还可以判断自身是否为共识块中的任一字节信息的首节点，若是，则输出该摘要信息的寻址信息给用户。用户在进行数据同步验证时可同时提供新交易数据的摘要信息和寻址信息，能够加快数据同步验证的效率。

[0025] 为避免单一算法的散列碰撞攻击，本发明在根据N个字节信息分别计算N个新区块数据的摘要信息之后，还包括对N个摘要信息进行划分；计算每个划分的摘要值，获取N个摘要信息的二级摘要值；对二级摘要值继续划分，并返回计算每个划分的摘要值的步骤直至获取元数据摘要值。而在计算每个划分的摘要值时，先根据第一散列规则计算划分的中间摘要值；再根据第二散列规则计算中间摘要值的摘要值作为划分的摘要值。采用上述优选实施例所提供的摘要值计算方法，可以防范单一算法的散列碰撞攻击并输出长度更短的摘要值。

[0026] 根据上述实施例所提供的区块数据更新方法，本发明以下实施例进一步提供一种对应上述更新方法的数据同步验证方法，对已写入公有链的数据进行数据同步验证，包括以下步骤：

[0027] 同步验证发起节点获取新交易数据的摘要信息，同步验证发起节点为T个节点的任一节点；

[0028] 从公有链中确定各区块是否包含摘要信息对应的字节信息；

[0029] 公有链中的每个区块包括交易数据包和区块元数据信息；交易数据包中包括各新交易数据分别对应的字节信息；区块元数据信息中包括区块的前序区块的区块元数据信息摘要值；

[0030] 若公有链中存在摘要信息对应的字节信息，则确认新交易数据同步验证通过。

[0031] 其中，公有链系统的T个节点中的任一节点都可以作为同步验证发起节点为用户提供数据同步验证服务。同步验证发起节点获取的新交易数据的摘要信息可以由用户直接提供，也可以根据用户提供的新交易数据计算获得。而同步验证发起节点遍历公有链中各区块所包含的字节信息所对应的摘要信息，获得摘要值后再与接受的新交易数据的摘要信息比对。更优选地，同步验证发起节点预先存储本地地址库；本地地址库中包含所述公有链各区块中字节信息所对应的摘要信息的寻址信息，同步验证发起节点通过寻址信息查询公有链特定位置的字节信息所对应的摘要信息是否与用户提供的新交易数据的摘要信息一

致。然后，从公有链中确定寻址信息对应的新交易数据的字节信息；根据新交易数据的字节信息计算新交易数据的摘要信息；当新交易数据的摘要信息与新交易数据的摘要信息一致时，确定公有链中存在摘要信息对应的字节信息。

[0032] 在同步验证发起节点提供数据同步验证服务时，进一步包括，在公有链的首节点处创建智能合约，并且本地地址库设置有其它T-1个节点对智能合约的访问许可，访问许可包括读许可和写许可。以此方式，私密数据可以通过智能合约进行管理，配置相应的访问许可。然后在首节点处使用公钥对智能合约进行加密，并将经加密的智能合约包括在首节点处的区块数据中。随后可以发送给公有链上的其它节点。以此方式保证智能合约以密文形式保存在公有链上，所有节点均可备份，不存在因节点数的限制带来的备份风险。

[0033] 在首节点处根据本地地址库向公有链的其它T-1个节点分发公钥，然后将区块数据发送到其它T-1个节点。优选地，在其它T-1个节点处接收公钥和区块数据，并使用公钥从区块数据中解密经加密的智能合约，以创建经解密的智能合约。或根据经解密的智能合约来执行交易。

[0034] 以此方式，在首节点处创建智能合约并将经加密的智能合约包括在首节点处的区块数据中之后，公有链上的其它节点都可接收区块数据，即实现所有节点可同步，但只有拥有该智能合约的公钥的节点才能进行解密，执行相应的交易，从而实现对公有链上数据的保护功能。

[0035] 在上述数据共识过程中，优选地，根据区块ID、智能合约的合约ID、以及智能合约的历史交易数据形成的交易数据摘要来进行。为获得区块ID及智能合约ID，每个智能合约的历史交易数据及当前状态在存储时逻辑隔离。执行完任一交易后，在智能合约的逻辑数据库中插入一条以区块ID及智能合约ID作为键值的记录，以便用于后续完成共识。相应地，智能合约的历史交易数据和当前状态可以被逻辑隔离地存储在数据库中，智能合约的当前状态根据数据库中存储的区块ID和智能合约的智能合约ID进行查询。

[0036] 在得到同步验证结果之后，如果确定公有链中已有区块数据出现错误，则采用以下方法进行校正：接收针对当前公有链中区块数据的数据校正请求，该数据校正请求中包括：待校正的错误数据在公有链中的位置信息，以及对错误数据进行校正后的替换数据。所述的错误数据被作为本次校正的对象数据，该错误数据可以是仅包括被校正的数据，或者是包含了被校正的数据在内的交易数据包。

[0037] 为了方便数据管理，在接收和处理数据校正请求时，均是以公有链中已存在的区块数据中的字节信息为单位逐一处理，即每次接收的数据校正请求中只包含针对一个字节信息的数据校正请求。

[0038] 具体地，当公有链管理者需要对公有链中区块的区块数据进行校正时，可向系统输入待校正的错误数据在公有链中的位置信息，该位置信息具体可以是错误数据所在的区块ID，以及该错误数据在区块的区块数据中的数据ID。针对某个字节信息中的交易数据进行校正是在决定进行数据校正时就已经确定的，而在具体执行数据校正时，只需要锁定被校正数据即错误数据在所述公有链中的位置信息即可。

[0039] 然后将公有链中的错误数据修改为替换数据；具体地，根据数据校正请求中包含的所述错误数据在公有链中的位置信息，将相应位置处的数据修改为替换数据即可实现数据的修改。根据数据校正请求，生成校正报告，该校正报告包括关联存储的错误数据在公有

链中的位置信息，以及对错误数据进行校正后的替换数据；并将这两个信息关联存储形成一个校正报告。可选地，在该校正报告中还可以包括本次校正报告生成的时间信息。

[0040] 将每次对公有链进行校正的校正报告进行存储，在查看公有链中记载的交易信息时可结合校正报告对公有链进行检查，还可根据校正报告的内容，对有数据修改的区块在公有链中的一致性进行强行验证通过。

[0041] 对于区块元数据，为了防止由于使用单一节点存储元数据造成安全性问题，假设有交易集合$S_C=\{c_1,c_2,\cdots,c_m\}$，每个交易对应的摘要集合$S_{Abs}=\{abs_1,abs_2,\cdots,abs_m\}$，$SF=\{f_1,f_2,\cdots,f_m\}$为每个交易待存储的数据集合，$S_P=\{p_{abs1},p_{abs2},\cdots,p_{absm}\}$为每个摘要数据存储到公有链系统后的位置信息，可以通过首节点获取，$SV=\{n^1_v,n^2_v,n^3_v,\cdots,n^s_v\}$为同步验证发起节点。存储元数据的过程包括以下步骤：

[0042] (1)对待存储的数据计算摘要，得到数据$SF'=\{<f_{abs1},abs_1>,<f_{abs2},abs_2>,\cdots,<f_{absm},abs_m>\}$保存到公有链，其中$f_{absi}$表示交易$c_i$摘要后的数据，其中$0<i\leq m$。

[0043] (2)将SF'发送给所有同步验证发起节点SV，同步验证发起节点验证每个交易的摘要信息，验证完所有摘要信息的节点的广播消息bct。其他同步验证发起节点收到bct后终止当前验证过程，等待下一次验证。同时，该同步验证发起节点获得记录权限，记为n'_v。

[0044] (3)n'_v向首节点获取SF'中所有数据的位置信息SP，通过元数据$S_M=\{<abs_1,p_{abs1}>,<abs_2,p_{abs2}>,\cdots,<abs_m,p_{absm}>\}$构造一个元数据区块MB，最后将元数据区块写入节点内部公有链中。

[0045] (4)n'_v将MB记录到全局公有链。记录成功后，n'_v广播消息bct，通知其他同步验证发起节点同步节点内部公有链状态。

[0046] 其中，所有同步验证发起节点S_V同时收集给定时间段内所有交易的摘要信息S_{Abs}和数据副本信息，在验证摘要过程中，最先完成所有交易摘要信息验证的节点可以获得记录权限，并广播消息通知其他节点。没有得到记录权限的同步验证发起节点，则终止当前操作，等待下个时间段内的请求。

[0047] 基于公有链自身的防篡改特点，元数据被存储到公有链后，交易方随时向同步验证发起节点发送验证请求来验证数据的完整性。此外，如果首节点发生错误，也可以通过读取全局公有链来恢复元数据。元数据验证过程通过交易摘要来查询元数据公有链的过程为：

[0048] (1)将摘要信息abs_c发送给所有同步验证发起节点SV。

[0049] (2)每个同步验证发起节点n^iv，其中$i\in[1,s]$，首先检查本地元数据公有链状态与全局状态是否一致，如果一致，则在节点内部公有链查询摘要信息absc对应的位置信息p_{fabsc}；反之如果状态不一致，先更新节点内部公有链再进行查询。

[0050] (3)当多于半数的同步验证发起节点查询到相同的结果时，将验证结果返回给交易方，同时广播消息bct，其他没有完成查询的同步验证发起节点在收到bct后终止当前查询过程。

[0051] 元数据验证阶段中，所有同步验证发起节点也是协作关系，即最先查询到位置信息的同步验证发起节点将结果返回给交易方。

[0052] 为实现交易方的节点间认证，将智能合约中的根合约经过许可后，加入公有链。加入公有链的根合约作为节点自生成根合约公有链证书，并将智能合约的哈希值记入公有链

内，作为信任凭证。通过同步验证发起节点查询验证存储在公有链上的信任凭证。所述公有链证书由许可加入公有链的多个域的根合约自生成，并记入公有链。优选地，在数字证书中添加了交易者类型与创建者类型的名称。在交易方实现节点间认证之后，认证类型的根合约对请求认证的交易方生成证书传给用户，并以哈希值的形式记入公有链，方便用户再次访问时提供快速认证。同步验证发起节点通过在公有链内查验多个类型的可信凭证，代替对智能合约的验证的过程。根据上述信任模型、系统架构和公有链证书，基于公有链的节点间认证开始之前，各个类型的根合约的哈希值和写入状态已经保存在公有链的区块中。

[0053] 综上所述，本发明提出了一种公有链数据加密备份方法，利用公有链自身系统实现了区块间的数据同步验证，并快速校正区块数据存在的错误。

[0054] 显然，本领类型的技术人员应该理解，上述的本发明的各模块或各步骤可以用通用的计算系统来实现，它们可以集中在单个的计算系统上，或者分布在多个计算系统所组成的网络上，可选地，它们可以用计算系统可执行的程序代码来实现，从而，可以将它们存储在存储系统中由计算系统来执行。这样，本发明不限制于任何特定的硬件和软件结合。

[0055] 应当理解的是，本发明的上述具体实施方式仅仅用于示例性说明或解释本发明的原理，而不构成对本发明的限制。因此，在不偏离本发明的精神和范围的情况下所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。此外，本发明所附权利要求旨在涵盖落入所附权利要求范围和边界、或者这种范围和边界的等同形式内的全部变化和修改例。

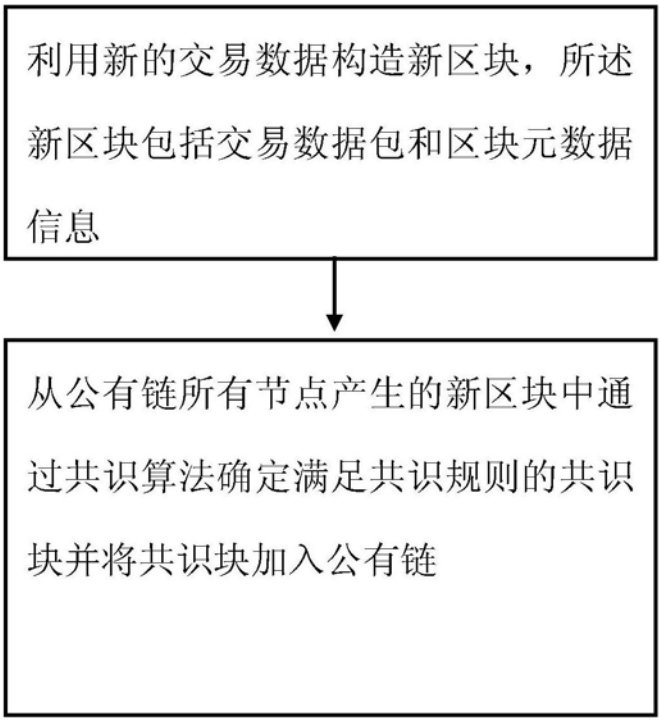

利用新的交易数据构造新区块，所述新区块包括交易数据包和区块元数据信息
从公有链所有节点产生的新区块中通过共识算法确定满足共识规则的共识块并将共识块加入公有链

图1